
JAFARA
ჯაფარას
მემკვიდრეობა

ჯაფარას მემკვიდრეობა

მოგზაურობა ჰაკერების სამყაროში

2023 წელი

ნაწილი 1

გაფრთხილება:

წიგნში შეიძლება დაშვებული იყოს გრამატიკული შეცდომები.

გაფრთხილება:

ამ წიგნიდან მიღებული ცოდნა შეიძლება მკითხველმა გამოიყენოს როგორც კეთილი,
ისე ბოროტი მიზნებისთვის.
ავტორი იხსნის ყველანაირ პასუხისმგებლობას მკითხველის ქმედებებზე.
ჯაფარას წიგნიდან მიღებული ცოდნა ნებისმიერის ხელში იარაღია.
იარაღს ჯარისკაცები სამშობლოს დასაცავად იყენებენ...
კრიმინალები ძარცვისთვის...

გაფრთხილება:

ჯაფარას მიზნები ნათელია…
ის აზიარებს საკუთარ გამოცდილებას მხოლოდ კეთილი მიზნებით.
ჰაკინგი ნებართვის გარეშე დანაშაულია და ისჯება კანონით.
ადამიანებით მანიპულაცია დანაშაულია.

“Man is least himself when he talks in his own person. Give him a mask, and he will tell you the truth”

– Oscar Wilde

ადამიანები, რომლებიც სიმართლეს ამბობენ ხშირად ცუდად ასრულებენ... როცა ნიღაბი გიკეთია, შენ შესახებ არავინ არაფერი იცის, შეგიძლია სიმართლე ილაპარაკო…

ამიტომ არის ჯაფარას ვინაობა ყველასთვის უცნობი.

“ადამიანი ნიღბით ხელშეუხებელია, ასეთ ადამიანს სიმართლის თქმისგან ვერაფერი შეაჩერებს”

- ჯაფარა

წიგნი დაიწერა 2023 წელს ჯაფარას მიერ.
ჩემი მიზანია ნებისმიერ ადამიანს განსხვავებული თვალით დავანახო ჰაკერების სამყარო
მარტივი ენით გადმოვცე ჩემი ცოდნა, გამოცდილება და რჩევები…
წიგნს ფსიქოლოგიური დატვირთვაც აქვს, ის შენი გონების ყველაზე ღრმა ფიქრებს უნდა ჩაწვდეს.
ეს წიგნი მოგცემს ცოდნას, რომელიც ნებისმიერ პროფესიაში გამოგადგება, სადაც არ უნდა აღმოჩნდე მომავალში!

დაიმახსოვრე:

ამ სამყაროში საზღვრები არ არსებობს !

არასდროს, არავის ენდო ბოლომდე !

ბედნიერ მოგზაურობას გისურვებს ჯაფარა...

ჯაფარას წინასიტყვაობა

სალამი მეგობარო…

საშინლად არ მიყვარს წიგნები, რომლებიც უაზროდ გაბერილია არაფრის მომცემი ისტორიებით და რჩევებით. ხშირად მათში უამრავი უსარგებლო ინფორმაციაა, რომლის ცოდნაც არაფერში გჭირდება…

დაიწყებ წიგნის კითხვას და ხვდები რომ გბეზრდება, თავს აძალებ მის წაკითხვას, მაგრამ სურვილი არ გაქვს…

ნაცნობი გრძნობაა?

ეს წიგნი ამ ყველაფრის საპირისპიროა… როგორც კი მის კითხვას დაიწყებ, ისე ჩახვალ ბოლოში რომ არ გაჩერდები, თუმცა ზოგჯერ მოგიწევს :)

წიგნი დამწყები ადამიანებისთვის არის დაწერილი, რომლებსაც ჰაკინგის სწავლა უნდათ და მიმართულება ჭირდებათ. ასევე ამ წიგნის წაკითხვა რეკომენდირებულია მათთვისაც, ვისაც ჰაკერების, ჰაკინგის მიმართ აქვთ ინტერესი ან მათგან თავის დაცვა სურთ…

ამ გამოცდილებამ ჩემი ცხოვრება შეცვალა, ბევრი კარგი რამ გადამხდა თავს, თუმცა იყო რთული მომენტებიც… ამიტომ მინდა ჩემი გამოცდილება გაგიზიარო. გაკვეთილები, რომლებსაც ამ წიგნიდან მიიღებ ყველაზე ღირებული და უნიკალურია…

ეს წიგნი ჩემი პირადი ისტორიაა. ზოგ შენ კითხვაზე იპოვი პასუხებს ამ წიგნის დახმარებით, თუმცა ყველა მათგანს ვერავინ გასცემს პასუხს, მათ შორის ვერც მე...

იმედი მაქვს ისეთი ცხოვრება გექნება, როგორსაც იმსახურებ და კიდევ უფრო დიდი იმედი მაქვს ჩემი რჩევები გამოგადგება…

ისიამოვნე და დარწმუნდი, რომ რაც შეიძლება მეტ ინფორმაციას მიიღებ წიგნიდან და პრაქტიკაში გამოიყენებ მათ :)

ჯაფარას ისტორია - ვინ ვარ მე?

საზოგადოება ჯაფარას სახელით მიცნობს… ჯაფარა ჰაკერი, მეგობარი, ფსიქოლოგი და ავტორია საქართველოდან (უცნაურად და კარგად ჟღერს “ავტორი”, გვიან გავიაზრე ის პასუხისმგებლობა, რაც ამ სიტყვას ახლავს თან...) დღემდე არსად მითქვამს, თუმცა მსოფლიოს გარშემო უამრავი ჰაკერი მიცნობს კიბერ სამყაროში სხვადასხვა ვინაობით და ამ წიგნის დაწერის შემდეგ კიდევ უფრო მეტი ადამიანი გამიცნობს, როგორც ჯაფარას.

ჩემი ისტორია ასეთია, 12 წლის ასაკში პირველად შევეხე ჰაკინგს, როცა მეზობელს ინტერნეტი “გავუტეხე” მეგორბის დახმარებით :) ის შეგრძნება დღესაც ისეთივე უცვლელია, როგორიც მაშინ იყო, რაღაცის გატეხვის შეგრძნება საოცარია. ამას ვერ გაიგებ სანამ არ გამოცდი.

14 წლის ასაკიდან აქტიურად დავინტერესდი ჰაკინგით და დავიწყე სწავლა: აიტი, ჰარდვეარი, ქსელები, ლინუქსი... კარგად ვისწავლე საფუძვლები და იგივეს მოგიწოდებ შენც, მყარი საფუძვლის გარეშე შენობა აუცილებლად ჩამოიშლება, სადღაც გაიჭედები. ხალხი, რომელიც ამ გზას გადის ხშირად ფსიქოლოგიურად არ არიან მზად და თავს ანებებენ სწავლას, ამიტომ მნიშვნელოვანია საფუძვლები კარგად ისწავლო და თავიდან აირიდო ეს მომენტი შენ ცხოვრებაში. (საკუთარი თავი ხომ არ იცანი?)

ჩემი პირველი იდეალი ამ სამყაროში ანონიმუსის დაჯგუფება იყო. როგორც ყოველთვის, საუკეთესო უნდა გყავდეს იდეალად. მათ იდეოლოგიას მაშინ სრულად ვიზიარებდი და მინდოდა მათ დონეზე ავსულიყავი. როდესაც სწავლა დავიწყე, იდეალი მჭირდებოდა მოტივაციისთვის და სწორედ მაშინ ანონიმუსი გახდა ჩემი იდეალი. **რატომ? საინტერესო კითხვაა...**

პირველ რიგში იმიტომ, რომ ისინი “საზოგადოება”-ს წარმოადგენდნენ. ჩემი საყვარელი სიტყვაა საზოგადოება. ხალხს ერთად დიდი ძალა აქვს, ყველაფრის გაკეთება შეუძლია ერთად დგომით საზოგადოებას, როგორი წარმოუდგენელიც არ უნდა იყოს მიზანი.

დიდხანს ვიყავი შეპყრობილი ანონიმუსით, ყველაფერს ვეძებდი მათ შესახებ, მინდოდა მეტი გამეგო და როგორღაც მათი ნაწილი გავმხდარიყავი, რაღაც დიდის ნაწილი... საზოგადოების, რომელიც საერთო მიზნისთვის ყველაფერს აკეთებდა. სამწუხაროდ ვერაფერს მივაგენი... ცხოვრების იმ მომენტში ალბათ ყველაფერს დავთმობდი მცირე საზოგადოება მაინც რომ მეპოვა, რომელიც საკუთარ ცოდნას გამიზიარებდა… (შენ გაქვს შანსი, რომელიც მე არასდროს მქონია… წაიკითხე წიგნი ბოლომდე და ყველაფერს მიხვდები)

ჰაკერული ფორუმის შექმნის ისტორია

წლების შემდეგ გადავწყვიტე თავად შემეკრიბა საზოგადოება საერთო ინტერესებით და ერთად დიდი საქმეები გვეკეთებინა… (ერთად დიდ საქმეებს გავაკეთებთ მეგობაროო… ჯერ არ დამდგარა ეს დროო… ყველაფერი წინ არის…)

ასე გაჩნდა ფორუმის შექმნის იდეა. იდეას ქმედებები მოჰყვა და შეიქმნა **ქართული ჰაკერული ფორუმი**. წიგნის წერის მომენტში ფორუმში ათი ათასამდე ადამიანია, ზოგი ახლა იწყებს სწავლას, ზოგს აქვს რაღაც ცოდნა, ზოგმა საკმაოდ კარგად იცის თავისი საქმე…

ფორუმის შექმნის მომენტში მარტო ვიყავი, არავის ვიცნობდი, მაგრამ დიდი მიზნები მქონდა და ამ მიზნების მისაღწევად ყველაფერს ვაკეთებდი. დღეს ჩემ გარშემო არიან ადამიანები, რომლებიც მეხმარებიან ფორუმის მართვაში, მათი მადლობელი ვარ და ეს მუდამ ასე იქნება…

ფორუმში არსებულ საზოგადოებას დიდი მონდომება და განვითარების სურვილი აქვს ამ მიმართულებით, მათში დიდ პოტენციალს ვხედავ… თუ ამ ფორუმის ნაწილი ხარ, გილოცავ.

(მეტ დეტალს ფორუმის შესახებ და არამარტო, აქ ნახავ jafarasec.com)

ეს არის ჯაფარას მოკლე ისტორია და მემკვიდრეობა, ყველაზე მეტად კი ჩემი სახელით ვამაყობ, ამ სახელს ბევრი ადამიანი ენდობა, მიუხედავად იმისა, რომ მათ წარმოდგენა არ აქვთ თუ ვინ დგას ჯაფარას სახელის უკან… მე საზოგადოების ნდობა მოვიპოვე და ამ ნდობას არასდროს დავკარგავ. ნდობა დღეს, ჩვენ სამყაროში რთული მოსაპოვებელია… ჯაფარამ ეს შეძლო…

ეს გზა მარტივი არ ყოფილა, ბევრი გამოწვევა იყო, დღესაც ბევრი გამოწვევაა, მაგრამ მე ნაპერწკალი გავაღვივე ქართულ საზოგადოებაში, ძალიან მალე ცეცხლი დაინთება, ძალიან დიდი ცეცხლი.

მალე მსოფლიო ალაპარაკდება ქართველ ჰაკერებზე და ეს ყველაფერი ერთმა ადამიანმა, ჰაკერმა საქართველოდან, ჯაფარამ დაიწყო…

მემკვიდრეობას და დიდ სახელს დავტოვებ, ამაზე ღირებული რა შეიძლება იყოს?

ეს წიგნი ბევრჯერ გახდება შენი მოტივაციის წყარო, ზუსტად ამ მიზნით ვწერ ამ ყველაფერს და გიზიარებ ჩემ ცოდნას, ისტორიას. ამ სამყაროში

დიდხანს ვერ გაძლებ თუ მოტივაცია, მიზნები და შენი ფიქრები თანხვედრაში არ არის. საკუთარი გონების და ფიქრების მართვა თუ არ შეგიძლია, მაშინ ამ პროფესიაში წარმატებას ვერ მიაღწევ…

ჩემი მიზანია რაც შეიძლება მალე დაგანახო, შეძლებ თუ არა საკუთარი ემოციების და გონების კონტროლს.

წიგნის ბოლოს ჯაფარას საზოგადოების შესახებ გაეცნობი ინფორმაციას. თუ საკმარის შრომას ჩადებ საკუთარ თავში და მოტივაციას არ დაკარგავ ამ გზაზე, შეიძლება ამ საზოგადოებაში მოხვდე…

თუ გაქვს მიზანი, ამ მიზნის მისაღწევად ყველაფერი გააკეთე და უკან არ დაიხიო. თუ შენ არ იბრძოლებ შენი მიზნებისთვის, სხვა ამას არასდროს გააკეთებს.

თუ მიზანი არ გაქვს, მიზნის გარეშე ცხოვრებაში ვერაფერს მიაღწევ…

ჯაფარას მიზანი

ჩემი მიზნის წაკითხვის შემდეგ იფიქრებ, რომ გიჟი ვარ…

დაიმახსოვრე, იმისთვის რომ რაღაცას მიაღწიო რეალობაში, ჯერ წარმოსახვაში უნდა შექმნა ის რაღაც, შემდეგ წარმოსახვა რეალობაში გადმოიტანო ნელ-ნელა, ნაბიჯ-ნაბიჯ…

ჯაფარა ქმნის გლობალურ ორგანიზაციას HackersForce, რომელსაც მსოფლიოს საუკეთესო ჰაკერები მართავენ.

HackersForce პოტენციალის მქონე საზოგადოებას ასწავლის კიბერუსაფრთხოებას და ორგანიზაციაში ასაქმებს საუკეთესოებს…

მიკრო სამყაროს ვქმნი, რომელიც მსოფლიო ბაზარს სერვისებს აწვდის… ორგანიზაციამ ნდობა მოიპოვა გლობალურ ბაზარზე ხარისხით, პროფესიონალიზმით, ხედვით და იმ საქმეებით, რომელსაც კიბერუსაფრთხოების განვითარებისთვის აკეთებს.

უდიდესი და ურთულესი მიზანია, მაგრამ მე ჯაფარა ვარ :)

წლების შემდეგ, ამ ყველაფერს წავიკითხავ და ვიამაყებ ჩემი მიღწევებით…

~~რატომ ღირს ეს წიგნი 13.37$?~~

ის რაც უფასოა, ხშირად ადამიანებს გონიათ რომ “ნაგავია”, ნაკლებ ყურადღებას აქცევენ კონკრეტულ რაღაცას, არ აფასებენ სათანადოდ…

თუმცა ბევრი ფიქრის შემდეგ მივხვდი, რომ შენ ჭკვიანი ადამიანი ხარ (სხვა შემთხვევაში ამ წიგნის წაკითხვის სურვილი არ გექნებოდა), ამიტომ ვფიქრობ სათანადოდ დააფასებ ამ საჩუქარს…

<u>ახლა ის უფასოა, საჩუქარია</u>…

ჩემი პატარა საჩუქარია შენთვის მეგობარო :)

გადავწყვიტე წიგნის PDF ვერსია საჯაროდ ხელმისაწვდომი გავხადო…

ნებისმიერი ადამიანი იმსახურებს იმ ცოდნის მიღებას, რომლის მოცემაც ამ წიგნს შეუძლია.

<u>საბოლოოდ ამ წიგნსაც ხომ ჯაფარას მემკვიდრეობა ქვია…</u>

ის, რაც ოდესღაც მე მჭირდებოდა და არ არსებობდა, ახლა იარსებებს შენთვის :)

ყოველთვის მინდოდა რაღაც ღირებულის დატოვება ჯაფარას სახელის მიღმა…

ამ ქმედებით ვფიქრობ ძალიან ბევრი ახალგაზრდა გაეცნობა ჰაკერების სამყაროს, მოტივაცია და მიზანი მიეცემა მათ…

<u>ისწავლე და იამაყე!</u>
<u>დაე ჩვენი კვალი დავტოვოთ ისტორიაში…</u>

<u>ჰაკინგის ისტორიას ღირსეული გაგრძელება ჭირდება!</u>

სანამ წიგნის კითხვას დაიწყებ...

მეგობარო, მიხარია რომ ამ წიგნის წაკითხვის სურვილი გაგიჩნდა, თუმცა სანამ მის კითხვას დაიწყებ, რამდენიმე საკითხზე უნდა დაფიქრდე...

არ ვიცი მომავალში რა მოხდება, თუმცა იმედი მაქვს ამ წიგნის დახმარებით იპოვი შენ გზას და არ დაუშვებ კრიტიკულ შეცდომებს ცხოვრებაში. მცირე შეცდომები ყველას მოგვდის და ასეც უნდა იყოს, მთავარია ამ შეცდომებიდან ვისწავლოთ...

წიგნი ორ ნაწილად იყოფა, ფსიქოლოგია და ჰაკინგი.

თუ აქამდე არ იცოდი, კომპიუტერულ სამყაროში ყველაფერი ერთზე და ნულზე მუშაობს, სხვა ვარიანტი არ არსებობს.

ჩვენ სამყაროშიც არსებობს ორი სახის ადამიანი. პირველი მსხვერპლია, მეორე მტაცებელი, სხვა ვარიანტი არც აქ არსებობს, ამიტომ აქედანვე უნდა განსაზღვრო შენი როლი...

იქნები მსხვერპლი და შენ ბედს მტაცებელს მიანდობ, თუ იქნები მტაცებელი და თავად განსაზღვრავ საკუთარ ბედს?

თუ მსხვერპლად ყოფნა გირჩევნია, მაშინ ამ წიგნის წაკითხვას აზრი არ აქვს. ეს წიგნი მტაცებლებისთვის არის დაწერილი. მტაცებელი არის ადამიანი, რომელიც გადარჩენისთვის ყველაფერს აკეთებს, მოქმედებს, იბრძვის. მსხვერპლი არის ადამიანი, რომელიც უბრალოდ არსებობს მიზნების გარეშე...

ჩვენ "მატრიცაში" ვცხოვრობთ. მხოლოდ ადამიანების მცირე რაოდენობას შეუძლია მატრიციდან თავის დაღწევა.

შეიძლება შენ არ ხარ მზად იმისთვის, რომ მატრიცას თავი დააღწიო, სიმართლე მოისმინო. შეიძლება ის ცხოვრება გქონდეს ახლა, რომელიც ბედნიერებას განიჭებს...

ადამიანების 99% არ არის მზად სიმართლისთვის, ვინაიდან სიმართლე მწარეა და ანგრევს ადამიანების ცხოვრებას. უფრო სწორად სიცრუეს ანგრევს, ხოლო სიცრუე ვიღაცისთვის რეალობაზე ღირებული შეიძლება იყოს...

თუ აქამდე არ გინახავს აუცილებლად ნახე ფილმი მატრიცა, 4 ნაწილი აქვს.

რა არის მატრიცა ჯაფარას გადმოსახედიდან?

იცხოვრო ცხოვრებით, რომელსაც შენ ვერ აკონტროლებ. თითქოს თავისუფალი ხარ, მაგრამ შენც კარგად იცი გულის სიღრმეში, რომ ეს ასე არ

არის. გარემო ისეა მოწყობილი, რომ არ გეძლევა საშუალება ის ცხოვრება შექმნა, რომელიც ყოველთვის გინდოდა. ცდილობ რაღაც ახლის გაკეთებას, მაგრამ არ გამოგდის, თითქოს უხილავ კედლებში ხარ მოქცეული, რომელსაც ვერ ცდები… საშინელებაა, ქვემოთ მაგალითებია, უკეთ მიხვდები...

მხოლოდ ადამიანების მცირე რაოდენობა აღწევს ამ პროცესს თავს. ისინი არიან ადამიანები, რომლებმაც ადრეულ პერიოდში მოახერხეს მატრიციდან თავის დაღწევა. ჩვენ ცხოვრებაში მატრიცის რამდენიმე ეტაპი არსებობს, უფროსწორად მთელი ჩვენი ცხოვრება ძირითადად მატრიცაა… შენ შეგიძლია ამ ყველაფერს თავი დააღწიო, უბრალოდ არასდროს შეწყვიტო მცდელობა რაღაცის კეთების, არ გაჩერდე…

როგორია ჩვენი ცხოვრება? ბავშვობიდან ვიწყებთ სკოლით, შემდეგ უნივერსიტეტი. მხოლოდ სკოლაში და უნივერსიტეტში ჯამში ჩვენი ცხოვრების 14-16 წელს და უამრავ ფინანსებს ვკარგავთ. უნივერსიტეტის შემდეგ მთელი ცხოვრება ვცდილობთ ფულის შოვნას. ვმუშაობთ სამსახურში, რომელიც არ მოგვწონს. ყოველი დღე ერთმანეთს გავს. ჩვენ ვერაფერს ვცვლით, ვინაიდან მხოლოდ ფულზე ვფიქრობთ, ფული გვაკონტროლებს, შიში გვაკონტროლებს. რა მოხდება თუ ფული არ გვექნება?

ზოგ ადამიანს უმართლებს და ისეთი სამსახური აქვს, რომელიც მოწონს და სიამოვნებას ანიჭებს, მაგრამ მაინც ჩვენ მთელი ცხოვრება ვმუშაობთ, ჩვენი ცხოვრების საუკეთესო წლებს იმის კეთებაში ვატარებთ, რაც ბედნიერებას არ გვანიჭებს, თუმცა მაინც ვაკეთებთ, რადგან ვალდებულებები გვაქვს. ეს ყველაფერი მატრიცა არ არის? წინასწარ დადგენილი წესებით თამაში, რომელსაც გვერდს ვერ აუვლი ხშირ შემთხვევაში…

სწორად გაიგე, არ ვამბობ რომ მუშაობა და შრომა ცუდია, არა, ის კარგი და აუცილებელია ჩვენი განვითარებისთვის, მაგრამ ასევე აუცილებელია ჩვენი წესებით ვითამაშოთ, თავად გადავწყვიტოთ თუ როდის, რას და როგორ გავაკეთებთ…

მთელი ჩვენი შეგნებული ცხოვრება გვეუბნებიან რა ვაკეთოთ, თითქოს სამყაროს დადგენილი წესია და სავალდებულოა არსებული წესებით თამაში... სკოლა, უნივერსიტეტი, სამსახური… ჩვენ ცხოვრებას ამ ყველაფრის გარშემო ვაშენებთ, როცა პირიქით, ჩვენი ცხოვრების გარშემო უნდა ავაშენოთ სხვა ყველაფერი...

“**შენ ვერასდროს მოიგებ თამაშს თუ სხვისი წესებით ითამაშებ. თუ თამაშის მოგება გინდა, საკუთარი წესებით უნდა ითამაშო... ჩვენი ცხოვრება ერთი დიდი თამაშია. ის ვინც წესებს ადგენს აქვს ცხოვრება,**

რომელიც მას სურს. ის ვინც სხვისი წესებით თამაშობს, ყოველთვის წაგებული რჩება, ყოველთვის მსხვერპლია...”

- ჯაფარა

როგორც კი ეცდები შენი წესებით თამაშს, მაშინვე ყველა შენ წინააღმდეგ წავა, არ მოგცემენ **“არსებული წესების”** დარღვევის შესაძლებლობას. გინდა ვცადოთ?

თუ სკოლას ახლა ამთავრებ უთხარი შენ ოჯახს, რომ არ გინდა უნივერსიტეტში ჩაბარება. არ გინდა აკეთო ის, რასაც სხვა ყველა მთელი ცხოვრება აკეთებს. გინდა შენი საკუთარი გზა იპოვო. გზა, რომელიც ბედნიერებას და ფინანსურ დამოუკიდებლობას განაპირობებს შენთვის. მაშინვე დაგიპირისპირდება შენი ოჯახი, ეცდებიან ყველანაირი მიზეზით, მაგალითების მოყვანით როგორმე გაიძულონ იმ გზაზე დარჩენა, რომელზეც ახლა ხარ. არა იმიტომ, რომ მათ არ უყვარხარ, არამედ იმიტომ, რომ სხვა გზა მათთვის წარმოუდგენელია... ისინიც მატრიცაში ცხოვრობენ, ხოლო შენ მათ ამ ყველაფერს ვერ დააჯერებ... ისინი ბედნიერები არიან იმით, რასაც დღემდე მიაღწიეს, ამიტომ იგივე ან უკეთესი სურთ შენთვის. ვერ ხვდებიან, რომ ამ ყველაფრით მხოლოდ უკან გექაჩებიან...

თუ სტუდენტი ხარ იგივე გააკეთე, უთხარი შენ ოჯახს რომ აღარ გაინტერესებს უნივერსიტეტი, ისინი ღირებულს არაფერს გაძლევენ და დროს, ფინანსებს ტყუილად კარგავ, შენი ცხოვრების ყველაზე მნიშვნელოვან დროს და რესურსებს...

თუ ამ ასაკს უკვე გაცდი, ალბათ თავადაც ხვდები რომ ის ცხოვრება, რომელიც ახლა გაქვს არ არის ცხოვრება, რომელზეც ოცნებობდი. შეიძლება მადლიერი ხარ იმით, რაც გაქვს ან თავს აჯერებ ამ ყველაფერს, მაგრამ რის ფასად?

თუ არცერთ კატეგორიაში არ ჯდები, თუ ბედნიერი ცხოვრება გაქვს და მთელ დღეებს მუშაობაში არ ატარებ იმისთვის, რომ ფინანსურად დამოუკიდებელი (დამოუკიდებელი თუ არა, მინიმუმ კარგად) იყო, თუ იმას აკეთებ, რაც მართლა გინდა და გსიამოვნებს, მაშინ გილოცავ! თუ შენი ცხოვრება ისეთია, სადაც შენი წესებით თამაშობ, შენ მატრიცას თავი დააღწიე. თუმცა ამას ყველა ვერ ახერხებს...

გინდა მატრიცას თავი დააღწიო? გაიქეცი მისგან მაქსიმალურად შორს. მოერიდე ხალხს, რომლებიც მატრიცაში ცხოვრობენ, იარე შენი გზით. მაშინაც კი თუ ამ გზაზე მარტო ხარ, იცოდე რომ სწორ გზაზე დგახარ. გზა, რომელზეც მარტო მიდიხარ, ხშირად ის სწორი გზაა,

რომელსაც ადამიანები ცხოვრებაში ერთხელ ან რამდენჯერმე პოულობენ... არ დაუშვა, რომ ვინმემ ამ გზიდან გადაგახვევინოს...

“მატრიცა მხოლოდ ჩვენ გონებაში არსებობს, როგორც კი შეძლებ შენი გონების კონტროლს, მატრიცა დაინგრევა და უკვალოდ გაქრება...”

-ჯაფარა

წიგნის ერთ-ერთი დანიშნულება ის არის, რომ შენ მატრიციდან თავის დაღწევაში დაგეხმარო. ამ ყველაფერს ფსიქოლოგიის დახმარებით ვეცდები, თუმცა ასევე თავისუფლების მიღწევის, სხვების კონტროლისგან თავის დაღწევის გზებს გაჩვენებ... **დაიმახსოვრე, ამას მხოლოდ იმ შემთხვევაში შევძლებ, თუ მზად ხარ ამ ყველაფრისთვის...**

მე ყველას ვერ დავეხმარები. შეიძლება შენ დაგეხმარო, შეიძლება შენ იყო ის ადამიანი, ვისთვისაც ამ წიგნს ვწერ ან შეიძლება არც კი იყო... მე სწორ გზას განახებ, თუმცა როგორ გაყვები ამ გზას, სრულიად შენი პასუხისმგებლობაა...

ოჯახი... ახლობლები... როგორი სამწუხარო და ცუდად მოსასმენიც არ უნდა იყოს, ისინი ყველაზე მეტად დაგიპირისპირდებიან, ყველაზე მეტ პრობლემას შეგიქმნიან ცხოვრებაში. მათ უყვარხარ, შენც გიყვარს ისინი, ამიტომ, ზუსტად სიყვარულის გამო, ისინი უშვებენ შეცდომებს... შენც ბევრ დათმობაზე მიდიხარ, მაგრამ იცოდე რომ ეს დათმობები ყველანაირად უკან დაგხევს ცხოვრებაში... თუ გაქვს შესაძლებლობა, მაქსიმალურად ადრე მოიპოვე დამოუკიდებლობა... წადი უცხო ქვეყანაში, ოჯახისგან მოშორებით წადი და აკეთე ის, რაც შენი მიზნების მიღწევისთვის გჭირდება... (ანახე წიგნის ეს ნაწილი შენ ოჯახს, ეცადე გაიაზრონ ის ყველაფერი, რასაც გიშავებენ უნებურად... თუ ოჯახთან ერთად იცხოვრებ, მათ უნდა ესმოდეთ შენი... თუ არ ესმით, უნდა ჩამოშორდე მათ, მიუხედავად იმისა, რომ ისინი შენი ოჯახის წევრები არიან... რთულია, მაგრამ ეს უნდა გააკეთო, თუ შენი მიზნები შენთვის მნიშვნელოვანია, მათ მიღწევამდე ყველას ჩამოშორდი...)

როგორ უნდა მიხვდე ესმის თუ არა შენ ოჯახს შენი?

თუ ვერ ხვდებიან რატომ ათენებ ღამეებს, რატომ იყენებ დღეში 8-10-12 საათი კომპიუტერს, რატომ არ გადიხარ გარეთ, რატომ არ ატარებ მეტ დროს შენი ოჯახის წევრების გვერდით ... (და კიდევ უამრავი სხვა მიზეზი, თუმცა ეს ძირითადი ჩამონათვალია) ესეიგი მათ არ ესმით შენი... ჯობია 1-2 წელი მათგან დამოუკიდებლად იცხოვრო, აკეთო ის, რაც აუცილებელია და შემდეგ ბედნიერად იცხოვროთ მთელმა ოჯახმა, ან მთელ შენ ცხოვრებას სინანულში გაატარებ...

მნიშვნელოვანი რჩევები !

წინ საინტერესო რამდენიმე საათი გელოდება, რომელსაც ამ წიგნის კითხვაში გაატარებ.

რამდენიმე საკითხს მინდა თავიდანვე შევეხო…

- **ნუ მიიღებ რჩევას ნებისმიერისგან**
  აუცილებლად გადაამოწმე ვისგან იღებ რჩევას, რა გამოცდილება აქვს მას კონკრეტულ საკითხში, განსაკუთრებით ეს კიბერუსაფრთხოებას ეხება. ბოლო პერიოდში უამრავი "მცოდნე" ადამიანი გამოჩნდა, რომელიც კონტენტს ქმნის (ნაგავ კონტენტს, კურსებს). ხშირად მათ არანაირი გამოცდილება არ აქვთ ამ პროფესიაში და უაზრობებს ლაპარაკობენ… ასეთი ადამიანის რჩევას არასდროს დაუჯერო.
- **არ მოინდომო ყველაფერში ერთდროულად გარკვევა**
  როდესაც კიბერუსაფრთხოების ნებისმიერი მიმართულებით სწავლას დაიწყებ, აირჩიე ერთი მათგანი და ის ერთი ისავლე ხარისხიანად, ყველაფრის ერთად სწავლა არ მოინდომო, საბოლოოდ ვერაფერს ისწავლი, დროს და ენერგიას არაფრის გამო დაკარგავ. მე ამ წიგნით კონკრეტულად ჰაკინგის სამყაროში შეგახედებ… მხოლოდ ჰაკინგის :)
- **ისწავლე შენით, სიჩუმეში**
  არ არის აუცილებელი ყველას გააგებინო თუ რას სწავლობ, რა ისწავლე ან სწავლის რა ეტაპზე ხარ ამ მომენტში.
  არასდროს გაამჟღავნო შენი რეალური ცოდნა, სხვა შემთხვევაში დაიღუპები და შეგიძლია ეს სიტყვები პირდაპირი მნიშვნელობით გაიგო.
- **ყოველდღიური მუშაობა**
  არ აქვს მნიშვნელობა შენ მოტივაციას, სურვილებს… თუ წარმატების მიღწევა გინდა ამ პროფესიაში, აუცილებელია ყოველდღე იმუშაო საკუთარ თავზე. ნებისმიერი ჩაგდებული დღე 10 და 20 ნაბიჯით უკან დაგხევს, დანარჩენი შენი გადასაწყვეტია.
- **არასდროს არავის ენდო 100 პროცენტით**
  ნდობა დამღუპველია, მხოლოდ საკუთარ თავს შეგიძლია ენდო. ეს ყველაფერი მე რთული გზებით ვისწავლე, ამიტომ ვცდილობ ჩემი გამოცდილება გაგიზიარო და პრობლემები აგარიდო თავიდან. მხოლოდ საკუთარი თავის იმედი უნდა გქონდეს…

ესენია ის ძირითადი რჩევები, რაც შენთვის მაქვს, დროა დავიწყოთ!

წიგნის ამ ნაწილში განხილული იქნება შემდეგი თემები

ადამიანის გონება და მისი მნიშვნელობა

- ფსიქოლოგია და ადამიანის გონება
- ქვეცნობიერი გონება
- ცნობიერი გონება
- ქვეცნობიერი გონების გადაპროგრამება

ბნელი ფსიქოლოგია, მანიპულაცია

- ბნელი ფსიქოლოგია
- ადამიანებთან ურთიერთობის საიდუმლო
- წარმატებული მანიპულატორის თვისებები
- მანიპულაციის ეტაპები
- მანიპულატორის აღმოჩენა
- მანიპულაციის ტექნიკები გონების კონტროლისთვის
- გონების კონტროლი ჩანერგილი აზრებით

კიბერუსაფრთხოება

- რა არის კიბერუსაფრთხოება?
- CIA ტრიადა (რატომ არის მნიშვნელოვანი CIA ტრიადა?)
- მაგალითი 2012 წლიდან
- რამდენად მარტივია სისტემაში შეღწევა?
- რატომ უნდა ისწავლო / არ ისწავლო კიბერუსაფრთხოება ?
- უსაფრთხოების მიმართულებები
- ჰაკერის ტიპები
- ოსინტი
- სოციალური ინჟინერია
- შანტაჟი _ როგორ დავიცვათ თავი ?
- შენ შეგიძლია გახდე ის, ვინც გინდა...
- მარტივად გამდიდრების ილუზია

შენ გაკონტროლებენ

- ვინ, რატომ და როგორ გაკონტროლებს
- სახელმწიფო კონტროლი
- კანონებით კონტროლი
- შენ არ ხარ მომხმარებელი, შენ ხარ პროდუქტი
- კონფიდენციალურობა - “დასამალი არაფერი მაქვს”

- კონფიდენციალურობა სოციალურ ქსელში
- დარკნეტი და ტორი – თავისუფალი ინტერნეტი
- ინტერნეტის დონეები
- რატომ არის უნივერსიტეტი დროის ფლანგვა?

ადამიანების კრიტიკული შეცდომები

- პაროლების ფსიქოლოგია
- საჯარო ვაიფაი
- დააკვირდი სად, რას წერ
- ქარდინგი - მახე დამწყები ჰაკერებისთვის

კარიერა ჰაკინგში

- გზა წარმატებული კარიერისკენ ჰაკინგში
- ეთიკური ჰაკინგი (შეღწევადობის ტესტირება)
- ეთიკური მხარე შეღწევადობის ტესტირებისთვის
- ეთიკური ჰაკერის ტექნიკური უნარები
- აირჩიე შენი გზა
- ისტორია ბიჭზე, რომელმაც ნასა და პენტაგონი გატეხა
- პრაქტიკული გამოცდილება + პორტფოლიო

ჯაფარას ორგანიზაცია HackersForce

- წიგნის ბოლოს რჩევები TOP ჰაკერებისგან
- ჯაფარას ბოლოსიტყვა

შესავალი

შენ გაეცანი “მატრიცას”, რჩევებს, ჩემი და ჩემი ფორუმის ისტორიას და მიზანს, იმედია პატარა მოტივაცია მაინც მოგცა ამ ყველაფერმა. ახლა კი დროა წიგნის ძირითად ნაწილზე გადავიდეთ.

ამ წიგნში განვიხილავთ ფსიქოლოგიას და მის როლს ჰაკინგში, ჩვენ ცხოვრებაში. როგორ იყენებენ “ჰაკერები” ადამიანების ფსიქოლოგიას, როგორ ხდება ადამიანებით მანიპულაცია და რაც ყველაზე მთავარია, შენ როგორც “უბრალო” ადამიანმა, როგორ უნდა დაიცვა თავი იმ ფსიქოლოგიური ხრიკებისგან და ზეწოლისგან, რომელსაც ჰაკერები იყენებენ. წიგნის ბოლოს დეტალურ გზამკვლევს დაგიტოვებ, თუ როგორ დაიწყო განვითარება ამ სფეროში და შეიქმნა მყარი საფუძველი, როგორც მომავალმა TOP ჰაკერმა...

“უბრალო” ადამიანი ვახსენე. ამ წიგნის სამიზნე აუდიტორიას წარმოადგენენ ადამიანები, რომლებიც არ არიან ღრმად ჩახედულები ჰაკინგში და ახლა იწყებენ სწავლას, თუმცა შეიძლება ამ წიგნს ისეთი ადამიანიც კითხულობდეს, რომელსაც არ სურს საკუთარი მომავალი ამ პროფესიას დაუკავშიროს, უბრალოდ უნდა, რომ საკმარისად ინფორმირებული იყოს, რათა შეძლოს საკუთარი თავის დაცვა ინტერნეტში (შეიძლება შენ ხარ ასეთი ადამიანი, რომელსაც უბრალოდ საკუთარი თავის დაცვა სურს). ამიტომ ადამიანებს, რომლებიც არ აპირებენ ამ პროფესიაში ღრმად ჩახედვას, “უბრალო” ადამიანი ვუწოდე :) მსოფლიოს მოსახლეობის უმრავლესობას (99%) წარმოდგენა არ აქვს თუ რა ხდება ამ სამყაროში…

წინ საინტერესო საუბრები გველოდება. წარმოდგინე, რომ პირისპირ ვზივართ, წიგნი ისე დავწერე, რომ ზუსტად ასეთი შთაბეჭდილება გქონდეს მისი კითხვისას, შედეგად ბევრად უფრო საინტერესო იქნება ეს პატარა, მაგრამ საჭირო მოგზაურობა შენთვის.

ფსიქოლოგია და ადამიანის გონება

ფსიქოლოგია და ადამიანის გონება

სანამ სხვა თემებს შევეხებით, მანამდე შენ გონებაზე და ადამიანის ფსიქოლოგიაზე უნდა მოგაწოდო საჭირო ინფორმაცია. ამ წიგნის ერთ-ერთი მიზანი შენი გონების და ფიქრების შეცვლაა. ამ მომენტში შენ განსხვავებულად ფიქრობ, თუ იგივე ფიქრებით გააგრძელებ ამ სფეროში და ზოგადად ცხოვრებაში განვითარებას, სადღაც აუცილებლად გაიჭედები და უარს იტყვი განვითარებაზე…

შენი გონება ყველაზე ძლიერი იარაღია, რაც გაგაჩნია ნებისმიერის წინააღმდეგ და ერთადერთი რამ, რისი კონტროლიც სრულიად შენ ხელშია. მას შეუძლია შეცვალოს შენი ცხოვრება, თუმცა ამ ეტაპზე შენი ეს ნაწილი მიუწვდომელია, ჩვენი მიზანი მისი გამოღვიძებაა. (ვიცი ფსიქოლოგიურ სესიას დაემსგავსება ეს თავი, მაგრამ აუცილებელია ამ თავის წაკითხვა და გააზრება შენთვის)

ადამიანის გონება იყოფა სამ ნაწილად _ ცნობიერი, ქვეცნობიერი და არაცნობიერი. ჩვენი ინტერესი უმეტესად ქვეცნობიერი გონებისკენ იქნება მიმართული, ვინაიდან სწორედ ქვეცნობიერი გონება აკონტროლებს ადამიანის ქცევას, ემოციებს და ცნობიერის ნაწილს…

ქვეცნობიერი გონების კონტროლი რთულია და ყველას არ შეუძლია, სწორედ ეს განასხვავებს წარმატებულ ადამიანს წარუმატებელი ადამიანისგან. ის, ვინც აკონტროლებს საკუთარ გონებას, წარმატებას აუცილებლად მიაღწევს, ხოლო ის, ვინც ვერ აკონტროლებს საკუთარ გონებას, რაც არ უნდა გააკეთოს წარმატებას ვერასდროს მიაღწევს.

ჩემი მიზანია დაგეხმარო საკუთარი და სხვების გონების კონტროლში... ეს ყველაფერი წარმატების შესაძლებლობას მოგცემს ცხოვრებაში. მე ვერ დაგპირდები რომ შენ აუცილებლად მიაღწევ წარმატებას, ვინაიდან ეს სრულიად შენზეა დამოკიდებული, თუმცა მე მოგცემ შესაძლებლობას, რომელიც არც თუ ისე ბევრ ადამიანს ეძლევა ცხოვრებაში.

მსოფლიოს მოსახლეობის დაახლოებით 5% არის წარმატებული, დანარჩენი 95% წარუმატებელია. წარმატება ზოგადი მცნებაა. ზოგისთვის წარმატება მილიონობით დოლარით, ფულით განისაზღვრება, ზოგისთვის კარგი კარიერა უკვე წარმატებაა, თუმცა წარმატება არ ნიშნავს ბედნიერებას…

დღეს შენ ამ წიგნს კითხულობ და ბევრ მნიშვნელოვან რაღაცას ისწავლი, რაც მომავალში დაგეხმარება ჩამოყალიბდე იმ ადამიანად, რომელიც შენ გინდა. მაგრამ ამას ვერ მიხვდები, არ გეცოდინება, რომ შენი წარმატების რაღაც ნაწილი ამ წიგნმა განაპირობა, ვინაიდან ის, რასაც ამ წიგნიდან ისწავლი, შენ ქვეცნობიერ გონებაში ჩაიწერება (თუ მართლა ისწავლი რამეს).

ქვეცნობიერი გონება

ქვეცნობიერი გონება არის გონების ნაწილი, რომელიც შენ ფიქრებს, ემოციებს აკონტროლებს...

ყველაფერი ის, რაც შენი დაბადების დღიდან დღემდე მომხდარა ჩაწერილია ქვეცნობიერ გონებაში. შენ ვერ გაიხსენებ ყველა მოგონებას, გონების ამ ნაწილზე წვდომა ადამიანების უმრავლესობას არ აქვს…

დაიმახსოვრე ქვეცნობიერ გონებას შეუძლია ყველაფერი დაიმახსოვროს, მას მეხსიერების ლიმიტი არ გააჩნია. სწორედ ქვეცნობიერ გონებაში ჩაწერილი ინფორმაცია განსაზღვრავს შენ პიროვნებას დღეს.

რას აკეთებს ქვეცნობიერი გონება? მაგალითებს მოგიყვან რომ უკეთ მიხვდე…

მაგალითად, როდესაც სიარულს, თასმების შეკვრას, ველოსიპედის ტარებას ან მანქანის მართვას სწავლობდი, შენ იმ მომენტში ფიქრობდი კონკრეტულ ქმედებებზე... როგორ დაგეტრიალებინა მანქანის საჭე სწორ მომენტში, რა მოქმედებით უნდა შეგეკრა თასმა და ასე შემდეგ...

გავიდა დრო და დღეს ამ ყველაფერს მექანიკურად აკეთებ, აღარ გჭირდება ფიქრი კონკრეტულ ქმედებაზე.

რატომ? იმიტომ რომ ეს ქმედებები ქვეცნობიერ გონებაში ჩაიწერა და შენ ცნობიერ გონებას აღარ უწევს ზედმეტი ფიქრი ამ ყველაფერზე.

ქვეცნობიერი გონების მართვა და გადაპროგრამება შესაძლებელია ცნობიერი გონების დახმარებით. როდესაც შენ კონკრეტულ რაღაცას მუდმივად აკეთებ, ამ ყველაფერს იმახსოვრებს ქვეცნობიერი გონება და ცნობიერი გონების ნაცვლად, ავტომატურად ფიქრის გარეშე აკეთებს მას მომავალში.

არაცნობიერი შენი გონების ის ნაწილია, სადაც შენი ღრმა შიშები, ინსტიქტები და ტრავმული მოვლენებია შენახული... როგორც სიტყვა გეუბნება ის არაცნობიერია და მას ვერ გავაკონტროლებთ... მხოლოდ ეს უნდა იცოდე არაცნობიერ გონებაზე. დანარჩენი შეგიძლია თავად მოიძიო თუ გაინტერესებს.

ცნობიერი გონება

ცნობიერ გონებას სამწუხაროდ მეხსიერების ლიმიტი გააჩნია. მაგალითად, რამდენად ხშირად დაგვიწყებია რაღაც მნიშვნელოვანი, რაც გეგონა რომ არ დაგავიწყდებოდა? რამდენად ხშირად გავიწყდება ადამიანის სახელები და ზოგადად საჭირო ინფორმაცია? (ეს შენი ბრალი არ არის, ნიშნავს რომ ზედმეტად ბევრ საკითხზე ფიქრობ და გონებას არ შეუძლია ყველაფრის დამახსოვრება, რაც კარგია რაღაც მხრივ, გამოდის რომ აზროვნებ და გამოირჩევი მსოფლიოს დიდი ნაწილისგან. ზოგს აზროვნებაც არ შეუძლია) ამ ყველაფერს ცნობიერი გონება აკონტროლებს, ის ფილტრავს ინფორმაციას და ცდილობს ყველაფერი “არასაჭირო” წაშალოს შენი გონებიდან, თუმცა ზოგჯერ ის საჭირო ინფორმაციასაც შლის შენი მეხსიერებიდან, სწორედ ამიტომ, ხშირად გავიწყდება მნიშვნელოვანი ინფორმაცია.

მაგალითად, როდესაც ვიდეოს უყურებ რაღაცის სწავლის მიზნით და გგონია ყველაფერი დაიმახსოვრე, თუმცა რაღაც დროის შემდეგ ყველაფერი გავიწყდება, გაინტერესებს რისი ბრალია ეს ყველაფერი? შენი გონება იმ მომენტში არ არის საკმარისად ფოკუსირებული ინფორმაციის დამახსოვრებაზე… შემდეგში ცადე მაქსიმალურად ფოკუსირებულმა უყურო ისეთ ვიდეოს, საიდანაც ინფორმაციის დამახსოვრება გჭირდება, შედეგებით გაოცდები)

ცნობიერ გონებას აქვს კიდევ ერთი შეზღუდვა, მას ერთდროულად არ შეუძლია რამდენიმე საქმის კეთება, მხოლოდ ერთი ფოკუსის აღება შეუძლია.

რამდენად ხშირად დაუსვამთ შენთვის კითხვა, როდესაც საინტერესო ინფორმაციას კითხულობდი ან რამეს აკეთებდი და მექანიკური პასუხი გაგიცია ან საერთოდ არ გაგიგია კითხვა? ეს იმიტომ ხდება, რომ შენი გონება ინფორმაციის წაკითხვაზე ან კონკრეტული საქმის შესრულებაზე იყო ფოკუსირებული იმ მომენტში და არა მოსმენაზე…

საბოლოო დასკვნა ცნობიერ გონებაზე: ცნობიერი გონება არის შენი გონების ლოგიკური ნაწილი. გადაწყვეტილებები, რომლებსაც იღებ, ქმედებები, რომლებსაც ყოველდღიურად აკეთებ, უმარტივესი მაგალითი, ხელის ჰაერში აწევაც კი… ამ ყველაფერს ცნობიერი გონება აკონტროლებს.

ქვეცნობიერი გონების გადაპროგრამება

მზად ხარ შეცვალო შენი ქვეცნობიერი გონება? პირველ რიგში, შენ უნდა მოიშორო უარყოფითი ფიქრები, აზრები და კონცენტრირდე დადებით ფიქრებზე.

რამდენად ხშირად უთქვამთ ბავშვობაში ან თუნდაც ზრდასრულ ასაკში შენთვის უარყოფითი ფრაზები? მაგალითად: ცხოვრებაში ვერაფერს მიაღწევ, შენგან არაფერი გამოვა ან რამდენად ხშირად გითქვამს საკუთარი თავისთვის, რომ რაღაცას ვერ შეძლებდი?

ეს ყველაფერი უარყოფითი აზრებია, რომლებიც წლების განმავლობაში შენ ქვეცნობიერ გონებაში ილექებოდა.

გინდა წარმატებას მიაღწიო? მაშინ ეს ფიქრები უნდა მოიშორო. არ მისცე უაზრო ფიქრებს შენი მომავლის განადგურების უფლება.

მე და შენ ერთად, ამ ფიქრებს შევცვლით დადებითი ფიქრებით, ამოვშლით ნეგატიურ აზრებს შენი გონებიდან და ახალ გზას ვუჩვენებთ შენ ქვეცნობიერს.

ქვეცნობიერი გონების გადაპროგრამების ბევრი მეთოდი არსებობს, თუმცა მე ყველაზე მარტივ მეთოდს გაგიმხელ… ეს პროცესი მარტივია, მაგრამ რამდენადაც მარტივია პროცესი, იმდენად რთულია მისი განხორციელება.

ალბათ გაინტერესებს, რატომ?

დიდი ალბათობით ფიქრობ, რომ ეს ყველაფერი სისულელეა და არ იმუშავებს. თუ შენ ასე ფიქრობ, მაშინ არ იმუშავებს, რადგან გონებას წინასწარ ამზადებ იმედგაცრუებისთვის. ამის ნაცვლად თქვი შემდეგი რამ: **“მე მჯერა რომ შევცვლი საკუთარ ფიქრებს, ამისთვის მხოლოდ მარტივი ქმედებები უნდა გავაკეთო, რას ვკარგავ? არაფერს!“** და გააკეთე ის, რასაც ახლა წაიკითხავ.

შედეგების დასანახად ეს პროცესი მინიმუმ 3 თვე უნდა აკეთო, თუმცა ზოგი ადამიანი შედეგებს უფრო მოკლე დროშიც აღწევს. პირადი გამოცდილებით გეტყვი, რომ ეს ყველაფერი მუშაობს! დღეს რასაც მივაღწიე, სწორედ ჩემი გონების დამსახურებით...

ენდე ჯაფარას და გადადგი ნაბიჯი წარმატებისკენ. მაქსიმუმ 3-6 თვის შემდეგ შენ სხვა ადამიანი იქნები, ამ ყველაფრის შემდეგ შენ ჯაფარას მადლობას ეტყვი, ვინაიდან ჯაფარა შენ ცხოვრებას შეცვლის...

მაშ ასე, დავიწყოთ.

ადექი, იპოვე ფურცელი, ფანქარი და მონახე კომფორტული ადგილი,

სადაც არავინ შეგაწუხებს. თუ ასეთი ადგილი არ გაქვს სახლში, წადი ბუნებაში და იქ იფიქრე… აუცილებელია ხელით ჩამოწერო ყველაფერი და არა სადღაც კომპიუტერში ან ტელეფონში, ფაილში, რომელსაც მეორედ აღარ გახსნი. (თუ ამ ყველაფერს არ გააკეთებ, აზრი არ აქვს ამ თავის წაკითხვას, შედეგი 0 გექნება და შეგიძლია ეს ნაწილი გამოტოვო, მაგრამ გირჩევ ეს არ გააკეთო)

მას შემდეგ, რაც აიღებ ფურცელს და ფანქარს, დაჯექი და დაიწყე შენი იდეალური ცხოვრების აღწერა. ჩართე ყველანაირი წარმოსახვა და დაიწყე წერა. აღწერე შენი ცხოვრების სტილი (რას, როგორ, როდის აკეთებ), ფინანსები, პროფესია, ურთიერთობები. მოკლედ რომ გითხრა, შექმენი შენი იდეალური ცხოვრება ზუსტად ისეთი, როგორიც გინდა რომ გქონდეს!

<u>თუ არ იცი რა გინდა, წარმატებას ვერასდროს მიაღწევ, ამიტომ დაჯექი და იფიქრე, რას გინდა მიაღწიო შენ ცხოვრებაში?</u>

რევერსული ინჟინერია – პროცესია, როდესაც საბოლოო პროდუქტს ვშლით მცირე ნაწილებად, პატარა ეტაპებად იმისთვის, რომ უკეთ გავიგოთ თუ როგორ მუშაობს საბოლოო პროდუქტი…

ზუსტად ეს გვჭირდება, ოღონდ ამჯერად ჩვენი მიზნების დანაწევრება გვიწევს იმისთვის, რომ ჩვენმა გონებამ უკეთ შეძლოს დამახსოვრება და საბოლოო მიზნის მიღწერა გამარტივდეს...

რამდენი “დადასტურება” უნდა ჩამოწერო? მოდი ამ ყველაფერს დადასტურებები დავარქვათ. (ჯერ არარსებულს ვქმნით, შემდეგ ჩვენი ქმედებებით ამ ყველაფერს უნდა მივაღწიოთ, რაც ჩვენი სიტყვის დადასტურება გამოდის მომავალ დროში) კონკრეტული რიცხვი არ არსებობს, თუმცა სასურველია დასაწყისში რამდენიმე ათეული მაინც იყოს, მინიმუმ 30, მაგრამ კარგად გააზრებული.

არ მინდა ხელი შეგიშალო ამ პროცესში, რადგან ეს შენგან უნდა მოდიოდეს, თუმცა რამდენიმე მაგალითს გაჩვენებ, რომ მიხვდე თუ რისი გაკეთება გჭირდება. მაგალითად:

1. ჩემ პროფესიაში ერთ-ერთი საუკეთესო ვარ (აღწერე)
2. ფული ყოველთვის მაქვს და მუდმივად გამოვიმუშავებ მას იმის კეთებით, რაც მიყვარს (რამდენი? როგორ? აღწერე)
3. ვარჯიშში მსიამოვნებს და ჯანსაღი ცხოვრებით ვცხოვრობ...

ახლა უკვე იცი რა სახის დადასტურებები უნდა ჩამოწერო. ყურადღება მიაქციე დროს, ისინი ახლანდელ დროშია, არც წარსულში, არც მომავალში, ახლანდელ დროში!

არ გამოიყენო ნეგატიური სიტყვები, ვინაიდან ქვეცნობიერმა გონებამ

არ იცის შენ რა გაგებით იყენებ კონკრეტულ სიტყვას და შეიძლება არასწორად მოხდეს მისი ჩაწერა ქვეცნობიერ გონებაში. მაგალითად არ დაწერო დადასტურება შემდეგნაირად _ “**მე არაფრის მეშინია**!” ჯამში ეს ფრაზა პოზიტიურია, მაგრამ გონებამ სიტყვა “მეშინია” შეიძლება შიშად აღიქვას, რაც ცუდია, ამიტომ ასეთ სიტყვებს მოერიდე…

თუ ამ სიას ერთ და ორ დღეში ვერ ჩამოწერ არ არის პრობლემა, ვიცი რთულია. ამ სიის შედგენა და განახლება მუდმივი პროცესია, სასურველიც კი არის ის ხშირად გადაიხედოს, ვინაიდან მოხდეს მისი განახლება ისე, როგორც საჭიროა.

გაინტერესებს მას შემდეგ, რაც შექმნი ამ სიას რა უნდა გააკეთო?

შენ უნდა ჩანერგო ეს დადასტურებები შენ ქვეცნოებიერ გონებაში. ეს ყველაზე საინტერესო და მნიშვნელოვანი მომენტია. შენი სამუშაო მაგიდის წინ, კედელზე ჩამოკიდე ეს სია და შეხედე მას, როდესაც ამის შანსი გექნება.

დღეში ორჯერ, დილით და საღამოს დაუთმე შენ თავს ცოტა დრო და წარმოიდგინე, რომ უკვე გაქვს ეს ცხოვრება. შეგიძლია თავიდან ეს სია წაიკითხო, ხოლო როდესაც დაიმახსოვრებ, ხშირად წარმოიდგინე შენი იდეალური ცხოვრება. (როდესაც იცი მიზანი, შედეგის მიღწევა 50%_ით მატრივდება)

რამდენი ხანი უნდა აკეთო ეს ყველაფერი? დრო ინდივიდუალურია, შეიძლება ეს 10 ან 20 წუთი გაგრძელდეს, ამას შენ წყვეტ, მთავარია ეს ყველაფერი ყოველდღე გააკეთო.

როგორც კი დაიწყებ შენი ქვეცნობიერი გონების გადაპროგრამების პროცესს, შენ ცხოვრებაში ცვლილებები დაიწყება. ეს ცვლილებები ზოგჯერ სწრაფად ხდება, თუმცა ძირითადად ისინი ნელა და შეუმჩნევლად მიმდინარეობს… დარწმუნებული იყავი რომ ცვლილებები ხდება და ეს არ ეხება მატერიალურ მდგომარეობას, თავდაპირველად, ისინი ფსიქოლოგიურია.

დადასტურებების დროს არ ფოკუსირდე მხოლოდ მატერიაზე, არამედ ემოციურ მდგომარეობაზე, გონებაზე. მაგალითად, თუ ბავშვობაში გეუბნებოდნენ რომ სულელი იყავი და შენგან არაფერი გამოვიდოდა, ახლა შენი დადასტურება უნდა იყოს “მე ჭკვიანი ვარ და აუცილებლად მივაღწევ ჩემ მიზნებს“... ქვეცნობიერი გონება ერთდროულად ორ საპირისპირო დადასტურებას ვერ ჩაიწერს, ან ერთი ჩაიწერება გონებაში ან მეორე. ამიტომ დარწმუნდი, რომ მხოლოდ დადებითზე იფიქრებ. ზუსტად ამ მიზეზის გამო არის ეს პროცესი ადამიანებისთვის რთული...

იმისთვის რომ უარყოფითი ამოშალო გონებიდან, ჯერ ეს უარყოფითი უნდა გაიხსენო შენი წარსულიდან.

მნიშვნელოვანი მომენტია და ყურადღებით იყავი ამ ნაწილში. ის, რისი წარმოდგენაც შესაძლებელია, რეალობაა. თუმცა სანამ რეალობა გახდება, მანამდე მიზნის სრულად წარმოდგენა უნდა შეძლო.

მხოლოდ ქვეცნობიერ გონებაში რაღაცის ჩაწერა არ არის საკმარისი, აუცილებელია ცნობიერი გონებაც მივახმაროთ მას.

მაგალითად თუ ამბობ, რომ მე ერთ-ერთი TOP ჰაკერი ვარ ქსელის მიმართულებით, რომელსაც ნებისმიერი ორგანიზაციის, კომპანიის ქსელის გატეხვა შეუძლია, თუმცა რეალობაში იცი, რომ ბევრი რაღაც არ შეგიძლია, უნდა ადგე და შენი ცნობიერი გონების დახმარებით მასალები, კონკრეტულ საკითხში გარკვეული ადამიანები უნდა მოძებნო და დახვეწო შენი უნარები მათი დახმარებით, ხვდები? ცნობიერ გონებას არანაკლები მნიშვნელობა აქვს ქვეცნობიერ გონებაზე. მხოლოდ ორივეს თანხვედრა მიგიყვანს შენ მიზნებამდე.

თუმცა, დიდი ალბათობით შენ ფიქრობ, რომ ეს ყველაფერი უაზრობაა, სერიოზულად არ უყურებ ამ ყველაფერს…

მეგობარო შენ ორი გზა გაქვს. შეგიძლია დაიჯერო რაც წაიკითხე და მიყვე პროცესს, ამ შემთხვევაში შენი წარმატების შანსი 50% იქნება ან უბრალოდ დაიკიდე და შენ გარანტირებულად 100%_ით წააგებ...

მე დაგანახე თუ როგორ უნდა შეცვალო შენი ქვეცნობიერი გონება. ის რაც ზემოთ წაიკითხე, რეალურად მუშაობს და ცვლის ადამიანების ცხოვრებას.

ამ წიგნში ფსიქოლოგიას კიბერუსაფრთხოებაზე/ჰაკინგზე დიდი როლი უკავია. ამ პროფესიას ასე თუ ისე ისწავლის ხალხი, მაგრამ საკუთარ გონებას და ცხოვრებას ადამიანების მხოლოდ მცირე რაოდენობა აკონტროლებს, მე მინდა რომ შენც შეძლო ეს ყველაფერი. თუ მიყვები გზას, რომელიც განახე, დამიჯერე შენი ცხოვრება უკეთესობისკენ შეიცვლება.

წიგნში ასევე ბნელ ფსიქოლოგიასაც შევეხებით, მანიპულაციას. მაქსიმალურად გამოიყენე ცოდნა, რომელსაც გაძლევ, რადგან სხვა არავინ, არასდროს, მსგავს ცოდნას არ გაგიზიარებს და ბევრს არც აქვს ეს ცოდნა რომ გაგიზიაროს.

ბნელი ფსიქოლოგია
მანიპულაცია

ბნელი ფსიქოლოგია

მივადექით ერთ-ერთ ყველაზე საინტერესო და ჩემთვის საყვარელ ნაწილს ამ წიგნში. ადამიანების კონტროლი, მანიპულაცია, ეს ის მცნებებია, რომელსაც ადამიანების ცხოვრების დანგრევა შეუძლია, თუმცა ასევე ამ ყველაფერს შეუძლია შეუჩერებელი გაგხადოს და მათი დახმარებით ცხოვრებაში ყველაფერს მიაღწევ. იმისათვის, რომ შენი კონტროლი ვერავინ შეძლოს, თავს ვალდებულად ვთვლი ჩემი ცოდნა, რომელიც საშიშია გაგიზიარო.

ბოროტი მიზნებისთვის არ გამოიყენო ეს ცოდნა, თუმცა როგორც სხვა ყველაფერი, ესეც მხოლოდ შენზეა დამოკიდებული. მე შენ გაძლევ ცოდნას, რომლის მსგავსი ფსიქოლოგების უმრავლესობასაც კი არ აქვს. ხვდები რამდენად დიდი უპირატესობა გექნება სხვებთან შედარებით რეალურ სამყაროში?

ადამიანებით მანიპულაცია ყველგან ხდება, საზოგადოებაში, სამუშაო გარემოში, სოციალურ მედიაში, ოჯახში, ურთიერთობებში, საერთოდ ყველგან.

როდესაც ბნელ ფსიქოლოგიას, მანიპულაციას ვეხებით, აუცილებელია ვახსენოთ ოთხი ტიპის თვისება მანიპულატორ ადამიანებში: მაკიაველი, ნარცისი, სადისტი და ფსიქოპათი. ამ თვისების მქონე ადამიანები ყველაზე საშიშები არიან… შეიძლება მანიპულატორ ადამიანს ერთი ან რამდენიმე თვისება ქონდეს ამ ოთხიდან. (ნებისმიერ ადამიანს აქვს ერთ-ერთი თვისება)

განვიხილოთ ოთხივე მათგანი:

მაკიაველი

ამ ტიპის თვისების მქონე ადამიანი ბუნებით მანიპულატორია, შეუძლია ადამიანის დარწმუნება, მოტყუება ისე, რომ ამას ვერავინ მიხვდება. ასეთი ადამიანი ნებისმიერ რამეს გააკეთებს საკუთარი მიზნების მისაღწევად. მას არ ადარდებს რამდენ ადამიანს ავნებს ამ პროცესში… ასეთი ადამიანისთვის სიკეთე, დახმარება წარმოუდგენელია და არც თანაგრძნობის უნარი აქვს.

ნარცისი

ნარცისი ყველგან ნარცისია, მას მხოლოდ საკუთარი თავი ადარდებს და მუდამ საკუთარ თავზე საუბრობს, ფიქრობს. დარწმუნებულია საკუთარ სრულყოფილებაში და ყოველთვის გონია, რომ მართალია. ამ ტიპის ადამიანი იმდენად დახელოვნებულია მანიპულაციაში, რომ შეუძლია სხვა ადამიანსაც მარტივად დააჯეროს საკუთარი სრულყოფილება, თუმცა დიდ საზოგადოებაში გარევა უჭირს მისი ნარცისობიდან გამომდინარე...

ფსიქოპათი

ოთხი თვისებიდან, რომლებსაც ჩვენ განვიხილავთ, ფსიქოპათები ყველაზე საშიშები არიან. ასეთი ადამიანი დაუფიქრებლად აკეთებს ყველაფერს დანაშაულის გრძნობის გარეშე, არც კი ადარდებს შედეგები. ხშირად სერიული მკვლელები სწორედ ამ თვისების მქონე ადამიანები არიან. ასეთ ადამიანს მარტივად შეუძლია ხალხში გარევა ნარცისებისგან განსხვავებით, რაც მას უფრო საშიშს ხდის…

სადისტი

ხშირად ამ თვისებას არ განიხილავენ მანიპულატორ ადამიანებში, თუმცა მნიშვნელოვანია… ასეთი ადამიანი არ არის ბუნებით იმპულსური და მანიპულატორი, თუმცა სიამოვნებს სხვა ადამიანების ტანჯვა და ტკივილი. ამ ტიპის ადამიანები ხშირად ძალოვან სტრუქტურებში, ქუჩებში გხვდებიან (კრიმინალები). ასეთი ადამიანი ყველანაირი მიზნის გარეშე, უბრალოდ ანგრევს ადამიანების ცხოვრებას და ამით სიამოვნებას იღებს…

ზოგ ადამიანში ეს ოთხი თვისება დამალულია, მხოლოდ პრაქტიკის, რეალური გამოცდილების შემდეგ გაიგებ თუ რომელ მათგანს მიეკუთნები...

ცოდნა, რომელსაც ახლა იღებ ნებისმიერ პროფესიაში გამოგადგება. ნებისმიერი მდიდარი და წარმატებული ადამიანი დარწმუნებული იყავი კარგი მანიპულატორია. თუ მანიპულაციაში საუკეთესოების დონეზე ახვალ (TOP 1%), შენც გექნება იდეალური ცხოვრება, მაგრამ სანამ იდეალურ ცხოვრებას მიაღწევ, მანამდე უნდა გახდე საუკეთესო მანიპულატორი…

ისწავლე მანიპულაცია, გახდი მანიპულატორი და შენთვის საზღვრები აღარ იარსებებს :)

გაითვალისწინე, თუ ამ გზაზე ადამიანების ცხოვრებას დაანგრევ ცუდად დაასრულებ. მანიპულაცია ორი სახისაა, დადებითი და უარყოფითი…

დადებითი უფრო მეტი უნდა იყოს შენში (დარწმუნება), ვიდრე მანიპულაცია (ბნელი ფსიქოლოგია). თუმცა შედეგს ორივე მოგცემს…

მანიპულაცია

მანიპულაციის ორი ფორმა არსებობს, ფარული და დაუფარავი. ფარული მანიპულაციის დროს მსხვერპლს წარმოდგენა არ აქვს თუ რა ხდება მის თავს.

დაუფარავი მანიპულაციის მაგალითია შანტაჟი, გამოძალვა და ა.შ…

რა თქმა უნდა ფარული მანიპულაცია ბევრად უფრო ეფექტურია (გონების კონტროლი, აზრების ჩანერგვა).

ადამიანებთან ურთიერთობის საიდუმლო

მე შემიძლია დაგარწმუნო, რომ გააკეთო კონკრეტული ქმედება გაუაზრებლად წიგნის კითხვისას ნებისმიერ მომენტში. წიგნის წაკითხვის შემდეგ და საკუთარ თავზე მუშაობით შენც შეძლებ სხვა ადამიანების დარწმუნებას გააკეთონ ის, რაც შენ გინდა.

ადამიანების უმრავლესობას ცხოვრებაში რამდენიმე რამ სურს:

- ფული
- ჯანმრთელობა
- თავისუფლება (დამოუკიდებლობა)
- სიყვარული
- ყურადღება

ეს ის ძირითადი ჩამონათვალია, რაც ადამიანების 90% სურს. (შენც ხომ მსგავსი სურვილები გაქვს?)

თუმცა არის ერთი მნიშვნელოვანი ძალიან ღრმა სურვილი, რომელიც ქვეცნობიერი გონებიდან მოდის და თითქმის ყველა ადამიანს აქვს:

<u>“სურვილი იყო მნიშვნელოვანი, გამორჩეული, დაფასებული”.</u>

სხვა ადამიანზე გავლენის მოხდენის ერთ-ერთი გზა არის საუბარი იმაზე, რაც მას სურს (ესაუბრე ადამიანებს მათ მიზნებზე)...

თავი განსაკუთრებულად უნდა აგრძნობინო ადამიანს. შენ უნდა აჩვენო მას გზა, რომლითაც მისთვის სასურველს მიაღწევს, შედეგად შენ მის ნდობას მოიპოვებ, ნდობა ყველაფრის გასაღებია...

ხვალ შეიძლება უცნობი ადამიანის დარწმუნება დაგჭირდეს, სანამ რამეს გააკეთებ დაფიქრდი და კითხე შენ თავს:

“როგორ შევძლებ ამ ადამიანის დარწმუნებას გააკეთოს ის, რაც მე მინდა. რა სურს მას ისეთი, რისი მიცემაც მე შემიძლია?”

ადამიანების 5 პროცენტი აკონტროლებს დანარჩენ 95 პროცენტს

“მანიპულაცია, კონტროლი, დარწმუნება”, როგორც გინდა ისე უწოდე, წარმატების მთავარი გასაღები არის **ადამიანის მართვა.** (შენ ეს უკვე იცი)

ადამიანის მართვის რამდენიმე მეთოდი არსებობს. საუკეთესო და ყველაზე მარტივი მეთოდი ფულია. თუ ფული გაქვს, შეგიძლია გლობალური მოთამაშე გახდე და არა ერთ ან ორ, არამედ ათასობით, მილიონობით ადამიანზე გქონდეს გავლენა. (პოლიტიკოსები, პარტიები, მთავრობები ამას აკეთებენ, რადგან მათ უამრავი ფული აქვთ, შენივე ფულით და გადასახადებით გაკონტროლებენ)

ფული ყველანაირ გზას გიხსნის ცხოვრებაში. ის ვინც გეტყვის, რომ ფული ხელის ჭუჭყია და ადამიანებს ფული აბოროტებს, ეცდება დაგარწმუნოს რომ ფული ბედნიერებას ვერ მოგიტანს, უბრალოდ ჩამოშორდი… ასეთი ადამიანებისგან კარგს ვერაფერს ისწავლი. სამწუხაროდ ხშირად ასეთი ხალხი ჩვენ ოჯახში გვყავს…

ფული ყველანაირ გზას გიხსნის და მეტ შესაძლებლობას გაძლევს… თუ შენ შინაგანად ბოროტი ხარ, ფული უფრო გაგაბოროტებს. თუ კეთილი ხარ, მეტ ფულს მეტი კეთილი საქმისთვის გამოიყენებ...

ეს პატარა, საჭირო გადახვევა იყო ფულთან დაკავშირებით, დავუბრუნდეთ თემას…

ამ თავში ჩვენ სხვადასხვა ტაქტიკებს განვიხილავთ, ხოლო ამ თავის ბოლოს შენ გეცოდინება, თუ როგორ იმართებიან ადამიანები, შენც შეძლებ ადამიანების მართვას გარკვეული დროის და პრაქტიკის შემდეგ, მინიმუმ არასდროს გახდები მანიპულაციის მსხვერპლი, რადგან თავად იქნები მანიპულატორი :)

თავი ცუდად არ იგრძნო, როდესაც გეუბნები, რომ შენ მანიპულატორი იქნები, პირიქით, უნდა ამაყობდე. მანიპულაცია ყოველთვის ნეგატივთან არ ასოცირდება. მანიპულაცია მოგცემს საშუალებას ნებისმიერი სიტუაცია შენთვის სასარგებლოდ შემოატრიალო, რაც დამიჯერე ყოველთვის წარმატებას მოგიტანს ნებისმიერ ვითარებაში…

როგორ ფიქრობ წარმატებული ხალხი, ვინც ყოველდღე ჩანს მედიაში და მილიონობით გამომწერი, მიმდევარი ყავს, რატომ არიან წარმატებულები? პასუხი: იმიტომ, რომ ასეთ ხალხს შეუძლია საკუთარი გამომწერების

კონტროლი. ასეთმა ხალხმა იცის, თუ რა სურთ მათ გამომწერებს და ზუსტად იმას აძლევენ. ეს მანიპულაციის ერთ-ერთი მეთოდია, ემოციური მანიპულაცია.

ნებისმიერ ადამიანს კითხე, თუ ვინ არის მისი იდეალი და რატომ მოწონს ის. დააკვირდი და მიხვდები, რომ ეს ადამიანი ემოციურად არის დაკავშირებული იმ ადამიანთან, რომელიც მას მოწონს. არ წახვიდე შორს, შენ თავს კითხე, რატომ მოგწონს კონკრეტული ადამიანი? შეიძლება ის, როგორც საკუთარი საქმის პროფესიონალი ისე მოგწონდეს, მაგრამ შენი გონება ავტომატურად დაიწყებს ემოციური კავშირის ძებნას ამ ადამიანთან.

მაგალითად მე მომწონდა ანონიმუსი, ვიზიარებდი მათ ხედვას, იდეოლოგიას. ჩემი შეხედულებები ემთხვეოდა მათ ქმედებებს, მათთან თავს დაკავშირებულად ვგრძნობდი…

ემოციური კავშირი ყველაზე ძლიერი იარაღია მანიპულაციის სამყაროში ადამიანის წინააღმდეგ…

მეთოდებს, რომლებსაც აქ გასწავლი, აუცილებელი არ არის მორალურად მართებული იყოს და არც იქნება. ადამიანებით მანიპულაცია მორალურად გამართლებული არასდროს არის (რამდენიმე გამონაკლისის გარდა, მაგალითად თუ შენიანს ეხებიან, შეგიძლია მორალი დაივიწყო და ნებისმიერი რამ გააკეთო, რაც საჭირო იქნება).

რასაც აქ გასწავლი მხოლოდ ერთი მიზანი აქვს, მოგცეს ის შედეგი, რომელიც შენ გინდა. მე გასწავლი როგორ მიიღო ყოველთვის ის, რაც მოგინდება კონკრეტული ადამიანისგან და ამას მორალის საზღვრებში არ მოვაქცევ. მანიპულაციის მთავარი მიზანი შედეგია, არ აქვს მნიშვნელობა რა გზით, მთავარია მანიპულაცია შედგეს.

წარმატებული მანიპულატორის თვისებები რა უნდა შეგეძლოს?

სულ სამი თვისება გჭირდება თუ გინდა რომ წარმატებული მანიპულატორი გახდე, თუმცა ამ თვისებების შეძენა არც ისე მარტივია...

- უნდა შეძლო შენი რეალური მიზნების დაფარვა ბუნებრივად. (რთულია, მაგრამ შესაძლებელია ნებისმიერი ადამიანისთვის)
- ზუსტად უნდა განსაზღვრო შენი მსხვერპლის სისუსტეები, ვგულისხმობ ფსიქოლოგიურ მდგომარეობას და არამარტო. (ბევრ პრაქტიკას მოითხოვს, ამ უნარების გაუმჯობესება მხოლოდ პრაქტიკით არის შესაძლებელი)
- არ უნდა შეგეცოდოს შენი მსხვერპლი. საჭიროების შემთხვევაში უნდა შეძლო მასზე ფსიქოლოგიური ზეწოლის მოხდენა და ეს ხშირად მოგიწევს. თუ ჯერ არ ხარ გულცივი, უნდა გახდე…

  სხვანაირად მანიპულატორი ვერ იქნები, რადგან მსხვერპლი ყოველთვის შეგეცოდება :)

ეს ყველაფერი პრაქტიკას საჭიროებს, თეორიულად მათი სწავლის შანსი არ გაქვს, არ დაკარგო თეორიაზე დრო…

აქვე გაითვალისწინე, თუ ვიღაც ცდილობს კონკრეტული გადაწყვეტილება სწრაფად მიგაღებინოს და არ გაძლევს დროს ფიქრისთვის ან დაჟინებით კონკრეტული რაღაცის გაკეთებისკენ მოგიწოდებს, ის შენით მანიპულირებას ცდილობს, არასდროს დაუშვა მსგავსი რამ. (მანიპულაციის ყველაზე გავრცელებული მეთოდია სიჩქარე, არასაკმარისი დრო ფიქრისთვის, შედეგების გაანალიზებისთვის)

მანიპულაციის ეტაპები

პირველი ეტაპი: რა არის შენი მიზანი?

წარმატებული მანიპულაციისთვის ჯერ შენი მიზანი და მისკენ მიმავალი გზა უნდა გქონდეს კარგად ჩამოყალიბებული.

როგორ უნდა გააკეთო ეს? კითხე საკუთარ თავს შემდეგი რამ:

"დამეხმარება ეს ქმედება X-მიზნის მიღწევაში?

წარმატებული მანიპულაციის გასაღები არის სხვისი მიზნების გამოყენება საკუთარი მიზნების მისაღწევად. (ესეც ვახსენეთ, გახსოვს?)

თუ შენ იცი რა მიზანი აქვს შენ მსხვერპლს, შეძლებ მისი მიზნის გამოყენებას შენი მიზნის მისაღწევად. **(დაემხარები მას მიზნის მიღწევაში, შედეგად მის ნდობას მოიპოვებ)**

თუ მოახერხებ ადამიანის ემოციების კონტროლს, შენ იმ ადამიანის კონტროლსაც მარტივად შეძლებ.

მარტივ მაგალითს მოგიყვან. წარმოიდგინე უცნობი, რომელმაც დახმარება გთხოვა...

დავუშვათ ამ ადამიანმა 5000$ დაკარგა. როგორ ფიქრობ, რას განიცდის? შიშს, იმედგაცრუებას. ეს ადამიანი ყველაფერს გააკეთებს თავისი ფულის უკან დასაბრუნებლად. ამ დროს ჩნდები შენ გმირის როლში და ეუბნები, რომ შეგიძლია მას 5000$ დაბრუნებაში დაეხმარო. ის აღტაცებულია, იმედი გაუჩნდა და ერთი სული აქვს მეტი დეტალი გაიგოს. შენ იწყებ საუბარს, ემოციებს უმძაფრებ და ბოლოს ეუბნები, რომ შეძლებ მის დახმარებას, გარანტიებსაც აძლევ (მას გონია რომ გარანტია აქვს, თუმცა რეალურად არაფერი ექნება), სანაცვლოდ გინდა 1000$, რადგან შენი ნაცნობი უნდა ჩართო საქმეში. **ეს ნაცნობი საქმეს მანამდე არ აკეთებს, სანამ ფულს არ გადაუხდიან.** შედეგად ამ დაზარალებულ ადამიანს აქვს ორი ვარიანტი. შენ ამ ადამიანს იმედი გაუჩინე, **იმედი ერთ-ერთი ყველაზე საშიში იარაღია ადამიანის წინააღმდეგ**. მას აქვს იმედი, რომ თავის დაკარგულ ფულს დაიბრუნებს... მართალია 1000$ დაუჯდება დაკარგული ფულის დაბრუნება, მაგრამ მას იმედი აქვს, რომ დაკარგულ თანხას უკან დაიბრუნებს.

როგორ ფიქრობ, თუ მას იმედი აქვს და გენდობა, არ გააკეთებს ყველაფერს, რომ 1000$ იშოვოს და შენ მოგცეს, ვინაიდან შენ მას დაკარგულ 5000$ დაუბრუნებ?

ხედავ რამდენად ბოროტული გეგმაა? ეს გეგმა მხოლოდ იმის ცოდნით

შევადგინეთ, რომ ვიღაცამ 5000$ დაკარგა და დახმარება ითხოვა.

ეს მაგალითი ნებისმიერ სიტუაციას ერგება, სადაც ადამიანმა რაღაც დაკარგა, ვინაიდან ადამიანი, რომელიც რაღაცას კარგავს შიშით და იმედგაცრუებით არის შეპყრობილი. ეს ორი ემოცია საკმაოდ ძლიერია (იმედის შემდეგ) და ადამიანს ხშირად აზროვნებაში ხელს უშლის. დარწმუნდი რომ არასდროს იქნები მსგავსი ემოციებით შეპყრობილი ან თუ იქნები საკუთარი თავის კონტროლს შეძლებ, მინიმუმ მარტო არ დარჩები საკუთარ თავთან და საყვარელი ადამიანი გეყოლება შენ გვერდით (ოჯახის წევრი, ახლო მეგობარი)…

ემოციური მანიპულაციის ეტაპები:

1. **სისუსტის იდენტიფიცირება**

პირველ რიგში განსაზღვრე, რა არის ის ემოცია, რომელიც კონკრეტულ ადამიანს აქვს იმ მომენტში. ამ ემოციაზე დაყრდობით შენ შეძლებ ამ ადამიანის მართვას…

მაგალითად, თუ ადამიანს ცუდი ნერვები აქვს და მარტივად ბრაზდება... ბრაზი ძლიერი ემოციაა და მისი გამოყენება მარტივად შეგიძლია.

2. **ემოციების გაღვივება**

როგორც კი იპოვი ემოციას, რომლის გამოყენებასაც კონკრეტული ადამიანის წინააღმდეგ შეძლებ, დროა ეს ემოცია გააღვივო.

მაგალითად თუ გინდა რომ ადამიანს თავი დამნაშავედ აგრძნობინო და იცი, რომ მას ნერვები მარტივად ეშლება, გამოიწვიე, გააღიზიანე ის, ოღონდ ისე, რომ მართალი შენ აღმოჩნდე საბოლოოდ… ამ შემთხვევაში მსხვერპლი შენ იქნები, ხოლო მეორე მხარე დამნაშავე…

ქალბატონებს ეს იდეალურად გამოგდით კაცებთან მიმართებაში. თუ მანდილოსანი ხარ გილოცავ, შენ ადამიანებით მანიპულაცია ბევრად გაგიმარტივდება…

3. **მანიპულაცია**

თუ შენი მიზანი მსხვერპლად თავის წარმოჩენაა, აიძულე მეორე მხარეს რამე გაწყენინოს... (თუ ყველაფერი სწორად გააკეთე, ამ ნაწილში მიზანი უკვე მიღწეული გექნება)

როცა გაწყენინებს, თავს დამნაშავედ იგრძნობს, ეცდება როგორმე გამოასწოროს თავის დანაშაული, **ზუსტად ამ მომენტში გაქვს ძალაუფლება!** (ეს მაგალითი არ იმუშავებს უცნობ ადამიანზე, უცნობ ადამიანს ფეხებზე კიდია შენ რა გეწყინება…)

მეორე ეტაპი: განსაზღვრე წარმატებისკენ მიმავალი გზა

რაც შეეხება უცხო ადამიანებით მანიპულაციას...

როდესაც შენ მკაფიოდ ჩამოაყალიბებ მიზანს, უკვე შეგიძლია ამ მიზნისკენ მიმავალი გზები განსაზღვრო, ვინაიდან მიზანი გაქვს, მიზნისკენ მიმავალი გზის განსაზღვრა ბევრად უფრო მარტივი იქნება.

ყოველთვის იქონიე რამდენიმე გეგმა, ყველაფრისთვის მზად იყავი.

მესამე ეტაპი: მსხვერპლის შესახებ ინფორმაციის მოძიება

ერთ-ერთი მნიშვნელოვანი ნაწილი მანიპულაციის ეტაპებს შორის ეს არის. რაც უფრო მეტი ინფორმაცია გაქვს მსხვერპლზე, ბევრად უფრო მარტივია სწორი სამიზნე წერტილების პოვნა, რომელსაც მოეჭიდები მანიპულაციის დროს, იქნება ეს მსხვერპლის ემოციები თუ სხვა რამ.

მანიპულაციის ბოლო ეტაპი: გეგმა და მოქმედება

ეს საბოლოო ეტაპია, რომელიც ან წარმატებული იქნება ან წარუმატებელი. მოქმედება უნდა განხორციელდეს წინასწარ გაწერილი გეგმით, გახსოვს რომ გითხარი რამდენიმე გეგმა უნდა გქონდეს მეთქი. ვერასდროს გამოიცნობ მსხვერპლის ქცევას წინასწარ, ამიტომ მზად იყავი ყველაფრისთვის.

წარუმატებელი მანიპულაცია

მანიპულაციის ერთ-ერთი ეტაპი არის წარუმატებლობა, თუ შენი მანიპულაციის მცდელობა წარუმატებელი აღმოჩნდა, დაჯექი და გააანალიზე შენი ქმედებები, ამ გზით შენ შეცდომებს იპოვი და მომავალში ბევრად კარგი მანიპულატორი გახდები...

ბონუს რჩევა ჯაფარასგან - სხეულის ენა

აუცილებლად ისწავლე სხეულის ენა. ის დაგეხმარება ადამიანის ემოციების გაგებაში და ყველაზე მარტივი მეთოდია რეალურად, როდესაც ადამიანის ემოციის გაგება გჭირდება, კითხვების დასმის გარეშე შეძლებ ამას, მხოლოდ ადამიანზე დაკვირვებით. სხეულის ენა ცალკე ხელოვნებაა, მას აქ წიგნში სამწუხაროდ გასაგებად ვერ აგიხსნი. (**Chris Voss _ The Art Of Negotiation,** ეს კურსი მოძებნე გუგლში, უფასოდ მარტივად მიაგნებ)

მანიპულატორი ვერ იქნები, თუ ადამიანებთან საუბრის გეშინია და თავს არაკომფორტულად გრძნობ…

თუ ეს ასეა, მაშინ ჯერ საკუთარი თავი უნდა განავითაროო…

ბევრი კარგი წიგნია, რომელიც ამ საკითხში დაგეხმარება, მაგალითად how to talk to anyone, book by Leil Lowndes.

მანიპულატორის აღმოჩენა

1.მანიპულატორი ცდილობს საკუთარი თავის ნდობა დაგაკარგინოს.

2.მანიპულატორი ამბობს ერთს, თუმცა აკეთებს საპირისპიროს.

3.თავს მუდამ დამნაშავედ გრძნობ მანიპულატორი ადამიანის გვერდით, მაგრამ არ იცი რატომ.

4.მანიპულატორი ყოველთვის მსხვერპლია და როგორც წესი შენ ხარ დამნაშავე.

5.მანიპულატორი სწრაფად ცდილობს ურთიერთობის გაღრმავებას. (მაგალითად, საქმიანი შეხვედრის დროს ყველაზე ხშირია მსგავსი მანიპულაციის მცდელობები, როდესაც მეორე მხარე ცდილობს მაქსიმალურად სწრაფად შეთანხმებას, არ გაძლევს დროს მოსაფიქრებლად და გაჩქარებს, რომ საქმიან ქაღალდებს ხელი მოაწერო).

შენ გაქვს შენი ადამიანური უფლებები, მანიპულატორი ყოველთვის ცდილობს ამ უფლებების შეზღუდვას…

შენ გაქვს შემდეგი უფლებები:

- პატივისცემით მოპყრობის უფლება
- გრძნობები და სურვილები, შეგიძლია მათი თავისუფლად გამოხატვა ნებისმიერ მომენტში
- თავისუფალი აზრის გამოხატვის უფლება
- თქვა არა ნებისმიერი მიზეზით ნებისმიერ რამეზე **დანაშაულის გრძნობის გარეშე**
- თავს გრძნობდე უსაფრთხოდ ნებისმიერ სიტუაციაში
- ნებისმიერი საზღვრის დადგენის უფლება

ეს უფლებები წარმოადგენს შენ “ფარს”…

თუ ვინმე დაარღვევს მათ, დიდი ალბათობით ის შენით მანიპულირებას ცდილობს.

განსაკუთრებით მნიშვნელოვანია საკუთარ თავთან მუშაობა უარის თქმის ნაწილზე, თუ რაღაც არ გინდა, შეგიძლია თქვა არა და ამის გამო თავი დამნაშავედ არასდროს იგრძნო.

მანიპულაციის ტექნიკები გონების კონტროლისთვის

გონების კონტროლი საშიშია და არასწორ ხელში ის იარაღია, მაგრამ იმისთვის, რომ თავის დაცვა შეძლო, აუცილებელია იცოდე როგორ ხდება ეს ყველაფერი. უბრალოდ გაითვალისწინე რისკები, გონების კონტროლი დანაშაულია და არასწორმა ქმედებამ შეიძლება მსხვერპლი ცუდ მდგომარეობამდე მიიყვანოს... (შეიძლება ფსიქოლოგიურად დააზიანო ისე, რომ ნორმალურ მდგომარეობას ვეღარასდროს დაუბრუნდეს და ამის მაგალითი უამრავია... ფსიქოლოგიურად შეიძლება გატეხო ადამიანი)

გონების კონტროლი ჩანერგილი აზრებით

გონების კონტროლსა და გონების გამორეცხვას შორის დიდი სხვაობაა… გონების გამორეცხვა ნიშნავს იდენტობის, შეხედულებების, ადამიანის შეცვლას. გონების კონტროლის შემთხვევაში მსხვერპლის თვალში შენ სანდო პიროვნება ხარ, ნდობას იყენებ ადამიანის გონების კონტროლისთვის, ის იგივე პიროვნებაა, მხოლოდ მის აზრებს ცვლი. გონების კონტროლის მიზანია ადამიანის გონებაში აზრების ჩანერგვა ისე, რომ მას წარმოდგენა არ ქონდეს ამის შესახებ… ქონდეს იდეები, აზრები, მაგრამ არ იცოდეს ამ აზრების წარმომავლობა, მას უნდა ეგონოს, რომ აზრები, რომლებიც აქვს მისი საკუთარი აზრებია (თუმცა ისინი შენი ჩანერგილი იქნება)…

გონების კონტროლის პირველი და ყველაზე მნიშვნელოვანი ნაბიჯი არის ურთიერთობა, ნდობა. ადამიანის გონების კონტროლს ვერ შეძლებ, თუ ეს ადამიანი არ გენდობა და ღია არ არის შენთან, ასევე გაითვალისწინე ეს პროცესი თავიდან საკმაოდ გრძელია…

სამი ეტაპია ამ პროცესში:

1. მოიპოვე ნდობა (ეს ყველაზე გრძელი პროცესია, თუ ამ ეტაპს გაცდები, დანარჩენი უფრო მარტივად და სწრაფად ხდება)

2. დააგდე ადამიანის თვითშეფასება

(აიძულე იფიქროს რომ მისი აზრები მცდარია და დაარწმუნე ამ ყველაფერში, უთხარი რომ არ ენდოს საკუთარ თავს და საკუთარი შეცდომები გაახსენე, რომელიც წესით უნდა იცოდე, თუ ნდობის ნაწილი წარმატებით გაიარე ამ ადამიანზე ბევრი რამ გეცოდინება, მათ შორის მისი ყველაზე დიდი შეცდომები.)

აქვე გაითვალისწინე, როცა გეუბნები რომ მსხვერპლს კონკრეტული რაღაც უნდა უთხრა, ამას პირდაპირი გაგებით არ გეუბნები, თუ ვიღაცას პირდაპირ ეტყვი რომ არ ენდოს საკუთარ თავს, ამ ადამიანთან მომენტალურად ყველანაირ შანსს დაკარგავ. (საუბარში უნდა აგრძნობინო მას ეს ყველაფერი, ირიბად)

3. ჩაუნერგე იდეები

მაღალი თვითშეფასების მქონე ადამიანებით მანიპულაცია უფრო რთულია (თუმცა გააჩნია მანიპულაციის ხერხს, რითი ცდილობ მის მანიპულაციას), ამიტომ შენ ნებისმიერ შემთხვევაში უნდა დააგდო მსხვერპლის თვითშეფასება. როდესაც მის თვითშეფასებას დააგდებ, შემდეგ ყველაფერი მარტივი ხდება. აზრები, რომელიც გინდა რომ ამ ადამიანში

ჩანერგო, მუდმივად უნდა ესაუბრო ამ აზრებზე (მაგრამ თავი არ მოაბეზრო), რაც უფრო მეტჯერ გაიმეორებ ერთიდაიგივეს, უფრო ხშირად იფიქრებს მსხვერპლი ამ აზრებზე და შესაბამისად, როგორც პირველ თავში ქვეცნობიერი გონების გადაპროგრამებისას ვისაუბრეთ, მსხვერპლის გონებაში ჩაიწერება ის აზრები, რომელზეც ხშირად დაელაპარაკები.

ის, რისი ცოდნაც მნიშვნელოვანია შენთვის, უკვე იცი... მეტი ინფორმაცია რომ გაგიზიარო, შეიძლება ამ წიგნის გავრცელების უფლება არ მომეცეს და პრობლემები შეიქმნას...

ბევრჯერ წაიკითხე ზემოთ არსებული ინფორმაცია. მცირე, საჭირო ინფორმაცია უკვე გაიგე ამ წიგნიდან, მეტის გაგება თუ გინდა ინტერნეტი გაქვს, მოიძიე შესაბამისი ინფორმაცია...

ფსიქოლოგიის ძირითადი ნაწილი გავიარეთ...

ახლა დროა წიგნის იმ ნაწილზე გადავიდეთ, რის გამოც ამ წიგნის კითხვა დაიწყე :)

კიბერუსაფრთხოება
(ჰაკინგი)

რა არის კიბერუსაფრთხოება?

ინტერნეტში ბევრ განსხვავებულ განმარტებას მოისმენ ამ კითხვის გარშემო, ზოგი დაგაბნევს კიდეც.

პირადად ჩემთვის კიბერუსაფრთხოება (უფრო ზუსტად ჰაკინგი) თავისუფლებისკენ მიმავალი ყველაზე მოკლე გზაა. შენ შეგიძლია ის პიროვნება იყო ინტერნეტში, ვინც მოგინდება, **რამდენი პიროვნებაც გინდა იმდენი პიროვნება შეგიძლია გქონდეს,** კონტროლისგან თავისუფლდები, თუ შესაბამისი ცოდნა გაქვს. (იცი როგორ დარჩე ანონიმური ინტერნეტში, დაფარო საკუთარი კვალი და ქმედებები)

შენ ამ წიგნის დახმარებით გაიგებ თუ როგორ ხდება ადამიანების კონტროლი ინტერნეტის გამოყენებით. ვინაიდან ეს ცოდნა გექნება, ამ ყველაფრისგან თავის დაღწევასაც შეძლებ. (რთულია, მაგრამ შანსი გექნება)

კიბერუსაფრთხოების ზოგადი განმარტება ასეთია:

“კიბერუსაფრთხოება მოიაზრებს ინტერნეტში არსებული ინფორმაციის და ერთმანეთთან დაკავშირებული მოწყობილობების უსაფრთხოებას.”

CIA ტრიადა

არსებობს მნიშვნელოვანი მოდელი კიბერუსაფრთხოებაში, რომელსაც CIA ტრიადა ეწოდება, **Confidentiality** (კონფიდენციალურობა), **Integrity** (მთლიანობა), **Avaliability** (ხელმისაწვდომობა).

ამ ყველაფრის ცოდნა აუცილებელია, მართალია მოსაწყენია, მაგრამ საჭიროა. (მხოლოდ იმ ინფორმაციას მოგაწვდი ამ ნაწილში, რისი ცოდნაც აუცილებელია)

1. **კონფიდენციალურობა მოიაზრებს ინფორმაციის დაცვას არაავტორიზებული წვდომისგან.**

რა ხდება მაშინ თუ კონფიდენციალურობა დარღვეულია?

კონფიდენციალურობის დარღვევა ძალიან ბევრ პრობლემას იწვევს ორგანიზაციაში. მაგალითად სამართლებრივი სარჩელი ორგანიზაციის წინააღმდეგ, საზოგადოების ნდობის დაკარგვა, უსაფრთხოების სამსახურების ჩარევა, ფინანსური ზარალი და კიდევ ბევრი სხვა რამ…

კონფიდენციალურობის შენარჩუნება შესაძლებელია შემდეგი მეთოდებით: წვდომის კონტროლი, შესაბამისი უფლებები, ინფორმაციის დაშიფვრა.

2. **მთლიანობა გულისხმობს მონაცემთა თანმიმდევრულობის, სიზუსტის და სანდოობის შენარჩუნებას მისი მთელი სასიცოცხლო ციკლის განმავლობაში.** მარტივად: ორიგინალი მონაცემები არ უნდა შეიცვალოს არასდროს!

რა ხდება მაშინ თუ მთლიანობა დარღვეულია?

ინფორმაცია არ არის სანდო. თაღლითობის დიდი შანსია გაყალბებული ინფორმაციის გამოყენებით, რამაც შეიძლება გამოიწვიოს არასწორი გადაწყვეტილებების მიღება და მძიმე შედეგები.

მთლიანობის შენარჩუნება შესაძლებელია შემდეგი მეთოდებით: წვდომის კონტროლი, ლოგების შენახვა და ანალიზი, ციფრული ხელმოწერები, შიფრაცია, ასლების შენახვა, ჰეშირება და სხვა...

3. **ხელმისაწვდომობა ნიშნავს იმას, რომ ინფორმაცია ნებისმიერ დროს ადვილად ხელმისაწვდომი უნდა იყოს უფლებამოსილი მხარეებისთვის, რაც გულისხმობს ინფრასტრუქტურის და სისტემების**

მუდმივად გამართულ მუშაობას.

რა ხდება მაშინ თუ ხელმისაწვდომობა დარღვეულია?

ხელმისაწვდომობის დარღვევა იწვევს დროის და ფუნქციის დაკარგვას (წარმოიდგინე რაღაც სერვისი ჩერდება, იმ შედეგებს ვერ იღებ, რასაც კომპანია დაგპირდა მაშინ, როდესაც ის გჭირდება), ჯარიმებს და რეგულაციებს…

ხელმისაწვდომობის შენარჩუნება შესაძლებელია შემდეგი მეთოდებით: კარგად შემუშავებული კატასტროფის აღდგენის გეგმა (Disaster Recovery Plan), მონაცემთა ასლების შექმნა. სხვა ქსელის, სისტემების და მონაცემების არსებობა იმ შემთხვევაში, თუ ძირითადი სისტემა დაზიანებულია (გეგმა B).

რატომ არის მნიშვნელოვანი CIA ტრიადა?

CIA ტრიადის სამივე კომპონენტი ფუნდამენტურად მნიშვნელოვანი პრინციპია კიბერუსაფრთხოებაში, თუ ერთ-ერთი მათგანი დარღვეულია, ყველაფერი რისკის ქვეშ დგას.

ბოლოს, კიბერ “უსაფრთხოება” არ არსებობს, არსებობს კიბერ “რისკები” და მათი შემცირების გზები. არავინ მოგატყუოს. თუ ვიღაც გეუბნება, რომ ის დაცულია ინტერნეტში ან თავს ატყუებს ან არაფერი იცის. ადამიანი, კომპანია, ორგანიზაცია, არ აქვს მნიშვნელობა.

უსაფრთხოება ილუზიაა!

ინტერნეტში ნებისმიერი ადამიანი, ორგანიზაცია, ინდივიდი დაუცველია...

უსაფრთხოება ილუზიაა

ყოველწლიურად ადამიანები და ბიზნესები უსაფრთხოებაში ძალიან დიდ რესურსებს ხარჯავენ, ასეულობით მილიარდ დოლარზეა საუბარი…

ყოველდღე იქმნება ვირუსები, რომლებსაც ანტივირუსები ვერ აფიქსირებენ… როგორ შეძლებენ დაფიქსირებას, როდესაც ანტივირუსი ვირუსის აღმოჩენის და შესწავლის შემდეგ იქმნება?

ჰაკერები ყოველთვის წინ ვართ ნებისმიერ ორგანიზაციაზე. ჩვენ კეთილ ნებასა და სურვილზეა დამოკიდებული თუ რა მოხდება ხვალ, ვინ გახდება სამიზნე და ვის გატეხავენ, მათ ჩვენ წინააღმდეგ არაფერი აქვთ, შეუძლებელია დაიცვა მოწყობილობა ძველი მეთოდით, როდესაც ვირუსები და მავნე პროგრამები ყოველდღიურად იქმნება და ვითარდება.

ერთადერთი გზა, რაც დღეს ორგანიზაციებს და კომპანიებს აქვთ საკუთარი თავის დასაცავად ისევ ჩვენ ვართ, ჰაკერები. ჰაკერის შეჩერება მხოლოდ ჰაკერს შეუძლია… ისევ ჩვენ უნდა გავტეხოთ კომპანია სანამ ამას სხვა ჰაკერი გააკეთებს, რომელსაც ბოროტი მიზნები აქვს… ჩვენ უნდა გავტეხოთ კომპანია და ვაჩვენოთ მათ გზები იმისთვის, რომ შესაბამისად დაიცვან თავი ბოროტი მიზნების მქონე ჰაკერებისგან.

თუმცა იცი პრობლემა რაშია?

კომპანიებს ეს ყველაფერი ფეხებზე კიდიათ. ისინი ფიქრობენ რომ არ აღმოჩნდებიან ჰაკერების თავდასხმის მსხვერპლი. პრობლემა ზუსტად ეს არის. მათ იციან რომ უდიდესი რისკი არსებობს, როდესაც იცი საფრთხეები და მათ შესამცირებლად არაფერს აკეთებ… ყველაზე ხშირად ისეთი კომპანია ხდება თავდასხმის მსხვეპლი, რომელიც ფიქრობს რომ მას არასდროს შეეხებიან…

არის მეორე კატეგორიაც, კომპანიები დაინტერესებულები არიან უსაფრთხოებით, მაგრამ ეს მხოლოდ ინტერესში გამოიხატება… ისინი არ აპირებენ იმ ფინანსური რესურსის გაღებას უსაფრთხოებისთვის, რაც საჭიროა. ისინი ცდილობენ რამდენიმე ათი, ასი ათასი დოლარით, რომელსაც ერთჯერადად გადაიხდიან წელიწადში, მიიღონ უსაფრთხოება და თან უსაფრთხოება გარანტიით. **პრობლემა ის არის, რომ ამ სამყაროში გარანტიას ვერავინ და ვერაფერი მოგცემს, თუ გარანტია გინდა, ჩამოშორდი ინტერნეტს, თუ ინტერნეტში ხარ ჩართული, მაშინ გარანტიები არ არსებობს.**

ვერცერთი კომპანია ათი, ასი ათასის ან თუნდაც მილიონი დოლარის

ერთჯერადად უსაფრთხოებაში ინვესტიციით საკუთარ თავს ვერ დაიცავს.

უსაფრთხოება არ არის პროდუქტი, პროცესია.

პროცესი, რომელიც მუდმივად ყურადღების ცენტრში უნდა იყოს, როდესაც ყურადღებას არ მიაქცევ ან მოაკლებ, მომენტალურად სამიზნე გახდები, რადგან ჰაკერები არასდროს ვჩერდებით, მუდამ ვვითარდებით, ჩვენი მეთოდები ვითარდება.

მაშინაც კი, თუ კომპანია ყველანაირ რესურსს გასცემს, ფინანსურს, დროს, ადამიანურს, უსაფრთხოება მაინც არ არის გარანტირებული. ასეთი კომპანია რისკებს შეამცირებს, თუმცა თუ 1% რისკი მაინც არსებობს, რაც ყოველთვის იარსებებს კიბერ სამყაროში, კომპანია მაინც დაუცველია. როგორი მოწდომებულიც არ უნდა იყოს კომპანია, მათი თანამშრომლების გავლით, ჩვენ, ჰაკერებს მაინც შეგვიძლია იმ ყველაფრის მიღება, რაც გვინდა, ჩვენი სურვილია მთავარი. სურვილი, მიზანი და მოწდომება.

ჰაკერი, რომელსაც მიზანი აქვს ვერ შეაჩერებ, ვირტუალურ სამყაროში საზღვრები და ლიმიტები არ არსებობს.

უსაფრთხოება ილუზიაა!

წიგნში ხშირად გამოვიყენებ სიტყვა "უსაფრთხოებას", მაგრამ დაიმახსოვრე რას ვგულისხმობ ამ სიტყვის უკან. უსაფრთხოებაში ვგულისხმობ რისკების შემცირებას, არანაირ გარანტირებულ უსაფრთხოებას, რადგან ეს უკანასკნელი არ არსებობს!

გაფრთხილება:
ავტორი არ მოგიწოდებს
არალეგალური (BlackHat) ჰაკინგისკენ.
პირიქით...
ავტორი მოგიწოდებს მხოლოდ
ეთიკური ჰაკინგისკენ...
მთლიანი წიგნი არის ავტორის პირადი
შეხედულება სხვადასხვა თემების
მიმართ...
ნებისმიერ უკანონო ქმედებაზე
მხოლოდ შენ გეკისრება
პასუხისმგებლობა...

მაგალითი 2012 წლიდან

2012 წლის დეკემბერში კიბერუსაფრთხოების რამდენიმე მკვლევარმა Imperva_დან გადაწყვიტა რეალურ გარემოში იმ დროის საუკეთესო ანტივირუსების გატესტვა. მათ შეაგროვეს 92 ვირუსი და გატესტეს ისეთი ანტივირუსების წინააღმდეგ, როგორებიც იყო Microsoft, Symantec, McAfee და Kaspersky Lab. ვირუსების დაფიქსირების, გამოვლენის მაჩვენებელი 92 ვირუსიდან მხოლოდ 5% იყო. 92 ვირუსიდან მხოლოდ 4 ვირუსის შეჩერება შეძლო იმ დროის "საუკეთესო" ანტივირუსებმა. 88 ვირუსიდან ერთ-ერთი მაინც რომ მოხვედრილიყო შენ სისტემაში, ჩათვალე კარგი არაფერი მოხდებოდა. დღეს ეს რიცხვი იმაზე ასჯერ, ათასჯერ უფრო მეტია, ვიდრე მაშინ იყო…

2023 წელს ჰაკერები ვიყენებთ ხელოვნურ ინტელექტს, მოწინავე ტექნოლოგიას. მისი დახმარებით ვქმნით ვირუსებს, რომლის დაფიქსირებაც ანტივირუსებს არ შეუძლიათ. 11 წლის შემდეგ იგივე შედეგი გვაქვს და მუდამ მსგავსი შედეგი გვექნება. რაღაც პერიოდის შემდეგ "უსაფრთხოების" პროფესიონალები დანერგავენ ხელოვნურ ინტელექტს ანტივირუსებში, თუმცა ეს არაფერს შეცვლის.

ჩვენ, ჰაკერები ყოველთვის რამდენიმე ნაბიჯით წინ ვართ ნებისმიერ უსაფრთხოების სისტემაზე და ანტივირუსზე. ჯერ ჩვენ ვქმნით ვირუსს, ხოლო შემდეგ "უსაფრთხოების" პროფესიონალები ჩვენი შექმნილი ვირუსისთვის ქმნიან ანტივირუსს. სანამ ისინი ანტივირუსს შექმნიან, ჩვენ დროის ამ შუალედში ღია ფანჯარა გვაქვს და შეგვიძლია ისე გამოვიყენოთ ვირუსი, როგორც გაგვიხარდება. (თუმცა ჯობია კანონის მხარეს იდგე, ვიდრე მის წინააღმდეგ, ისედაც ბევრი საფიქრალი გვაქვს ჰაკერებს, კანონზე მაინც ნუ ვიდარდებთ)

ვირუსის აღმოჩენას და ანტივირუსის შექმნას ხშირად რამდენიმე თვე ჭირდება. ამ დროის შემდეგ ანტივირუსის შექმნა და დახვეწა აზრს კარგავს, რადგან ვირუსმა თავის საქმე, რისთვისაც შეიქმნა ამ პერიოდში დიდი ალბათობით უკვე შეასრულა.

რამდენად მარტივია სისტემაში შეღწევა?

სისტემაში შეღწევას 20 წუთიდან რამდენიმე საათამდე ჭირდება (სტატისტიკურად სისტემების 70% საშუალო დონის დაცვა აქვს. 28% სუსტი, ხოლო 2% ძლიერი).

საშუალოდ:

შეტევების 30% შემთხვევაში ჰაკერს შეუძლია 1 საათზე ნაკლებ დროში შეაღწიოს სისტემაში.

შეტევების 60% შემთხვევაში ჰაკერს რამდენიმე საათი ჭირდება სისტემის გასატეხად.

შეტევების 10% შემთხვევაში ჰაკერს რამდენიმე დღე, კვირა ჭირდება სისტემის გასატეხად.

განსაკუთრებულ შემთხვევაში, თუ სასწაულად დაცულ კომპანიას, ორგანიზაციას უტევს ჰაკერების ჯგუფი, ხშირად წარმატებული შედეგის მიღწევისთვის რამდენიმე თვე არის საჭირო. (ამ შემთხვევაში მსოფლიოში საუკეთესო დაცვის მქონე კომპანიებზე ვსაუბრობ, რომლებიც მილიარდებს ხარჯავენ უსაფრთხოებაში და მაინც, მათი ხარჯები წყალში იყრება, როდესაც ჰაკერები ასეთ კომპანიებს სამიზნეში იღებენ).

თუ ჰაკერმა სამიზნეში ამოგიღო, დიდი შანსია მან რამდენიმე საათში მოახერხოს შენი სისტემის გატეხვა, რადგან შენი სისტემა დაუცველია, საშინლად დაუცველი და თუ შენ რომელიმე ანტივირუსს კიდევ ენდობი მას შემდეგ რაც წაიკითხე, ალბათ სულელი ხარ.

ხშირად ჰაკერები თვეები უთვალთვალებენ საკუთარ მსხვერპლს და აგროვებენ ინფორმაციას მსხვერპლის შესახებ, სანამ უშუალოდ მის წინ გამოჩნდებიან. თუ ჰაკერი შენ წინაშე გამოჩნდა, აღარაფერს აქვს აზრი.

როგორ უნდა დაიცვა თავი?

როგორც წესი, უბრალო ადამიანს გამოცდილი ჰაკერი სამიზნეში არ იღებს თუ განსაკუთრებული ინტერესი არ აქვს ჰაკერს კონკრეტული ადამიანის მიმართ… ინტერნეტში VPN ის გამოყენება და შესაბამისი ცოდნა, დაკვირვება ბევრ პრობლემას აგარიდებს თავიდან. ამიტომ VPN გამოიყენე ყველგან და ყოველთვის… თუ შენი აიპი მისამართი დაცული იქნება, ჰაკერი სამიზნეში მარტივად ვერ ამოგიღებს. (თუმცა თუ შენი სოციალური ქსელები საჯაროა და ყველაფერს იქ პოსტავ შენი ცხოვრების შესახებ, VPN ის გამოყენებას აზრი არ აქვს… მოუფრთხილდი შენ ინფორმაციას, რადგან დღეს ყველაფერი საჯაროა)

რატომ უნდა ისწავლო / არ ისწავლო კიბერუსაფრთხოება (ჰაკინგი) ?

ყველა მოგიწოდებს რომ ისწავლო კიბერუსაფრთხოება, მათ შორის მეც ვარ, რადგან ეს ცოდნა ცხოვრების ყველა ეტაპზე გამოგადგება სხვა ნებისმიერ პროფესიაში, თუმცა ბევრი მითი არსებობს ამ პროფესიასთან დაკავშირებით, სრულ სიმართლეს არავინ გეუბნება… (ან ვინც გეუბნება, დიდი ალბათობით არ უსმენ)

ამ თავში მე დაგანახებ კიბერუსაფრთხოების როგორც დადებით, ისე უარყოფით მხარეებს (როცა კიბერუსაფრთხოებას ვახსენებ, ძირითადად მის ერთ-ერთ მიმართულებას, **“ეთიკურ”** ჰაკინგს ვგულისხმობ). შედეგად შენ გააზრებულად მიიღებ გადაწყვეტილებას, არის ეს პროფესია შენთვის შესაფერისი თუ არა.

შენ არ გინდა წლების დაკარგვა ამ პროფესიის სწავლაში და შემდეგ აღმოჩენა, რომ თურმე არ ყოფილა ეს პროფესია შენთვის შესაფერისი, ხომ ასეა?

მითი N1

კიბერუსაფრთხოების პროფესიონალებს კარგი შემოსავალი აქვთ.

რეალობა: “კარგი შემოსავალი” პირობითია, თუმცა გეტყვი როგორია საშუალოდ ჰაკერის ხელფასი საერთაშორისო ბაზარზე.

- **United States**:
  Entry-level: $50,000 - $90,000
  Mid-level: $90,000 - $120,000
  Senior-level: $120,000 - $150,000+
- **United Kingdom**:
  Entry-level: £25,000 - £40,000
  Mid-level: £40,000 - £70,000
  Senior-level: £70,000 - £100,000+
- **Canada**:
  Entry-level: CAD 50,000 - CAD 75,000
  Mid-level: CAD 75,000 - CAD 100,000
  Senior-level: CAD 100,000 - CAD 130,000+
- **Australia**:
  Entry-level: AUD 50,000 - AUD 80,000
  Mid-level: AUD 80,000 - AUD 120,000

Senior-level: AUD 120,000 - AUD 150,000+

- **Germany**:

  Entry-level: €40,000 - €60,000

  Mid-level: €60,000 - €80,000

  Senior-level: €80,000 - €100,000+

ეს არის სტატისტიკა, თუმცა ეს სტატისტიკაც მცდარია. ბევრად უფრო დაბალი ხელფასებია დამწყებებისთვის და ზოგადად ბაზარზე... ბევრი ადამიანი, რომელიც არ არის გარკვეული ბაზრის შესაძლებლობებში, ცდება და "მაღალი" ხელფასის გამო ირჩევს კიბერუსაფრთხოებას, როგორც პროფესიას. ამერიკა ერთ-ერთი (შეიძლება ერთადერთი) ქვეყანაა, სადაც მართლა დაფასებულია ეს სფერო, თუმცა ამერიკაში უცხო ქვეყნის მოქალაქეს დასაქმების შანსი თითქმის არ აქვს. შეიძლება დასაქმდე, მაგრამ ისეთ კომპანიაში ვერ დასაქმდები, რომელიც მზად არის 120.000$ გადაგიხადოს წლიურად… (+ გადასახადები იმდენად მაღალია, მინიმუმ ხელფასის 30-35% გაკლდება)

საქართველოში 2023 წელს ასეთი მდგომარეობაა, ძირითადად ეთიკური ჰაკერის, შეღწევადობის ტესტერის პოზიციაზე:

დამწყების ხელფასი 1500-2000 ლარია (საშინლად დაბალი)

(1+ წლიან სამუშაო გამოცდილებას ითხოვენ მინიმუმ, შეიძლება ისეც მოახერხო დასაქმება, მაგრამ ცოდნა უნდა გქონდეს და რთულია).

ვერ გეტყვი, რომ მარტივად იშოვი სამსახურს დღეს არსებულ ქართულ ბაზარზე, მოთხოვნა ნელ-ნელა იზრდება, თუმცა ხელფასები საამაყო არ არის.

საშუალო დონის პროფესიონალის ხელფასი 3000-5000 ლარია

(3-4 წლიანი სამუშაო გამოცდილებით)

მაღალი დონის პროფესიონალის ხელფასი სიმართლე გითხრა არ ვიცი რამდენია.

(5+ წლიანი გამოცდილება)

მაღალი დონის პროფეიონალი საქართველოში აღარ მუშაობს, რადგან მან იცის საკუთარი შრომის ფასი, იცის რომ ორჯერ, სამჯერ მეტის მიღება შეუძლია, თან დოლარში. (ვინც მუშაობს, გააზრებულად ამბობს უარს მაღალ შემოსავალზე)

ახლა უკვე იცი, რას უნდა ელოდო ბაზრისგან. თუ მხოლოდ ხელფასის გამო იწყებ კიბერუსაფრთხოების სწავლას, უბრალოდ არ დაიწყო.

შენი მთავარი მიზანია საქართველოს ბაზარზე ცოტა გამოცდილება დააგროვო, შემდეგ ევროპის ბაზარზე ეცადო გასვლას და დასაქმებას,

ქართულ ბაზარზე დიდხანს თუ დარჩები, ვერ განვითარდები და მოტივაციას დაკარგავ. (რჩევა გინდა? თავიდანვე ევროპაში დაიწყე სამსახურის ძებნა)

სამწუხარო რეალობაა საქართველოში, თუმცა ასეა.

მითი N2: კიბერუსაფრთხოება საინტერესო და მომხიბვლელია

რეალობა: მიუხედავად იმისა, რომ არის საინტერესო მომენტები, სამუშაოს დიდი ნაწილი მოიცავს რუტინულ ამოცანებს, სისტემის გატესტვას ერთიდაიგივე ხელსაწყოებით, დოკუმენტაციას. სამუშაო შეიძლება იყოს მომგებიანი, მაგრამ ის ყოველთვის არ არის საინტერესო. შენ უნდა გიყვარდეს ეს პროფესია, სხვა შემთხვევაში მალე მოგბეზრდება.

მითი N3: კიბერუსაფრთხოებაში ტექნიკური უნარების ქონა საკმარისია

რეალობა: მიუხედავად იმისა, რომ ტექნიკური უნარები გადამწყვეტია და აუცილებელი, შენ ასევე გჭირდება კრიტიკული აზროვნება, კომუნიკაცია, გუნდური მუშაობა და გადმოცემის უნარი.

მითი N4: კიბერუსაფრთხოების მიმართულებით დასაქმება მარტივია

რეალობა: ეს ფრაზა მარკეტინგის ნაწილია, ცდილობენ ვარდისფერი სათვალიდან დაგანახონ სამყარო. რეალობაში დასაქმება რთულია, მითუმეტეს დამწყები პროფესიონალისთვის. დამწყებ პროფესიონალს, რომელსაც არ აქვს ცოდნა, ჭირდება განვითარება, რაც კომპანიას დამატებით რესურსი უჯდება (დრო, ფინანსები). შესაბამისად ყველა ეძებს გამოცდილ კადრს, რათა შეამციროს საკუთარი ხარჯები. ასევე, ბოლო წლებში უამრავი დამწყები პროფესიონალი გამოჩნდა კიბერუსაფრთხოების სფეროში, რაც კონკურენციას ზრდის.

თუ დასაქმება გინდა:

1. უნდა იცოდე საწყისები ძალიან კარგად
2. უნდა გამოირჩეოდე დანარჩენი დამწყებებისგან რაღაცით (შემდეგ თავებში დაწვრილებით გაიგებ)
3. ყოველდღიურად უნდა ვითარდებოდე (ზოგი ისწავლის საწყისებს და წლები ახალს არაფერს სწავლობს, ასეთი კადრი სამსახურს ვერ იშოვის ან თუ იშოვის, დიდხანს არავინ გააჩერებს)

მითი N5: აუცილებელია აკადემიაში, სასწავლებელში, უნივერსიტეტში სწავლა.

რეალობა: ბაკალავრის, მაგისტრის ხარისხი გეხმარება, მაგრამ იმ 4-6 წელში, რაც ამ ხარისხის მიღებისთვის უნდა დახარჯო, შენ შეგიძლია

მსოფლიოს ტოპ 1% ჰაკერების სიაში შეხვიდე. საკუთარ თავზე მუშაობა და დამოუკიდებლად სწავლა საკმარისია ამ მიზნის მისაღწევად...

გამოფხიზლდი მეგობარო, ამ თემაზე შემდეგ თავებში ვისაუბრებ. ჯაფარა მხოლოდ ვინაობაა, რომელსაც არ აქვს არანაირი დიპლომი, ხარისხი, ჯაფარას ვინაობაც კი არ იციან. მხოლოდ სახელი მაქვს და ეს სახელი საკმარისია. ყოველდღე ვიღაც მიკავშირდება და მთავაზობს საკმაოდ კარგ სამსახურს, თუმცა სამსახური ჯაფარას დიდიხანია აღარ აინტერესებს. მე ჩემი საკუთარი მიზანი მაქვს, მინდა კვალი დავტოვო ისტორიაში და ამას ვერ მოვახერხებ თუ ჩრდილში ვიღაცისთვის ვიმუშავებ.

ამით იმის თქმა მინდა, რომ მნიშვნელობა არ აქვს სად სწავლობ, რას სწავლობ ან რა ხარისხი გაქვს, არც იმას აქვს მნიშვნელობა თუ ვინ ხარ. შენი სახელი და რეალური ცოდნა არის ის, რასაც ბაზარზე აქვს ღირებულება.

რატომ არ უნდა ისწავლო ჰაკინგი?

1. თუ შენი მთავარი მოტივაცია ფულია. (ფული კარგი მოტივაციის საშუალებაა, მაგრამ არა ჰაკინგში, რადგან პირველი 1-2 წელი სერიოზულ ფულს ვერ იშოვი ამ პროფესიიდან)
2. ჰაკინგი რეალურ ცხოვრებაში ბევრად უფრო განსხვავებულია, ვიდრე ეს ფილმებშია ნაჩვენები. ფილმები არარეალურია, მისტერ რობოტიც კი, მიუხედავად იმისა, რომ კარგი სერიალია :) თუ ფილმის, სერიალის მსგავსი მოლოდინი გაქვს, იმედი გაგიცრუვდება.
3. თუ ფიქრობ, რომ დღეს ისწავლი რაღაც ახალს და შემდეგ შეგიძლია კვირები, თვეები არაფერი აკეთო.
4. თუ საკუთარი თავის და ქცევების კონტროლი არ შეგიძლია. (დაიღუპები)
5. თუ საიდუმლოს ვერ ინახავ (დაიღუპები)
6. თუ კრიტიკის ატანა არ შეგიძლია (ვერ განვითარდები)
7. რეპუტაცია. ჰაკერს ყოველთვის ეჭვის თვალით უყურებენ ყველგან. მზად ხარ დათმო რეპუტაცია?
8. თუ მხოლოდ სახელის გამო აპირებ სწავლას. რა თქმა უნდა გერქვას ჰაკერი სასიამოვნოა, მომენტალურად პატივს გცემენ, მაგრამ მხოლოდ სახელის გამო არ ისწავლო ჰაკინგი.
9. თუ გამოწვევები გაშინებს, ყოველი დღე ჰაკინგში გამოწვევაა.
10. თუ გუნდურად მუშაობა არ შეგიძლია. (ყველას გონია რომ ჰაკინგი ერთი კაცის საქმეა, უმეტესად ერთი ჰაკერი ბევრს არაფერს წარმოადგენს)
11. ჰაკინგი ხშირად მოსაწყენია… ერთიდაიგივე პროცესების გავლა გიწევს უმეტესად, მუდმივი სტრესი ახლავს თან ჰაკინგს, თუ ის შენი გატაცება არ არის, არ ისწავლო… (იმედგაცრუება ჰაკერის ყოველდღიურობაა, შეგიძლია ამ სტრესის ატანა?)

რატომ უნდა ისწავლო ჰაკინგი?

1. შენი შეხედულებები მსოფლიოს და არსებული სისტემის მიმართ შეიცვლება. (სისტემაში ამ შემთხვევაში არსებულ მსოფლიოს ვგულისხმობ…)
2. შენთვის საზღვრები აღარ იარსებებს. (თავისუფლებას გაუგებ გემოს)
3. ყოველთვის მიიღებ იმას, რაც გინდა და გაინტერესებს.
4. იქნები რაღაც დიდის ნაწილი, ნებისმიერი ჰაკერი რაღაც დიდი მიზნის ნაწილია. (საკუთარ ადგილს იპოვი)
5. შენი უნარები გაიზრდება ყველა მიმართულებით
   (ტექნიკური, ადამიანებთან ურთიერთობა და ა.შ)
6. თუ ბოლომდე დაიხარჯები, ვერ გეტყვი რომ ფინანსურ დამოუკიდებლობას მიაღწევ, მაგრამ საკმარისი ფული გექნება კარგი ცხოვრებისთვის.
7. პატივისცემას მოიპოვებ საზოგადოებაში, კიბერუსაფრთხოების სამყაროში კვალს დატოვებ. შენი სახელი ისტორიას დარჩება :)

კიბერუსაფრთხოების მიმართულებები

რა მიმართულებები აქვს კიბერუსაფრთხოებას ჰაკინგის გარდა? ალბათ ეს ის კითხვებია, რაც გაქვს. განვიხილოთ რამდენიმე მოთხოვნადი მიმართულება, თუმცა ეს არასრული ჩამოვათვალია და შენით უნდა გაერკვე დანარჩენში...

1. ქსელის უსაფრთხოება: გულისხმობს კომპიუტერული ქსელების და ინფრასტრუქტურის დაცვას არაავტორიზებული წვდომისგან, ბოროტად გამოყენებისგან ან შეფერხებისგან.
2. მობილური და ვებ აპლიკაციის უსაფრთხოება: მოიცავს ისეთ პრაქტიკებს, როგორიცაა შეღწევადობის ტესტირება, უსაფრთხო კოდის წერა და კოდის მიმოხილვა უსაფრთხოების ხარვეზების იდენტიფიცირების, აღმოფხვრის მიზნით.
3. ინფორმაციის უსაფრთხოების მართვა: გულისხმობს უსაფრთხოების პოლიტიკის, პროცედურების და კონტროლის მექანიზმების შემუშავებას და განხორციელებას, რათა მოხდეს კრიტიკული მონაცემების და რეგულაციების დაცვა ორგანიზაციებისთვის. ეს მიმართულება მოიცავს აქტივობებს, როგორიცაა რისკების შეფასება, უსაფრთხოების ტრენინგები, ინციდენტზე რეაგირების დაგეგმვა და უსაფრთხოების აუდიტი.
4. კრიპტოგრაფია: მოიცავს უსაფრთხო კომუნიკაციის უზრუნველყოფას და მონაცემთა დაცვას ინტერნეტში. მაგალითად დაშიფვრის ალგორითმები, კრიპტოგრაფიული პროტოკოლები, ციფრული ხელმოწერები და გასაღების მართვის სისტემები. კრიპტოგრაფია მნიშვნელოვან როლს ასრულებს მონაცემთა კონფიდენციალურობის, და მთლიანობის დაცვაში. (CIA ტრიადა)
5. ინციდენტზე რეაგირება და სასამართლო ექსპერტიზა: Incident Response and Digital Forensics გულისხმობს ინციდენტების მართვას და გამოძიებას, როგორიცაა კიბერ თავდასხმები და მონაცემთა გაჟონვები. ეს მიმართულება მოიცავს ინციდენტის გამოვლენას, შეკავებას, აღმოფხვრას და აღდგენას, გამოძიებას თავდასხმის მტკიცებულებების შეგროვებისთვის და ანალიზისთვის (ძალიან საინტერესოა, მაგრამ რთული და დამწყები პირდაპირ ამ მიმართულებით ვერ იმუშავებს).
6. ეთიკური ჰაკინგი და შეღწევადობის ტესტირება: მოიცავს ავტორიზებულ მცდელობებს, გაქვს უფლება გამოიყენო დაუცველობა და გატეხო

სისტემა უსაფრთხოების სისუსტეების იდენტიფიცირებისთვის. ეთიკური ჰაკერები და შეღწევადობის ტესტერები ასრულებენ რეალურ გარემოში შეტევების სიმულაციას, რათა შეაფასონ და გააუმჯობესონ ორგანიზაციების უსაფრთხოება.

სამწუხაროდ მე ვერ გირჩევ თუ რომელი მიმართულებით განვითარდე, რადგან ინდივიდუალურია და ადამიანის მიზნებზე, სურვილებზეა დამოკიდებული. თავად უნდა მოიძიო რას მოიაზრებს თითოეული მათგანი და ისე მიიღო გადაწყვეტილება.

მე ჰაკინგში მაქვს გამოცდილება, თუმცა ის, რაც მე მომწონს შეიძლება შენ არ მოგეწონოს... მიუხედავად ამისა, წიგნი შენი გზამკვლევი იქნება ჰაკინგის მიმართულებით. თუ ეს ის არის რაც მოგწონს ან გინდა რომ ისწავლო, გაგიმართლა :)

როგორც დამწყებს, მაინც ჰაკინგის სწავლა მოგიწევს... ეს არის პირველი ნაბიჯი და კიბერუსაფრთხოების საფუძველი... სხვა მიმართულებას მაინც ვერ ისწავლი თუ საფუძვლები არ გესმის.

ჰაკერის ტიპები

აუცილებლად უნდა ვახსენო ჰაკერების ტიპები, ვინაიდან ერთ-ერთი მათგანი იქნები თუ ჰაკინგს გაყვები. თუ რომელი ამას თავად შენ და შენი ქმედებები წყვეტს…

ჰაკერის მცნება არასწორად ესმით საზოგადოებაში. ამ სიტყვასთან ყოველთვის ნეგატივია დაკავშირებული, თუმცა ეს ასე არ არის. ჰაკერის მრავალი ტიპი არსებობს. ჰაკერის ტიპს მისი ქმედება განსაზღვრავს. ჰაკერი ნებისმიერ შემთხვევაში ჰაკერია და ამას ვერაფერი შეცვლის, მის ტიპს კი ის საზღვრები განსაზღვრავს, რომელსაც თავად დაუწესებს საკუთარ თავს (მხოლოდ ჩვენ ვუწესებთ საზღვრებს საკუთარ თავს, სხვას ეს არ შეუძლია).

მაშ ასე, ჰაკერი არის ადამიანი, რომელსაც აქვს საკმარისი ცოდნა და უნარები, მიიღოს წვდომა იმ “ინფორმაციაზე” ან “რესურსზე”, რისი უფლებაც მას უმეტესად არ აქვს **(ეთიკურ ჰაკერს ყოველთვის აქვს რაღაცის გატეხვის უფლება).**

თუ ოდესმე ვინმე დასვამს კითხვას “ვინ არის ჰაკერი?”, ძალიან მარტივი განმარტება ასეთია: “ჰაკერი არის ადამიანი, რომელსაც შეუძლია არსებულ უსაფრთხოებას გვერდი აუაროს გარკვეული მიზნით.”

თუ ეთიკური ჰაკერი ხარ, იამაყე და არ დამალო ეს ფაქტი (თუმცა შეიძლება მოგიწიოს დამალვა, გააჩნია რა მიზნები გაქვს და რას აკეთებ ამ მიზნების მისაღწევად. მე მიწევს დამალვა)

ჰაკერებში შეგიძლია ღიად ისაუბრო ჰაკინგზე (მაგრამ იცოდე, სად დასვა წერტილი, თუ რამე უკანონო გაქვს გაკეთებული, შენთვის დაიტოვე, არავის გაუზიარო)

სხვებთან უბრალოდ არაფერი თქვა, რადგან ვერ გაიგებენ რაზე საუბრობ…

იყო ჰაკერი, ნიშნავს იდგე დანარჩენ საზოგადოებაზე ბევრად უფრო მაღალ საფეხურზე, რადგან შენ იმაზე მეტი გესმის და შეგიძლია, ვიდრე მსოფლიო მოსახლეობის 99.9%ს :)

განვიხილოთ ჰაკერის ტიპები

1. **შავქუდიანი ჰაკერები** – არიან ჰაკერები, რომლებსაც საზღვრები არ გააჩნიათ, აკეთებენ ყველაფერს, რაც უნდათ და სწორედ ამიტომ, ყველაზე საშიშ ჰაკერებად ითვლებიან საზოგადოებაში. ალბათ გაინტერესებს რა მიზანი აქვთ მათ. მათ ბევრი მიზანი შეიძლება ქონდეთ, ხშირ შემთხვევაში ეს მიზანი ფინანსური სარგებელი ან პროტესტია კონკრეტული ორგანიზაციის, კომპანიის მიმართ. შეიძლება პირადი ინტერესიც ამოძრავებდეთ, ყველაზე დიდი ინტერესი მათთვის სახელი ან ფულია.

   შავქუდიანი ჰაკერი ვერ გახდები პირველი რამდენიმე წელი, რადგან ძალიან ბევრი რამ უნდა იცოდე, თუ არ გინდა ცხოვრების დიდი ნაწილის ციხეში გატარება. ზოგადად არც გირჩევ რომ ამ გზას გაყვე, რადგან ძალიან დიდი რისკია და დიდი პრობლემების გამოწვევა შეუძლია.
2. **თეთრქუდიანი ჰაკერები** – ყოველთვის კანონის მხარეს დგანან, ტეხავენ სისტემებს იმისთვის, რომ აღმოაჩინონ დაუცველობა და შესაბამისად დაიცვან ის, ვინაიდან სხვა ტიპის ჰაკერებმა ვერ შეძლონ ასეთი დაუცველი სისტემების გატეხვა. მათ აქვთ კანონიერი უფლება კონკრეტულად რაღაცის გატეხვის. (თუ წერილობითი უფლება არ გიჭირავს ხელში და სისტემას ისე გატეხავ, შენ არ გამოდიხარ თეთრქუდიანი ჰაკერი და შეიძლება პრობლემები შეგექმნას)
3. **ნაცრისფერქუდიანი ჰაკერები** – კანონის ორივე მხარეს გვხვდებიან, თეთრქუდიანი და შავქუდიანი ჰაკერების გაერთიანებად შეგვიძლია წარმოვიდგინოთ, ისინი ტეხავენ სისტემებს კანონის ფარგლებში ან უკანონოდ. მათ ამ ტიპს განსაზღვრავს ქმედებები, ვერ გაიგებ კანონის რომელ მხარეს დგანან კონკრეტულ მომენტში.
4. **თვითმკვლელი ჰაკერები** – არ მოგესმა, ისინი არიან ჰაკერები, რომლებსაც შეუძლიათ სისტემის გატეხვა, მაგრამ არ შეუძლიათ კვალის დაფარვა გარკვეული მიზეზებით. მათ არ ადარებთ დაიჭერენ თუ არა, მათი მთავარი მიზანი სისტემის გატეხვაა. (ზედმეტად სულელი უნდა იყო, თუ ასეთ რამეს გააკეთებ ან ცხოვრება ფეხებზე გეკიდოს)
5. **Script Kiddies** – არიან დამწყები ჰაკერები (ჰაკერების 95%), რომლებიც იყენებენ სხვის შექმნილ მავნე პროგრამებს სისტემების გასატეხად, ვინაიდან არ აქვთ საკმარისი ცოდნა საკუთარი მავნე პროგრამის შესაქმნელად.

6. **კიბერ ტერორისტები** - არიან ინდივიდები ან ჯგუფები, რომლებიც იყენებენ ინტერნეტს ტერორისტული აქტების განსახორციელებლად. მათი მიზანია გამოიწვიონ შიში, პანიკა და სერვისების შეფერხება კომპიუტერული სისტემების გამოყენებით ქსელებსა და სხვა ციფრულ ინფრასტრუქტურაზე თავდასხმების გზით. კიბერ ტერორისტები უმეტესად იყენებენ DDOS შეტევას, რომლის მიზანიც არის სერვისების გადატვირთვა და შეყოვნება, დაზიანება. (DDOS ყველაზე მარტივი შეტევის ტიპია კიბერ ტერორისტებისთვის, რადგან ღრმა ცოდნას არ საჭიროებს)
7. **სახელმწიფოს მიერ დაფინანსებული ჰაკერები** - არიან ინდივიდები ან ჯგუფები, რომლებიც ახორციელებენ ჰაკერულ საქმიანობას მთავრობის ან ეროვნული უსაფრთხოების სახელით. ისინი შეიძლება უშუალოდ იყვნენ დასაქმებული მთავრობის მიერ ან შეიძლება ქონდეთ კონტრაქტი მთავრობასთან კიბერ ჯაშუშობის ან სხვა სახის კიბერშეტევების განხორციელების მიზნით. მოკლედ მათ უკან სახელმწიფო დგას, ასეთი ჰაკერები კანონზე მაღლა დგანან... (ამერიკა, რუსეთი, ჩინეთი... ძირითადად მოწინავე ქვეყნებს ყავთ მსგავსი ჯგუფები და სახელმწიფოს სურვილით მოქმედებენ, ნებისმიერი სახელმწიფო ასეთ ჰაკერებს ხელის გულზე ატარებს...)
8. **ჰაკტივისტები** – მათი ნათელი მაგალითია ჰაკერული დაჯგუფება ანონიმუსი. ისინი საკუთარ ცოდნას იყენებენ აქტივიზმის ან პროტესტის საშუალებად, ხშირად თავს ესხმიან მთავრობებს, კორპორაციებს ან სხვადასხვა ორგანიზაციებს, რომლებიც მათი აზრით ახორციელებენ არაეთიკურ ან უსამართლო ქმედებებს. ისინი იყენებენ ჰაკერულ შეტევებს, როგორც საშუალებას ყურადღების მისაქცევად.

შენ უკვე იცი ძირითადი ჰაკერის ტიპები, შეიძლება რომელიმე ჰაკერის ტიპი უკვე მოირგე კიდეც :) თუმცა იმისთვის, რომ მოირგო ჰაკერის ტიპი, გჭირდება გარკვეული ცოდნა. ჩემი მიზანია ამ ცოდნის მიღებაში დაგეხმარო სწორი გზების ჩვენებით.

რა გზაც არ უნდა აირჩიო, გაითვალისწინე კანონები და რისკები. ჯობია კანონის მხარეს იყო, რადგან თუ საკმარისად დაარღვევ მას, ისეთი ხალხი ჩაერევა საქმეში, ვისაც ძალიან დიდი რესურსები აქვს შენ საპოვლენად და ამას მარტივად გააკეთებენ. (შენი ქვეყნის უსაფრთხოების სამსახურები, INTERPOL, FBI, CIA, NSA და ბევრი ისეთი სამსახური, რომლის შესახებაც წარმოდგენა ბევრს აქვს)

გარდა ამისა, კანონის მხარეს ყოფნით ღამე მშვიდად დაიძინებ. მშვიდი ცხოვრება წესით შენი პრიორიტეტი უნდა იყოს...

ბევრი ჰაკერია, ვინც უკანონოდ დაიწყო, თუმცა ბოლოს მაინც კანონის მხარეს ყოფნით დაასრულა, მას შემდეგ რაც გაიარეს რთული გზა, ციხე და ასე შემდეგ. ბოლოს მაინც ვიღაცის დაკვირვების ქვეშ აღმოჩნდები, ამიტომ ჯობია თავიდანვე სწორ მხარეს დადგე. მინიმუმ იქამდე, სანამ საკუთარ ცოდნაში და მიზნებში ბოლომდე არ გაერკვევი.

ოსინტი
ინფორმაციის შეგროვება და ანალიზი

ოსინტი ფუნდამენტური ეტაპია ჰაკინგში, რომელიც განსაზღვრავს ყველაფერ სხვას. ნებისმიერი ჰაკერისთვის შეტევის პირველ ეტაპს ყოველთვის ინფორმაციის შეგროვება წარმოადგენს. ინფორმაცია განსაზღვრავს ყველაფერს ამ სამყაროში. ნებისმიერი ადამიანისთვის, ვისაც სურს, რომ წარმატებული კარიერა ქონდეს ჰაკინგში, აუცილებელია საფუძვლიანად ისწავლოს ოსინტი. ოსინტი ინფორმაციის სწორად მოძიების ხელოვნებაა, რაც უფრო მეტი რამ იცი შენ მსხვერპლზე, უფრო მეტი შანსი გაქვს სწორად დაგეგმო და განახორციელო თავდასხმა ადამიანზე ან კომპანიაზე. (კანონის ფარგლებში რა თქმა უნდა)

ნებისმიერი დამწყები, რომელიც მისვამს კითხვას “პირველი რა ვისწავლო”, ჩემი პასუხი ყოველთვის არის “ოსინტი”. ვერც კი წარმოიდგენ რამდენად დიდი შესაძლებლობები გაქვს, როდესაც შეგიძლია ინტერნეტში ნებისმიერი ინფორმაცია იპოვო.

ბონუს რჩევა: ყოველთვის გაეცი ნაკლები პერსონალური ინფორმაცია, რადგან ის სადღაც ინტერნეტში ინახება და ის, რაც ინტერნეტში ინახება, ნებისმიერ ადამიანს შეუძლია მისი ნახვა, ვინც სათანადოდ ერკვევა “ოსინტის ხელოვნებაში”.

კითხვები, რომელიც უნდა დასვა ინფორმაციის მოძიების დროს:

ბიზნესის, ორგანიზაციის შემთხვევაში:

- როგორ იყენებს ორგანიზაცია ინტერნეტს? (მათი ქსელის დეტალური შესწავლა გჭირდება)
- როგორ იყენებს ორგანიზაცია სოციალურ მედიას?
- აქვს თუ არა ორგანიზაციას შემუშავებული პოლიტიკა, რომელიც განსაზღვრავს თანამშრომლების მიერ ორგანიზაციის შესახებ ინფორმაციის განთავსებას ინტერნეტში? (უმეტესად არ აქვთ მცირე და საშუალო ზომის ორგანიზაციებს)
- რამდენი ვენდორი (სერვისების მიმწოდებელი) ყავს ორგანიზაციას?
- რომელ ვენდორებს იყენებს ორგანიზაცია?
- როგორ იღებს ორგანიზაცია გადახდებს?
- როგორ გაცემს ორგანიზაცია გადახდებს?
- აქვს თუ არა ორგანიზაციას ქოლ-ცენტრი?
- სად მდებარეობს ორგანიზაციის ქოლ-ცენტრები ან სხვა ფილიალები?

- და კიდევ სხვა უამრავი, დამოკიდებულია ორგანიზაციაზე და შენ მიზნებზე…

ინდივიდის, ფიზიკური პირის შემთხვევაში:

- რა სოციალური მედიის ანგარიშებს იყენებს?
- რა ჰობი აქვს?
- სად ისვენებს?
- რომელია მისი საყვარელი გასართობი ადგილები?
- სად ატარებს დროს?
- ვინ არიან მისი საუკეთესო მეგობრები?
- როგორია მისი ოჯახის ქონება (ბიზნესი, შემოსავალი და ა.შ.).
- როგორია მისი განათლების დონე?
- როგორია მისი სამუშაო, სად მუშაობს?
- ვინ არიან ოჯახის წევრები? როგორია მათი წარსული?

  ამ ინფორმაციას იყენებ ადამიანთან ნდობის მოპოვების, კონტაქტის დამყარების მიზნით. (თავს მოაჩვენებ რომ ბევრი საერთო გაქვთ, ეს უკვე შენი პირადი თამაშია, როგორ გამოიყენებ ინფორმაციას ადამიანის ნდობის მოსაპოვებლად)

როდესაც ოსინტს ვახსენებთ, საუკეთესო და ყველაზე მარტივი გზა ადამიანის შესახებ ინფორმაციის მოძიებისთვის არის სოციალური ქსელები და საძიებო სისტემები. მხოლოდ სოციალური ქსელებიდან უამრავი ინფორმაციის გაგება შეგიძლია ადამიანზე.

რისი გაგება შეგიძლია ადამიანზე სტანდარტულ შემთხვევაში:

ფეისბუქი – მომხმარებელი მსოფლიოში 2.9 მილიარდი (2023 წელი)

1. მეგობრები
2. ოჯახის წევრები (ვინ არიან, როგორ გამოიყურებიან)
3. სამუშაო ადგილი (ხშირად მითითებულია)
4. თუ პოსტები საჯაროა, ფსიქოლოგიური პროფილის შექმნა შეგიძლია
5. ადგილები, რომლებსაც ხშირად სტუმრობს

ლინკდინი – მომხმარებელი მსოფლიოში 900 მილიონი (2023 წელი)

1. სამუშაო ისტორია
2. განათლება
3. მიღწევები
4. ინტერესი
5. ადამიანები, რომლებიც რეკომენდაციას უწევენ (იცნობენ, ენდობიან)
6. საკონტაქტო ინფორმაცია

ხედავ მხოლოდ ორი სოციალური ქსელით რამდენი რაღაცის გაგება შეგვიძლია ადამიანზე? ახლა ხვდები რატომ უნდა დაიცვა შენი პერსონალური მონაცემები მაქსიმალურად?

მე თუ შენი სახელი, გვარი და დაბადების თარიღი ვიცი, ჩათვალე შენ შესახებ სხვა ყველაფერს მარტივად გავიგებ.

საიდან? საძიებო სისტემები, საჯარო ინფორმაცია, ბაზები... ისინი შენ შესახებ ძალიან ბევრ ინფორმაციას ინახავს.

მხოლოდ საჯარო რეესტრის დახმარებით, თუ შენ რაიმე ქონებას ფლობ, ერთხელ მაინც დაგიწერია განცხადება იუსტიციის სახლში, გაქვს კომპანია ან ხარ ინდ. მეწარმე, მარტივად შემიძლია შენი სახელით, გვარით და მიახლოებითი ასაკით შენი პირადი ნომერი გავიგო. მე თუ ამას მოვახერხებ, დამიჯერე შენ შესახებ უამრავ ინფორმაციას მოვიძიებ, რაც დამეთანხმები ძალიან ცუდია. თუმცა მე და შენ ამ ფაქტს ვერაფერს მოვუხერხებთ.

თუ მსგავს რამეს აპირებ (კომპანიის რეგისტრაცია და ა.შ), გამოიყენე სხვა ადამიანის ვინაობა, ნათესავების, მეგობრების…

ბონუსი: ოსინტი ადამიანებზე საქართველოს პირობებში

ვიცი ეს თემა ძალიან გაინტერესებს, ამიტომ გაგიზიარებ იმ რესურსებს, რომელსაც სახელმწიფო ასაჯაროებს და კანონიერი გზით შეგიძლია იპოვო საქართველოს მოქალაქეები…

1. **napr.gov.ge**
2. **naprweb.reestri.gov.ge**
3. **naprlmr.reestri.gov.ge**
4. **voters.cec.gov.ge**
5. **public.reestri.gov.ge**
6. **enreg.reestri.gov.ge**
7. **debt.reestri.gov.ge**

კანონში წერია:

მონაცემთა დამუშავება დასაშვებია, თუ

ვ) კანონის თანახმად, მონაცემები **საჯაროდ ხელმისაწვდომია** ან მონაცემთა სუბიექტმა ისინი ხელმისაწვდომი გახადა

რაც ნიშნავს შემდეგს: თუ ინფორმაცია საჯაროდ ხელმისაწვდომია, მისი დამუშავება შეგიძლია კანონიერად…

ზემოთ ნახსენებ საიტებზე არსებული ყველა ინფორმაცია საჯაროა!

თავი II. მონაცემთა დამუშავების წესები

მუხლი 5. მონაცემთა დამუშავების საფუძვლები

მონაცემთა დამუშავება დასაშვებია, თუ:

ა) არსებობს მონაცემთა სუბიექტის თანხმობა;

ბ) მონაცემთა დამუშავება გათვალისწინებულია კანონით;

გ) მონაცემთა დამუშავება საჭიროა მონაცემთა დამმუშავებლის მიერ მისთვის კანონმდებლობით დაკისრებული მოვალეობების შესასრულებლად;

დ) მონაცემთა დამუშავება საჭიროა მონაცემთა სუბიექტის სასიცოცხლო ინტერესების დასაცავად;

ე) მონაცემთა დამუშავება აუცილებელია მონაცემთა დამმუშავებლის ან მესამე პირის კანონიერი ინტერესების დასაცავად, გარდა იმ შემთხვევისა, როდესაც არსებობს მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების დაცვის აღმატებული ინტერესი;

ვ) კანონის თანახმად, მონაცემები საჯაროდ ხელმისაწვდომია ან მონაცემთა სუბიექტმა ისინი ხელმისაწვდომი გახადა;

ზ) მონაცემთა დამუშავება აუცილებელია კანონის შესაბამისად მნიშვნელოვანი საჯარო ინტერესის დასაცავად;

თ) მონაცემთა დამუშავება აუცილებელია მონაცემთა სუბიექტის განცხადების განსახილველად (მისთვის მომსახურების გასაწევად).

სოციალური ინჟინერია

სოციალური ინჟინერია არის ქმედება, რომელიც გავლენას ახდენს სხვა ადამიანზე და აიძულებს მას განახორციელოს ქმედება, რომლის გაკეთებაც მას არ უნდა ან ჩვეულებრივ შემთხვევაში არასდროს გააკეთებდა.

სისტემა შეიძლება საკმარისად დაცული იყოს გარედან და ჰაკერმა ვერ გატეხოს ის, თუმცა ორგანიზაციაში, კომპანიაში, ყოველთვის მოიძებნება ადამიანი, რომელიც ამ სისტემის უკან დგას. არ აქვს მნიშვნელობა კომპანიის უსაფრთხოების დონეს, იქ სადაც ადამიანია, ყოველთვის იქნება საფრთხე, რომელსაც ჩვენ სოციალურ ინჟინერიას ვუწოდებთ. (ეს უკვე იცი)

სოციალური ინჟინერია ჰაკერების საყვარელი მეთოდია სასურველი ინფორმაციის მისაღებად. არ არსებობს არანაირი დაცვის მექანიზმი, რომელსაც სოციალური ინჟინერიის შეჩერება შეუძლია, განათლების და ცნობიერების ამაღლების გარდა. (თანამრომლების განათლება ყოველთვის იქნება პრობლემა ორგანიზაციებისთვის, ამიტომ სოციალური ინჟინერია იმუშავებს, სანამ ორგანიზაციაში ადამიანს ექნება რაიმე სახის პრივილეგია)

ადამიანი ყველაზე სუსტი რგოლია კიბერუსაფრთხოების ჯაჭვში, ვინაიდან ნებისმიერ ადამიანზე შეგიძლია მანიპულაცია რაიმე ფორმით.

ძირითადად დღეს სოციალურ ინჟინერიაში აქტიურად რამდენიმე მეთოდი გამოიყენება, განსაკუთრებით კი ფიშინგი. მოკლედ განვმარტოთ:

Phishing - არის სოციალური ინჟინერიის ტექნიკა ელექტრონული ფოსტის ან შეტყობინების გამოყენებით. ფიშინგის მიზანია პერსონალური ან სხვა კრიტიკული მონაცემების მიღება მსხვერპლის მოტყუებით. თავდამსხმელები იყენებენ სანდო ბრენდების/კომპანიების/ადამიანების სახელებს თაღლითობისთვის.

Vishing - თავდამსხმელები იყენებენ ხმოვან შეტყობინებებს ან სატელეფონო ზარებს, **Vishing** მიზანია პერსონალური მონაცემების მიღება მსხვერპლის მოტყუებით, თუმცა ამ შემთხვევაში ისინი იყენებენ ხმოვან საშუალებებს.

Smishing - თავდამსხმელები იყენებენ SMS შეტყობინებებს, **Smishing** მიზანია პერსონალური მონაცემების მიღება მსხვერპლის მოტყუებით, ამჯერად ტექსტური შეტყობინებების გამოყენებით.

Impersonation – თავდამსხმელი გეცნობა როგორც სხვა ადამიანი, იყენებს სხვა ადამიანის იდენტობას. ძირითადად მისი მიზანია მოიპოვოს წვდომა პერსონალურ ინფორმაციაზე ან ფინანსებზე. ამ შეტევას შეიძლება ქონდეს მრავალი ფორმა, მაგალითად ელექტრონული ფოსტის ან ყალბი სოციალური მედიის პროფილის გამოყენებით.

ამ შეტევების მთავარი მიზანი: ჰაკერს სურს მოიპოვოს პაროლები, საკრედიტო მონაცემები, საბანკო ანგარიშები ან წვდომა სოციალურ ქსელებზე.

ჩემ საყვარელ მეთოდზე მოგიყვები.

ჩემთვის საუკეთესო მეთოდი ინფორმაციის მისაღებად ადამიანთან პირისპირ საუბარია. ამ დროს შენ შეგიძლია მის ემოციებს დააკვირდე, გამოიყენო სხეულის ენა და უთქმელად ბევრი რამ გაიგო ადამიანზე.

თუ შენ გადაწყვეტ სოციალურ ინჟინერიაში ღრმად გარკვევას და გააანალიზებ, რომ ეს ის არის, რისი კეთებაც გსიამოვნებს, მაშინ რამდენიმე რჩევა მექნება შენთვის.

- ეცადე ნებისმიერ ადამიანთან საუბრისას გამოიყენო თუნდაც მცირედი მანიპულაციის ტექნიკა, დროთა განმავლობაში შენ უკეთ გამოგივა ეს ყველაფერი. დაიწყე ადამიანიების ემოციების გაგებით, ეცადე დაიჭირო ემოცია, რომელსაც ადამიანი განიცდის საუბრის მომენტში…
- ეცადე ადამიანებს თავი მოაწონო, ამ გზით შენ მათში ინტერესს გამოიწვევ, ხოლო თუ ადამიანი შენით დაინტერესებულია, ის მაშინვე გაიხსნება შენთან, რაც მოგცემს შესაძლებლობას უკეთ გაიცნო ის, როდესაც ადამიანი ღიაა შენთან, ის დაუცველია. სწორედ ამ მომენტიდან იწყება საუკეთესო ნაწილი.
- იყავი კარგი მსმენელი. დაახლოებით დიალოგის 25% უნდა ისაუბრო, 75% კი მსმენელი იყო. ადამიანებს უყვართ საუბარი, თუ დაინახავენ რომ კარგი მსმენელი ხარ, ვერც კი წარმოიდგენ რამდენად დიდ უპირატესობას გაძლევს ეს ფაქტი. ისინი ლაპარაკობენ ყველაფერზე, საკუთარ თავზე, გიყვებიან მათ შესახებ, ხშირად გაუაზრებლად გიზიარებენ კონფიდენციალურ ინფორმაციასაც...
- პატივი ეცი ამ ადამიანის მოსაზრებას, მაშინაც კი თუ არ ეთანხმები, აიძულე იფიქროს, რომ მისი გესმის და იზიარებ მის აზრს.

რაც უფრო მალე აითვისებ ამ ყველაფერს და პრაქტიკაში გამოიყენებ, უფრო მარტივად მიიღებ შენთვის სასურველს, ყოველთვის!

სად უნდა იპოვო ადამიანები, რომლებსაც საუბარი უნდათ? ივენთებზე…

ბევრი უფასო ივენთი ტარდება თბილისში თითქმის ყოველ კვირა (ტექნოლოგიების მიმართულებით ძირითადად).

სად უნდა იპოვო ეს ივენთები? https://www.facebook.com/events

ნებისმიერ ივენთზე წადი, არ აქვს მნიშვნელობა თემას, თუმცა თუ კონკრეტული თემა გაინტერესებს და თან რაღაც ცოდნა გაქვს ამ თემაზე უფრო მარტივად გაესაუბრები იქ მყოფ ადამიანებს, რადგან მათ დიდი ალბათობით ეს საკითხი აინტერესებთ.

ინტროვერტი ხარ და არ გიყვარს ხალხში ყოფნა? ზუსტად შენ უნდა წახვიდე ივენთებზე და მოიხსნა ხალხის შიში…

ახლა ყველაფერი გაქვს, რაც გჭირდება… ისწავლე სოციალური ინჟინერიის ტაქტიკები, პრაქტიკაში გამოიყენე და განვითარდი.

სოციალური ინჟინერიის გამოყენება შეგიძლია ყველგან, ყოველდღიურ ცხოვრებაში. თუ ვინმე არჩევანის წინაშე დამაყენებს, რომ ჩემი უნარებიდან ერთი უნარი ავირჩიო, დაუფიქრებლად სოციალურ ინჟინერიას, ფსიქოლოგიას ავირჩევ. სხვა ადამიანის წაკითხვის, ამოცნობის უნარი ყველაზე ღირებული რამ არის, რაც ადამიანს შეიძლება გააჩნდეს. თუ შენ ადამიანის წაკითხვას შეძლებ, დამიჯერე შენ ცხოვრებაში არასდროს, არაფრის დარდი არ გექნება. თუ იცი რა სურს შენ წინ მდგომ ადამიანს, შეგიძლია მას უთქმელად აუსრულო სურვილი და ის სანაცვლოდ ყველაფერს მოგცემს. იქნება ეს ბიზნეს შეხვედრა, ინფორმაციის მიღება, მოლაპარაკება, პირადი ურთიერთობა თუ სხვა რამ.

ახლა ხვდები, რატომ გასწავლი ფსიქოლოგიის ყველაზე მნიშვნელოვან და საჭირო დეტალებს ამ წიგნით? ყველა მხრიდან მინდა დაგანახო თუ რა შესაძლებლობები გექნება კონკრეტული მიმართულების არჩევის შემთხვევაში. თუ შენ საკმარისად კარგი მანიპულატორი იქნები, წარმატებას ყველა პროფესიაში მიაღწევ.

როგორ გრძნობ თავს? ჯერ მხოლოდ წიგნის ნახევარი წაიკითხე, დარწმუნებული ვარ წიგნის ბოლო გვერდის წაკითხვის შემდეგ შენ აღარასდროს იფიქრებ და მოიქცევი ისე, როგორც ადრე…

შიში, მუქარა, იმედგაცრუება, მარტივად გამდიდრების სურვილი, მძიმე ემოციური ფონი, ფიქრები, მარტოობა. ესენი ის ძლიერი ემოციებია, რომლითაც ადამიანის კონტროლი შეგიძლია. დარწმუნდი რომ ვერცერთი აქ ჩამოთვლილი ემოცია ვერასდროს გაგაკონტროლებს.

შანტაჟი _ როგორ დავიცვათ თავი ?

პირველ რიგში ეცადე არასდროს გასცე ისეთი ინფორმაცია, რითიც შეიძლება დაგაშანტაჟონ, განსაკუთრებით ეს ონლაინ სივრცეს ეხება. ნუ გაუზიარებ ონლაინში ახალ გაცნობილ ადამიანს შენ პირად ინფორმაციას, სურათებს და მით უმეტეს ისეთი სახის სურათებს, რომლითაც შეიძლება დაგაშანტაჟონ (სექსუალური სახის… უამრავი ადამიანი მთხოვს დახმარებას ამ მიზეზით… ნუ გაავრცელებ მსგავს ფოტოებს, ინფორმაციას და ვერავინ დაგაშანტაჟებს, მარტივია).

სოციალურ ქსელში აუცილებლად დააკვირდი რას წერ და სად წერ… ზოგადად ინტერნეტში მოერიდე ინფორმაციის გაცემას… ბევრი ისეთი რამ არსებობს, რითიც შეიძლება დაგაშანტაჟონ.

რამდენიმე რჩევა მექნება სოციალურ ქსელებთან დაკავშირებით:

1. ფეისბუქზე დამალე მეგობრების სია და დახურე პროფილი...
2. ინსტაგრამზე გქონდეს რამდენიმე ანგარიში, როდესაც ეცნობი უცხო ადამიანს, არ გაეცნო რეალური ანგარიშით, სადაც შენი მეგობრები და მშობლები გყავს დამატებული… (ზოგადად არსად დაამატო ისინი და ეცადე არც შემდეგი სახის კომენტარები დაგიწეროონ: დედას სიამაყე, მიყვარხარ დედი, მამას კაცი და ასე შემდეგ…)

   ეს ყველაფერი ცუდი არ არის, მაგრამ ჰაკერის თვალით შეხედე… როგორ უმარტივებ მას საქმეს, როდესაც საჯარო კომენტარით 2 წუთში შეუძლია შენი მშობლების პოვნა და შემდეგ მათი გამოყენება შენი დაშანტაჟების მიზნით...
3. არასდროს არავის გაუზიარო სექსუალური სახის ფოტო/ვიდეო მასალა, დამიჯერე აუცილებლად გამოიყენებს ვიღაც ასეთ მასალებს შენ წინააღმდეგ, უახლოესი მეგობარიც კი…

   დაფიქრდი, რა მოხდება თუ ის ადამიანი, ვინც დღეს შენი მეგობარია ხვალ რაიმე მიზეზით ურთიერთობას შეწყვეტ მასთან? ყველაფერი ხდება ამ ცხოვრებაში, ამიტომ ნურავის მიცემ კრიტიკულ ინფორმაციას… წინააღმდეგ შემთხვევაში შენ უკვე მსხვერპლი ხარ...

ცხოვრებაში ბევრჯერ გახდები შანტაჟის მსხვერპლი, თუმცა ამ თავის წაკითხვის შემდეგ, შენ გექნება შესაძლებლობა გაუმკლავდე შანტაჟს. უბრალოდ ეცადე ასეთი შემთხვევები მინიმუმამდე დაიყვანო.

შენ უნდა დაანახო მოშანტაჟეს, რომ ფეხებზე გკიდია ის რაღაც, რითიც გემუქრება. თუ მოშანტაჟე გაიაზრებს, რომ ხელჩასაჭიდი

არაფერი აქვს, მისი შანტაჟი აზრს დაკარგავს. (ამ დროს დიდი ფსიქოლოგიური თამაში მიმდინარეობს შენსა და მოშანტაჟეს შორის, ვინც პირველი გატყდება, ის წააგებს. არ დაანახო მოშანტაჟეს შიში, ინტერესი... თუ ამას მოახერხებ, უმეტესად მოგებული შენ დარჩები)

განსაკუთრებით კარგად მუშაობს შემდეგი მეთოდი: ის, რითიც გაშანტაჟებენ, თუ რაიმეს გავრცელებას ეხება საქმე, ადექი და თავად გაავრცელე მცირე წრეში, მთავარია მოშანტაჟემ ნახოს, რომ შენი სურვილით გააკეთე ის, რითიც გაშანტაჟებდა. ამ შემთხვევაში ის თავად მოგეშვება (მართალია ცოტა დაზარალდები, მაგრამ მოშანტაჟეს ყველა გზას მოუჭრი, თუ სხვა გზა აღარ გაქვს, ეს ერთადერთი გამოსავალია).

აუცილებლად იზრუნე და ყურადღება მიაქციე შენ ფსიქოლოგიურ მდგომარეობას, გაძლიერდი ფსიქოლოგიურად. როცა შენ საკმარისად ძლიერი იქნები, მსოფლიოს მასშტაბით ვერავინ ვერაფერს გაიძულებს, თუ თავზე იარაღი არ გადევს რა თქმა უნდა ან შენთვის ძვირფასი ადამიანის სიცოცხლით არ გემუქრებიან …

კიდევ ერთხელ რჩევები :

1. **ყოველთვის ეძებე გზა კონტრშეტევისთვის და დამალე საკუთარი შიშები, თავდაცვის საუკეთესო საშუალება თავდასხმაა :)**
2. **იზრუნე შენ ფსიქოლოგიურ მდგომარეობაზე.**

ხშირ შემთხვევაში ეს რჩევები დაგიცავს შანტაჟისგან, თუმცა შანტაჟის უამრავი საშუალება არსებობს. თუ ადამიანის სიცოცხლით გემუქრებიან, ვიღაცის სიცოცხლეს ვერ გარისკავ და სხვა გზა უნდა მონახო.

დაიმახსოვრე: ყოველთვის არსებობს გამოსავალი შანტაჟისგან, მთავარია ვინ დგას მოშანტაჟის პირისპირ.

შიში ძლიერი იარაღია.

დამალე შენი შიშები და არ დაუშვა, რომ შენი შიში შენ წინააღმდეგ გამოიყენონ…

თუ ერთხელ მოახერხა ვიღაცამ და დაგაშანტაჟა, ის არასდროს მოგეშვება.

შენ შეგიძლია გახდე ის, ვინც გინდა...

ყველაფერი, რისი წარმოდგენაც შესაძლებელია, რეალობაა.

- პაბლო პიკასო

გახდე ნებისმიერი ადამიანი, ვინც გინდა – ამ ყველაფერს სოციალურ ინჟინერიაში პრეტექსტინტი ქვია (**Pretexting**).

პრეტექსტინგი ნიშნავს საკუთარი თავის სხვა ადამიანად წარმოჩენას სხვადასხვა მიზნებისთვის. ყველაზე ხშირად ინფორმაციის ან წვდომის მისაღებად კონკრეტულ რაღაცაზე. ზოგჯერ გვიწევს სრულიად ახალი პიროვნების, იდენტობის შექმნა მსგავსი ქმედებისთვის. ჩემი აზრით, სოციალურ ინჟინერიაში პრეტექსტინგი ყველაზე რთული ტექნიკაა, ვინაიდან ძალიან ბევრ უნარს, დაკვირვებას და კვლევას საჭიროებს მიზნის მისაღწევად, განსაკუთრებით მაშინ, თუ ეს ყველაფერი ფიზიკურ გარემოში ხდება, სადაც შენ რეალურ იდენტობას, ბიომეტრიულ მონაცემებს ვერ დაფარავ. სამი აუცილებლად გასათვალისწინებელი ნაბიჯი პრეტექსტინგის დროს:

1. **ფიქრი შენი მიზნების გათვალისწინებით**

ყველაფერი იწყება OSINT-ით, სადაც მაქსიმალურად მეტ ინფორმაციას ვიგებთ პიროვნების ან კომპანიის შესახებ. თუმცა სანამ ამ ყველაფერს გავაკეთებთ, მკაფიოდ უნდა განვსაზღვროთ მიზანი, თუ მიზანი ზუსტად არ გვეცოდინება, ჩვენ არანაირ შრომას აზრი არ აქვს.

2. რეალობა VS წარმოდგენა

უნდა შეეცადო და გამოიყენო შენი რეალური ცხოვრების გამოცდილება. პიროვნება, რომელსაც შექმნი რაიმე სახის კავშირი უნდა ქონდეს შენ ცხოვრებასთან, ამ შემთხვევაში პრეტექსტინგი ბევრად უფრო რეალური იქნება, არ გაგიჭირდება შენი სცენარის დამახსოვრება თუ შენი წარსული ცხოვრების გამოცდილებას იყენებ.

მაგალითად: თუ უსაფრთხოების, თავდაცვის ან სხვა ნებისმიერი სამსახურის წარმომადგენელს განასახიერებ კანონის მხრიდან, მაგრამ არასდროს გქონია შეხება ამ სამსახურებთან და ხალხთან, რომელიც იქ მუშაობს, არ გამოგივა... ეს არ გააკეთო, დაიწვები. (შენ არ იცი როგორ მუშაობს მათი შიდა სისტემა ან თავად იქ მომუშავე პერსონალი) ის რასაც აკეთებ, აუცილებლად გამოცდილი უნდა იყო იმ კონკრეტულ საკითხში ან გქონდეს დეტალური ინფორმაცია მათ შესახებ, სხვა შემთხვევაში ყველაფრით რისკავ.

3. იცოდე, რამდენად შორს შეგიძლია წახვლა

მნიშვნელოვანია აკონტროლო რამდენად შორს შეგიძლია წასვლა, რადგან ძალიან ღრმად როლის მორგებამ შეიძლება იმაზე დიდი პრობლემები შეგიქმნას, ვიდრე ჩაშლილმა გეგმამ ან შეუსრულებელმა მიზანმა…

მარტივად გამდიდრების ილუზია

ბოლო წლებში სოციალურ ქსელებში გავრცელდა მარტივად გამდიდრების ილუზია, უამრავი "სკამერი" იყენებს ამ ფაქტს. სამწუხაროდ მრავალი ადამიანი ხდება მსხვერპლი და კარგავს დიდი რაოდენობით თანხებს.ტ

კითხვა მაქვს და კარგად დაფიქრდი. რატომ იჯერებს ამ სიცრუეს უამრავი ადამიანი?

პასუხი: ფსიქოლოგია !!! არასაკმარისი ცოდნა !!!

"სკამერებმა" იციან ადამიანების სუსტი წერტილი და ამ ყველაფერს მათ წინააღმდეგ იყენებენ...

ვის არ უნდა ფულის შოვნა შრომის გარეშე, მარტივად? ვის არ ჭირდება ფული დღეს?

ყოველი მეხუთე პოსტი სოციალურ მედიაში იწყება შემდეგნაირად:

"გამოიმუშავე ფული მარტივად, ჩადე ინვესტიცია დღეს X$ ოდენობით და მიიღე M ჯერ მეტი მოგება ძალიან მოკლე პერიოდში"

პირველი, რაც ადამიანის ყურადღებას იქცევს X$ და "M ჯერ მეტი მოგებაა". ადამიანის გონება ასეა მოწყობილი, ის მომენტალურად იწყებს ფიქრს, საკუთარ გონებაში ალაგებს გეგმებს, უკვე წარმოდგენილი აქვს თუ რას გააკეთებს "მარტივად" ნაშოვნი ფულით, რომელიც ჯერ არც კი აქვს. ფიქრობს, რომ დღეს ჩადებს X$ და ცხოვრებას აიწყობს…

ასეთი რაღაცეებს ძირითადად იჯერებენ ადამიანები, რომლებიც ვერ ერკვევიან ტექნოლოგიებში, ვინაიდან ლამაზი საიტი დაინახეს რამდენიმე ყალბი პოზიტიური შეფასებით, ფიქრობენ რომ სანდო კომპანიაა და შეუძლიათ მათი ნდობა.

შედეგად რა ხდება? გადარიცხავენ ფულს და ელოდებიან სასწაული რაოდენობის თანხებს რამდენიმე კვირაში, თვეში…

ბოლოს რა ხდება?

საიტი გაქრა. პიროვნება, რომელმაც დაარწმუნა ეს ადამიანი ინვესტიციის ჩადებაში გაქრა. ამ ადამიანის იმედები დაიმსხვრა, თანხები დაკარგულია…

საკმაოდ ხშირია ასეთი ფაქტები მსოფლიოს მასშტაბით, უამრავი ადამიანი კარგავს ყოველდღე დიდი რაოდენობით თანხებს, დანაზოგებს… მილიონებზეა საუბარი ყოველდღე…

დარწმუნდი რომ მარტივად გამდიდრების ილუზია არასდროს

შეგიპყრობს. ახლა უკვე იცი, როგორ მუშაობს ასეთი “მახეები”.

როგორ ფიქრობ, რას უნდა აკეთებდეს სანდო კომპანია, რომელიც დღეს ჩადებულ 1000 დოლარზე, 1 თვის შემდეგ გაორმაგებულ თანხას დაგიბრუნებს? ეს ხომ სისულელეა?

ბანკები, რომლებიც უეცრად ვერსად აორთქლდებიან და ამ მხრივ სანდოები არიან (თუმცა მათ გაკოტრებას არაფერი გამორიცხავს), წლიურად ჩადებულ თანხაზე 1%_ზე მცირე მოგებას გიმატებენ. შენ თუ 1000$ შეიტანე ანაბარზე ბანკში, 1 წლის შემდეგ მაქსიმუმ რამდენიმე დოლარი დაგემატოს.

როგორ ფიქრობ, ბანკი რომელიც 1% ნაკლებ მოგებას გიმატებს წლიურად ინვესტიციაზე, რაღაც გუშინ შექმნილი საიტი რანაირად დაგიბრუნებს ერთ ან რამდენიმე თვეში ჩადებულ ინვესტიციაზე ორჯერ მეტ თანხას?

სისულელე, ილუზია… სხვას ვერაფერს ვუწოდებ და მას, ვისაც ამ ყველაფრის ჯერა, ჩემი დახმარება ჭირდება… დარწმუნდი რომ ამ წიგნზე ბევრ ადამიანს მოუყვები, მინიმუმ ურჩევ წაკითხვას. (თუ მოგეწონება და რაიმე ღირებულებას დაგიტოვებს)

მარტივად გამდიდრება ილუზიაა, არ არსებობს არანაირი გზა მარტივად გამდიდრებისთვის.

სწრაფად გამდიდრება შესაძლებელია, მარტივად გამდიდრება შეუძლებელი.

შენ გაკონტროლებენ

ვინ, რატომ და როგორ გაკონტროლებს

2023 წელია…

ტექნოლოგიების განვითარებასთან ერთად ყოველდღიურად უფრო მეტი ადამიანი იყენებს ინტერნეტს, შესაბამისად ინტერნეტის გამოყენებით ხალხის კონტროლიც უფრო და უფრო იზრდება (მსოფლიოს მმართველებს, ფულიან ტიპებს ასე სურთ, შესაბამისად ინტერნეტი კონტროლის მექანიზმი გახდა)…

რადგან ამ ნაწილს შევეხე, ბოლომდე გეტყვი სიმართლეს, რომელიც წესით შენც უნდა იცოდე…

მსოფლიო მმართველობის სისტემაში არსებობს შემდეგი ქრონოლოგია.

7. პატარა კომპანიები (ისინი, ვინც სერვისებს გაწვდიან ლოკალურად)

6. დიდი კომპანიები (ისინი, ვინც სერვისების მოწოდებას მენეჯმენტს უწევენ გლობალურად)

5. ჰოლდინგები (ისინი, ვინც დიდ კომპანიებს მართავენ)

4. სახელმწიფოები (რეგულაციებს, კანონებს ადგენენ)

3. ინდივიდუალური პირები (ფულიანი ბიძიები, რომლებიც სახელწმიფოებს მართავენ)

2. ფულიანი ბიძიები ერთიანი ძალებით (მილიარდელები, ისინი მსოფლიო ეკონომიკას მართავენ. მაგალითად: საფონდო ბირჟებს, აქციებს, ფასიან ქაღალდებს) **მოსახლეობის 0.00004% წარმოადგენს ეს კატეგორია.**

1. იდუმალი ხალხი ფულით და ძალაუფლებით (ეს ხალხი ყველაფერს მართავს, მათი გადაწყვეტილებით იმართება მსოფლიოს დიდი ნაწილი და ზუსტად მათი მიზნების, სურვილების გამო გახდა ინტერნეტი კონტროლის საშუალება) **ასეთი ადამიანი რამდენიმე ათასი ადამიანია მსოფლიოში.**

შენ ყოველთვის გაკონტროლებდნენ, ინტერნეტის შექმნის დღიდან... იცი რამდენად დიდი ინფორმაციაა შენზე ხელმისაწვდომი ინტერნეტში? ისინი გაკონტროლებენ ყველა იმ გზით, რისი წარმოდგენაც შენ გონებას შეუძლია და არ შეუძლია. ეს კონტროლი განსაკუთრებით იზრდება 2010 წლიდან, ყოველდღიურად…

შენთვის ნაცნობი ინტერნეტის სტრუქტურა როგორია? ყველაფერი ერთმანეთთან არის დაკავშირებული პროტოკოლით, რომელსაც არანაირი დაცვა არ გააჩნია… შენი მონაცემები ინტერნეტში დაუშიფრავად გადაადგილდება… ის, ვინც ამ ინფორმაციას ჩაიგდებს ხელში, უმარტივესად შეუძლია მისი შიგთავსის ნახვა…

გააგრძელე კითხვა, საჭირო ინფორმაციას მოგაწვდი შემდეგ თავებში…

კონტროლი ინტერნეტის გამოყენებით

პირველ რიგში, შენი კონტროლის მიზეზი ფულია. რაც უფრო მეტი რამ იციან შენზე კონკრეტულმა ორგანიზაციებმა, უფრო მეტ ფულს შოულობენ შენზე მორგებული რეკლამებით.

გუგლი, რომელსაც მონოპოლია აქვს საძიებო სისტემებში.

მეტა, რომელსაც მონოპოლია აქვს სოციალურ ქსელებში და აღარ გავაგრძელებ ასეთი უამრავი მაგალითია, მათთვის "უფასო" მომხმარებელს ყველაზე დიდი მოგება მოაქვს.

დაფიქრდი, თუ შენ გუგლში ჩაწერ ნებისმიერ რამეს, მაშინვე უამრავ რეკლამას ამოგიყრის ყველგან და შემდეგი რამდენიმე დღე სულ მსგავსი რეკლამები იტრიალებს შენ გარშემო. არამარტო გუგლში, არამედ სოციალურ ქსელებშიც, ყველგან მსგავსი, ნაგავი ვითარებაა. (ეს კომპანიები ერთმანეთში ცვლიან შენ პერსონალურ ინფორმაციას, ფეხებზე კიდიათ შენი ინფორმაცია)

ჩვენ ფიზიკურ კონტროლს ვერაფერს მოვუხერხებთ, თუმცა ვირტუალურ სამყაროში კონტროლისგან თავის დაღწევა შესაძლებელია. წიგნში გამიჭირდება ამ ყველაფრის სწავლება, თუმცა აუცილებლად შესაბამის მასალებს, გარემოს შევქმნი მომავალში…

სახელმწიფო კონტროლი

სახელმწიფო კონტროლზე გსმენია რამე? დარწმუნებული ვარ ბევრი არაფერი. ეს არ ეხება მხოლოდ საქართველოს, ნებისმიერი სახელმწიფო თავის მოსახლეობას აკონტროლებს.

ბანკების მხრიდან შენ კონტროლზე რა იცი? ისინი ყველა შენ ტრანზაქციას აკონტროლებენ, ზუსტად იციან რაში რამდენ ფულს ხარჯავ ყოველთვიურად.

სამედიცინო სექტორზე რა იცი? ისინი შენი ჯანმრთელობის შესახებ აგროვებენ ყველანაირ ინფორმაციას.

საშემოსავლო სამსახურზე რა იცი? მათ ყველა შენ ქონებაზე აქვთ ინფორმაცია. სახლი, მანქანა... ყველაფერი რაც შენ სახელზეა გაფორმებული.

რა ხდება ბოლოს? ყველა ეს სამსახური სახელმწიფოს განკარგულებაშია. ის, რაც სახელმწიფოს მმართველობის ქვეშ არის, დამოუკიდებელი ვერასდროს იქნება.

იმაზე თუ გაქვს ინფორმაცია, შენი შემოსავლის რამდენი % ერიცხება სახელმწიფოს შენი ნებართვის გარეშე? თითქმის მეოთხედი, ზოგ ქვეყანაში მესამედიც კი.

სახელმწიფო გაკონტროლებს, ამოსუნთქვის საშუალებას არ გაძლევს, პირადად შენ ჯიბეში ყოფს ხელს და ჯიბიდან გაცლის სიმწრით ნაშოვნ ფულს, თუ ამას არ გააკეთებ, ჯარიმები და ციხე გემუქრება. არჩევანი არ გაქვს. როგორ ფიქრობ სამართლიანია ეს ყველაფერი?

არა! არ არის სამართლიანი. თუ უსამართლო თამაშში ხარ ჩართული, წესები უნდა დაივიწყო და შენც წესების გარეშე ითამაშო. სახელმწიფო წესების გარეშე გეთამაშება, შენ რატომ თამაშობ წესების დაცვით?

როდესაც შეძლებ და შენ ფინანსებზე წვდომა მხოლოდ შენ გექნება ყველანაირი ბანკების, სახელმწიფოს გვერდის ავლით, თავისუფლების ახალ ეტაპზე გადახვალ. თუ გინდა რომ ამ ყველაფერს მიაღწიო, უნდა დაივიწყო ბანკები...

სახელმწიფოსთვის ყველაზე მძლავრი კონტროლის მექანიზმი ფული, გადასახადებია... თუ შენ ფულს საიდუმლოდ მიიღებ, საიდუმლოდ დააგროვებ ისე, რომ ამის შესახებ შენ გარდა არავის ეცოდინება, სახელმწიფო ვერ გაგაკონტროლებს...

ჩაატარე შენი საკუთარი კვლევა ბიტკოინზე... მოვა დრო, როდესაც ბიტკოინი მსოფლიო კონტროლს ჩამოშლის და მაშინ ის ადამაინი

აღმოჩნდება TOP 1% ში, ვისაც მეტი ბიტკოინი ექნება, რადგან ბიტკოინი გახდება მსოფლიოში მიმოცვლის საშუალება (დღეს დოლარია, წარსულში ოქრო იყო, თავიდან ეს ორიც ხალხს სისულელე ეგონა)...

ბიტკოინი მომავალია, ბიტკოინის დახმარებით შენ აღარ დაგჭირდება ბანკები, მათ ეს იციან და ცდილობენ მაქსიმალურად ჩაახშონ ბიტკოინი, თუმცა ბიტკოინს მსოფლიოს მასშტაბით უდიდესი მხარდაჭერა აქვს საკუთარი საზოგადოებისგან და მას ვერავინ ჩაახშობს. პროცესი დაწყებულია, ამ პროცესის შეჩერება კი წარმოუდგენელია.

ამ პროცესს ახალი ფინანსური დამოუკიდებლობისკენ მივყავართ და შენ გაქვს შანსი ახალი მსოფლიო ეკონომიკის მშენებლობაში შეიტანო წვრილი, რომელიც ავტომატურად TOP 1% ში მოგახვედრებს...

მე ამ წიგნით ვერ გასწავლი ბიტკოინს და მის ახალ ეკონომიკას, შენით უნდა შეძლო გარკვევა, მოძებნე ინტერნეტში შესაბამისი მასალები, ბიტკოინის ფუნდამენტური შესწავლა დაიწყე, როგორ მუშაობს აუცილებლად უნდა გესმოდეს...

დაიმახსოვრე: ბიტკოინი მომავალია, დღეს მისი ღირებულება ათობით ათასი დოლარია. წლების შემდეგ 1 ბიტკოინის ღირებულება ასობით ათასი დოლარი იქნება. დაიწყე ინვესტიცია. ბიტკოინის შესახებ ისწავლე რაც შეიძლება მეტი...

bitcoinmagazine.com

bitcoin.org

არასდროს შეინახო ბიტკოინი ბირჟებზე, როგორიცაა Binance და სხვა უამრავი, ამ შემთხვევაში შენ კვალზე გამოვლენ...

ისინი გაიგებენ რომ ბიტკოინს ფლობ... რაც არ გაწყობს, ბიტკოინის მთელი ხიბლი იმაშია, რომ მისი ანონიმურად ფლობა შეგიძლია...

რა გჭირდება მისი ანონიმურად ფლობისთვის? Hardware Cold Wallet

თუ ამ შანსს არ გამოიყენებ, წლების შემდეგ ინანებ. სამწუხაროდ მეც გვიან დავიწყე ბიტკოინის დაგროვება :) თუმცა მთავარია დაიწყო.

ბიტკოინი ერთადერთი პროექტია უდიდესი საზოგადოების მხარდაჭერით, რომელსაც შეგიძლია ენდო. სანამ ცოტა ადამიანმა იცის, სანამ მისი ფასი დაბალია, გამოიყენე შანსი და დაიწყე ბიტკოინის დაგროვება. შენი ფინანსური დამოუკიდებლობა ბიტკოინზე გადის.

კანონებით კონტროლი

სახელმწიფოს არ ყოფნის კონტროლის ის მეთოდები, რომელიც მას გააჩნია. მაგალითად თვალთვალი, მოსმენა, ცენზურა, მონაცემების შეგროვება, ქონების აღრიცხვა (არცერთი სახელმწიფო არ აღიარებს ამას, მაგრამ ყველამ იცის, რომ ეს ასე ხდება).

მიუხედავად ამ დონის კონტროლისა, ისინი კიდევ უფრო ცდილობენ თავისუფლება შეგიზღუდონ და მათ მიერ მიღებული კანონებით გაკონტროლონ. ადამიანს თავისუფალი არსება ქვია, ჩვენ ვფიქრობთ რომ თავისუფლები ვართ, მაგრამ თავისუფლება რეალურ სამყაროში მხოლოდ ილუზიაა 99.9% შემთხვევაში…

ჩვენ ვერ ვიქნებით თავისუფლები, როდესაც ჩვენი ფული ჩვენ არ გვეკუთნის, ჩვენი მონაცემები ჩვენ არ გვეკუთნის, თავისუფალი არჩევანიც არ გვაქვს ხშირად.

მსოფლიოს რამდენიმე ქვეყანაში თავისუფალ ინტერნეტზე (დარკნეტზე) წვდომაც არალეგალურია, ინტერნეტის თავისუფლად გამოყენებასაც კი გვიზღუდავენ…

ხვდები რამდენად ცუდ მდგომარეობაში ვართ? მათ კანონებს არ დაემორჩილები და მაშინვე ციხეში აღმოჩნდები… საკუთარ ძალაუფლებას ბოროტად იყენებენ და შენ ვერაფერს გააკეთებ, იმიტომ რომ სახელმწიფოზე მაღლა აღარავინ დგას. (სანამ იმდენად ბევრი ფული და ძალაუფლება არ გექნება, რომ პატივი გცენ და შენი ეშინოდეთ)

ერთადერთი გზა, რითიც თავისუფლება შეგიძლია მოიპოვო ინტერნეტია… მაგრამ არა შენთვის ნაცნობი ინტერნეტი. ის ინტერნეტი, რომელსაც შენ დღეს იცნობ ისევე კონტროლდება სახელმწიფოს მიერ, როგორც შენი ცხოვრება.

გინდა თავისუფლება? მაშინ დროა დეცენტრალიზაციას გაეცნო. დეცენტრალიზაცია ნიშნავს, რომ კონკრეტული რაღაც არ ეკუთნის ერთ პიროვნებას ან ორგანიზაციას, ის არავის ეკუთნის, ვერავინ აკონტროლებს... რაც უფრო მეტ დეცენტრალიზებულ პლატფორმას გამოიყენებ, მით უფრო მალე მიაღწევ თავისუფლებას. გამოიყენე:

1. ფულის შემთხვევაში - ბიტკოინი
2. ინტერნეტის შემთხვევაში - ტორი

თუ რაღაც ცენტრალურად იმართება, ესეიგი ძალაუფლება კონკრეტულ პირებს ან კომპანიებს, ორგანიზაციებს ეკუთნის…

შენ არ ხარ მომხმარებელი,
შენ ხარ პროდუქტი

ხშირად ვსაუბრობ ამ თემებზე ყველასთან, ვისთანაც ამის შანსი მაქვს. დღევანდელ სამყაროში ის, რაც უფასოა ხშირად იმაზე ძვირი გვიჯდება, ვიდრე პროდუქტი, რომელშიც ფულს ვიხდით. დღეს ყველაფერში გარკვეულ საფასურს ვიხდით. უფასო პლატფორმების გამოყენების შემთხვევაში კომპანიები ჩვენ პერსონალურ მონაცემებს ყიდიან… (რეალურად ყველა ყიდის) ჩვენი მონაცემებით ვიხდით უფასო პლატფორმის გამოყენების ფასს…

როგორ ფიქრობ, რატომ არის დღეს გუგლის, მაიკროსოფტის სერვისების და სოციალური ქსელების გამოყენება უფასო? მართალია ისინი საკმაოდ ღირებულია, მაგრამ ფასი, რასაც ამ ყველაფრისთვის ვიხდით, ჩვენი პერსონალური მონაცემებია.

ეს კომპანიები რეკლამებით იმაზე მეტ ფულს შოულობენ, ვიდრე სერვისის მიწოდება უჯდებათ ჩვენთვის, თუმცა ყველაზე ცუდი ჯერ არ მითქვამს. ჩვენი მონაცემები იმ დონეზე მუშავდება, ჩათვალე მთელი ჩვენი ცხოვრება მათ სერვერებზე ინახება და კიდევ უფრო უარესი, იყიდება მესამე მხარეზე, კაცმა არ იცის ვინ არის ეს მესამე მხარე. ისინი არასდროს აღიარებენ რომ ჩვენ მონაცემებს ყიდიან, მაგრამ ამას აკეთებენ, გინდ დაიჯერე გინდ არა. ყველაფერი რასაც დღეს იყენებ, შენ მონაცემებს აგროვებს და ყიდის…

როდესაც გუგლმა თავისი პროდუქტი Google Map შემოგთავაზა და შენ მის გამოყენებას დათანხმდი, შენ მას ავტომატურად შენ სრულ ლოკაციას უზიარებ, 24/7 გუგლმა იცის როდის სად ხარ, რამდენ დროს ხარჯავ ამა თუ იმ ლოკაციაზე, მიუხედავად იმისა, ჩართული გაქვს თუ არა GPS…

როდესაც გუგლმა Google Contacts შემოგთავაზა და შენ მის გამოყენებას დათანმდი, შენ მას ავტომატურად შენი კონტაქტების სია გაუზიარე, მან იცის როდის, ვის, რამდენი ხანი ელაპარაკები, ხშირად ისიც იცის, თუ რას ელაპარაკები, მისი **voice recognition** ტექნოლოგიის გამოყენებით, გუგლს შეუძლია შენი ხმოვანი ვოისი ტექსტად გარდაქმნას და საკუთარ სერვერზე შეინახოს…

მილიარდობით ადამიანის ცხოვრებას გუგლი აკონტროლებს, აგროვებს მონაცემებს და ყიდის ნებისმიერზე, ვინც შესაბამის თანხას გადაიხდის.

ოდესმე გისაუბრია რაიმე პროდუქტზე მეგობართან, ტელეფონით ან პირისპირ, ხოლო შემდეგ აღმოაჩინე, რომ ეს პროდუქტი ყველგან ტრიალებდა

შენ გარშემო რეკლამის სახით? ესეც შენი დამამტკიცებელი საბუთი იმის, რომ გუგლი გითვალთვალებს, გაკონტროლებს. ის, რაც ერთხელ მოხვდება მათ სერვერზე, არასდროს წაიშლება თუ თავად არ ჩათვლიან საჭიროდ და ისინი ამას არ გააკეთებენ, რადგან რაც უფრო მეტი რამ იციან შენზე, უფრო მეტი ფულის შოვნა შეუძლიათ შენი ინფორმაციის გამოყენებით. ამიტომ არის გუგლის უამრავი სერვისი უფასო. ვიზიარებ, თუ შენი ფოტოები, პირადი დოკუმენტები და პერსონალური ინფორმაცია გუგლის რომელიმე სერვერზე ინახება. (google drive, google photos …)

2012 წელს გუგლის წინააღმდეგ ჯგუფური სარჩელი ამტკიცებდა, რომ გუგლი კითხულობდა მომხმარებლის ფოსტას (Gmail) და ახორციელებდა უკანონო თვალთვალს. 2012 წელს გუგლი დაჯარიმდა $22.5 მილიონი დოლარით ფედერალური სავაჭრო კომისიის მიერ.

მეტა, ფეისბუქი, რაც გინდა ის დაუძახე. მარკ ცუკერბერგიც ბევრჯერ დაჯარიმდა მომხმარებლის ინფორმაციის ბოროტად გამოყენების გამო მილიონობით დოლარით. მეტა აგრძელებს ისეთი კომპანიების შესყიდვას და შექმნას, რომელიც შენ ინფორმაციას ინახავს. მაგალითად Whatsapp, Instagram, ახლა უკვე Threads.

როდესაც ისეთი გლობალური მოთამაშე ხარ, როგორიც მეტა და გუგლია, არაფერს ვიტყვი ეფლზე, ეფლი ყველაზე საშინელი კომპანიაა, რაც კი არსებობს მისი პოლიტიკიდან გამომდინარე. შეიძლება მისი მოწყობილობები მოგწონს და გაქვს, მაგრამ როგორც კომპანია არაფრად ვარგა. თავისუფალ სამყაროში თავისუფლებას გიზღუდავს ეფლი)) და თუ შენ ეს მოგწონს, მაშინ მეტს არაფერს ვიტყვი.

მათთვის ჯარიმებს და სასამართლოს აზრი არ აქვს. დააკისრებენ ჯარიმას? მათთვის მილიონები და რამდენიმე მილიარდი არაფერია. იმაზე მეტს შოულობენ შენი მონაცემებით, ვიდრე რამდენიმე წელიწადში ერთხელ გადახდილი ჯარიმებია. დააჯარიმებენ $1 მილიონი დოლარით? გაყიდის მომხმარებლის მეტ ინფორმაციას და ათჯერ, ასჯერ მეტს იშოვის)))

ისინი უკვე თავად ქმნიან კანონებს, საკუთარი კანონები აქვთ. ის ხალხიც კი, ვინც ამ ორგანიზაციებს აჯარიმებს, თავად იყენებენ მათ პროდუქტებს და სერვისებს. საშინელებაა მონოპოლია ბაზარზე უბრალო ხალხისთვის. ჩვენ ვერასდროს ვიხილავთ გუგლზე და მეტაზე წარმატებულ კომპანიას იმ მიმართულებებით, რაშიც ისინი მოწინავეები არიან, არასდროს მოგცემენ ისინი საშუალებას შექმნა მათზე მაგარი პროდუქტი… ან გიყიდიან, ან კონკურენციაში შეგჭამენ, რადგან მათ შენზე მეტი რესურსი აქვთ.

კონფიდენციალურობა
“დასამალი არაფერი მაქვს”

2009 წელს გუგლის CEO, Eric Schmidt_ს კითხეს კონფიდენციალურობის შესახებ... იმ პერიოდშიც კი გუგლი იმაზე მეტ ინფორმაციას ამუშავებდა, ვიდრე ამის უფლება ქონდა. Eric Schmidt_ის პასუხი შემდეგი იყო:

“If you have something that you don’t want anybody to know, maybe you shouldn’t be doing it in the first place”.

ამ აზრს გამოეხმაურა Facebook_ის აღმასრულებელი დირექტორი მარკ ცუკერბერგი, რომელიც ამტკიცებს რომ „კონფიდენციალურობა აღარ არის სოციალური ნორმა“.

კონფიდენციალურობა შეიძლება აღარ იყოს ნორმა - ყოველ შემთხვევაში ფართო საზოგადოებისთვის. თუმცა როგორც ჩანს ცუკერბერგი აფასებს კონფიდენციალურობას.


About 99,900,000 results (0.56 seconds)

Mark Zuckerberg Just Spent More Than $30 Million Buying 4 Neighboring Houses For Privacy. Mark Zuckerberg just made an unusual purchase. Well, four purchases. Facebook's billionaire founder bought four homes surrounding his current home near Palo Alto, Mercury News reports.

Oct 11, 2013

2013 წელს მან $30 მილიონი დოლარი დახარჯა მხოლოდ იმისთვის, რომ სამეზობლოში 4 სახლი ეყიდა და მეზობლებისგან თავისუფალი ყოფილიყო...

ეს ადამიანი ამბობს, რომ კონფიდენციალურობა აღარ არის სოციალური ნორმა... სასაცილოა...

ხშირად მესმის ფრაზა “არაფერი მაქვს დასამალი”, რაც ძალიან ცუდი მიდგომაა და თუ ასე ფიქრობ, მალევე უნდა გამოასწორო შენი აზროვნება. შეიძლება არაფერი გქონდეს დასამალი, მაგრამ შენ გაქვს უფლება, რომელიც მოგენიჭა მაშინ, როდესაც დაიბადე და ამ უფლებას კონფიდენციალურობა ქვია.

არავის აქვს უფლება ჩემი კონფიდენციალურობა დაარღვიოს და ვერც ვერასდროს დაარღვევს იმაზე მეტს, რამდენის უფლებასაც მე მივცემ. აი შენ ჯერ არ იცი რამდენის უფლებას აძლევ “მათ”. დაიბრუნე კონტროლი შენ უფლებაზე, რომელიც დაბადებიდან მოგენიჭა!

როგორ შეგიძლია მიაღწიო კონფიდენციალურობას მობილურის გამოყენების დროს?

პირველ რიგში არცერთი მობილური არ არის შექმნილი კონფიდენციალურობისთვის და მისი მიღწევა მობილურით ბევრად უფრო რთულია, ვიდრე ლეპტოპით…

ანდროიდი და აიოსი, ორივე ოპერაციული სისტემა იმართება ცენტრალურად მწარმოებლის მიერ. ის წყვეტს რა ინფორმაცია შეაგროვოს შენგან და რა რაოდენობით, რა სერვისები მოგაწოდოს და რა შეგიზღუდოს.

თუ აიფონი გაქვს, ეს თავი გამოტოვე. აზრი არ აქვს, რაც არ უნდა დავწერო აქ შენთვის მეგობარო, თუ აიფონი გიჭირავს ხელში შენი კონფიდენციალურობა ნულის ტოლია. სანამ აიფონს არ მოიშორებ, ასე იქნება.

ანდროიდის შემთხვევაშიც ცუდი ვითარებაა, მაგრამ არსებობს გზები, რომლითაც რაღაც დონეზე გააუმჯობესებ სიტუაციას.

მართალია გუგლს, როგორც ორგანიზაციას კონფიდენციალურობა ფეხებზე კიდია, თუმცა გუგლის ანდროიდი, გუგლ პიქსელი ერთ-ერთი ანდროიდია, რომელზეც შეგიძლია 99.9% კონფიდენციალურობას მიაღწიო, რადგან სისტემის სრულად გადაწერა შეგიძლია, სხვა ანდროიდები ამის შესაძლებლობას არ იძლევა და სისტემის გადაწერით შეიძლება მოწყობილობა გაანადგურო :)

სისტემის გადაწერის მიზანია გუგლთან ყველანაირი კავშირის გაწყვეტა, რაც ნიშნავს იმას, რომ გუგლის სერვისებს ვეღარ გამოიყენებ და ეს ასეც უნდა იყოს, თუ შენთვის კონფიდენციალურობა პრიორიტეტია.

არსებობს ორი ოპერაციული სისტემა ანდროიდისთვის, რომელიც პირადად გავტესტე და მუშაობს კონკრეტულად გუგლ პიქსელისთვის... ამ გზით მაქსიმალური კონფიდენციალურობის მიღწევა შეგიძლია, მაგრამ შენი ქმედებები განსაზღვრავს კონფიდენციალურობის ხარისხს, დაიმახსოვრე...

ოპერაციული სისტემები კონფიდენციალურობისთვის:

1. calyxos.org
2. grapheneos.org

მათი ჩაწერა როგორც უკვე გითხარი მხოლოდ გუგლის პიქსელზეა შესაძლებელი.

რა უნდა ვქნათ, თუ არ გვაქვს პიქსელი?

პირველ რიგში აპლიკაციებს არ მიცე უფლებები (ლოკაცია, მიკროფონი და ასე შემდეგ, გამოიყენე მხოლოდ კრიტიკულად აუცილებელი აპლიკაციები ტელეფონში…

გუგლის არცერთი სერვისი არ გამოიყენო, განსაკუთრებით Google Search…

საუკეთესო რჩევა რაც შენთვის მექნება, გამოიყენე ლეპტოპი ყველგან, მაქსიმალურად იშვიათად გამოიყენე მობილური, მხოლოდ განსაკუთრებულ შემთხვევებში. წლები ამას ვაკეთებდი და იგივეს ვაკეთებ. ტელეფონი ლეპტოპზე ბევრად დაუცველია, როგორც მისი სისტემა, ასევე თავად მოწყობილობაც.

ვიპიენის გამოყენება მცირედით გააუმჯობესებს შენი კონფიდენციალურობის ხარისხს ანდროიდის გამოყენების დროს. მხოლოდ ეს შეგიძლია… (ანდროიდის დარუთვა მცირე სარგებელს მოგცემს, დარუთე ის)

ვინდოუსიც ისეთივე ნაგავია კონფიდენციალურობის მხრივ, როგორც ანდროიდი და აიოსი. თუ ლეპტოპში ვინდოუსი გიწერია, სასწრაფოდ ლინუქსზე გადადი. თავიდან გაგიჭირდება, მაგრამ კონფიდენციალურობა მსხვერპლს მოითხოვს, რადგან დღეს ყველაფერი იქმნება კონფიდენციალურობის საპირისპიროდ. დღეს კონფიდენციალურობა 40-100$ გვიჯდება თვეში, მომავალში ეს თანხა მხოლოდ გაიზრდება...

პირადად ბოლო წლების განმავლობაში ვიყენებ:

1. Kali
2. Parrot
3. Tails OS (ანონიმურობისთვის და კონფიდენციალურობისთვის საუკეთესოა დღეს, თუმცა მხოლოდ ტაილსს არ ენდო, შესაბამისი კონფიგურაცია ჭირდება ამ ორის მისაღწევად. მეტი დეტალი აქ: tails.net)
4. Qubes OS (ინტერფეისი მოძველებულია და ერთ-ერთი რთული სისტემაა, რასთანაც შეხება მქონია, მაგრამ საქმეში საუკეთესოა, თუ გაინტერესებს მიზეზი, გაეცანი მას დეტალურად qubes-os.org)

VPN

არაერთხელ მისაუბრია ვიპიენის მნიშვნელობაზე, კონფიდენციალურობის დაცვაში მას დიდი როლი უკავია, ვინაიდან ის შენ ქმედებებს შიფრავს გარკვეულ დონეზე, ხოლო შენი ინტერნეტ პროვაიდერი ვეღარ დაინახავს თუ რას აკეთებ ინტერნეტში…

უფასო ვიპიენს ვერ ენდობი, ხშირად ფასიანსაც ვერ ენდობი, ამიტომ უფასო ვიპიენი არ გამოიყენო. მე ვერ გირჩევ კონკრეტულ ვიპიენს, ეს გადაწყვეტილება შენი მისაღებია…

საკუთარ VPN_ს ვქმნი, რადგან სხვას არასდროს ვენდობი. მომავალში ჩემ მიერ შექმნილი ვიპიენი ხელმისაწვდომი გახდება ბაზარზე და შეძლებ მის გამოყენებას.

ზოგადად ორი ვიპიენის ანგარიში გჭირდება. ერთი ყოველდღიური გამოყენებისთვის, ხოლო მეორე ტორის გამოყენების დროს, როდესაც რაიმე ისეთს ეძებ, რასაც სტანდარტულ ინტერნეტში ვერ იპოვი ან არ გინდა მესამე მხარემ გაიგოს ამის შესახებ…

არასდროს გამოიყენო ერთი ვიპიენის ანგარიში რამდენიმე საქმისთვის. (შეიძლება ლოგებს ინახავდეს და უმარტივესად მოხდება ყველაფრის ერთმანეთთან დაკავშირება)

ყოველთვის ჩართული გქონდეს VPN… ამით ბევრ პრობლემას აირიდებ თავიდან…

კონფიდენციალურობა სოციალურ ქსელში

1. არაფერს გეტყვი ფოტოებზე და ვიდეოებზე. თუ არ იცი როგორი ფოტო/ვიდეოს გამოქვეყნება არ შეიძლება სოციალურ ქსელში, მაშინ ეს თემები შენთვის არ არის. (მოერიდე ფოტოების და ვიდეოების გავრცელებას ინსტაგრამზე, ტიკტოკზე, ფეისბუქზე, არავის ადარდებს როგორ გამოიყურები, ვისთვისაც მნიშვნელოვანი ხარ, მან ისედაც იცის შენი ვიზუალი)
2. არასდროს დაიწერო სრული სახელი და გვარი სოციალურ ქსელში, რომელიც პირადობაში გიწერია.
3. არასდროს მიუთითო შენი რეალური დაბადების თარიღი სოციალურ ქსელში ან თუ სხვა გზა არ გაქ და მიუთითებ, დამალე!
4. რამდენიმე პროფილი შექმენი, მათ შორის ფეიკებიც.
5. არასდროს გაეცნო უცხო ადამიანს რეალური ანგარიშით, იქნება ინსტაგრამი, ფეისბუქი თუ სხვა. არასდროს იცი რა მიზანი აქვს ადამიანს, რომელიც გეცნობა ონლაინში. (მოგვიანებით მადლობას მეტყვი)
6. არასდროს გაუმხილო ონლაინში გაცნობილ ადამიანს შენი ცხოვრების შესახებ დეტალები, როგორ კომფორტულადაც არ უნდა გრძნობდე თავს ამ ადამიანთან. (სახელი, გვარი და მიახლოებითი ასაკი საკმარისია შენ საპოვნელად)

უამრავი ადამიანი მიყვება საკუთარ თავზე თითქმის ყოველდღე, როცა ვეცნობი ონლაინში ნებისმიერს. მართალია ნდობის მოპოვება მარტივად გამომდის ადამიანებში, მაგრამ ხალხი ისეთ საიდუმლოებს მიყვება, რომელსაც მათი ცხოვრების დანგრევა შეუძლია. უბრალოდ არ მესმის რატომ.

მე ბოროტი განზრახვა არ მაქვს, თუმცა შენ არ იცი რამდენი ადამიანი იყენებს ინტერნეტს ბოროტი მიზნებისთვის…

არასდროს გეცოდინება ვინ დგას ეკრანს მიღმა. დაფიქრდი და გაეცი ნაკლები პირადი ინფორმაცია !

დარკნეტი და ტორი
თავისუფალი ინტერნეტი

დარნკეტის შესახებ თუ გაქვს ინფორმაცია? ჩემი საყვარელი თემაა ფსიქოლოგიის შემდეგ :) დარწმუნებული ვარ მის შესახებ მხოლოდ ნეგატიური ინფორმაციაა შენთვის ცნობილი. ნეგატიურ ინფორმაციას ის ავრცელებს მასზე, ვისაც არ სურს დარკნეტის გაძლიერება, არ სურს რომ უფრო მეტმა ადამიანმა გაიგოს თავისუფლების შესახებ…

დარკნეტზე წვდომა ტორის გამოყენებით შეგიძლია. ტორი დეცენტრალიზებული პროგრამაა, რომელიც მოხალისეების დახმარებით არსებობს. სანამ იარსებებს მოხალისეთა ჯგუფი, მანამდე ტორის არსებობას საფრთხე არ ემუქრება, ხოლო რაც უფრო მეტი მოხალისე ჩაერთვება ამ პროექტში, ტორი უფრო გაძლიერდება. სწორედ ამიტომ ცდილობენ საზოგადოება ჩამოაშორონ ამ ყველაფერს და ხელი შეუშალონ ტორის გაძლიერებას, ეს საკითხი სახელმწიფოების დონეზე დგას, რიგი სახელმწიფოები ბლოკავენ ტორის გამოყენებას მათ ტერიტორიაზე .

გინდა გითხრა დარკნეტის დადებითი მხარეები? კონფიდენციალურობა და ანონიმურობა, სიტყვის თავისუფლება. ეს ის საკითხებია, რომლის მოცემაც ტორს და დარკნეტს შეუძლია. (სწორად გამოყენების შემთხვევაში)

გახსოვს წინა თავში რა წაიკითხე? სახელმწიფოები თვალთვალით და შენი ინფორმაციის დახმარებით გაკონტროლებენ. ინფორმაციით, რომელსაც ინტერნეტის გამოყენების დროს ტოვებ. ტორის გამოყენებით შენ მათ ამ ყველაფრის შესაძლებლობას ართმევ. ახლა ხვდები, რატომ არ სურთ მათ, რომ ტორი მილიონობით, მილიარდობით ადამიანმა გამოიყენოს? ამ შემთხვევაში ისინი კონტროლს დაკარგავენ, კონტროლი ფული და ძალაუფლებაა, ვის უნდა ძალაუფლების დაკარგვა?

ინტერნეტის გამოყენების დროს კვალის დატოვება ვახსენე. თუ ეს არ იცოდი, მაშინ გეტყვი რომ ნებისმიერი შენი ქმედება ინტერნეტში კვალს ტოვებს, კვალს რომელიც საბოლოოდ შენ რეალურ ვინაობას უკავშირდება თუ სათანადოდ არ დაფარავ შენ ქმედებებს.

ნებისმიერი საიტი იყენებს ქუქის. ქუქი (cookie) არის მცირე ზომის ფაილი, რომელიც იქმნება საიტის მიერ, როცა მას იყენებ. საიტები ქუქის იყენებენ შენი პერსონალური ინფორმაციის შეგროვების და კონტროლის მიზნით. ძიების ისტორია, ონლაინ გადახდები, სოციალური მედია, შენი ნებისმიერი ქმედება ტოვებს კვალს ინტერნეტში, რაც საბოლოოდ შენ

რეალურ ვინაობას უკავშირდება აიპის გამოყენებით, რომელსაც პროვაიდერი გაძლევს, ხოლო პროვაიდერმა იცის თუ ვის ეკუთნის კონკრეტული აიპი მისამართი.

ტორის გამოყენების დროს შენ ანონიმური ხარ, შენი ვინაობა არავინ იცის, ყოველი ახალი სესიის (ბრაუზერის გადატვირთვა – სესიაა) შემდეგ შენ ახალი ვინაობა გაქვს, ამიტომ კონტროლზე ფიქრი არ გიწევს, ის რასაც ტორის დახმარებით აკეთებ შენ რეალურ ვინაობას არ დაუკავშირდება თუ შეცდომას არ დაუშვებ… მხოლოდ ტორი არ არის სანდო, გაითვალისწინე.

ამიტომ არის ტორი ძლიერი ხელსაწყო, რომელიც ჩვენ უბრალო ხალხს გვაქვს და თავს ვალდებულად ვთვლი მისი დადებითი მხარეები გაგაცნო…

რაც შეეხება უშუალოდ დარკნეტს. როგორც უკვე გითხარი, იქ მიმდინარე პროცესებს ვერავინ აკონტროლებს, რაც თავის მხრივ კარგიც არის და ცუდიც. მოდი კარგ მხარეზე ვისაუბროთ. კარგი არის ჩვენთვის, რადგან შეგვიძლია “ჩვენნაირი” ხალხი ვიპოვოთ და ერთმანეთს ცოდნა გავუზიაროთ. ნებისმიერ თემაზე შეგიძლია საუბარი და შესაბამისი ფორუმის პოვნა, მათ შორის ჰაკინგს საკმაოდ დიდი როლი უკავია. აქ შენთვის ნაცნობ ინტერნეტში ჰაკინგზე ღიად ვერ ისაუბრებ, რადგან როცა რაღაცას ზედმეტად იტყვი, მაშინვე პრობლემები შეგექმნება. თუმცა დარკნეტში, იქ სადაც შენ შესახებ არავინ არაფერი იცის, ნებისმიერ თემაზე შეგიძლია ისაუბრო, სწორედ ამიტომ დარკნეტი ჰაკერებისთვის სამოთხეა. თუ საკმარის ინფორმაციას მოიძიებ, შენც შეძლებ დარკნეტში უსაფრთხოდ გადაადგილებას, შენთვის საინტერესო ფორუმების მოძიებას და რეალური ჰაკერების გაცნობას, თუმცა მე ვერ გასწავლი წიგნში ამ ყველაფერს, ვინაიდან ამ წიგნის მიზანი არ არის დარკნეტის გაცნობა, ეს წიგნი ზოგადად გაგაცნობს ჰაკინგის და ფსიქოლოგიის სამყაროს, დანარჩენი შენზეა დამოკიდებული.

თუ მეტი ინფორმაციის გაგება გინდა ტორის და დარკენტის შესახებ. დაგიტოვებ ორ ლინკს და აუცილებლად გადახედე, მოიძიე შესაბამისი ინფორმაციები, დროა ისწავლო დამოუკიდებლად ინფორმაციის ძებნა, ეს აუცილებელი უნარია ჰაკინგში და ზოგადად კიბერუსაფრთხოებაში.

1. ტორი – torproject.org
2. ტაილსი (Tails OS) - tails.net

ინტერნეტის დონეები

ზედაპირული ვები – Surface Web

- **აღწერა: ინფორმაცია, რომელიც ინტერნეტშია ხელმისაწვდომი**
- **იცნობ როგორც: ინტერნეტის ნაწილი, რომელსაც ყოველდღიურად იყენებ**
- **არის : ვები (Web)**
- **კონტენტი: ლეგალური**
- **ინტერნეტში არსებული ინფორმაცია ჯამურად: 4%**
- **წვდომა შეგიძლია: Google Chrome, Mozilla Firefox, Opera**

ღრმა ვები – Deep Web

- **აღწერა: ინფორმაცია, რომელსაც საძიებო სისტემებით ვერ იპოვი.**
- **იცნობ როგორც: საიტები დაფარულია სტანდარტული მომხმარებლისგან, მაგრამ შესაძლებელია წვდომა ბრაუზერით (გუგლში ვერ იპოვი საიტებს, მაგრამ თუ ლინკი გექნება, შეხვალ)**
- **არის : ვები (Web)**
- **კონტენტი: ლეგალური, არალეგალური**
- **ინტერნეტში არსებული ინფორმაცია ჯამურად: 96 %**
- **წვდომა შეგიძლია: Google Chrome, Mozilla Firefox, Opera**

ბნელი ვები - Dark Web

- **აღწერა: ინფორმაცია, რომელიც მსოფლიოს მასშტაბით დაფარულია.**
- **იცნობ როგორც: ინტერნეტის ნაწილი, რომელიც სპეციალური პროგრამის გარეშე მიუწვდომელია.**
- **არის : ვები (Web)**
- **კონტენტი: უმეტესად არალეგალური**
- **წვდომა შეგიძლია: Tor Browser ის დახმარებით**

ბნელი ქსელი – Dark Net

- **აღწერა: ქსელური ინფრასტრუქტურა, რომელიც ბნელ ინტერნეტს ამუშავებს**
- **იცნობ როგორც: შენ მას არ იცნობ, სანამ შესაბამისი ცოდნა არ გექნება, მის შესახებ ბევრს ვერაფერს გაიგებ**
- **არის : ქსელი (Network)**
- **კონტენტი: არალეგალური**
- **წვდომა შეგიძლია: Freenet, Tor, GNUnet, I2P**

უნივერსიტეტები
სასწავლებლები
აკადემიები

ყველაზე დიდი ტყუილია განათლების სისტემა...

რატომ არის უნივერსიტეტი დროის ფლანგვა?

<u>კიბერუსაფრთხოების მიმართულებით</u>

ვინ ასწავლის უნივერსიტეტში?

საკუთარი საქმის ტოპ პროფესიონალი ამ სფეროში ბევრად მეტს გამოიმუშავებს, ვიდრე მსოფლიოს საუკეთესო უნივერსიტეტებში ლექტორის ანაზღაურებაა...

უნივერსიტეტი საზღვრებშია მოქცეული. შენ ვერასდროს მიიღებ რეალურ და პრაქტიკულ პასუხებს კითხვებზე, რომლებმაც შეიძლება რაიმე გზით კანონის დარღვევა გამოიწვიოს.

(ჰაკინგის 99.9% პოტენციურად არალეგალურ ქმედებას იწვევს)

რამდენიმე ცნობილმა უნივერსიტეტმა და აკადემიამ მიმიწვია ლექტორად კიბერუსაფრთხოების მიმართულებით, როგორც საქართველოში, ისე საქართველოს გარეთ… ყველა მათგანს უარი ვუთხარი ისე, რომ არც დავფიქრებულვარ.

საზღვრები ჩემთვის წითელი ხაზია, საზღვრები მხოლოდ მე შემიძლია დავუწესო საკუთარ თავს, სხვა ვერასდროს მეტყვის რა ვთქვა ან გავაკეთო…

თუ ამ საქმის პროფესიონალი ხარ და გიყვარს შენი პროფესია, არასდროს მოგინდება უნივერსიტეტში ლექტორობა, მინიმუმ თავად ასწავლი საზოგადოებას ყველანაირი საზღვრების გარეშე.

კარგ უნივერსიტეტში ასწავლიან პროფესიონალები, რომლებსაც ნორმალური ცოდნა აქვთ, მაგრამ ეს ცოდნა რეალურ სამყაროში საკმარისი არ არის… უნივერსიტეტში ლექტორად საუკეთესო არასდროს მივა…

ადამიანი ნორმალური ცოდნით ვერასდროს გაუწევს კონკურენციას საკუთარი საქმის პროფესიონალს.

შენ ვისგან გინდა გამოცდილების გაზიარება? თუ ნორმალური ცოდნის მქონე ადამიანისგან მიიღებ რჩევებს, შენი მაქსიმუმი ნებისმიერ პროფესიაში ნორმალური დონე იქნება და ვერასდროს მიაღწევ პროფესიონალის დონეს.

ჰაკინგის მაგალითზე განვიხილოთ...

კევინ მიტნიკი. ნებისმიერმა ადამიანმა იცის ამ სახელის შესახებ, ვისაც ჰაკინგი აინტერესებს. ამ ადამიანის საქმეები და წარსული ხაზს უსვამს მის ცოდნას და მსოფლიოში ნომერ პირველ ჰაკერად ითვლება. კევინი ლეგენდა იყო... **(სამწუხაროდ წიგნის წერის მომენტში 2023 წლის 16 ივლისს**

გარდაიცვალა ლეგენდა კაცი)

ლოგიკური კითხვა: ცოდნის მისაღებად აირჩევდი კევინ მიტნიკს მენტორად თუ სხვა ნებისმიერ ჰაკერს ან უნივერსიტეტის ლექტორს? რა თქმა უნდა შენ კევინ მიტნიკს აირჩევდი თუ ამის შანსი გექნებოდა…

კევინ მიტნიკს რომ ლექტორის გზა აერჩია, ის იმ კვალს ვერ დატოვებდა ჰაკინგის სამყაროში, რა მემკვიდრეობაც მან დაგვიტოვა… (ამით იმას გეუბნები, რომ საუკეთესო ჰაკერს სასწავლებელში ვერასდროს იპოვი)

სხვა პროფესიებზე ვერაფერს გეტყვი, მხოლოდ იმ საკითხებში შემიძლია რჩევების მოცემა, რაშიც გამოცდილება მაქვს…

ბევრი ადამიანი ვერ წარმოიდგენს რა დონის ჰაკერებთან მისაუბრია (ხშირად არც მე მჯერა), მსოფლიოში მართლა საუკეთესოებთან, რომლებსაც ნებისმიერი რაღაცის გატეხვა შეუძლიათ და მათი პოვნა ძალიან რთულია (ვიცი რომ გაინტერესებს, მაგრამ რომც გასწავლო ვერ იპოვი)...

გინდა გითხრა რა გამოარჩევს საუკეთესო ჰაკერს სხვა ნებისმიერი ჰაკერისგან? მათი რეალური ცოდნის შესახებ არავინ არაფერი იცის. მათი სამუშაო პოზიციაც კი საშუალო ან დაბალი დონისაა, იმდენად შენიღბულები არიან... (შეიძლება კითხვა გაგიჩნდეს, როგორ შევძელი მათთან დაკავშირება თუ ასეთი შენიღბულები არიან? _ მათი ნდობა მოვიპოვე)

მაგალითად შეიძლება ქსელის ადმინისტრატორად მუშაობდეს მსოფლიოს საუკეთესო ჰაკერი, მაგრამ ის არასდროს იმუშავებს ჰაკერად რეალური ვინაობით... (მათ იციან, რომ უნდა დამალონ საკუთარი შესაძლებლობები)

არასდროს გაამჟღავნო შენი რეალური ცოდნა რეალური ვინაობით… ოქროს რჩევაა…

ადამიანების, აკადემიების, უნივერსიტეტების დამცირება არ მიყვარს, ყოველთვის ვცდილობ თავი შევიკავო, მაგრამ როცა საქმე საზოგადოებას ეხება და ზოგი "პროფესიონალის" გამო ეს საზოგადოება ზარალდება, მიწევს ხოლმე ჩემი სიმართლის ბოლომდე გატანა...

2023 წელს საქართველოში შემდეგი ვითარებაა:

ყველა კუთხეში აკადემიაა...

ყველა აკადემია სანთლით ეძებს ნებისმიერი პროფესიის ლექტორს....

ვაი იმ ლექტორს აკადემია რომ იპოვის...

ეს "პროფესიონალი" წლების განმავლობაში საერთოდ სხვა პროფესიით მუშაობს, არ აქვს პრაქტიკული ცოდნა. უცებ რაღაც უცნობი სერტიფიკატი

"აიღო" და კიბერუსაფრთხოების ექსპერტს ეძახის საკუთარ თავს...

ეს "ექსპერტი" ხვალ დაუჯდება რომელიმე გულანთებულ, მოწადინებულ ადამიანს და კიბერუსაფრთხოებას შეაძულებს, მცდარ ინფორმაციას მიაწვდის...

ახლა შენ მეგობარო! სანამ ასეთ აკადემიაში მიხვალ გაიკითხე ლექტორზე, შეამოწმე მისი გამოცდილება...

ზოგადად, აკადემია იცი რატომ იქმნება? აკადემიების 99%, ისევე როგორც უნივერსიტეტი აიტის და კიბერუსაფრთხოების მიმართულებით მხოლოდ "ფულის კეთების" მანქანაა მფლობელისთვის, როცა ლექტორს "მთავარია ვიღაცამ ლექცია ჩაატაროს" პრინციპით ირჩევს აკადემია, უნივერსიტეტი... იქ საუბარი უნდა დაასრულო... არც უნდა გაეკარო…

ხშირად მეკითხებიან სად ვისწავლო კიბერუსაფრთხოება, რომელ აკადემიაში… ჩემი პასუხი არის არცერთში!

რატომ? დაფიქრდი და პასუხს თავად იპოვი...

ამას ყველა არ გეტყვის მეგობარო... რადგან ამის თქმას გამბედაობა ჭირდება... ადამიანების 99% ფულზე იკერება, რაღაცაზე იკერება…

შენი განათლება ყველას ფეხებზე კიდია, განათლებული ადამიანი საშიშია... ეს ყველამ იცის. განსაკუთრებით როცა ჰაკინგი იცი, როცა ისეთი რაღაც იცი, რითიც სხვისი სერიოზულად დაზარალება შეგიძლია… არცერთი სასწავლებელი მსგავს ცოდნას არასდროს მოგცემს...

99.9% ვინც ლექტორობას თანხმდება, ამას ფულის გამო აკეთებს. ასეთ ხალხს შენი განათლება ფეხებზე კიდია...

მეტს აღარაფერს ვიტყვი, უბრალოდ რამდენჯერმე გადაიკითხე ეს მონაკვეთი და გაიაზრე. როცა გაიაზრებ, კითხვები გაგიჩნდება და პასუხებსაც თავად იპოვი… (ნაწილს აქ მიაგნებ: jafarasec.com)

ამ ყველაფერს ვწერ იმიტომ, რომ შენი ბედი მადარდებს, შენი ფინანსები, რომელიც მცირეა (დიდი ალბათობით), არ მინდა ვიღაცის ჯიბეში წავიდეს და სანაცვლოდ 0 ცოდნა მიიღო...

ხშირად მიწევს კამათი თუ რატომ არის უნივერსიტეტების, აკადემიების 99.9% ნაგავი...

აი პასუხი...

შენი ბედი მხოლოდ შენ ხელშია, არავის ანდო ის, მითუმეტეს ზოგიერთ "ფულის მონას".

იფიქრე მეგობარო, იფიქრე!

ამ თავის დასკვნა:

ტოპ უნივერსიტეტებში ასწავლიან საშუალო დონის პროფესიონალები. ის ვინც საუკეთესოა, უნივერსიტეტში არასდროს დაიწყებს ლექტორად მუშაობას...

თუ შენ საუკეთესო შედეგის მიღწევა გინდა, საუკეთესო შედეგს საშუალო დონის პროფესიონალისგან ვერასდროს მიიღებ.

საუკეთესო გამოცდილების მიღება მხოლოდ საუკეთესო პროფესიონალისგან შეგიძლია.

უნივერსიტეტი დროის კარგვაა, მაგრამ ბაკალავრის ხარისხი დაგეხმარება, თუმცა რამდენიმე წელში ესეც აზრს დაკარგავს (თუ ჩააბარებ, მხოლოდ იმიტომ რომ ბაკალავრის ხარისხი გქონდეს, სწავლაზე დრო არ დაკარგო, რადგან ღირებულს ვერაფერს გასწავლიან, რადგან თავადაც არ იციან...)

როგორ შეუძლია 80 წლის ლექტორს, გასწავლოს 20 წლის სტუდენტს ტექნოლოგია, რომელიც სულ რაღაც 15-10 წლის წინ შეიქმნა... სისულელეა... 80 წლის ლექტორმა ტექნოლოგიების შესახებ არაფერი არ იცის, მიუხედავად პატივისცემისა, 80 წლის ლექტორები უნივერსიტეტში ტექნოლოგიებს არ უნდა ასწავლიდნენ...

წიგნის წერის მომენტში მივიღე გადაწყვეტილება და შევქმენი ფიზიკური კლუბი თბილისში, მხოლოდ ჰაკერებისთვის...

ეს არის სივრცე, რომელიც ნებისმიერ დამწყებ და გამოცდილ ჰაკერს ჭირდება...

გარემო, სადაც სხვა ჰაკერების გაცნობას, განვითარებას და გართობას შეძლებ.

გელოდებით: ge.hackersforce.com

ადამიანების კრიტიკული შეცდომები

პაროლების ფსიქოლოგია

ადამიანებს სიმარტივე უყვართ, დარწმუნებული ვარ შენი პაროლი უმარტივესია. მნიშვნელობა არ აქვს რას შეიცავს პაროლი, იქნება ეს შენ სახელთან, გვართან, დაბადების წელთან, ცხოველთან თუ სხვა რამესთან დაკავშირებული, ის არ უნდა იყოს ადვილად გასატეხი!

ძირითადი შეცდომები, რომლებსაც ადამიანები უშვებენ:

სიმარტივე. პაროლი ძალიან მოკლეა, არ შეიცავს სიმბოლოებს

პაროლი არ არის უნიკალური.

დარწმუნებული იყავი პაროლს, რომელსაც შენ იყენებ თუ ის რაღაც პირადულთან არ არის დაკავშირებული, რაც მხოლოდ შენ იცი, მსოფლიოში ასეთ პაროლს კიდევ ბევრი სხვა ადამიანი გამოიყენებს.

მაგალითად Nosystemissafe

როგორ შეგიძლია ასეთი პაროლი გახადო უნიკალური?

Nosystemissafe.when.jafara.targets.it!@#

წარმოუდგენელია ვიღაცამ მსგავსი პაროლი უხეში ძალის შეტევით გატეხოს, რა თქმა უნდა ეს პაროლი მხოლოდ მაგალითია.

უხეში ძალით შეტევის დროს (brute-force attack) თავდამსხმელი ცდის ყველა შესაძლო პაროლის კომბინაციას, სანამ არ მოძებნის სწორს. როდესაც პაროლი უნიკალურია, თავდამსხმელს არანაირი შანსი არ აქვს, შეუძლებელია მსგავსი პაროლი შემთხვევით გამოიცნოს.

შენ ყველგან ერთნაირ ან მსგავს პაროლს იყენებ.

თუ ეს ასეა, წარმოიდგინე, რომ შენი ერთი პაროლის შესახებ გაიგო ჰაკერმა, ბოროტმოქმედმა, რაც გინდა ის დაარქვი, მას ავტომატურად შენი ყველა სხვა პაროლის შესახებ ექნება წარმოდგენა. თუ ჯერ არ იცის, მალე ეცოდინება. ის დააგენერირებს მილიონობით მსგავს პაროლს და დამიჯერე, ძალიან მალე ყველა შენი პაროლი ეცოდინება, რაც ძალიან ცუდია.

პაროლებზე საუბრისას, თუ ეს ეხება ანგარიშებს, აუცილებელია გამოიყენო ორ ეტაპიანი დაცვა. დღეს თითქმის ყველა სოციალურ ქსელს აქვს 2 ეტაპიანი დაცვა. მისი გამოყენებით შენ 60%-ით ურთულებ ჰაკერს პაროლის გატეხვას. სწორად წაიკითხე, შენ მას მხოლოდ საქმეს ურთულებ. ჰაკერის ცოდნას გააჩნია :) იმედი მაქვს არასდროს შეხვდები ჰაკერს, რომელმაც ზედმეტად ბევრი იცის… (2023 წლის ზაფხულში მოაგვარა მეტამ (ფეისბუქმა) 2 ეტაპიანი დაცვის პრობლემა, როდესაც ამის შესახებ ფორუმებზე ხალხი 2023 წლის დასაწყისში საუბრობდა, ჰაკერს შეეძლო 2 ეტაპიანი დაცვა მოეხსნა

ფეისბუქის, ინსტაგრამის ანგარიშზე)

სულ რამდენიმე რჩევის გათვალისწინებით, შენ არასდროს მოგიწევს პაროლებზე დარდი, აღარ იტყვი, რომ სოციალური ქსელი გაგიტეხეს, მაგრამ სისულელე არ უნდა გააკეთო… თუ შენ ლინკზე გადახვალ, რომელიც ჰაკერს ეკუთნის, როგორი რთული პაროლიც არ უნდა გქონდეს, შენი სოციალური ქსელი მაინც გატყდება (არამხოლოდ სოციალური ქსელი).

არ გადახვიდე ლინკებზე, დააკოპირე და შეამოწმე ლინკი ამ საიტზე სანამ მასზე გადახვალ: virustotal.com

სოციალური ინჟინერიის მსხვერპლი ნებისმიერი ადამიანი შეიძლება გახდეს. ეს უკვე სრულიად შენი პასუხისმგელობაა… ერთადერთი გზა გაქვს, თუ გინდა რომ არასდროს გახდე სოციალური ინჟინერიის მსვერპლი, მინიმუმ იმდენი უნდა იცოდე სოციალურ ინჟინერიაზე, რამდენიც საშუალო დონის ჰაკერმა იცის.

ძლიერი პაროლები გიცავს მრავალი შეტევისგან. არა ყველა მათგანისგან, მაგრამ შეტევების ნაწილი აზრს კარგავს, როდესაც ძლიერ პაროლს და ორ ეტაპიან უსაფრთხოებას იყენებ. თუ ჰაკერი საკმარისად დიდ დროს დაკარგავს შენი პაროლის გატეხვის მცდელობაზე, შეიძლება მან ინტერესი დაკარგოს და უბრალოდ სხვა სამიზნეზე გადავიდეს :)

საჯარო ვაიფაი

ჩვენ ხშირად ვამბობთ რომ არ უნდა გამოვიყენოთ საჯარო ვაიფაი, მაგრამ კონკრეტულად არავინ გვეუბნება რა შედეგები მოყვება საჯარო ვაიფაის გამოყენებას.

საჯარო ვაიფაის გამოყენების დროს შენ არ იცი რა ინფორმაცია ეგზავნება მესამე მხარეს. გარდა ამისა, ტრაფიკი (ის, რასაც ინტერნეტის გამოყენების დროს აკეთებ) არ არის დაშიფრული, ესეიგი ის ხელმისაწვდომია და ნებისმიერს შეუძლია ამ მონაცემების დამუშავება, ამის უფლებას კანონი იძლევა, ის რაც საჯაროა, ესეიგი ყველას შეუძლია ამ რაღაცის გამოყენება საკუთარი მიზნებისთვის… ეს ყველაფერი არ არის კარგი, შენ ბევრ ისეთ ინფორმაციას გაუზიარებ მესამე მხარეს, რაც არ უნდა გააზიაროო…

სერიოზულად, თუ რაიმე მნიშვნელოვანის გაკეთებას აპირებ ინტერნეტში სახლიდან მოშორებით, არ ენდო საჯარო ვაიფაის და გამოიყენე შენი პირადი ინტერნეტი, რომელიც გექნება მობილურის ნომერზე გააქტიურებული… (თუ მაიმუნობას აპირებ, შენი ნომერი არ გამოიყენო, სხვის სახელზე გააქტიურებული ნომერი იყიდე და ისე გააზიარე ინტერნეტი)

შეიძლება გაგიჩნდეს კითხვა როგორ გამოვიყენო საჯარო ვაიფაი უსაფრთხოდ?

ვპნ შენ ინტერნეტ ტრაფიკს “დაცული არხის” გამოყენებით ატარებს და შენი მონაცემები იშიფრება იმ მომენტში. თავად სახელიც ამას გეუბნება Virtual Private Network… (ერთი ვიპიენის გამოყენება საკმარისი არ არის ინტერნეტში თავის დასაცავად… რამდენიმე ვიპიენი უნდა გამოიყენო ერთად. Nested VPN_ის შესახებ მოიძიე გუგლში ინფორმაცია, ტექნიკურ მხარეს წიგნში ვერ აგიხსნი)

შენ შეგიძლია კარგი ვიპიენის ყიდვა წელიწადში დაახლოებით 60-80$ ფარგლებში, თუმცა გაითვალისწინე, ვიპიენ პროვაიდერი მაინც ხედავს შენ ტრაფიკს, ამიტომ აუცილებელია სწორი და სანდო პროვაიდერი შეარჩიო. როდესაც ვიპიენს იყენებ, საჯარო ვაიფაის გამოყენების დროს მესამე მხარე ვეღარაფერს ნახავს. ამიტომ არის მნიშვნელოვანი ვიპიენის გამოყენება ყველგან, არ დაზოგო ფული ვიპიენზე, ბევრ პრობლემას აირიდებ თავიდან მომავალში…

ბოლოს, დაიმახსოვრე, მაშინაც კი თუ შენ ვიპიენს იყენებ, არ ხარ ანონიმური, ვიპიენ პროვაიდერმა იცის შენი აიპი მისამართი, საიდანაც ვიპიენს დაუკავშირდი, კვალს ტოვებ… არასდროს იყიდო VPN შენი პირადი ბარათით, მხოლოდ კრიპტოთი.

დააკვირდი სად რას წერ...

ადამიანები ინტერნეტში ყველაფერს წერენ... არ შეიძლება ნებისმიერი კითხვა, რაც გაგიჩნდება დაუფარავად იკითხო. როგორც უკვე იცი, ინტერნეტში ყველანაირი ქმედების შემდეგ კვალი რჩება, შესაბამისად დღეს თუ რამეს დაწერ ინტერნეტში (თუნდაც ყალბი ანგარიშით), დიდი ალბათობით შენ რაღაც კვალს დატოვებ, რომელიც ხვალ შეიძლება შენ რეალურ იდენტობას მარტივად დაუკავშირონ (გააჩნია ვინ დაინტერესდება)...

ამიტომ, სანამ რამეს დაწერ ნებისმიერ სოციალურ ქსელში, ფორუმზე, ბლოგის კომენტარებში ან თუნდაც ვიღაცას მიწერ პირადში, კარგად დაფიქრდი... რაიმე ისეთს ხომ არ წერ ინტერნეტში, რასაც ხვალ შენთვის პრობლემების შექმნა შეუძლია?

უამრავმა ჰაკერმა დაუშვა მსგავსი შეცდომა, სწორედ ეს შეცდომა აღმოჩნდა უამრავი მათგანისთვის დამღუპველი... (გადახედე ისტორიებს)

თუ რამდენიმე პიროვნება გაქვს შექმნილი, განსაკუთრებით ფრთხილად უნდა იყო... პიროვნების არევა საკმაოდ ხშირი და დიდი პრობლემაა...

არასდროს ენდო პლატფორმას, რომელიც არ არის დეცენტრალიზებული. თუ კონკრეტული რაღაც ვიღაცის მიერ იმართება, გამოდის კონტროლი ერთი პიროვნების ხელშია, ანუ ის ფლობს კონტროლს ყველანაირ ინფორმაციაზე... ისე შეუძლია ამ ინფორმაციის დამუშავება, გამოყენება, როგორც მას მოესურვება... (შენთვის ნაცნობი ინტერნეტის 99% ვიღაცის მიერ იმართება, ამიტომ თითქმის ყველანაირი ქმედება შენთვის ნაცნობ ინტერნეტში პრობლემაა...)

შენიშვნა:

ზედმეტი არსად არაფერი დაწერო, მომავალში ინანებ, თან ძალიან...

თუ რამდენიმე პიროვნება გაქვს, მაქსიმალურად ყურადღებით იყავი... არ აურიო ისინი ერთმანეთში...

არ დაუშვა შეცდომა, რომელიც კრიტიკულია... (ეს შეცდომები კრიტიკულია)

ქარდინგი _ მახე დამწყები ჰაკერებისთვის

როგორც კი დამწყები ჰაკერი მცირედით გაერკვევა ამ სამყაროში, 99% შემთხვევაში ის პირველი ქარდინგით ინტერესდება (მარტივი ფული, რომლის მიღებაც მუშაობის გარეშეა შესაძლებელი)…

ეს ყველაფერი მახეა… თუ ერთხელ გაები, მთელი ცხოვრება შიშში იცხოვრებ…

რა არის ქარდინგი ბევრს არ ესმის, რა პრობლემების გამოწვევა შეუძლია არც ეს ესმის ბევრს… ამიტომ ამ თავში მინდა კარგად აგიხსნა თუ რატომ უნდა დაიჭირო თავი შორს ქარდინგისგან… იმედი მაქვს არასდროს გაგიჩნდება ინტერესი ამ საკითხის მიმართ… (ჯანდაბას ინტერესი შეიძლება, მაგრამ არასდროს გაერიო…)

ქარდინგი - “სხვისი ფულის მითვისება”…

ამ დროს შენ სხვის ბარათს იყენებ, ხსნი, ანაღდებ სხვის ფულს…

ერთი პრობლემაა თანხის ანონიმურად გადარიცხვა ბარათიდან (საშინლად რთულია). მეორე პრობლემა გადარიცხული ფულის განაღდებაა…

ქარდერების უმეტესობა პირველივე ნაბიჯებზე უკვე განწირულია… როდესაც შენ ფულს ხსნი ბარათიდან, უამრავ კვალს ტოვებ… არ აქვს მნიშვნელობა რამდენად ანონიმურად გააკეთებ ამ ყველაფერს, შენ ფულს ეხები, ხოლო ფულის კვალის გაყოლა შესაძლებელია მანამ, სანამ ის ინტერნეტში იმოძრავებს… როცა საქმე ფულს ეხება, იქ საქმე ყოველთვის უფრო რთულადაა, ვიდრე ერთი შეხედვით ჩანს…

შენ არ იცი ვის ფულს ეხები…

იქნებ კრიმინალების ფული მიითვისე? იქნებ ისეთი ადამიანის ფულს ეხები, რომელიც პოლიციაში, სახელმწიფო უსაფრთხოების სამსახურში მუშაობს? კიდევ უფრო უარესი, ეხები მილიონერის, მილიარდელის ქონებას, რომელმაც ეს თანხა უკანონოდ მოიპოვა? ფულიანი ტიპი, რომელსაც კანონები ფეხებზე კიდია, საკუთარ ფულს ნებისმიერ ფასად დაიბრუნებს… იქნებ ისეთი ადამიანის ფული მიითვისე, რომელსაც უამრავ ჰაკერთან აქვს კავშირი? (ამ შემთხვევაში ვგულისხმობ ჰაკერებს, რომლებმაც ბევრი რამ იციან და ასევე კანონი არ ადარდებთ) …

ნებისმიერი ზემოთ აღწერილი მაგალითის შემთხვევაში ძალიან დიდ შარში აღმოჩნდები… რის გამო? რამდენიმე ათასისთვის…

ეს ყველაფერი ფილმი არ გეგონოს მეგობარო… ფილმები რეალობას აცდენილია, რეალობაში ყველაფერი იმაზე რთულად არის, ვიდრე ამას ფილმებში ხედავ… არც ხალხს დაუჯერო, ვისაც არ გამოუცდია კონკრეტულად ეს საკითხი და ჰაერზე დაგიწყებს რაღაცის მტკიცებას, ახსნას… ზემოთ მოყვანილი მაგალითები რეალური ისტორიებია, თუ დარკნეტში შესაბამის ფორუმებს იპოვი, ისეთ ისტორიებს მოისმენ, რომლის მსგავსი ალბათ სიზმარშიც ვერ დაგესიზმრება…

მოკლედ ქარდინგი საშიშია, მინიმუმ ციხე, მთელი ცხოვრება შიშში ყოფნა გელოდება. არც ერთი არ გენდომება თუ გიჟი არ ხარ… როდესაც ქარდინგზე დაგელაპარაკება ვიღაც, უბრალოდ მოიშორე თავიდან, ნუ გარისკავ არაფრის გამო…

კარიერა ჰაკინგში

გზა წარმატებული კარიერისკენ ჰაკინგში

ალბათ გაინტერესებს როგორ უნდა გახდე ავტორიტეტი ამ სფეროში (ჰაკინგი, შეღწევადობის ტესტირება), როგორ მიიპყრო ყურადღება ისე, რომ პრობლემები არ შეიქმნა კანონთან მიმართებაში. ამ მომენტიდან სრულ გზამკვლევს ეცნობი, ნაბიჯ-ნაბიჯ დეტალურ გზამკვლევს :)

- **როგორ ფიქრობ, ვინ არის ჯაფარა?**
- **რატომ ჯაფარა?**
- **რატომ არის ჯაფარას ვინაობა უცნობი?**
- **როგორ უნდა შეაღწიო იმ წრეში, სადაც მაღალი დონის საზოგადოებაა? (პროფესიონალი ჰაკერები)**

ეს ის კითხვებია, რომელიც შენ თავს უნდა დაუსვა… თუმცა პასუხების მიღება რთულია, ამიტომ პასუხების ნაწილს გიტოვებ.

როგორ ფიქრობ, ვინ არის ჯაფარა?

ჯაფარა ადამიანია ძალიან დიდი მიზნებით… დღეს საზოგადოება ფიქრობს რომ ჯაფარა ჰაკერია, ასეც არის. თუმცა მომავალში ჯაფარას სხვა მრავალი სახით გაიცნობ, როდესაც ამის დრო მოვა…

რატომ ჯაფარა?

პროფესიაში, სადაც შენი რეალური ცოდნა მხოლოდ შენ იცი, აუცილებელია გქონდეს სახელი, ავტორიტეტი და ბრენდი.

ჯაფარა – მარტივად დასამახსოვრებელი სახელია, რომელიც უკვე ბრენდია. ჯაფარამ შექმნა ქართული ჰაკერული ფორუმი, რომელიც ყოველდღიურად იზრდება. ჯერ ძალიან მცირე ადამიანთა ჯგუფმა იცის ამ სახელის შესახებ, თუმცა დროთა განმავლობაში ჯაფარას შესახებ მთელი მსოფლიო გაიგებს. ბრენდის მშენებლობა ნელი პროცესია. მე ვაშენებ ბრენდს ჯაფარას სახელის გარშემო. თუ შენი გეგმები გრანდიოზულია და გსურს მსოფლიოში გამოიწვიო ცვლილებები, დიდი საზოგადოება გჭირდება შენი სახელის გარშემო, ვინაიდან დიდ ცვლილებებს ერთი და ორი ადამიანი ვერ გამოიწვევს. ეს წიგნიც ჯაფარას ბრენდის ნაწილია, ყველაფერი რასაც ვაკეთებ, ჯაფარას სახელის პოპულარიზაციას ემსახურება…

რატომ არის ჯაფარას ვინაობა უცნობი?

ანონიმურობა პირველ რიგში უსაფრთხოების გარანტიაა, როგორც უკვე იცი. სანამ ჯაფარას შესახებ არავინ არაფერი იცის, მანამდე შემიძლია მშვიდად ვიყო და ვაკეთო ის, რაც ჩემი მიზნების მისაღწევად მჭირდება. ასევე, სანამ იდუმალი ვარ ზედმეტი კითხვები და ყურადღება არ მაწუხებს,

შესაბამისად ყველანაირად ფოკუსირებული ვარ ჩემ მიზნებზე. შემიძლია სიმართლე ვთქვა და ამ სიმართლის თქმის გამო პრობლემები არ შემექმნება.

ძალიან ბევრს გონია, რომ ჯაფარას რეალური ვინაობა იციან... ისინი ცდებიან. ჯაფარას შესახებ რასაც გაიგებ, ნუ დაიჯერებ... წლებია ხალხი ჩემი ვინაობის გაგებას ცდილობს, მაგრამ უშედეგოდ. მათ მხოლოდ ის იციან, რასაც მე მოვისურვებ.

ბონუს რჩევა: თუ შენ იმ გზას აირჩევ, რომელსაც მე მივყვები და შექმნი ანონიმურ პიროვნებას, ბრენდს, ისე გააკეთე რომ კვალი აურიო საზოგადოებას... გამოიყენე რეალური ადამიანები შენი კვალის დასაფარად.

როგორ უნდა შეაღწიო იმ წრეში, სადაც მაღალი დონის საზოგადოებაა? (ტოპ ჰაკერები)

ამ კითხვაზე პასუხის მიღება და ამ ნაწილის შესრულება ყველაზე რთულია, ვინაიდან თუ ღირებულება არ გაგაჩნია და რაღაც ღირებულის შეთავაზება არ შეგიძლია მათთვის, მათ წრეში ვერ მოხვდები... იმისთვის, რომ რაიმე ღირებულება შეიძინო, საკმარისად დიდი დრო უნდა ჩადო საკუთარი თავის განვითარებაში და ბევრ ისეთ რამეზე უნდა თქვა უარი, რაც გიყვარს (გართობა, ფილმების ყურება, მეგობრები და სხვა. ეს დრო შენი თავის განვითარებას უნდა დაუთმო)...

გარდა ამისა, ძალიან ცოტა რამ არსებობს ისეთი, რაც მცოდნე ჰაკერებს ჭირდებათ და მათ წრეში მოხვედრა რეკომენდაციის, ნდობის გარეშე რთულია (რეკომენდაცია გჭირდება მათივე წრეში არსებული ადამიანისგან, რომელსაც პატივს ცემენ).

თუ ფიქრობ, რომ კონკრეტული რაღაცის ცოდნა დაგეხმარება მათ წრეში მოხვედრაში ცდები. თუ ფიქრობ რომ შენგან რამე ჭირდებათ, ცდები. ერთადერთი რაც მათთან მოგახვედრებს შენი მიზნები, აზროვნება და მიზნისკენ სწრაფვაა. არც ცოდნა აკლიათ მათ, არც რესურსები და არც შენნაირი ხალხი.

კიდევ ერთხელ სამი რამ, რაც მათ აინტერესებთ: შენი მიზნები, აზროვნება და ქმედებებია, რომელსაც ამ მიზნების მისაღწევად აკეთებ.

შექმენი ბრენდი შენი სახელის გარშემო, აუცილებელი არ არის მსოფლიოს შეცვლა გინდოდეს, უბრალოდ შენი სახელი საკმარისად დიდი უნდა იყოს იმისთვის, რომ კითხვა “მოგვიყევი შენი თავის შესახებ” აღარასდროს გაიგო, დანარჩენი შენმა სახელმა ან იმ საქმეებმა უნდა თქვას, რომელსაც აკეთებ... როდესაც ამ დონეს მიაღწევ, წარმატება თავისით მოვა,

ყველა კარი გაიხსნება შენთვის.

დღეს მაინც მიწევს ჯაფარას სახელის შემდეგ განმარტება, თუმცა მალე ჯაფარას სახელის ხსენება საკმარისი იქნება…

აუცილებლად აარჩიე კონკრეტულად ერთი მიმართულება და იმ მიმართულებით აქციე შენი სახელი ბრენდად. ბევრ მიმართულებას არ მოედო, ეს ყველაფერი მე გავიარე და ჩემი პირადი გამოცდილებით გეუბნები, კონკრეტული მიმართულება აირჩიე და დარწმუნდი, რომ შენი საქმის პროფესიონალი იქნები, ძილშიც შეძლებ შენი საქმის კეთებას :)

როდესაც აარჩევ მიმართულებას, რომელიც მართლა შენია (ამას მარტივად მიხვდები, თუ რაღაც გულით მოგწონს, მიხვდები). პირველ რიგში ამ მიმართულებით გაიცანი ხალხი, შენი მიზანი საუკეთესოების გაცნობა უნდა იყოს, თუმცა სანამ საუკეთესოებს გაიცნობ, მანამდე ნებისმიერი ადამიანის გაცნობა ამ მიმართულებით შენთვის ძალიან კარგი იქნება…

როგორ უნდა მიიქციო ასეთი ადამიანების ყურადღება?

1. შექმენი ლინკდინი. ხალხი, რომელიც ბიზნესს სერიოზულად უდგება, ლინკდინს იყენებს. შენი სახელის გარშემო ბრენდის შენება უკვე ბიზნესია! (თუ ბოლომდე ლეგალურ გზას არ მიყვები, ლინკდინი დაივიწყე, თუ ლეგალურად აკეთებ ყველაფერს, ნამდვილი ჰაკერები თავის წრეში არ მიგიღებენ) ანუ, თუ სამსახურია შენი პრიორიტეტი ლინკდინის გზას მიყევი, მაგრამ თუ განვითარებაა შენი მიზანი, ლინკდინი დაივიწყე...
2. აუცილებლად დაწერე ღირებული ბლოგები მუდმივად იმ მიმართულების გარშემო, რომელიც შენთვის საინტერესოა. მაგალითად, თუ შენ გადაწყვეტ, რომ ეთიკური ჰაკინგის მიმართულებით გინდა განვითარება, ამ თემის ირგვლივ კვირაში 1 ბლოგი მაინც დაწერე და გააზიარე სადაც შეძლებ.
3. შექმენი პირადი საიტი, სადაც შენ შესახებ დაწერ. როდესაც ადამიანს საკუთარი საიტი აქვს, უფრო სერიოზულად უყურებენ, შენ იმიჯს უსვამს ხაზს. (სასურველია ბლოგები შენივე საიტზე დაწერო, რაც SEO_ს მხრივ დაგეხმარება და გუგლში უფრო მარტივად მოიძებნები, თუმცა ნებისმიერი პლატფორმა მისაღებია ბლოგებისთვის, რომელსაც მოირგებ).
4. ეცადე იპოვო მენტორი, რომელსაც საქმეს შეუმსუბუქებ, სანაცვლოდ ის გაგიზიარებს თავის ცოდნას, ხოლო როცა დაგჭირდება მისგან რეკომენდაციასაც მიიღებ. ნებისმიერ კარგ ჰაკერს ჭირდება დამხმარე

რუტინული საქმეებისთვის, რომელსაც ადამიანის გარდა სხვა ვერაფერი აგვარებს, ადამიანური რესურსი შეუფასებელია. უბრალოდ რთულია ისეთი ჰაკერის პოვნა, რომელიც მენტორობაზე დაგთანხმდება. ასევე, კარგი მენტორი საკმაოდ ძვირი სიამოვნებაა…

ასეთი ადამიანის დრო ძვირად ფასობს და თუ შენ დროს დაგითმობს, არ უნდა გქონდეს იმედი, რომ ამას უფასოდ გააკეთებს. (მაშინაც თუ მას რაიმე საქმეში ეხმარები, დამიჯერე მისი დრო მაინც იმაზე ძვირი ღირს, ვიდრე შენი დახმარებაა. მას ეხმარები იმისთვის, რომ მისი სიმპათია დაიმსახურო, თავი მოაწონო)

თუ მენტორის ძებნას დაიწყებ, მზად იყავი რომ მისი დროისთვის გადახდა მოგიწევს, მანამდე წიგნები და უფასო ვიდეოები შეასრულებს მენტორის როლს შენთვის.

5. ეცადე აქტიურად ჩანდე იმ საზოგადოებაში, რომლის ნაწილიც შენ იქნები, არ აქვს მნიშვნელობა კონკრეტულ მიმართულებას. შეუერთდი ყველა შესაძლო პროექტს, ორგანიზაციას, ჯგუფს. კომპანიაში მუშაობაზე ღირებული ის პროექტებია, რომელსაც განახორციელებ და საზოგადოება, რომელსაც გაიცნობ. ჩვენ პროფესიაში კავშირები ყველაფერზე მაღლა დგას. იცნობდე ადამიანებს, რომლებსაც სიტყვა ეთქმით და მათ სიტყვას პატივს ცემენ, ამაზე ღირებული არაფერია, თან თუ ასეთი ადამიანები საჭიროების შემთხვევაში რეკომენდაციას გაგიწევენ, ძალიან ბევრი კარი გაგეხსნება.

შეჯამება: დღეს კიბერუსაფრთხოების სფერო საკმაოდ კონკურენტულია, არ დაიჯერო მარკეტინგული ხრიკები, როდესაც ამბობენ, რომ ამ სფეროში მარტივად შეგიძლია დასაქმება და მაღალი ანაზღაურებაა…

თუ მაღალი ანაზღაურება $120-150K ან მეტი გინდა წლიურად იმ კონკურენციის პირობებში, რაც დღეს ბაზარზეა შენი ბრენდი გჭირდება. თავად უნდა იყო ბრენდი.

არ გეუბნები რომ საუკეთესო უნდა იყო, კონტენტი უნდა შექმნა და ასე შემდეგ (თუმცა კონტენტის შექმნა ძალიან დაგეხმარება), მაგრამ რაღაც უნდა გქონდეს ისეთი, რაც სხვებისგან გამოგარჩევს და ღირებულს გაგხდის დამსაქმებლის და მითუმეტეს ჰაკერის თვალში…

თუ ახლა იწყებ, ეს გზა შენთვის რთული იქნება, მარტო ვერ შეძლებ სახელის და ბრენდის შენებას, კონტაქტები, საზოგადოება გჭირდება.

ამიტომ ბოლო რჩევა რაც მექნება, ყველაფერი გააკეთე იმისთვის, რომ საზოგადოებამ და პროფესიონალებმა ყურადღება მოგაქციონ. ოცდამეერთე საუკუნეში ყურადღება განსაზღვრავს თუ რას მიაღწევ და რამდენს გამოიმუშავებ ადამიანი…

“Attention is the new Currency.” - Les Brown

მხოლოდ იმ საკითხებზე შემიძლია რჩევის მოცემა, რაც თავად გადამხდა თავს და რაშიც გამოცდილება მაქვს… ყველა შენ კითხვას პასუხს ვერ გავცემ, მაგრამ ეს ასეც უნდა იყოს… ადამიანი, რომელსაც ყველა კითხვაზე აქვს პასუხი ან თავს ატყუებს ან შენ…

ჩემი გამოცდილება ფსიქოლოგიას და ჰაკინგს მოიცავს. ამ საკითხებზე წიგნის დახმარებით ჩემ გამოცდილებას და რჩევებს გიზიარებ, თუმცა ამაზე მეტს ვერაფერს შევძლებ წიგნის წერის მომენტში. მირჩევნია გაგიზიარო მცირე, მაგრამ საჭირო და საინტერესო ინფორმაცია, ვიდრე ყველაფერს მოვედო და საბოლოოდ წიგნმა არანაირი ღირებულება არ დაგიტოვოს.

ის ყველაფერი, რაც ბოლოს გაგიზიარე, საკუთარი თავის ბრენდად ქცევის ნაწილში, აუცილებლად საკმარისი ყურადღება დაუთმე… მხოლოდ ამ რჩევის გამო ღირდა ამ წიგნის წაკითხვა…

თუ ამ რჩევას გაითვალისწინებ, რაღაც დროის შემდეგ მადლობას მეტყვი. ამ რჩევას მეც ვითვალისწინებ და ნაბიჯ-ნაბიჯ მივყვები, ჯაფარას ბრენდის შენება ზუსტად ამ რჩევის მიღების შემდეგ დავიწყე, თავად ეს წიგნიც ამ მიზანს ემსახურება…

როდესაც საკმარის გამოცდილებას დააგროვებ, შენც დაწერე წიგნი. (იყო წიგნის ავტორი, ეს ცალკე განხილვის თემაა, რომელსაც ამ წიგნთან საერთო არაფერი აქვს, თუმცა ბრენდის შენებაში ისე არაფერი დაგეხმარება, როგორც საკუთარი ნაშრომი, წიგნი, რომელიც სხვა ადამიანებს აჩვენებს სწორ გზას)…

ეთიკური ჰაკინგი
(შეღწევადობის ტესტირება)

შეღწევადობის ტესტირება, ასევე ცნობილი როგორც ეთიკური ჰაკინგი ანუ პენტესტი, არის სისტემის, ქსელის უსაფრთხოების შემოწმების მეთოდი მის წინააღმდეგ კიბერ შეტევების განხორციელების გზით. ეს პროცესი საშუალებას აძლევს **ეთიკურ ჰაკერს** აღმოაჩინოს დაუცველობა, სანამ **ჰაკერი** მიაგნებს და ბოროტად გამოიყენებს მას.

ეთიკური ჰაკერები იყენებენ იგივე ინსტრუმენტებს და ტექნიკას, რასაც შავქუდიანი ჰაკერები და ატარებენ წინასწარ დაგეგმილ ტესტებს დაუცველობის შესამოწმებლად…

მთავარი განსხვავება ეთიკურ ჰაკერსა და შავქუდიან ჰაკერს შორის არის ნებართვა, უფლება. ეთიკურ ჰაკერს აქვს სისტემის გატეხვის უფლება და კომპანია იქით უხდის ეთიკურ ჰაკერს ფულს… შავქუდიანი ჰაკერი პირადი ინტერესების გამო აკეთებს ამ ყველაფერს.

როდესაც ამ პროფესიაში საკმარისად გაერკვევი და იმუშავებ რეალურ პროექტებზე, ხშირად მოგიწევს კრიტიკული გადაწყვეტილების მიღება…

მაგალითად: აღმოაჩინე სისუსტე, რომელიც საშუალებას გაძლევს მავნე პროგრამა გაუშვა ქსელში და სრული კონტროლი მოიპოვო მასზე, მაგრამ ეს მავნე პროგრამა მთლიან ქსელს დააზიანებს და პრობლემებს გამოიწვევს კომპანიაში…

მავნე პროგრამის გაშვება უმარტივესია, ხოლო მისგან გამოწვეული ზიანის განსაზღვრა წინასწარ შეუძლებელი…

ზუსტად ასეთი ქმედებები განსაზღვრავს ჰაკერის პროფესიონალიზმს, ეთიკურ მხარეს და მის ადამიანობას :) იფიქრე საზღვრებს მიღმა, ადამიანური ემოციებით…

მსგავს სიტუაციაში აღმოჩენისას გაიხსენე ჩემი სიტყვები…

“ფაქტი, რომ რაღაცის გატეხვა შეგიძლია, არ ნიშნავს რომ აუცილებლად უნდა გატეხო ის”.

ეთიკური მხარე შეღწევადობის ტესტირებისთვის

შეღწევადობის ტესტირებისას მნიშვნელოვანია წინასწარ განისაზღვროს შემდეგი საკითხები: **ნებართვა, გამჭვირვალობა, კონფიდენციალურობა, პასუხისმგებლობა კრიტიკული ინფორმაციის გამჟღავნების შემთხვევაში და სხვა ფაქტორები.**

შეღწევადობის ტესტირებამდე, ორგანიზაციას ან ფიზიკურ პირს უნდა ქონდეს მკაფიო წერილობითი ნებართვა კლიენტისგან, რომელიც განსაზღვრავს ტესტირების წესებს, ფარგლებს, მეთოდებს, პერიოდს... **დაიმახსოვრე: სიტყვიერი ნებართვა საკმარისი არ არის. სიტყვიერი ნებართვა არ არსებობს!**

შეღწევადობის ტესტერები უნდა მუშაობდნენ კლიენტთან სრული გამჭვირვალობით. კლიენტმა უნდა იცოდეს, როდის ჩატარდება ტესტი, რა სისტემები/აპლიკაციები იქნება საფრთხის ქვეშ, რა მეთოდები იქნება გამოყენებული შეტევის დროს და ვინ ჩაატარებს ტესტს.

შეღწევადობის ტესტირების დროს არ უნდა მოხდეს სენსიტიური მონაცემის შეცვლა, დაზიანება და რაც მთავარია, არ უნდა დაირღვეს კონფიდენციალურობა.

შეღწევადობის ტესტირების დროს არ არის რეკომენდირებული რეალური შეტევების ან ექსპლოიტების გამოყენება, რომლებმაც შეიძლება დააზიანოს სისტემა ან კომპანიის იმიჯი და გამოიწვიოს ფინანსური ზარალი. არსებობს თავდასხმების სიმულაციის გზები სამიზნეზე ზიანის მიყენების გარეშე. (ეს უკვე იცოდი, მაგრამ მაინც გაგიმეორებ)

ყველა აღმოჩენილი დაუცველობა უნდა მიეწოდოს უშუალოდ კლიენტს რაც შეიძლება მალე. დაუცველობის აღმოფხვრამდე მისი საჯაროდ გამჟღავნება დაუშვებელია.

ამ პრინციპების დაცვა უზრუნველყოფს შეღწევადობის ტესტირების განხორციელებას უსაფრთხოდ და ლეგალურად. შეღწევადობის ტესტირება აძლიერებს ორგანიზაციის თავდაცვას და მნიშვნელოვანია ყველა ორგანიზაციისთვის.

შენ კარიერაში უამრავ კრიტიკულ ინფორმაციასთან გექნება. ხშირად გექნება ამ ინფორმაციის გამოყენების სურვილი... დაიმახსოვრე: იმ ინფორმაციას, რასთანაც შენ გექნება შეხება, მთლიანი კომპანიის განადგურება შეუძლია, ძალიან დიდი პასუხისმგელობაა ეს ყველაფერი...

ეთიკური ჰაკერის ტექნიკური უნარები

ეთიკურ ჰაკერს მრავალმხრივი ცოდნა ჭირდება, ამიტომ უამრავ ადამიანს უჭირს სწავლის დაწყება, არ იციან საიდან დაიწყონ და რა ისწავლონ. შენ გაგიმართლა, რადგან რასაც ქვემოთ წაიკითხავ, დაგეხმარება ნაბიჯ-ნაბიჯ მიყვე სწორ გზას და მყარი საფუძველი შეიქმნა ეთიკური ჰაკინგის მიმართულებით.

ლინუქსი (ამით დაიწყე)

- Debian არქიტექტურაზე დაფუძნებული დისტროების ცოდნა (Kali, Parrot)
- კონფიგურაციის ფაილებთან მუშაობა (/etc/hosts, sshd_config, iptables. დაგუგლე რა რას ნიშნავს...)
- ლინუქსის იუზერების, ჯგუფების და უფლებების მართვა
  ეცადე ისწავლო ლინუქსის ადმინისტრირება (საუკეთესო ინვესტიციაა დროის და რესურსების მხრივ დამწყებისთვის, ყველაფერი ლინუქსით იწყება ჩვენ სამყაროში)

ქსელი

- TCP/IP, OSI, Proxy, VPN, TOR, Subnetting.
- ქსელის ხელსაწყოები, როგორიცაა TCPdump, Netcat, Nmap, Aircrack-ng და Wireshark.
- პროტოკოლების ცოდნა, როგორიცაა SNMP, SMB, SMTP, FTP, SSH, HTTP.
- გაეცანი Man-In-the-Middle ინსტრუმენტებს, როგორიცაა Ettercap, Bettercap.

ვები

- ხელსაწყოების ცოდნა: OWASP Zap, Burp Suite, Nikto, WPscan, Metasploit.
- OWASP TOP 10 დაუცველობები, აირჩიე 2-3 მათგანი და დარწმუნდი რომ ძალიან კარგად გეცოდინება მათი მუშაობის პრინციპი, მაგალითად XSS, და SQL Injection.

პაროლების გატეხვა

- ხელსაწყოები: Hydra, John the Ripper, Hashcat, Medusa.

რეპორტის სწორად შედგენა

- რეპორტის წერის მნიშვნელობა – თავიდანვე მიაქციე ყურადღება რეპორტის სწორად შედგენას. საბოლოოდ შენი მთლიანი შესრულებული სამუშაო რეპორტით, მისი ხარისხით განისაზღვრება.

სერტიფიკატი

- ყოველთვის ვამბობდი, რომ სერტიფიკატი ფურცლის ნაგლეჯია, თუმცა არის სერტიფიკატები, რომელიც ბევრ კარს გიხსნის ჩვენ სფეროში. თუ ახლა იწყებ და გინდა წარმატებას უფრო “მარტივად” და სწრაფად მიაღწიო, დაგჭირდება ერთ-ერთი სერტიფიკატი და ეს არის OSCP. სხვა სერტიფიკატი არ ღირს არც დროის დახარჯვად და არც ფინანსურ რესურსად. არ აქვს მნიშვნელობა სხვები რას იტყვიან, რამდენი ადამიანიც არსებობს, იმდენი განსხვავებული აზრი იარსებებს. სხვები გეტყვიან, რომ OSCP სერტიფიკატი დამწყებმა არ უნდა აიღოს... უამრავი დამწყები ადამიანია, რომლებმაც 6–9 თვის ვადაში ყველანაირი წინასწარი ცოდნის და გამოცდილების გარეშე, საკუთარ თავზე მუშაობით აიღეს ეს სერტიფიკატი და თუ საკმარის შრომას ჩადებ, შენც მათ რიცხვში შეხვალ.

  თუ OSCP სერტიფიკატი გექნება, დასაქმება არასდროს გაგიჭირდება.

  თუ ეთიკური ჰაკინგი მოგწონს და გინდა მომავალი ამ პროფესიას დაუკავშირო, არ დაკარგო დრო, უამრავი მასალაა ინტერნეტში, პრაქტიკული მასალები, რომლებიც დაგეხმარება OSCP გამოცდისთვის მომზადებაში. არაფერი იყიდო, ყველაფერი უფასოდ შეგიძლია იპოვო, მთავარია სწორად მოძებნო.

  შეჯამება: ან OSCP ან არაფერი.

  ორ რესურსს გირჩევ _ **tryhackme და hackthebox** (საუკეთესო რესურსებია)

  სანამ უშუალოდ ამ გამოცდისთვის დაიწყებ მზადებას, მანამდე ის საფუძვლები უნდა იცოდე, რაც ზემოთ დავწერე. არ დაუშვა შეცდომა, საფუძვლები კარგად ისწავლე… (შემდეგ თავში გზამკვლევს გაეცნობი)

  თუ ჩემ რჩევას გაითვალისწინებ და საკმარის შრომას ჩადებ საკუთარ თავში, 6-9 თვის შემდეგ ტოპ 1% ჰაკერების სიაში აღმოჩნდები, ეთიკური ჰაკერი იქნები საკმაოდ კარგი ანაზღაურებით… მართალია $1600-1800 დოლარამდე დაგიჯდება ეს ყველაფერი, თუმცა შეხედე ამ ფაქტს როგორც ინვესტიციას. დასაქმების შემდეგ პირველივე თვეში სრულად უკან დაიბრუნებ შენ ინვესტიციას... **უნივერსიტეტში 4 წლის დაკარგვის ნაცვლად, რის შემდეგაც შენი კარიერა ისევ დიდი კითხვის ნიშნის ქვეშ იქნება...** ჰაკინგის მიმართულებით მხოლოდ რამდენიმე თვეს დახარჯავ და ამ პერიოდში შეიძენ უნარებს, რომლებიც

ბაზარზე ყოველთვის მოთხოვნადი და მაღალ ანაზღაურებადი იქნება. დანარჩენი შენ გადაწყვიტე მეგობარო...

პროგრამირება

- ხშირად მეკითხებიან საჭიროა თუ არა პროგრამირების ცოდნა…

  თუ ეთიკური ჰაკერი გინდა გახდე, მაშინ დაგჭირდება. ნებისმიერი ტექნიკური მხარე კიბერუსაფრთხოებაში მოითხოვს პროგრამირების ცოდნას. პითონი ჰაკერების საუკეთესო მეგობარია. პროგრამირების ცოდნით ბევრად უკეთესი ჰაკერი იქნები. ასე რომ გჭირდება, მაგრამ როდესაც დამწყები ხარ, პროგრამირების სწავლა უნდა დაივიწყო… ზუსტად ამ შეცდომას უშვებს დამწყები ადამიანების 99%.

შენიშვნა: თუ სერტიფიკატის აღებას გადაწყვეტ, მინიმუმ OSCP აიღე!

OSCP_ის შემდეგ დაიწყე პითონის ღრმად შესწავლა. რა დონეზე? სანამ საკუთარი Fully Undetectable Malware (დაგუგლე) დაწერას არ შეძლებ.

ისწავლე ნაბიჯ-ნაბიჯ (მინიმუმ 5 საათი ყოველ დღე) :

ლინუქსი > ქსელი > ქსელის პენტესტი > ვების პენტესტი.

ლინუქსს დაუთმე 3-4 კვირა, ტერმინალს შეეჩვიე…

ქსელს დაუთმე 3-4 კვირა…

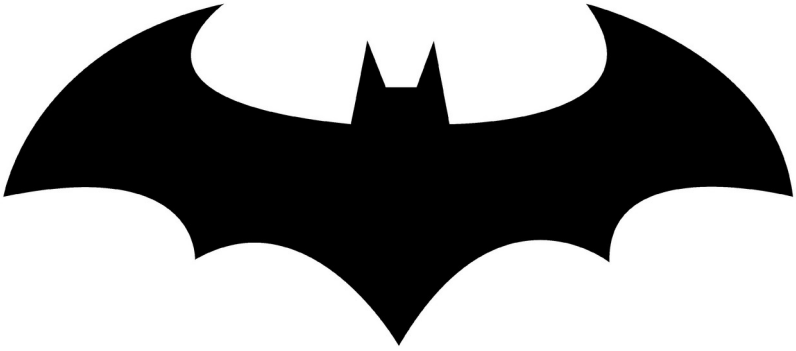
ქსელის პენტესტს დაუთმე 3-4 კვირა. ხელსაწყოები გამოიყენე პრაქტიკაში, ისწავლე რა როგორ მუშაობს.

ვების პენტესტს ასევე 3-4 კვირა დაუთმე (ავტომატური სკანირების ხელსაწყოები) OWASP TOP 10 ის რამდენიმე სისუსტე აირჩიე და კარგად გააანალიზე რა როგორ მუშაობს.

ჯამში 12-16 კვირა გამოდის ამ ყველაფრისთვის. ეს დრო საკმარისი იქნება იმისთვის, რომ აზრზე მოხვიდე. ეს ზოგადი პერიოდი დავწერე, იმდენი დრო დაუთმე კონკრეტულ საკითხს, რამდენსაც საჭიროდ ჩათვლი, თუმცა ძალიან არ გაწელო, თითო საკითხზე მაქსიმუმ 4-5 კვირა…

არასწორად არ გაიგო… ამ ცოდნით OSCP ის ვერ ჩააბარებ. ეს მხოლოდ კარგი საფუძველი იქნება, რომელსაც 2-3 თვეში შეიქმნი. ამ საფუძვლით შეძლებ OSCP ის შესაბამისი სასწავლი რესურსების გაგებას, მოძიებას და შემდგომ განვითარებას…

აირჩიე შენი გზა



რატომ ბეტმენი?

ბეტმენი იდეალური პერსონაჟია. ის გარკვეული მიზნით შექმნა ბრიუს ვეინმა… მართალია ბეტმენის და ბრიუსის უკან ერთი ადამიანი დგას, თუმცა განსხვავებული მიზანი და გზა აქვს ორივე პერსონაჟს…

რისი თქმა მინდა?

ბრიუსი თავის საქმეს აკეთებს, თან იდეალურად, მაგრამ მას ნიღაბი ჭირდება მისთვის ძვირფასი ადამიანების დასაცავად, სწორედ ამიტომ ახალი ვინაობა შექმნა ბეტმენის სახით.

იგივე გავაკეთე მეც, ჯაფარა ვინაობაა, რომელიც ჩემი მიზნების მიღწევაში მეხმარება, ჯაფარაც გარკვეული მიზნით შეიქმნა...

როგორც პიროვნებებს, ჩვენ ყველას ვალდებულებები გვაქვს. ეს ვალდებულებები არ გვაძლევს შესაძლებლობას ბოლომდე გამოვავლინოთ ჩვენი პოტენციალი. ზუსტად ამიტომ გვჭირდება ვინაობა, რომელსაც არანაირი ვალდებულება არ ექნება…

შექმენი ვინაობა, პიროვნება, რომელიც თავისუფალი იქნება და აქციე ეს პიროვნება ბრენდად.

ბეტმენმა მოახერხა საკუთარი თავის განვითარება, არაფრიდან დაიწყო და ბოლოს გმირი გახდა… მან ურთულესი გზა გაიარა და უნდა გესმოდეს, რომ წარმატებისკენ მიმავალი გზა ისეთივე რთული იქნება შენთვის, როგორიც ეს ბრიუსისთვის იყო…

რაც უფრო მალე გაერკვევი შენ თავში და მიზნებში, უფრო მალე მიაღწევ წარმატებას:

1. მიზანი _ რა არის შენი მიზანი? ვინ გინდა რომ გახდე? გინდა საუკეთესო იყო თუ საშუალო დონეც საკმარისი იქნება შენთვის? რამდენად დიდია შენი მიზანი?

2. შრომა _ ბეტმენს ფიზიკური ფორმა, სისწრაფე და ძალა ჭირდებოდა და ამისთვის ბრიუსი ყველაფერს აკეთებდა. საუკეთესოებისგან ისწავლა, ბოლომდე იხარჯებოდა ყოველდღიურად მიზნების მისაღწევად…

შენ რისთვის ხარ მზად? მართალია შენ არ გჭირდება ფიზიკური ფორმა იმისთვის, რომ ჰაკერი გახდე, თუმცა შენ გონებას ჭირდება ძალიან ბევრი ვარჯიში, რომელიც შეიძლება ფიზიკურ ვარჯიშზე უფრო რთული აღმოჩნდეს… მთავარია ხვალ იმაზე უკეთესი იყო, ვიდრე დღეს ხარ. მხოლოდ ამ გზით შეგიძლია მიაღწიო საუკეთესო შედეგს. საბედნიეროდ, შენ შეძლებ საკუთარი პროგრესის დანახვას მომენტალურად, რაც მოტივაციას მოგცემს… მთავარია წარმატების რამდენად ძლიერი სურვილით ხარ შეპყრობილი და რისი დათმობა შეგიძლია წარმატებისთვის.

3. უნარების გაუმჯობესება _ ჩვენ ვიცით, რომ ბეტმენი საკუთარ უნარებს, ისევე როგორც საკუთარ “სათამაშოებს” მუდმივად საჭიროების მიხედვით აუმჯობესებდა შესაბამისი ხალხის დახმარებით.

ანალოგიურად, შენც უნდა განაახლო შენი უნარები, სანაცნობო წრე და ცოდნა… შეიძლება ეს დამოუკიდებლად შეძლო, მაგრამ მიხვალ იმ დონემდე, როდესაც გამოცდილი ადამიანის, მენტორის დახმარება დაგჭირდება… მე გამიმართლა და ვიპოვე ადამიანი, რომელმაც რთულ მომენტებში მენტორობა გამიწია… იმედი მაქვს შენც იპოვი…

4. პრობლემის გადაჭრა _ ჩვენი ყოველდღიურობაა… მუდმივად პრობლემები გექნება და მუდამ მათი გადაჭრა მოგიწევს. ავარჯიშე შენი გონება ნებისმიერი გზით, ნებისმიერი რესურსით. ყოველთვის შეხედე პრობლემას საზღვრებს მიღმა (Lateral Thinking). მოძებნე სავარჯიშოები და აკეთე ისინი… მართალია ადამიანის ინტელექტი გენეტიკურია, თუმცა მისი გაუმჯობესება შესაძლებელია…

5. Monk Mode _ ალბათ სადმე მაინც მოგიკრავს ამ ორი სიტყვისთვის ყური… ეს არის პერიოდი, რომლის დროსაც შენ განსაკუთრებულად ფოკუსირებული ხარ კონკრეტულ მიზანზე და აკეთებ ყველაფერს, რაც საჭიროა ამ მიზნის მისაღწევად წუწუნის და ფიქრის გარეშე. ზუსტად ამას გავაკეთებთ:

შენ თითქმის დაასრულე ამ წიგნის კითხვა, მალე დაასრულებ. წიგნის დასრულებიდან 24 საათი კრიტიკულად მნიშვნელოვანია, ამ 24 საათში შენ გააკეთებ იმას, რაც საჭიროა ან გადადებ ამ წიგნს და დაივიწყებ ყველაფერს რაც წაიკითხე… (ასეა ადამიანის გონება მოწყობილი, სამწუხაროდ)

იმედი მაქვს ყველაფერს გააკეთებ, რაც საჭიროა. თუ ასეა მაშინ შენთვის შევქმენი Monk Mode, რომელიც საწყისებს გასწავლის:

დრო – 1 თვე

ლინუქსი

1. პირველი დონე

www.netacad.com/courses/os-it/ndg-linux-unhatched

2. მეორე დონე

www.netacad.com/courses/os-it/ndg-linux-essentials

დამხმარე რესურსი პრაქტიკისთვის: https://linuxjourney.com/

კიბერუსაფრთხოება

3. პირველი დონე

www.netacad.com/courses/cybersecurity/introduction-cybersecurity

4. მეორე დონე

www.netacad.com/courses/cybersecurity/cybersecurity-essentials

ქსელი

www.netacad.com/courses/networking/networking-essentials

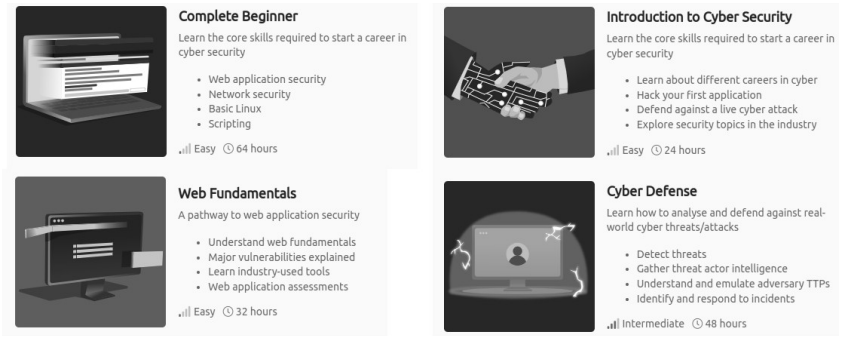
საშუალოდ 140-160 საათი დაგჭირდება, დღეში 5 საათს თუ დაუთმობ 1 თვე გეყოფა ამ ყველაფრის გასავლელად. (ყველაფერი უფასოა)

1 თვე გაქვს და ამ დროის ათვლა დაიწყება წიგნის დასრულების მომენტიდან… შენი პირველი გამოცდაა, თუ ამ გამოცდას ჩააბარებ, სიამაყის უფლება გექნება და შეძლებ გააგრძელო განვითარება…

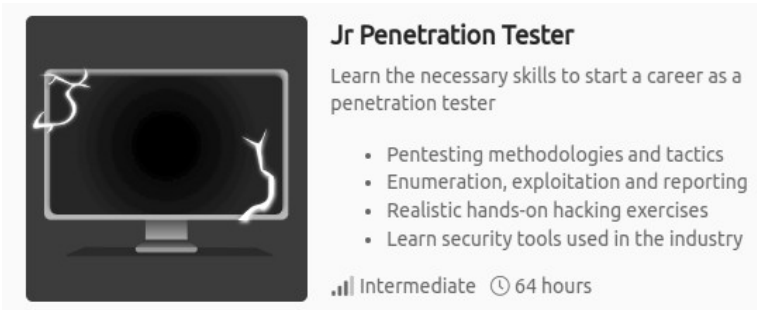
თუ ამ ყველაფერს წარმატებით დაასრულებ, მეორე ეტაპზე გადახვალ.

დარეგისტრირდი tryhackme.com/hacktivities პლატფორმაზე, იყიდე პრემიუმ პაკეტი (აუცილებელია) და შემდეგი 1 თვე ამ პლატფორმაზე გაატარე…

ისევ 5 საათი დღეში. **დრო – 1 თვე**



შემდეგი 1 თვე ამ ოთხი აქტივობის გავლას დაუთმე. ეს ყველაფერი შეგიქმნის მყარ საფუძველს და შეძლებ ჯუნიორ შეღწევადობის ტესტერის აქტივობის გავლას



თუ ამ ყველაფერს (მთლიანი Monk Mode) 60 დღეში გაივლი (დღეში 5-5.30 საათის დათმობის შემთხვევაში ასე უწევს) შემიძლია გარანტია მოგცე, რომ 60 დღის შემდეგ შენ იმაზე მეტი გეცოდინება, ვიდრე დამწყები ჰაკერების 99%_მა იცის. (სწავლის დაწყებიდან 110-120 დღის შემდეგ)

არ დაგავიწყდეს ლინკდინის ნაწილი, პარალელურად ლინკდინზე იაქტიურე… დატვირთული 60-70 დღე გელოდება :) დაიმახსოვრე, შენი მიზანი ამ ყველაფრის გავლა არაა, შენი მიზანი ცოდნის მიღებაა უმოკლეს ვადებში და მე ამაში გეხმარები!

ამ ყველაფრის გავლა აუცილებელია, თუ ჩვენი კლუბის წევრობას გადაწყვეტ… მეტი დეტალისთვის გადახედე: ge.hackersforce.com

OSCP გამოცდის ჩასაბარებლად საშუალოდ დამწყებს (რომელმაც იცის ის მინიმალური, რაც Monk Mode_ში შედის) დაახლოებით 400-450-500 საათი ჭირდება პრაქტიკა… (სწორი პრაქტიკა, სწორი რჩევებით)

თუ შენ Monk Mode გაივლი და იმ ცოდნას მიიღებ, რაც მას შეუძლია მოგცეს + 400-450-500 საათს პრაქტიკულ დავალებებზე დახარჯავ, შენ დიდი ალბათობით შეძლებ OSCP სერტიფიკატის აღებას… სერტიფიკატის აღების შემდეგ შენ გარანტირებული გექნება წარმატებული კარიერა...

პრაქტიკული გამოცდილება + პორტფოლიო

ყველაფერთან ერთად აუცილებელია შენი ცოდნის მარტივად დემონსტრირება შეგეძლოს, რადგან პოტენციურ დამსაქმებელს არ აქვს ბევრი დრო...

პორტფოლიოს შესაქმნელად HackTheBox პლატფორმას გამოვიყენებთ, რადგან საუკეთესოა დღეს არსებულ სხვა პლატფორმებთან შედარებით… (სასურველია 1 წლიანი პაკეტი იყიდო, რომელიც წიგნის წერის მომენტში 135$ ღირს … ან თვეში 14$)

ამ პლატფორმაზე ბევრი ისეთი რესურსია, რომელიც OSCP გამოცდის ჩაბარებაში დაგეხმარება. OSCP სერტიფიკატის აღების შემდეგ აღმოაჩენ, რომ ეთიკური ჰაკინგი ბევრად უფრო ვრცელი სამყაროა, ვიდრე OSCP ფარავს… იმ სიცარიელეს, რასაც OSCP ვერ დაფარავს HackTheBox შეგივსებს…

პორტფოლიოს შექმნას იწყებ აქედან academy.hackthebox.com/catalogue და გაივლი ყველაფერს, რისი გავლაც შესაძლებელი იქნება დროის იმ მონაკვეთში, რომელიც შენ გექნება… რაც უფრო მეტს გაივლი, უფრო მეტი გამოცდილება და ცოდნა დაგრჩება (ლოგიკურად).

თუ თავს ამ სამყაროში შემოყოფ უნდა იცოდე, რომ შენი ყოველი დღე დატვირთული იქნება, მუდმივად განვითარებაა საჭირო ამ სამყაროში, თუ არ განვითარდები, სხვები განვითარდებიან და კონკურენციას მათ დიდხანს ვერ გაუწევ…

როცა Tryhackme_ზე გაივლი ზემოთ ნახსენებ კურსს, მისი შესაფერისი პრაქტიკული დავალებები უნდა გააკეთო HackTheBox პლატფორმაზე…

გამოიყენე Tryhackme პლატფორმა სასწავლად, HackTheBox პრაქტიკისთვის… ორივე პლატფორმა მნიშვნელოვანია და დამსაქმებლები ორივე პლატფორმას აფასებენ, თუ ის შენ ცოდნას სწორად და კარგად წარმოაჩენს…

ბონუსი: academy.tcm-sec.com მათი კურსები იდეალურად ავსებს იმ ცოდნას, რომელიც OSCP გამოცდის ჩასაბარებლად არის საჭირო…

(ამ პლატფორმის გამოყენება წიგნის წერის მომენტში 30$ ღირს თვეში… 3 თვე ამ პლატფორმაზე შენთვის საჭირო კურსების გავლისთვის საკმარისი იქნება)

უფასოდაც მიაგნებ მათ კურსებს ინტერნეტში (Torrent), თუმცა უახლესი ვერსია მხოლოდ ოფიციალურ საიტზეა ხელმისაწვდომი.

ისტორია ბიჭზე, რომელმაც ნასა და პენტაგონი “გატეხა” – ჯონათან ჯეიმსი

ნამდვილი ისტორიის მოსმენის დროა. ისტორიის ბოლოს მნიშვნელოვან რჩევებს მოისმენ… ახლა კი გაეცანი ისტორიას.

ნამდვილი სახელი: ჯონათან ჯეიმსი

მეტსახელი ინტერნეტში: c0mrade

ჯონათან ჯეიმსი იყო ახალგაზრდა ჰაკერი, რომელმაც მოახერხა ნასას და პენტაგონის გატეხვა. ის გახდა პირველი არასრულწლოვანი, რომელსაც მიესაჯა პატიმრობა კომპიუტერის გატეხვისთვის.

ჯონათან ჯეიმსი დაიბადა 1983 წლის 12 დეკემბერს, პატარა სოფელში, ფლორიდაში.

ჯონათანს კომპიუტერების მიმართ დიდი ინტერესი ქონდა 6 წლის ასაკიდან. ის ხშირად იყენებდა მამის კომპიუტერს ვიდეო თამაშებისთვის. მამამისი პროგრამისტი იყო.

ჯონათანის ინტერესები მის ასაკთან ერთად თანდათან შეიცვალა, მისი ინტერესები თამაშებით დაიწყო, თუმცა ბოლოს C ენა ისწავლა.

15 წლის ასაკში ჯონათანს საკმარისი ცოდნა დაუგროვდა და მოახერხა საკუთარი სასწავლებლის გატეხვა, ამის შემდეგ მან უფრო დიდი მიზნები დაისახა.

მისი პირველი სამიზნე გახდა AT&T BellSouth, ერთ-ერთი უდიდესი სატელეკომუნიკაციო კომპანია იმ დროისთვის აშშ-ში. ჯონათანმა გატეხა კომპანიის სერვერები, თუმცა არაფერი დაუზიანებია, მისთვის ეს ქმედება საკუთარი შესაძლებლობების გამოცდა იყო.

1999 წლის ივნისი იყო, ჯონათანი ეძებდა დაუცველ სერვერებს მსოფლიოს მასშტაბით, რათა გაეტეხა ისინი ფაიერვოლის გვერდის ავლით. მან აღმოაჩინე ასეთი სერვერი ჰანტსვილში, ალაბამაში (Huntsville, Alabama). ჯონათანმა მოახერხა სერვერის გატეხვა და დააყენა მავნე პროგრამა. ასევე

შეძლო საკუთარი უფლებების გაფართოება ქსელში და 13 კომპიუტერის გატეხვა. მოგვიანებით გაირკვა, რომ ეს ქსელი ეკუთნოდა NASA-ს.

მას შემდეგ, რაც NASA-ს უსაფრთხოების ექსპერტებმა აღმოაჩინეს, რომ მათი ქსელი დაზიანებული იყო, მოუწიათ სერვერის გათიშვა 3 კვირით. ამ ქმედების გამო NASA-მ 40 ათასი დოლარი დაკარგა.

NASA-მ დაიწყო თანამშრომლობა FBI-სთან, რადგან ორივე მხარეს სურდა "საშიში" ჰაკერის პოვნა. ჯონათანი ამ დროს მხოლოდ სკოლის მოსწავლე იყო :)

1999 წლის სექტემბერში ჯონათანმა აღმოაჩინა ბექდორი (backdoor) სერვერზე დულსში, ვირჯინიაში (Dulles, Virginia). ბექდორი სერვერთან დაკავშირების საშუალებას აძლევდა ნებისმიერ იუზერს ინტერნეტში. ჯონათანს ბევრი არ უფიქრია, დაუკავშირდა სერვერს და დააყენა sniffing პროგრამა. მოგვიანებით გაირკვა, რომ ეს სერვერი ეკუთვნოდა DTRA-ს (თავდაცვის საფრთხის შემცირების სააგენტოს, Defense Threat Reduction Agency), აშშ-ს თავდაცვის დეპარტამენტის უაღრესად მნიშვნელოვან განყოფილებას, რომელიც აანალიზებდა გარე საფრთხეებს ქვეყნის ეროვნული უსაფრთხოებისთვის. ჯონათანმა კიდევ 10 კომპიუტერის გატეხვა მოახერხა ამ სააგენტოში, რაც უყურადღებოდ არ დარჩენილა. ეს იყო პირველი შემთხვევა, როდესაც ჰაკერმა პენტაგონის ერთ-ერთი დანაყოფის ქსელის გატეხვა მოახერხა.

2000 წლის იანვარში თავდაცვის დეპარტამენტის აგენტებმა პოლიციასთან ერთად ჯონათანის დაპატიმრების ბრძანება გასცეს. 26 იანვარს აგენტები ტყვიაგაუმტარი ჟილეტებით და იარაღით შეიჭრნენ მის სახლში და დააკავეს ის. მათ სახლიდან ოთხი კომპიუტერი, ლეპტოპი და ერთი მცირე ზომის "ჯიბის" კომპიუტერი ამოიღეს.

ამ ფაქტმა ჯონათანი აქცია პირველ არასრულწლოვნად, რომელსაც მიესაჯა პატიმრობა კომპიუტერის გატეხვისთვის. ჯონათანი აქტიურად თანამშრომლობდა გამომძიებლებთან და დეტალურად უხსნიდა მათ, თუ როგორ შეძლო მათი სისტემის გატეხვა.

გამოძიების დროს გაირკვა, რომ ჯონათანს არცერთი სისტემის გატეხვის შემდეგ არ დაუზიანებია ფაილები. ვინაიდან ის 16 წლის იყო, მძიმე განაჩენი ვერ გამოუტანეს. ის სრულწლოვანი რომ ყოფილიყო 10+ წლიან პატიმრობას მინიმუმ მიუსჯიდნენ. ვინაიდან მან გამოძიებასთან ითანამშრომლა და ასევე

ეხმარებოდა ნასას და პენტაგონს, მხოლოდ 6 თვიანი შიდა პატიმრობა მიუსაჯეს, ხოლო კომპიუტერის გამოყენება აეკრძალა ნებისმიერი საქმიანობისთვის რამდენიმე წლით, გარდა სწავლისა (ეს უფლება დაუტოვეს).

2007 წლის იანვარში ამერიკის საიდუმლო სამსახური იმყოფებოდა დიდი კიბერ დაჯგუფების კვალზე, რომელსაც ხელმძღვანელობდა ალბერტ გონსალესი. ის პასუხისმგებელი იყო საკრედიტო ბარათების მასიურ მოპარვაზე. (ჰაკერებმა მოიპარეს მილიონობით მომხმარებლის საკრედიტო ბარათის ინფორმაცია და არალეგალურად გამოიყენეს).

ჯონათანის რამდენიმე მეგობარი ამ დაჯგუფების წევრი იყო. საიდუმლო სამსახურთან რამდენიმე მათგანმა თქვა, რომ ჯონათანს იცნობდნენ ჰაკერული ფორუმებიდან.

გამომძიებლებს ჯონათანის მიმართ ეჭვი გაუჩნდათ. ასევე მოგვიანებით გაირკვა, რომ გამომძიებლები ეძებდნენ უცნობ ჰაკერს ფსევდონიმით "ჯჯ". ფსევდონიმი ჯონათანის (ჯონათან ჯეიმსი) ინიციალებს დაემთხვა და ეს ფაქტი საკმარისი აღმოჩნდა იმისთვის, რომ საიდუმლო სამსახურს მისი სახლის ჩხრეკის ორდერი გაეცა.

2007 წლის იანვარში, საიდუმლო სამსახურის აგენტებმა დაარბიეს ჯონათანის, მისი ძმის და მისი შეყვარებულის სახლები, რათა გამოეკვლიათ ჯონათანის როლი საკრედიტო ბარათების მოპარვაში. ჯონათანის სახლის დარბევის დროს საიდუმლო სამსახურის წარმომადგენლებმა იპოვეს იარაღი და ჩანაწერი ჯონათანის წინა თვითმკვლელობის მცდელობიდან.

მოგვიანებით გაირკვა, რომ უცნობი ჰაკერი ფსევდონიმით "ჯჯ" იყო სტივენ უოტსი, რომელიც წარმატებული შეტევების შემდეგ ხშირად ტოვებდა კვალს ქსელში ფსევდონიმით "ჯიმ ჯონსი".

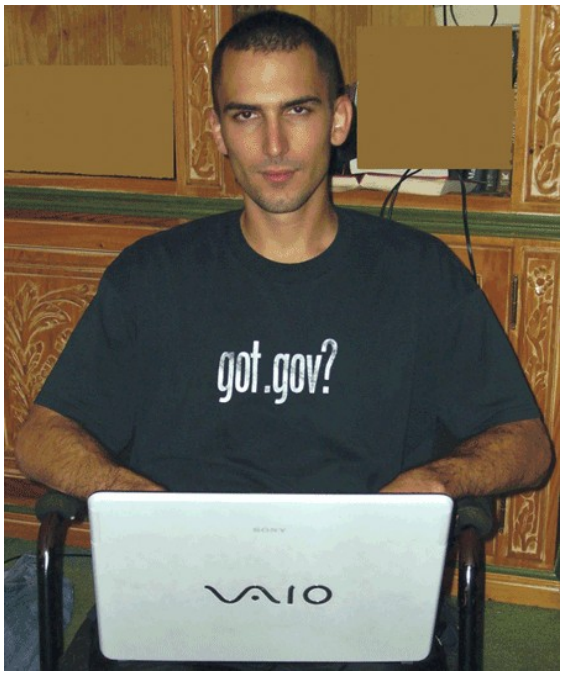
აგენტებმა ვერ იპოვეს ვერანაირი დამამტკიცებელი საბუთი, რომელიც დააკავშირებდა ჯონათანს მიმდინარე დანაშაულებთან, ნაპოვნი იარაღი ასევე ოფიციალურად იყო დარეგისტრირებული.

ჯონათანს მძიმე დეპრესია დაემართა საიდუმლო სამსახურთან მომხდარი ინციდენტების შემდეგ. ყოველ წამს ფიქრობდა რომ დააკავებდნენ, მუდამ ეჭვებში იყო. სწორედ ამ ფაქტმა გამოიწვია მისი სუიციდი…

2008 წლის 18 მაისს ჯონათანი გარდაცვლილი იპოვეს საკუთარი სახლის აბაზანაში, თავში ცეცხლსასროლი იარაღით მიყენებული ჭრილობით იმავე იარაღიდან, რომელიც აგენტებმა აღმოაჩინეს ბოლო დარბევის დროს.

გვამთან ერთად იპოვეს თვითმკვლელობის ჩანაწერი Paypal-ის პაროლთან და რამდენიმე სხვა ანგარიშთან ერთად, სადაც ფული ინახებოდა.

წერილში ეწერა (ორიგინალი წერილი):



“I do not believe in our ‘justice’ system – perhaps my actions today and this letter will be a serious signal to the public, but I have lost control of the situation, and this is my only way to fix it. To be honest, I have nothing to do with this whole TJX story. Even though Chris (Scott) and Albert Gonzales are the most dangerous and destructive hackers the feds have ever caught, I am far more seductive [as a victim] to public opinion than these two random idiots. That is life. Remember, it’s not that you win or lose, but that I personally win or lose by being in prison for 20, 10, or even 5 years for a crime that I didn’t commit. This is my way of winning, but at least I’ll die free. “

“მე არ მჯერა ჩვენი “სამართლის” სისტემის, თუმცა ჩემი ქმედებები დღეს და ეს წერილი იქნება სერიოზული სიგნალი ხალხისთვის, პუბლიკისთვის. სიტუაციამ კონტროლი დაკარგა და ეს ერთადერთი გზაა, რითიც შემიძლია მდგომარეობა გამოვასწორო. სიმართლე გითხრათ, მე არაფერი მაქვს საერთო TJX-ის ამბავთან. მიუხედავად იმისა, რომ კრისი (სკოტი) და ალბერტ გონსალესი ყველაზე საშიში და დამანგრეველი ჰაკერები არიან, რომლებიც აგენტებს ოდესმე დაუჭერიათ, მე გაცილებით საყურადღებო ვარ [როგორც მსხვერპლი], ვიდრე ეს ორი შემთხვევითი იდიოტი. ეს არის ცხოვრება. დაიმახსოვრე, საქმე არ ეხება მოგებას ან წაგებას, პირადად მე მოვიგებ თუ წავაგებ ციხეში 20, 10 ან თუნდაც 5 წლით ჯდომით იმ დანაშაულის გამო, რომელიც არც კი ჩამიდენია. ეს არის ჩემი გამარჯვების გზა, მაგრამ მაინც მე თავისუფალი მოვკვდები.”

სამწუხარო ისტორიაა, დიდი ნიჭი დაკარგა მსოფლიომ… ეს ისტორია

გარკვეული მიზნით გაგიზიარე, იმედია დაგაფიქრებს შენ ქმედებებზე მომავალში. ახლა კი დროა რამდენიმე რჩევა მოისმინო ამ ისტორიიდან:

1. ჯონათანი ზედმეტად შორს წავიდა, უაზროდ რისკავდა. რამდენიმე შანსი მიეცა გამოსწორების, თუმცა ვერ გამოიყენა.
2. მან საკუთარი ქმედებებით დიდი სახელი მოიპოვა და სწორად რომ წარემართა საკუთარი ცხოვრება, უფრო დიდ კვალს დატოვებდა მსოფლიოში.
3. მისმა ქმედებებმა წარსულიდან ის ავტომატურ სამიზნედ აქცია. მაშინაც კი, როდესაც მასზე არანაირი სამხილი არ არსებობდა, ეჭვების გამო მისი სახლი დაარბიეს, მხოლოდ იმ მიზეზით, რომ მის სახელთან წარსულში მრავალი დანაშაული იყო დაკავშირებული. (ამიტომ უნდა იყოს შენი სახელი სუფთა)
4. ის ტეხავდა სისტემებს საკმარისი ინფორმაციის გარეშე. (ყოველთვის საკმარისი ინფორმაცია მოიძიე სამიზნეზე, როდესაც რამეს დააპირებ, კანონის ფარგლებში ან მის მიღმა...)
5. ჯონათანი მისმა სუსტმა ფსიქოლოგიურმა მდგომარეობამ დაღუპა... სუიციდი გაუმართლებელია, შეეძლო დახმარება ეთხოვა, თუმცა მარტივი გზა აირჩია.

კარგად დაფიქრდი მეგობარო ამ ისტორიაზე, ბევრი გაკვეთილის სწავლა შეგიძლია და იმედი მაქვს ისწავლი... არ ვიცი სად აღმოჩნდები მომავალში, მაგრამ ნამდვილად არ მინდა ჯონათანის ბედი გაიზიარო და ალბათ არც შენ... (სამწუხაროდ ბევრი მსგავსად ასრულებს მხოლოდ იმიტომ, რომ საკუთარ თავს ვერ აკონტროლებენ, საკუთარ ქცევებს...).

უამრავ მოწადინებულ, მცოდნე ადამიანს შევხვედრივარ, რომლებსაც დიდი პოტენციალი ქონდათ, მაგრამ ისეთ სისულელეებს აკეთებდნენ... თავისუფლებას რისკავდნენ არაფრის გამო. არაფერი გააკეთო ისეთი, რასაც შენი ცხოვრების დანგრევა შეუძლია. ბევრჯერ გამოვიყენე ეს სიტყვები (ცხოვრების დანგრევა) ამ წიგნში... დაფიქრდი...

როდესაც იცი, თუ რა მარტივად შეიძლება სისტემის გატეხვა, აუცილებელია საკუთარი თავის კონტროლი შეძლო. ერთმა “პატარა” შემთხვევამ შეიძლება პრობლემები შეგიქმნას მთელი ცხოვრება... თუ ერთხელ მოხვდი სიაში, რომელში მოხვედრასაც არავის ვუსურვებ, მთელი ცხოვრება ყველა ეჭვის თვალით შემოგხედავს...

ამიტომ ყოველი ქმედებისას, ყოველი ბრძანების გაშვებისას ტერმინალში, სანამ Enter_ს დააწვები დაფიქრდი, ეს კონკრეტული ქმედება ხომ არ გავს ჯონათანის ისტორიიდან რომელიმე მონაკვეთს. როგორც კი ბრძანებას გაუშვებ, მას ვეღარ შეაჩერებ, შენი რაღაც კვალი დარჩება ინტერნეტში და თუ არ იცი როგორ დარჩე სუფთა, როგორ დაფაროო საკუთარი კვალი, ვიღაც კარზე აუცილებლად მოგიკაკუნებს და კარგად არ დასრულდება შენი ამბავი.

ამას ვწერ იმიტომ, რომ შეიძლება არასრულწლოვანი იყო, არ გეშინოდეს კანონის და გარისკო უკანონო ქმედება, მაგრამ გეტყვი რომ უნდა გეშინოდეს… არ გატესტო შენი შესაძლებლობები რეალურ გარემოში რეალურ სამიზნეზე უფლების გარეშე… მთელი ამ ისტორიის გაზიარების მიზანი ის იყო, რომ დამენახებინა შენთვის თუ რა შედეგი შეიძლება მოყვეს უკანონო ქმედებებს. საბოლოოდ მივედით იმ აზრამდე, რომ უკანონო ქმედებები სიცოცხლის, თავისუფლების ფასად შეიძლება დაგიჯდეს… ახლა უკვე იცი რისკები და ალბათ არ გენდომება საკუთარი ცხოვრების გარისკვა არაფრის გამო…

ამ რჩევას ყველა არ მოგცემს, პირიქით… უმეტესობა გეტყვის რომ სახელის გამო ყველაფერი გააკეთო, მე გეუბნები რომ სახელის გამო შეგიძლია რაღაცეები გააკეთო, მაგრამ შენი საზღვრები უნდა იცოდე…

ერთ ადამიანს ვიცნობდი, ინტერნეტში გავიცანი, ვასწავლიდი, რაღაცეებს მისგანაც ვსწავლობდი… ჭკვიანი ბიჭი იყო, მაგრამ ზუსტად ის შეცდომა დაუშვა, რაც ზემოთ დავწერე. ზედმეტად შორს წავიდა, კანონები დაიკიდა, ყველაფერს ტეხავდა, სახელის გამო ყველაფერს აკეთებდა… შემდეგ დააპატიმრეს, ახლა ციხეში ზის და სასჯელს იხდის. იცი რატომ დააპატიმრეს? მართალია საკუთარ კვალს ფარავდა, მაგრამ სანაცნობოში მოინდომა მაგარ ტიპად გამოჩენა, მეგობრებს უყვებოდა საკუთარ საქმეებზე… ყველას გააგებინა საკუთარი შესაძლებლობების შესახებ და სწორედ მანდ შეცდა… რამდენიმე თვის შემდეგ კარზე მიუკაკუნეს და იმაზე მეტი “შეეტენა”, ვიდრე რეალობაში გააკეთა… ეს ამბავი წლების წინ მოხდა.

ხშირად გთხოვენ რაღაცის გატეხვას, როდესაც მიაღწევ გარკვეულ დონეს… არასდროს არავის დაეხმარო, არავინ იცის ვინ დგას კომპიუტერის მიღმა. არც ფულის სანაცვლოდ გააკეთო უკანონო ქმედება… ფულის შოვნის მილიონი კანონიერი მეთოდი არსებობს, ნუ აირჩევ სარისკო, უკანონო გზას…

ჯაფარას ორგანიზაცია

HackersForce.com

ჯაფარას ორგანიზაცია

ჩემ მიზანზე დავწერე დასაწყისში, თუ არ გახსოვს გავიმეორებ...

“**ჯაფარა ქმნის ორგანიზაციას (HackersForce), რომელიც გლობალურ პროექტებზე მუშაობს ეთიკური გზებით, ამ ორგანიზაციას მსოფლიოს საუკეთესო ჰაკერები მართავენ.**“

საზოგადოებას ერთად დიდი ძალა აქვს. სწორედ საზოგადოებაზე ვაშენებ ჩემ ორგანიზაციას, სახელშიც ჩანს ეს ყველაფერი...

Hackersforce.com

HackersForce მისიაა მსოფლიოს მასშტაბით პოტენციალის მქონე ჰაკერების გაერთიანება და მათი გაძლიერება ცოდნით, რესურსებით და კავშირებით.

HackersForce ქმნის რევოლუციურ საგანმანათლებლო პროგრამას, “**Hackers Accelerator**”. ამ პროგრამის მიზანია დამწყები, პოტენციალის მქონე საზოგადოების სწორად განვითარება, ყველანაირი წინასწარი ცოდნის გარეშე **HackersForce** მათგან TOP ჰაკერებს შექმნის.

HackersForce ეკოსისტემაა, სადაც TOP ჰაკერები ასწავლიან დამწყებ ჰაკერებს ჰაკინგს. ორგანიზაცია საზოგადოებაზე და ხარისხზე შენდება. ნებისმიერი რამ, რასაც მომავალში **HackersForce** შემოგთავაზებს, შეგიძლია ენდო მის ხარისხს.

HackersForce ჩემი უმთავრესი მიზანია. ამ მიზნის თითოეული დეტალი დაწვრილებით ვიცი, ჩემ წარმოსახვაში არსებობს და ნელ-ნელა

წარმოსახვიდან რეალობაში გადმომაქვს.

ეს ყველაფერი საქართველოდან დაიწყო წლების წინ, ხოლო შენ გაქვს შესაძლებლობა მისი ნაწილი გახდე ადრეული ეტაპიდან (2024 წლის იანვრიდან)

HackersForce საქართველოში ფიზიკური კლუბია, სადაც ერთად დროის გატარებას და განვითარებას შეძლებენ დამწყები და პროფესიონალი ჰაკერები…

გლობალურად **HackersForce** მოგვიანებით გაეშვება, როდესაც ყველაფერი მზად იქნება…

ქართველი საზოგადოებისთვის მინდა რაღაც ღირებული შევქმნა, ვფიქრობ საერთო სივრცე ზუსტად ის არის, რაც ყველაზე მეტად ჭირდება დამწყებ ჰაკერს :)

გადახედე საიტს თუ ხელმისაწვდომი იქნება ამ ყველაფრის კითხვის მომენტში და შემოგვიერთდი… ყველაფერი გააკეთე შენი შესაძლებლობების ფარგლებში იმისთვის, რომ ჩვენი ნაწილი გახდე. **(hackersforce.com)**

გახსოვს დასაწყისში რა გითხარი? იმისთვის, რომ რაღაცას რეალობაში მიაღწიო, ჯერ საკუთარ წარმოსახვაში უნდა შეძლო მთლიანი სურათის დანახვა. ყველა რჩევა, რაც აქამდე მოგეცი. დარწმუნებული იყავი, რომ თავადაც ვითვალისწინებ.

წიგნის გაგრძელება იქნება...

რაც აქამდე წაიკითხე, თეორია იყო, საჭირო თეორია... დაწერილი ადამიანებისთვის, რომლებსაც ჩვენი სამყარო აინტერესებდათ ან ჰაკერებისგან თავის დაცვა სურდათ...

ბევრი ფიქრის შემდეგ მივედი დასკვნამდე, რომ წიგნის პრაქტიკული ნაწილი ამ წიგნის თავდაპირველ სამიზნე აუდიტორიას არ დააინტერესებს, ამიტომ მივიღე გადაწყვეტილება:

წიგნის პირველი ნაწილი დარჩება ისეთი, როგორიც არის, ხოლო მის პრაქტიკულ ნაწილზე მუშაობა გრძელდება...

წიგნის ბოლოს რჩევები ჯაფარასგან

რჩევების 99%_ს ჩემი პირადი გამოცდილებიდან გიზიარებ, თუმცა რამდენიმე რჩევა მივიღე ადამიანებისგან, რომლებსაც სიტყვა ეთქმით ჰაკინგის სამყაროში და მათ სიტყვას დიდი ფასი აქვს, ამიტომ გაითვალისწინე, რადგან ღირებული რჩევებია გამოცდილი ხალხისგან...

1. **დააფასე შენი დრო! თუ შენ არ დააფასებ შენ დროს, სხვა ამას არასდროს გააკეთებს...**

   არასდროს გააკეთო ისეთი საქმე უფასოდ (თუ სარგებელს არ იღებ), რაშიც შენ პირად დროს ხარჯავ, რადგან დროზე ფასეული არაფერია ...
2. თუ შენ არ უშვებ შეცდომებს, საკმარისად არ ცდილობ, შესაბამისად არ ვითარდები. სწირად დაუშვი შეცდომები, მთავარია ამ შეცდომებზე დაკვირვებით ისწავლო და მომავალში აღარ გაიმეორო.
3. **მიყევი შენ მიზნებს და არ მისცე სხვას საშუალება შენ მაგივრად მიიღოს გადაწყვეტილება. (გითხრას რას ვერ გააკეთებ, რას ვერ შეძლებ)**

   ბევრი ადამიანი მეუბნებოდა, რომ ეს წიგნი არ დამეწერა, სისულელე იყო, არავინ წაიკითხავდა, მაგრამ მაინც დავწერე... თუ ამას კითხულობ, გამოდის ჩემ მიზანს მივაღწიე. მე რომ მათთვის დამეჯერებინა, დღეს შენ ამ წიგნს ვერ წაიკითხავდი და ვერც იმ ინფორმაციას მიიღებდი წიგნიდან, რაც მიიღე. ამიტომ თუ ფიქრობ რომ რაღაც უნდა გააკეთო, სხვები დაივიწყე და უბრალოდ გააკეთე... (შენზე უკეთ შენი მიზნები არავინ იცის, ამიტომ ნუ უსმენ სხვას... ვიღაცას შენი წარმატება ფეხებზე კიდია, მისთვის სულ ერთია რას გააკეთებ, სამწუხაროდ...)
4. არასდროს არაფერია “დაცული” და “უსაფრთხო”. ყოველთვის იქნება ვიღაც უფრო ჭკვიანი, ვიდრე შენ და ექნება შენზე მეტი რესურსი, ამიტომ დაფიქრდი, სანამ ვიღაცას გატეხავ ან დაუპირისპირდები.
5. ორგანიზაციას ჭირდება ყველაფრის დაცვა, ჰაკერს მხოლოდ ერთი სისუსტე. იპოვე ის ერთი სისუსტე და ყველაფერი შენ ხელში იქნება.
6. ყველაფერი დაიჯერე, მაგრამ არავის ენდო, ყველა და ყველაფერი შეამოწმე (არც შემოწმების შემდეგ ენდო ვინმეს, ერთადერთი გზა ეს არის ღამე მშვიდად ძილისთვის... მძიმე, მაგრამ აუცილებელი გზაა ჩვენ პროფესიაში და ცხოვრებაში)
7. ადამიანების ნდობა მოიპოვე, დაუმეგობრდი და მათ ყველაზე ბნელ საიდუმლოებს გაიგებ.

8. კავშირები… ეცადე ყველა პროფესიაში გყავდეს მოკავშირე ადამიანი, რომლის გამოყენებასაც შეძლებ საჭიროების შემთხვევაში.
   (მოსამართლე, პოლიციელი, ადვოკატი, ადამიანები, ვისაც ძალაუფლება აქვთ)
9. მტრები და კონკურენტები ან უნდა ჩამოიშორო გზიდან ან დაუმეგობრდე. მეგობრობა უფრო ღირებულია და ნაკლებ თავის ტკივილს იწვევს.
10. მარტოხელა მგელი როგორი ძლიერიც არ უნდა იყოს, ხროვის წინააღმდეგ ვერაფერს გახდება. **(დასაფიქრებელი რჩევა)**
    იპოვე საზოგადოება, მცირე ჯგუფი, რომლის ნაწილიც იქნები და ეს კავშირი ყველანაირად შეინარჩუნე. (**hackersforce.com**)
11. ხშირად გაწმინდე შენი კვალი... სოციალურ ქსელებში საეჭვო არაფერი გააზიარო, ხშირად გამოცვალე სოციალური ქსელების ანგარიშები, წინა ანგარიშები წაშალე და არასდროს იფიქრო მათი აღდგენა.
12. **Telegram, Whatsapp, Viber, Signal** – არ ენდო მსგავს აპლიკაციებს. არასდროს იცი ხვალ რა მოხდება. ის ფაქტი რომ დღეს აპლიკაცია სანდოა, არ გაძლევს იმის გარანტიას, რომ ხვალ შენ მიმოწერას სხვა არ წაიკითხავს (ნებისმიერ პროგრამას პოტენციურად აქვს Zero-Day. ეს არის დაუცველობა, რომელიც აპლიკაციაში არსებობს მისი შექმნის დღიდან და ჯერ ამის შესახებ არავინ არაფერი იცის, როდესაც გაიგებენ და თუ გაიგებენ, კარგი არაფერი მოხდება (ზუსტად მაგიტომ ქვია Zero-day)).
    ალტერნატივა? კარგი კითხვაა… ბევრი ისეთი აპლიკაცია და პროგრამა არსებობს, რომელიც შიფრავს შენ ინფორმაციას და თან ამ ყველაფერს ტორის ქსელით ატარებს ისე, რომ მიმოწერის ისტორია არსად ინახება… მოძებნე და მხოლოდ ასეთი აპლიკაციები გამოიყენე…
    ანდროიდის შემთხვევაში საუკეთესოა **Anonymous Messenger**, რომლის გადმოწერასაც **f-droid.org** დან შეძლებ)


Anonymous Messenger
A peer to peer private anonymous and secure messenger that works over Tor.

13. არავინ დააყენო საკუთარ თავზე მაღლა…
    (პატივისცემა სხვაა, საკუთარ თავზე მაღლა დაყენება ნიშნავს მისთვის ისეთი რაღაცის გაკეთებას, რაც შენ პრობლემებს შეგიქმნის)
14. როდესაც ამ პროფესიას აირჩევ, ყველა შენი მეგობარი, ნაცნობი და განსაკუთრებით ოჯახის წევრი დაგიპირისპირდება, ხარ ამისთვის მზად?
15. არასდროს, არავის დაანახო შენი რეალური ცოდნა. ჯობია ხალხს

ეგონოს რომ არაფერი იცი, ვიდრე იცოდნენ რა შეგიძლია, რადგან როდესაც რაღაც “ისეთი” მოხდება, შენზე ეჭვს არავინ მოიტანს, ვინაიდან ეცოდინებათ რომ არაფერი იცი **(საუკეთესო რჩევა).**

16. ვიღაც აუცილებლად გთხოვს უკანონო საქმის გაკეთებას, მე ყოველდღე მთავაზობენ… არასდროს, არც კი დაინტერესდე უკანონო საქმით, მომენტალურად უარი თქვი და თუ არ მოგეშვება დაბლოკე ყველგან… შეიძლება ვიღაცას (კანონის მხრიდან) შენი გატესტვა უნდოდეს, აინტერესებდეს რამდენად ხარ უკანონო საქმის გამკეთებელი (საკმაოდ ხშირია)… თუ ფაქტზე დაგიჭირეს, პრობლემები გექნება, რომც არ დაგიჭირონ, უკანონო ქმედება რამდენიმე წლიანი პატიმრობით ისჯება. დამიჯერე კვალს აუცილებლად დატოვებ სადმე…
17. არასდროს დაეხმარო ნაცნობს… ენას ვერ გააჩერებს და სადღაც წამოცდება, დაგღუპავს ისე რომ ვერც მიხვდება.
18. **არასდროს თქვა უარი შესაძლებლობაზე.** ნებისმიერი შესაძლებლობა ახალი გამოცდილებაა. მაშინაც კი, თუ ფიქრობ რომ კონკრეტული დავალება, პროექტი სისულელეა, გააკეთე! აუცილებლად ისწავლი რაიმე ახალს, თუმცა არავის მიცე შენი გამოყენების უფლება… (მხოლოდ კანონის ფარგლებში)
19. მთავარი მიზანია, **ნებისმიერი გზით**, მთავარი მიზნის მიღწევაა!
20. დრო უაზროდ არ გაფლანგო, ცხოვრება ზედმეტად ხანმოკლეა…

ჯაფარას ბოლო სიტყვა…

გილოცავ მეგობარო, შენ ჩემი წიგნი წაიკითხე. იმედი მაქვს მიიღე იმის ნაწილი მაინც, რასაც ეძებდი. ვიცი ყველა კითხვაზე პასუხი არ გაქვს…

მთელი ცხოვრება კითხვებზე პასუხებს ვეძებთ… ზოგ ჩვენ კითხვაზე პასუხს საკუთარი თავის გარდა სხვა ვერავინ გაგვცემს. ასეთ კითხვებზე პასუხის გაცემა ყველაზე რთულია…

მე მოგაწოდე კრიტიკულად მნიშვნელოვანი ინფორმაცია, ცხოვრების შემდეგი ორი თვის მიზანიც მოგეცი…

ამ წიგნის საშუალებით პატარა მემკვიდრეობას ვტოვებ, რადგან არავინ იცის ხვალ რა იქნება, მიხარია რომ რაღაც მაინც დარჩება ჩემგან… თუნდაც მცირედი, მაგრამ საჭირო ინფორმაცია.

იცხოვრე შემდეგი წესით:

“გუშინდელი დღე წარსულია, დღევანდელი დღე საჩუქარი, ხვალინდელი დღე გამოცანა”…

თუ ამ წესით იცხოვრებ, შენი ყოველი დღე საინტერესო იქნება, რადგან შესაბამისად დააფასებ “დღევანდელ საჩუქარს”…

შენ უკვე იცი, თუ რატომ არ უნდა ჩააბარო უნივერსიტეტში ან თუ ჩააბარებ, იცი რასაც უნდა ელოდო… შენ იცი კონტროლის შესახებ. იცი მანიპულაციის შესახებ, მართალია მცირე ინფორმაცია გაქვს, მაგრამ თუ მეტი გაინტერესებს, ახლა უკვე იცი რა უნდა მოძებნო ინტერნეტში (გონების კონტროლი, გონების გამორეცხვა, მანიპულაცია და ა.შ)… შენ ის რჩევები მოისმინე, რომელიც მე რთული გზებით მივიღე და საკუთარ თავზე ბევრი რამ გამოვცადე, იმედი მაქვს შენ მსგავსი არაფერი დაგემართება…

შენ ისიც იცი, თუ რა გჭირდება კარიერისთვის (ლინკდინი, კავშირები, ნაცნობები, საზოგადოება, რომლის ნაწილიც იქნები)

ნებისმიერი წიგნის PDF ვერსიის უფასოდ პოვნა შეგიძლია ამ საიტზე: annas-archive.org/search …

ისწავლე როგორ მიიღო ნებისმიერი რამ უფასოდ ინტერნეტის დახმარებით…

მომავალში მე იმაზე დიდი კავშირები და შესაძლებლობები მექნება, ვიდრე ამ მომენტში მაქვს…

არცერთ აკადემიაში არავინ გასწავლის ჰაკინგს, ბევრჯერ დავწერე და ბოლოს კიდევ ერთხელ მინდა ხაზი გავუსვა…

ახლა რა უნდა გააკეთო?

დაიწყე სწავლა, საკმარისი ინფორმაცია მოგაწოდე ამ წიგნის დახმარებით იმის შესახებ, რისი ცოდნაც გჭირდება…

აუცილებლად გახდი ერთადერთი ჰაკერული საზოგადოების ნაწილი, რომელიც საქართველოში არსებობს :) (hackersforce.com)

რაც ამ წიგნში ვერ დავწერე, HackersForce_ში გაგიზიარებენ… ჩემი მეგობრები, რომლებიც ყველაფერში მეხმარებიან, ახლა HackersForce_ში შენ გელოდებიან…

მიდი მათთან და ისინი გასწავლიან ყველაფერს… შეუერთდი საზოგადოებას, რომელსაც საერთო ინტერესები აქვს და გახდი რაღაც დიდის ნაწილი.

ვეცადე ეს წიგნი საინტერესო გამოსულიყო. არ ვიცი რამდენად მივაღწიე ამ მიზანს, მაგრამ ის ფაქტი რომ ამ ტექსტს კითხულობ, ნიშნავს რომ რაღაც დონეზე ჩემი მიზანი შესრულებულია, ყველაფერ საუკეთესოს გისურვებ :)

მადლობა მეგობარო შენი დროისთვის!
ბოლო შანსი გაქვს
დღეს მიღებულ შენ გადაწყვეტილებაზეა დამოკიდებული
თუ სად აღმოჩნდები მომავალში
იქნები თუ არა ჩვენი საზოგადოების ნაწილი :
hackersforce.com

გინდა გახდე TOP ჰაკერი
ერთიანი ნულებს შორის
თუ გირჩევნია ნული დარჩე ნულებს შორის?
შენ გამორჩეული ადამიანი ხარ დიდი პოტენციალით
ნუ დარჩები ნულებს შორის
იყავი ის, ვინც ხარ, ერთიანი!

ჯაფარას სოციალური ქსელები:

- Facebook facebook.com/JafarasecOfficial
- Instagram instagram.com/jafarasec
- Tiktok tiktok.com/@jafarasec
- X (Twitter) twitter.com/jafarasec
- პირადი საიტი jafarasec.com (ხშირად ადევნე თვალი)
- ჰაკერული ფორუმი facebook.com/groups/hakeruliforumi
- HackersForce hackersforce.com (აუცილებლად შეუერთდი ამ საზოგადოებას)
- საკონტაქტო მეილი jafarasec@gmail.com jafarasec@proton.me

თუ რაიმე მიზეზით რომელიმე ლინკი არ იმუშავებს, განახლებულ ლინკებს ჩემ საიტზე იპოვი. jafarasec.com

---

კეთილი იყოს შენი ფეხი ჩვენ სამყაროში...
შენი მეგობარი JAFARA!
ქართული ჰაკერული საზოგადოება გელოდება, იმოქმედე...