ციფრული უსაფრთხოება

გზამკვლევი

როგორ შეიძლება დაიცვათ თქვენთვის მნიშვნელოვანი ინფორმაცია თუ კომუნიკაცია ციფრულ სივრცეში? [1]

1. გამოიყენეთ მხოლოდ ძლიერი პაროლი

- შეარჩიეთ გრძელი პაროლი. ეცადეთ შეარჩიოთ 10 ან მეტი სიმბოლოსგან შემდგარი პაროლი. შეგიძლიათ გამოიყენოთ რამდენიმე სიტყვა. გრძელი პაროლი ახანგრძლივებს თქვენი პაროლის გატეხვის დროს.
- შეარჩიეთ რთული პაროლი. პაროლს დაამატეთ სიმბოლოები, შეურიეთ დიდი და პატარა ასოები, შეგიძლიათ გამოიყენოთ გამოტოვება სიტყვებს შორის და ა.შ. დაიმახსოვრეთ, თქვენი პაროლის სირთულე მისი გატეხვის სისწრაფის პირდაპირპროპორციულია: მარტივი პაროლი - ნაკლები დრო, რთული პაროლი- მეტი დრო.
- ყველა ტექნიკისთვის/აპლიკაციისთვის/ანგარიშისთვის შექმენით უნიკალური პაროლი. ერთი შეხედვით, შეიძლება რთულად მოგეჩვენოთ რთული პაროლების დამახსოვრება, თუმცა არსებობს დამხმარე საშუალებები.
- შეგიძლიათ პაროლები შექმნათ თქვენთვის კარგად ნაცნობი და ადვილად დასამახსოვრებელი სიტყვებიდან (თუმცა, არა პერსონალიზებული და თქვენთან ადვილად დასაკავშირებელი სიტყვებისგან), ამისთვის შეგიძლიათ ამ სიტყვებში გადაათამაშოთ დიდი და პატარა ასოები, სიმბოლოები, ციფრები და ამგვარად გაართულოთ ისინი.
- შეგიძლიათ გამოიყენოთ პაროლების გენერატორი (მაგ. Keepass, Lastpass) Keepass ქმნის და უსაფრთხოდ ინახავს თქვენს პაროლებს მოწყობილობაზე და შეუძლია სინქრონიზება ბევრ მოწყობილობასთან პაროლის შენახვა- გამოყენებისთვის. Lastpass, ქმნის და ინახავს დაცულ და სანდო პაროლებს, აქვს ულიმიტო მოწყობილობების რაოდენობაზე ულიმიტოდ პაროლების მხარდაჭერის ფუნქცია. Lastpass-ის უპირატესობას წარმოადგენს ის, რომ გააჩნია რამდენიმესაფეხურიანი ავტორიზაციის სისტემა და იმ შემთხვევაშიც კი, თუ ვინმეს თქვენს პაროლზე წვდომა ექნება, მის გამოყენებას მაინც ვერ შეძლებს საავტორიზაციო მოწყობილობის გარეშე.

[1] გამოყენებული წყაროები:
FrontLine Defenders - Security in a Box
https://www.safetydetectives.com/blog/lastpass-vs-keepass/

- პაროლი, რომელიც გარკვეულ ტექნიკაზე (კომპიუტერი, სმარტფონი და ა.შ.) ყენდება, საჭიროებს ზრუნვას. კერძოდ, არ გაანდოთ თქვენი პაროლი სხვა პირებს, მოერიდეთ პაროლის შეყვანას უცხო პირების თანდასწრებით, არ შეიყვანოთ პაროლი კამერების თანდასწრებით. არ დაამახსოვრებინოთ სისტემას თქვენი პაროლი (პირველად პაროლის შეყვანისას, ხშირად ბრაუზერები გვთავაზობენ პაროლის შემდგომისთვის შენახვას), განსაკუთრებით უცხო და დაუცველი კომპიუტერით ან მოწყობილობით სარგებლობისას.
- პაროლზე ზრუნვა ასევე გულისხმობს მის პერიოდულ განახლებას. არაა სასურველი პაროლის ხშირი ცვლილება, რაც ხშირად ხელს უწყობს პაროლის დავიწყებას. იქონიეთ რთული პაროლი, რომელზე წვდომაც გექნებათ მხოლოდ თქვენ, ან რამდენიმე პირს, რომელსაც თქვენ ენდობით. გამოცვალეთ პაროლი 6 თვეში ერთხელ.

პაროლის მაგალითი	პაროლის გატეხვის დრო ყოველდღიური გამოყენების კომპიუტერიდან	პაროლის გატეხვის დრო სწრაფი კომპიუტერიდან
Banana	1 დღეზე ნაკლები	1 დღეზე ნაკლები
Bananalemonade	2 დღე	1 დღეზე ნაკლები
BananaLemonade	3 თვე და 14 დღე	1 დღეზე ნაკლები
B4n4n4L3m0n4d3	3 საუკუნე და 4 ათწლეული	1 თვე და 26 დღე
We Have No Bananas	19151466 საუკუნე	3990 საუკუნე
W3 H4v3 N0 B4n4n45	20210213722742 საუკუნე	4210461192 საუკუნე

2. ტექნიკის დაშიფვრა

- ლეპტოპი/პერსონალური კომპიუტერი უნდა დაიშიფროს სპეციალური სისტემების გამოყენებით, რომელიც დამატებით დაცვას უზრუნველყოფს ტექნიკისთვის. იმ შემთხვევაში თუ თქვენ სარგებლობთ Microsoft Windows 10 Pro ან Microsoft Windows 7, თქვენს კომპიუტერს აქვს ფუნქცია დაშიფროს D დისკი Bitlocker დამცავი სისტემის გამოყენებით. Bitlocker არის Microsoft Windows დაცვის პროდუქტი, რომელიც უზრუნველყოფს თქვენი კომპიუტერის დამატებით უსაფრთხოებას.
- იმ შემთხვევაში თუ თქვენ გარკვეული მიზეზების გამო (მაგალითად, გაქვთ Microsoft Windows Home ვერსია, ან სხვა კომპიუტერული სისტემა გიყენიათ) ვერ ახერხებთ Bitlocker-ით სარგებლობას, შეგიძლიათ ე.წ. მფრინავი(on-the-fly) შიფრის სისტემა დააყენოთ(მაგ, Veracryft). იგივე პრინციპით, აუცილებელია მყარი დისკის/მეხსიერების ბარათის დაშიფვრა და მათზე პაროლის დაყენება.

3. ინფორმაციის შენახვა ან განადგურება

- არასასურველი/ზედმეტი ინფორმაცია, რომელიც შეიცავს პერსონალურ მონაცემებს, საქმესთან დაკავშირებულ სენსიტიურ დეტალებს, სასურველია წაიშალოს ან თუ ფიზიკური სახით არსებობს, განადგურდეს შრედერის მეშვეობით.
- დასაშრედერებელ დოკუმენტებს და/ან მნიშვნელოვანი ინფორმაციის შემცველ დოკუმენტებს (მაგ, მიმდინარე ან დასრულებული საქმეები, ფინანსური დოკუმენტები ბენეფიციარის პირადი მონაცემებით) ნუ დატოვებთ თქვენს მაგიდაზე ყველასთვის ხელმისაწვდომ ადგილას. მოათავსეთ ისინი სეიფში ან უჯრაში, რომელიც იკეტება და დარწმუნდით, რომ გასაღებზე წვდომა გაქვთ მხოლოდ თქვენ, ან რამდენიმე ადამიანს, რომლის ვინაობაც თქვენ კარგად იცით და ენდობით.
- იმისთვის, რომ მნიშვნელოვანი დოკუმენტაცია არ დაიკარგოს სხვადასხვა მიზეზით (მაგ, ლეპტოპისა და მყარი დისკის დაზიანება და ა.შ.), აუცილებელია ატვირთოთ გარკვეული პერიოდულობით ეს ინფორმაცია სხვა ტექნიკაზე ან ღრუბელზე (ე.წ. „ქლაუდზე“). მაგალითად, თუ თქვენ ინფორმაციის შესანახად ძირითადად ლეპტოპს იყენებთ, სასურველია გარკვეული პერიოდულობით ეს ინფორმაცია ატვირთოთ სანდო ქლაუდზე ან გადაიტანოთ დაშიფრულ მოწყობილობაზე (მეხსიერების ბარათი, მყარი დისკი).
- რეკომენდებული დაცული ქლაუდები, რომელზეც შეგიძლიათ ინფორმაციის ატვირთვა: Google Drive (2 საფეხურიანი ავტორიზაცია) და Mega Cloud
- ინფორმაციის შესანახად სასურველია არ გამოიყენოთ დაუშიფრავი ტექნიკას.

4. ტექნიკის შემოწმება

- აუცილებელია ტექნიკა (ლეპტოპი, პერსონალური კომპიუტერი, მობილური და ა.შ.) 6 თვეში ერთხელ მაინც შემოწმდეს. მაგალითად, ხომ არ საჭიროებს რომელიმე პროგრამა განახლებას, მუშაობს თუ არა ტექნიკა გამართულად (ბატარეა, პროცესორი). ეს საჭიროა ტექნიკის მოულოდნელად მწყობრიდან გამოსვლის თავიდან ასაცილებლად.
- ახალი ტექნიკის შეძენის შემთხვევაში აუცილებელია ტექნიკა შემოწმდეს. დარწმუნდით, რომ ახალ ტექნიკას აქვს ყველა ფუნქცია, რომელიც თქვენ დაგჭირდებათ უსაფრთხო მუშაობისთვის.
- იმ შემთხვევაში, თუ ახალი ტექნიკა ლეპტოპი ან პერსონალური კომპიუტერია, შეძენის შემდეგ დააყენეთ Windows ან სხვა ოპერაციული სისტემა და ყურადღება მიაქციეთ, რომ ოპერაციული სისტემა იყოს ლიცენზირებული. ლიცენზირებული ოპერაციული სისტემის დაყენების შემდეგ დაშიფრეთ კომპიუტერი და დააყენეთ სხვა საჭირო პროგრამა. ასევე, დარწმუნდით რომ გაქვთ აქტიური და სანდო ანტივირუსი.

5. დაშიფრული კომუნიკაცია

- ყოველდღიური, რუტინული მიმოწერისთვის სასურველია ისარგებლოთ Gmail-ის საშუალებით. თუ თქვენ სარგებლობთ Gmail-ით და თქვენს Google Drive-ზე არსებული ინფორმაცია განსაკუთრებით მნიშვნელოვანია, აუცილებელია დააყენოთ Gmail-ზე ორსაფეხურიანი ავტორიზაცია.
- ორსაფეხურიანი ავტორიზაციის საშუალებით თქვენი ელექტრონული ფოსტა Gmail-ზე მიებმება სხვა მეორე ელექტრონულ ხელსაწყოს (მობილურს), რომელზეც Gmail-ზე შესვლისას მოგივათ შეტყობინება, ნამდვილად თქვენ ხართ თუ არა ის პირი, რომელიც თქვენს ელექტრონულ ფოსტაზე ცდილობს შესვლას.
- იმ შემთხვევაში, თუ თქვენ არ გაქვთ Gmail, სენსიტიური ინფორმაციის ელექტრონული ფოსტის საშუალებით გასაზიარებლად გამოიყენეთ Mailvelope (თავსებადია Gmail-თან, Yahoo mail-თან) ან დაშიფრული ფოსტის სისტემა Protonmail.
- სენსიტიური ინფორმაციის მიმოწერისას გამოიყენებთ მხოლოდ ისეთი მობილური აპლიკაციები, **როგორიცაა Signal ან WhatsApp,** არ გამოიყენოთ Facebook Messenger, sms მიმოწერა და სატელეფონო ზარები.

6. ფიშინგი და მისი ამოცნობა

- ფიშინგი არის კიბერთაღლითობის ფორმა, რომლის მიზანია ინდივიდს მოჰპაროს სენსიტიური ინფორმაცია ან შეაღწიოს მის კომპიუტერში. ფიშინგის დროს გამოიყენება მეილი, რომელიც ერთი შეხედვით წარმოჩენილია, როგორც სანდო წყაროსგან მიღებული შეტყობინება, როგორიცაა კომპანია, ორგანიზაცია თუ პირი. მეილი შენიღბულია როგორც სასწრაფო შეტყობინება, რომელშიც დამატებითი სარწმუნოობისთვის მოთავსებულია ვებ-ბმულები ან მიმაგრებული დოკუმენტები.
- ფიშინგ მეილში მოთავსებულ ბმულზე გადასვლის, ან ფაილის გახსნის შედეგად, შესაძლებელია კომპიუტერში შეღწევა, ან მისგან დამატებით სენსიტიური ინფორმაციის მოთხოვნა (პაროლი, მომხმარებლის სახელი, ბარათის ინფორმაცია და სხვა).
- ფიშინგისგან თავდაცვის საუკეთესო მეთოდია კარგად დააკვირდეთ გამომგზავნის ელექტრონულ მისამართს. თუ ეჭვი გეპარებათ, ყოველთვის შეგიძლიათ გადაამოწმოთ მათი ელექტრონული მისამართი/საკონტაქტო ინფორმაცია, მათ ოფიციალურ ვერ-გვერდზე მოცემული საკონტაქტო ინფორმაციის საშუალებით და შეადაროთ ის გამოგზავნილს.

7. ინტერნეტ ანონიმურობა და VPN

- საკუთარი მონაცემების დაცვას და ინტერნეტ ანონიმურობას, რომელიც გულისხმობს საკუთარი IP კვალის დაფარვას (მაგალითად, სენსიტიური ინფორმაციის ძებნისას და ა.შ.) და ელექტრონულ პროდუქტზე წვდომაში, რომელიც თქვენი ქვეყნისთვის არაა ხელმისაწვდომი დაგეხმარებათ VPN.
- VPN - ის (ვირტუალური პირადი ქსელი) ძირითადი მიზანი არის თქვენი მონაცემებისთვის უსაფრთხო გვირაბის შექმნა, რომელიც გადაეცემა სერვერებს

ინტერნეტში გადასვლამდე და სხვა სერვერის მეშვეობით თქვენ მოგეწოდებათ სასურველი ინფორმაცია.

- VPN თქვენი კომპიუტერისთვის- CyberGhost; VPN Free Proxy (Google Chrome extension)
- VPN თქვენი მობილურისთვის- ProtonVPN app