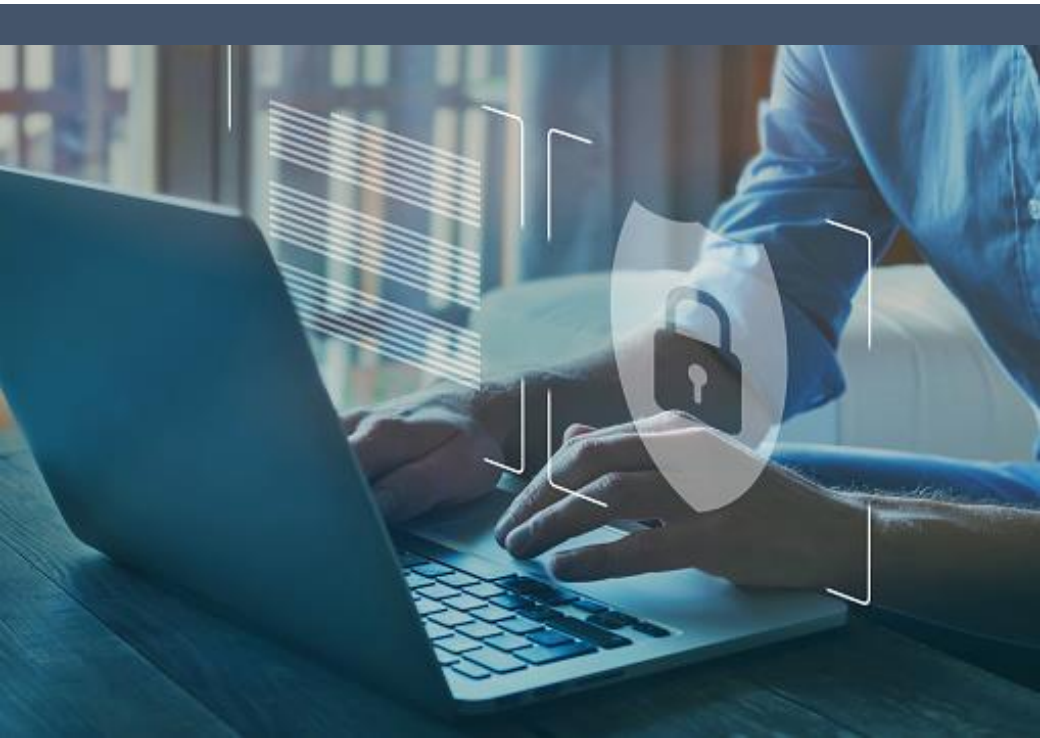
საქართველოს ეროვნული ბანკი
National Bank of Georgia

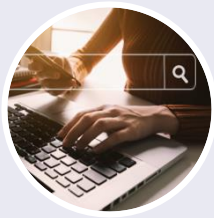
რა უნდა იცოდეთ კიბერუსაფრთხოების შესახებ



შეიტანე წვლილი
იყავი #კიბერფრთხილი

თანამედროვე სამყაროში სულ უფრო დამოკიდებული ვხდებით ინტერნეტზე, კომპიუტერზე და სმარტფონებზე. ციფრული ტექნოლოგიების როლის ზრდასთან ერთად კი იზრდება კიბერდანაშაული.

როგორ დავიცვათ თავი კიბერთაღლითებისგან და **რა უნდა ვიცოდეთ კიბერუსაფრთხოების შესახებ?**



[სოციალური ინჟინერია და კიბერშეტევები]

[უსაფრთხო ბრაუზინგი]

[მავნე პროგრამები]

[სმარტფონის უსაფრთხოება]

საქართველოს ეროვნული ბანკი
National Bank of Georgia

სოციალური ინჟინერია და კიბერშეტევები

რა არის სოციალური ინჟინერია?

სოციალური ინჟინერია არის ხალხის მანიპულირების ხელოვნება - თაღლითობის, ნდობის ფაქტორის, ფსიქოლოგიური ზეწოლის და ტყუილის მეშვეობით, რომელსაც კიბერთაღლითები კომპიუტერული ან ფინანსური ინფორმაციის ხელში ჩასაგდებად იყენებენ.

უსაფრთხოების სისტემაში ყველაზე სუსტი რგოლი ადამიანური ფაქტორია. სოციალური ინჟინერია იმდენად მრავალფეროვანია, რომ მსხვერპლი შეიძლება ნებისმიერი ადამიანი გახდეს - წლიდან წლამდე მილიონობით ადამიანი ტყუვდება.

ჩამოვთვალოთ სოციალური ინჟინერიის რამდენიმე სახეობა:

ფიშინგი - ალბათ, მიგიღიათ მეილი, რომ თქვენმა შორეულმა აფრიკელმა ნათესავმა ანდერძი დაგიტოვათ და კუთვნილი მილიონების მისაღებად მხოლოდ საბანკო მონაცემები უნდა გააგზავნოთ. ეს ფიშინგია -კიბერთაღლითობა, როცა ცდილობენ პირადი ინფორმაცია და ფული დაგტყუონ.

ფიშინგია ასევე, როცა მოულოდნელად მოგდით წერილი ნაცნობი კომპანიიდან, (მაგ. თქვენი ბანკი, სადაზღვევო), რომელიც "სასწრაფოდ" ითხოვს გადახვიდეთ ბმულზე და განაახლოთ პაროლი, პირადი ან საბანკო მონაცემები. ან გთავაზობენ საჩუქარს, გილოცავენ, რომ რაღაც მოიგეთ და საჩუქრის მისაღებად ბარათის მონაცემების შეყვანას გთხოვენ. სინამდვილეში კი გადადიხართ ყალბ გვერდზე და მახეში ებმებით. გვხვდება სატელეფონო და სმს- ფიშინგიც, ანუ **სმიშინგი**.

Search engine phishing - ფიშინგი საძიებო სისტემის და სპეციფიკური სიტყვების (keyword) გამოყენებით. ქმნიან ყალბ ვებგვერდს, რომელიც რომელიმე ცნობილი კომპანიის ვებგვერდის ასლია, საძიებო სისტემა კი შედეგებში ყალბ და ავთენტურ გვერდებს განურჩევლად გვთავაზობს.

Scam - კიბერ კრიმინალები უკავშირდებიან მსხვერპლს ელ. ფოსტით ან ტელეფონით და სთავაზობენ ფინანსურ სარგებელს, თანხის სანაცვლოდ.

სპამი - სპამიც სოციალური ინჟინერიის სახეობაა. ის თითქოს, ნაკლებად სარისკოა, თუმცა დაუკითხავად "გბომავთ" სარეკლამო წერილებით, სიფხიზლეს გაკარგინებთ და ერთხელაც, შეიძლება ასე მავნე ბმული შემოგაპაროონ.

Road apple - მავნე პროგრამებით გაძეძგილი ინფორმაციის მატარებელს (USB ან დისკი) ათავსებენ მსხვერპლისთვის თვალსაჩინო ადგილას - ის კი "შემთხვევით" პოულობს, "ამოწმებს" რა არის ჩაწერილი და... დაღუპულია საქმე!

რას ნიშნავს კიბერშეტევა?

კიბერ შეტევა არის ინდივიდის ან ორგანიზაციის მიერ მიზანმიმართული მცდელობა დაარღვიოს კერძო პირის ან ორგანიზაციის ინფორმაციული სისტემის ხელმისაწვდომობა, კონფიდენციალურობა ან მთლიანობა. როგორც წესი, თავდამსხმელი ამგვარად ცდილობს მიიღოს რაიმე სახის სარგებელი.

სტატისტიკის თანახმად, მსოფლიო მასშტაბით, 39 წამში ერთხელ კიბერ შეტევა ხორციელდება.

რა ტიპის კიბერ-შეტევები არსებობს?

Denial of Service (DoS) – ასეთი შეტევის დროს თავდამსხმელი აგზავნის მოთხოვნებს, რათა გადაავსოს და გადატვირთოს სისტემა დაგახადოს ხელმიუწვდომელი. ამ შეტევის ქვეტიპია Distributed Denial of Service (DDoS), როცა მოთხოვნები სამიზნე რესურსზე იგზავნება ერთდროულად რამდენიმე სხვადასხვა სისტემიდან.

Man in the Middle Attack (MitM) – ამ დროს, თავდამსხმელი ორ სუბიექტს შორის კავშირს უერთდება - მათ ჰგონიათ, რომ კომუნიკაცია უსაფრთხოდ მიმდინარეობს, სინამდვილეში, კი ყველაფერს მესამე პირი აკონტროლებს და მას შეუძლია არა თუ წაიკითხოს მიმოწერა, არამედ შეცვალოს მისი შინაარსი და ადრესატიც კი.

Drive by Attack – მავნე სკრიპტის გამოყენებით, მსხვერპლის მოწყობილობაზე, ხდება მავნე პროგრამების გადმოწერა, თანაც ყოველგვარი დასტურის გარეშე.

Eavesdropping Attack – ხდება ქსელით. ბოროტმოქმედი ხელში იგდებს ქსელში გამავალ შეტყობინებებს, პაროლებს, საკრედიტო ბარათის მონაცემებსა თუ სხვა კონფიდენციალურ ინფორმაციას. ამ ტიპის შეტევებისგან თავის დაცვის საუკეთესო გზაა მონაცემთა შიფრაცია.

Password Attack –
პაროლები ავთენტიფიკაციის ყველაზე გავრცელებული მეთოდია, შესაბამისად მათი ხელში ჩაგდება კიბერ შეტევის განსახორციელებლად ეფექტური მეთოდია.

პაროლის მისაღებად გავრცელებული შეტევები:

- **Brute-force –** პაროლის გამოცნობა მსხვერპლის სახელის, გვარის, დაბადების წელის, და ა.შ დაყრდნობით.
- **Dictionary Attack –** გამოცნობა გავრცელებული პაროლების სიის მიხედვით - რაც უფრო მარტივი და გავრცელებულია პაროლი, მით უფრო ადვილია მისი გატეხვა.

როგორ დავიცვათ თავი სოციალური ინჟინერიისგან?

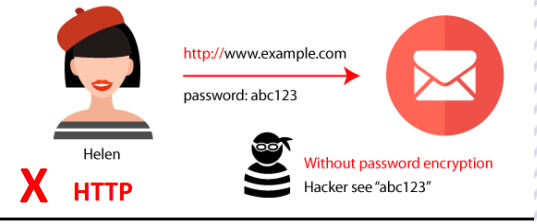
- დიდი სიფრთხილით მოეკიდეთ ნებისმიერ მოულოდნელ ელ.წერილს
- დარწმუნდით, რომ გამომგზავნის ელ.ფოსტის მისამართი ავთენტურია! განსხვავება შეიძლება ერთ სიმბოლოში იყოს
- არ გახსნათ და არ გადმოწეროთ მიმაგრებული ფაილები უცნობი გამომგზავნისგან
- ნუ ენდობით ელ.ფოსტაზე მოსულ ბმულს; გახსნამდე შეამოწმეთ hover over-ით
- არასდროს მოათავსოთ შემთხვევით ნაპოვნი მოწყობილობა/დისკი თქვენს კომპიუტერში
- თავიდან რომ აირიდოთ საფოსტო ყუთის სპამით "წალეკვა", ვებსაიტებზე რეგისტრაციისას ნუ გამოიყენებთ კორპორატიულ ელ.ფოსტას

უსაფრთხო ბრაუზინგი

რატომ უნდა იყოს ბრაუზინგი უსაფრთხო?

World Wide Web - ინტერნეტი მილიარდობით ადამიანის ცხოვრების განუყოფელი ნაწილი გახდა. სწორედ ამიტომ, აქ დიდი ასპარეზია კიბერ დამნაშავეებისთვის, რომლებიც ახალ-ახალ თაღლითურ სქემებს იგონებენ. თუმცა, ძალას არც ძველი და გადაღეჭილი ტრიუკები კარგავს.

დღეისათვის, მსოფლიოს მასშტაბით, 12.8 მილიონამდე ინფიცირებული ვებგვერდია. ასეთი საიტების მავნე მიმაგრებებიდან ყველაზე გავრცელებულია ფაილები გაფართოებებით: **exe, pdf, swf, doc, apk, msi, rtf, js, html, xls.**



რას უნდა მივაქციოთ ყურადღება?

Web Browser
ვებ ბრაუზერი ბრაუზინგის უმთავრესი ნაწილია, ამიტომ აუცილებელია მისი რეგულარული განახლება. ამით მცირდება ძველ ვერსიაში აღმოჩენილი სისუსტეების თქვენ წინააღმდეგ გამოყენების რისკი.

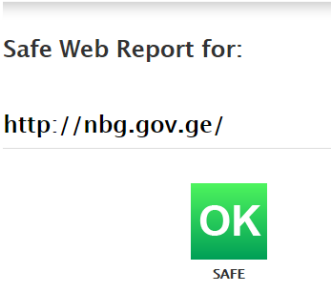
Add-ons
Add-on-ები, plugin-ები და ნებისმიერი დამატებითი მცირე პროგრამირება მომატებულ საფრთხეს ქმნის ბრაუზინგისას, ამიტომ ისინი სიფრთხილით შეარჩიეთ.

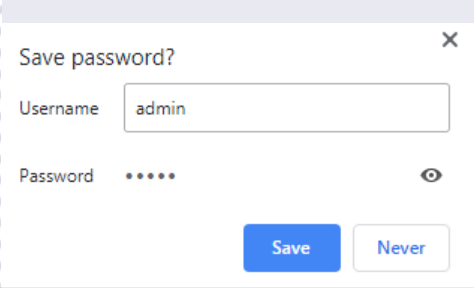
HTTP vs HTTPS
ვებსაიტზე ინფორმაციის შეყვანისას ყურადღება მიაქციეთ თავსართს!

ვებგვერდს უნდა ჰქონდეს კომუნიკაციის შიფრაცია, ანუ **https** თავსართი. სხვა შემთხვევაში თქვენ მიერ შეყვანილი ინფორმაცია დაუცველია ჰაკერის თვალისთვის.

საძიებო სისტემის ფიშინგი
კიბერ თაღლითები ხშირად ქმნიან ყალბ ვებგვერდს, რომელიც ცნობილი კომპანიის ვებგვერდის ასლია. საძიებო სისტემა არ ასხვავებს ყალბ და ავთენტურ ვებგვერდებს, ამიტომ, შეიძლება უნებურად ყალბი ვებგვერდის ბმულზე გადახვიდეთ. ამიტომ, უმჯობესია თავად აკრიფოთ-ხოლმე ვებგვერდის მისამართი.

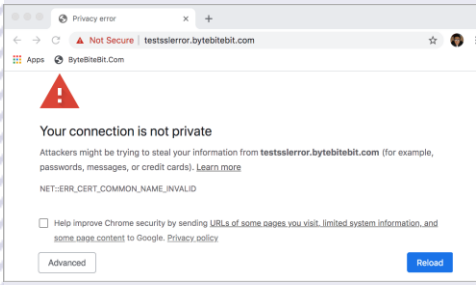
საეჭვო ვებგვერდები
ერიდეთ საეჭვო რეპუტაციის ვებ გვერდებს და არ გადმოწეროთ მიმაგრებები. უმჯობესია, თუ წინასწარ გადაამოწმებთ რამდენად უსაფრთხოა ვებგვერდი.





პაროლებისა და მონაცემების შენახვა ბრაუზერში
თანამედროვე ბრაუზერების უმრავლესობას აქვს პაროლისა და მომხმარებლის სახელის შენახვის ფუნქცია, თუმცა, მისი გამოყენება საფრთხის შემცველია.

გამაფრთხილებელი შეტყობინება
ვებგვერდზე ვიზიტისას თუ ბრაუზერი გამაფრთხილებელ შეტყობინებას გაჩვენებთ, გამოდით და მომავალშიც მოერიდეთ ამ ვებგვერდს.



მავნე პროგრამები

რა არის მავნე პროგრამა?

მავნე პროგრამა ე.წ. Malware, არის საგანგებოდ ზიანის მისაყენებლად შექმნილი პროგრამული უზრუნველყოფა, რომელიც უკანონოდ და მალულად მოიპოვებს წვდომას მსხვერპლის კომპიუტერზე და იპარავს ინფორმაციას.

რა ტიპის მავნე პროგრამები არსებობს?

ვორმი (Worm) - კომპიუტერული ჭია, რომელსაც არ სჭირდება ჰოსტ პროგრამა და არის "თვით ტირაჟირებადი"; ვრცელდება ქსელით ან ინფორმაციის მატარებელი გარე მოწყობილობით.

ვირუსი - კომპიუტერული კოდის მცირე ნაწილი, რომელიც ახდენს მოწყობილობის მუშაობის მოდიფიკაციას, სჭირდება ჰოსტ პროგრამა, რომელზეც მიმაგრდება.

Adware - ავტომატურად "გიგდებთ" რეკლამებს თქვენს ინტერნეტ ქცევაზე დაკვირვებით. ერთხელ მაინც გამოცდილი გექნებათ, რამდენად გამაღიზიანებელია.

Malvertising - კიბერ თაღლითები ლეგიტიმური ვებსაიტების სარეკლამო ბანერებსაც იყენებენ მავნე ბმულების და კოდების მისაბმელად. ერთი შეხედვით, უწყინარი სარეკლამო ბანერი მავნე ვებ გვერდზე გადაგიყვანთ მოწყობილობაზე და მავნე პროგრამება დაყენდება ისე, რომ ამას ვერც გაიგებთ.

ჯაშუში პროგრამები (Spyware) - ძირითადად Adware-თან ან ტროიანთან ერთად მოქმედებს. მონაცემების მოპოვების გარდა, შეუძლია ინტერნეტის სიჩქარის შენელება ან საერთოდ გათიშვა, სისტემის დაზიანება, ფაილებზე წვდომის შეზღუდვა და ა.შ.

Ransomware - კრიპტოვირუსი რომელსაც კომპიუტერში მოხვედრისას "მძევლად აჰყავს" სისტემა და ახდენს ფაილების დაშიფრვრას ისე, რომ მათ ვეღარ გამოიყენებთ. დეშიფრატორი, ანუ ე.წ. გასაღები აქვს მხოლოდ თავდამსხმელს, რომელიც სანაცვლოდ თანხას გძალავთ.

კრიპტოჯეკინგი - ინფიცირების შემთხვევაში იყენებს მოწყობილობას კრიპტო ვალუტის მაინინგისთვის.

ტროიანი - ყველაზე გავრცელებული მავნებლობაა პირადი ინფორმაციის მოსაპარად. აღწევს სისტემაში ონლაინ თამაშებზე რეგისტრაციისას, Drive Downloads-ით და პირატული პროგრამების გადმოწერისას. მას შემდეგ, რაც ტროიანი მოწყობილობაში აღმოჩნდება, ის აზიანებს სისტემას და აფერხებს მის მუშაობას, კიბერ დამნაშავეს კი ხელი მიუწვდება ყველაფერზე, რაც ამ კომპიუტერით მოხდება: შეუძლია ნაბიჯ-ნაბიჯ ჩაიწეროს ეკრანზე მიმდინარე ოპერაციები, ფინანსური მონაცემები, პაროლები და სხვ.

როგორ ხვდება მავნე პროგრამა მოწყობილობაში?

მავნე პროგრამა მოწყობილობაში რამდენიმე გზით ხვდება:

1. **ფიშინგი** - ელ. წერილზე მიმაგრებული ფაილები და ბმულები რომელსაც დაუფიქრებლად ხსნიან

2. **თაღლითური ან ინფიცირებული ვებგვერდები** - ასეთი ვებ გვერდიდან ფაილების ჩამოტვირთვით

3. **USB ფლეშ მეხსიერების ბარათი** ("ფლეშკა") ან დისკები - ინფიცირებულ მატარებელს ათავსებენ მსხვერპლისთვის თვალსაჩინო ადგილას

4. **მონაცემთა გაცვლისა და გადმოწერის პლატფორმები** (torrent, wetrasfer) - გადმოსაწერ ან გაზიარებულ ფაილებზე თანდართული სხვადასხვა მავნე კოდებით

5. **კომპრომეტირებული** პროგრამული უზრუნველყოფა

6. **Crack** - ანუ არალიცენზირებული პროგრამული უზრუნველყოფა

როგორ დავიცვათ თავი მავნე პროგრამებისგან?

- ✗ არ გადმოწეროთ /არ გახსნათ მიმაგრებული ფაილები (attachment) ელ.ფოსტიდან სანამ არ დარწმუნდებით, რომ ისინი უსაფრთხოა
- ✗ არ მოათავსოთ შემთხვევით ნაპოვნი USB ან დისკი კომპიუტერში
- ✗ უარი თქვით არალიცენზირებულ პროგრამებზე
- ✓ რეგულარულად განაახლეთ სისტემური პროგრამები (ე.წ. update)

გახსოვდეს:

ყველაზე ძლიერი ანტივირუსიც კი ვერ დაგიცავს ყველა სახის მავნე პროგრამისგან. კიბერ დამნაშავეები ყოველთვის რამდენიმე ნაბიჯით წინ არიან და ძლიერი უსაფრთხოების სისტემების გაცურებასაც ახერხებენ.

ამიტომ, **იყავი კიბერფრთხილი,** რომ იყო დაცული.

საქართველოს ეროვნული ბანკი
National Bank of Georgia

სმარტფონის უსაფრთხოება

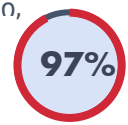
რატომ უნდა დავიცვათ ჩვენი სმარტფონი?

თანამედროვე სამყაროში, სმარტფონი აღარაა მხოლოდ დარეკვის და სმს-ის გაგზავნის საშუალება. ამ მოწყობილობაში ჩვენ შესახებ ზღვა ინფორმაცია ინახება.

პირადი მონაცემების გარდა, ჩვენს სმარტფონზე შესაძლოა მოხვდეს კორპორატიული ინფორმაციაც, სწორედ ამიტომ, აუცილებელია მათი სათანადო დაცვა.

2020 წლის გამოკითხვის თანახმად:

კიბერშეტევის მსხვერპლი ორგანიზაციების 97%-ში, თავდასხმა სმარტფონებიდან განხორციელდა.



ორგანიზაციების 46%-ში თანამშრომლის მიერ მავნე აპლიკაციის გამოყენებამ საფრთხე შეუქმნა ორგანიზაციის მთელ ქსელს.

რა ტიპის საფრთხეები არსებობს?

სმარტფონებთან და მობილურ მოწყობილობებთან დაკავშირებული საფრთხეები რამდენიმე კატეგორიად იყოფა:

ფიზიკური საფრთხეები - თუ სმარტფონს დაკარგავთ ან მოგპარავენ, დაუცველი მოწყობილობიდან დიდია ინფორმაციის გაჟონვის საფრთხე.

მავნე აპლიკაციები - ხშირად კიბერ კრიმინალები ქმნიან აპლიკაციებს, რომლებიც სანდოდ გამოიყურება და საჭირო ფუნქციებსაც ასრულებენ, თუმცა, პარალელურად მალულად იღებენ წვდომას მოწყობილობაზე და იპარავენ მონაცემებს. ასეთი აპლიკაციები ხშირად გასართობი სახისაა და უცებ ხდება პოპულარული.

ქსელები -
ღია ან დაუცველი WiFi-ის გამოყენებისას, კიბერკრიმინალებს შეუძლიათ დაინახონ და მოიპარონ დაუშიფრავი ინფორმაცია.

როგორ დავიცვათ სმარტფონი?

- **დააყენეთ ე.წ Screen Lock** (პაროლი ან ბიომეტრიული მონაცემები) - ტელეფონის დაკარგვის შემთხვევაში უცხო პირები ვერ მოახერხებენ თქვენს პირად ინფორმაციაზე წვდომას.
- **ნუ გამოიყენებთ საჯარო WiFi ქსელებს!**

- გამოყენების შემდეგ გათიშეთ WiFi, NFC და Bluetooth კავშირი.
- **არ დააყენოთ არაოფიციალური პროგრამები** - მათი უმრავლესობა შეიცავს მავნე პროგრამებს; გადაამოწმეთ აპლიკაციის ავტორიც და დარწმუნდით მის სანდოობაში.
- **პროგრამის დაყენებისას შეამოწმეთ მოთხოვნილი უფლებები**, რადგან ზოგიერთი პროგრამა შეიძლება ითხოვდეს მისთვის არასაჭირო ფუნქციას საეჭვო მიზნებისთვის.
- **რეგულარულად განაახლეთ** პროგრამული და ოპერაციული სისტემა (Updates) არსებული სისუსტეების აღმოსაფხვრელად.