ქიბერდანაშაული

მარიანა ხუნძაყიშვილი | ზაქარია კაპანაძე

წინამდებარე მასალა შეიქმნა „სკოლის, საზოგადოებისა და პოლიციის ჩართულობის პროგრამის“ (SCOPE) ფარგლებში, რომელსაც ახორციელებს ორგანიზაცია PH International-ის ფილიალი საქართველოში, აშშ-ის სახელმწიფო დეპარტამენტის ანტინარკოტიკული და სამართალდამცავ ორგანოებთან ურთიერთობის საერთაშორისო ბიუროს (INL) ფინანსური მხარდაჭერით.

სასწავლო მასალა მომზადდა ამერიკელი ხალხის მხარდაჭერით. ერთპიროვნული პასუხისმგებლობა მოცემულ კრებულში ასახული ინფორმაციისა და მასში გამოთქმული მოსაზრებების თაობაზე ეკისრება ავტორებს და ის არ წარმოადგენს აშშ-ის სახელმწიფო დეპარტამენტის ანტინარკოტიკული და სამართალდამცავ ორგანოებთან ურთიერთობის საერთაშორისო ბიუროს ან აშშ-ის მთავრობის შეხედულებებს.

ავტორები: მარიანა ხუნძაყიშვილი, ზაქარია კაპანაძე
კონსულტანტები: თინათინ ებანოიძე, ნუცა გოგუაძე
რედაქტორი: რიტა ბაინდურაშვილი
ილუსტრატორი: სოფო კირთაძე
დიზაინერები: სოფო კირთაძე, ზურა მჭედლიშვილი

ISBN

მარიანა ხუნძაყიშვილი
ზაქარია კაპანაძე

კიბერდანაშაული

დამხმარე სახელმძღვანელო საჯარო და კერძო სკოლების უფროსკლასელთათვის

თბილისი, 2019

შესავალი

თანამედროვე ტექნოლოგიების განვითარებამ ეფექტური გახადა ადამიანებს შორის კომუნიკაცია და ისეთი მომსახურებების მიღება, რაც მანამდე ხელმიუწვდომელი ან დროში გაწელილი იყო. 21-ე საუკუნეში ინტერნეტი და მასთან დაკავშირებული მომსახურება თითოეული ჩვენთაგანის ყოველდღიურ ცხოვრებაში მნიშვნელოვან ადგილს იკავებს.

თუმცა თანამედროვე ტექნოლოგიების სწრაფმა განვითარებამ და მისმა პოპულარიზაციამ შექმნა ისეთი საფრთხეებიც, რომლებიც რამდენიმე ათეული წლის წინ არ არსებობდა, რადგან თანამედროვე ტექნოლოგიები ჯერ კიდევ არ იყო ყველასათვის ხელმისაწვდომი. დღეს კი ტექნოლოგიური რევოლუციის ერამ ახალი გამოწვევების წინაშე დააყენა სამართალდამცავი ორგანოს წარმომადგენლები, რადგან გაჩნდა დანაშაულის ახალი სახე - კიბერდანაშაული. შესაბამისად, საჭირო გახდა კიბერსივრცეში ადამიანის უფლებების დაცვა და მათ უსაფრთხოებაზე ზრუნვა.

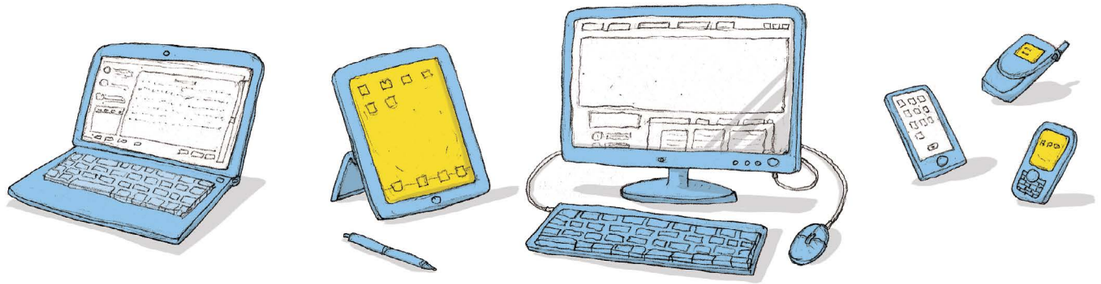
რა არის კიბერდანაშაული და რითი განსხვავდება ის კიბერმეთოდებით ჩადენილი დანაშაულისგან?

კიბერდანაშაულსა და კიბერმეთოდებით ჩადენილ დანაშაულებს შორის მნიშვნელოვანი განსხვავებაა:

კიბერდანაშაულს წარმოადგენს ნებისმიერი მართლსაწინააღმდეგო ქმედება, რომელიც ჩადენილია კომპიუტერული სისტემის გამოყენებით კიბერსივრცეში; **1**

კიბერმეთოდებით ჩადენილი დანაშაულის შემთხვევაში დანაშაულის ჩამდენი არ ჩადის კიბერდანაშაულს, ჩადის სხვა დანაშაულს (მაგალითად: თაღლითობა, გამოძალვა და ა.შ.) და კომუნიკაციის მეთოდად იყენებს ინტერნეტს (კიბერსივრცეს). **2**

კომპიუტერული სისტემა არის ნებისმიერი მექანიზმი ან მექანიზმთან დაკავშირებული ჯგუფი, რომელიც პროგრამის მეშვეობით ან ავტომატურად ამუშავებს მონაცემებს (მაგ: პერსონალური კომპიუტერი, ლეპტოპი, პლანშეტური კომპიუტერი, მობილური ტელეფონი სმარტფონი და ნებისმიერი მოწყობილობა მიკროპროცესორით).



დამატებითი ინფორმაცია კიბერდანაშაულის განმარტებასთან დაკავშირებით: კიბერდანაშაულის ზემოთ მოცემული განმარტება ხშირად გვხვდება იურიდიულ ლიტერატურაში. ამ განმარტების სწორად გააზრებისთვის სისხლის სამართლის კოდექსში სპეციალური თავია გამოყოფილი, რომლის შინაარსზე დაყრდნობითაც შესაძლებელია კიბერდანაშაულის კიდევ უფრო ზუსტი განმარტების გაკეთება.

კიბერდანაშაულს წარმოადგენს ნებისმიერი მართლსაწინააღმდეგო ქმედება, რომელიც ჩადენილია კომპიუტერული სისტემის გამოყენებით კიბერსივრცეში და ხელყოფს კომპიუტერული სისტემის ფუნქციონირებასა და კომპიუტერული მონაცემების დაცულობას.

ვიდრე კითხვას გააგრძელებთ, დაფიქრდით:

1. რა ტიპის კიბერდანაშაულია გავრცელებული დღეისათვის საქართველოში ანუ რა ხერხებს მიმართავენ კიბერდანაშაულის ჩადენისათვის (გავრცელებული კიბერდანაშაული)?

2. რა საფრთხის წინაშე შეიძლება აღმოჩნდეს კიბერდანაშაულის მსხვერპლი (კიბერდანაშაულით გამოწვეული საფრთხეები)?

3. რა გზები არსებობს კიბერდანაშაულის თავიდან ასარიდებლად (კიბერდანაშაულის თავიდან არიდების გზები)?

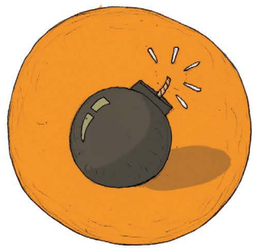
ამ კითხვებზე პასუხი ქვემოთ მოცემული გრაფიკული ორგანიზატორის გამოყენებით წარმოადგინეთ. გადაიტანეთ ის თქვენს სამუშაო რვეულებში და ინდივიდუალურად იმუშავეთ.

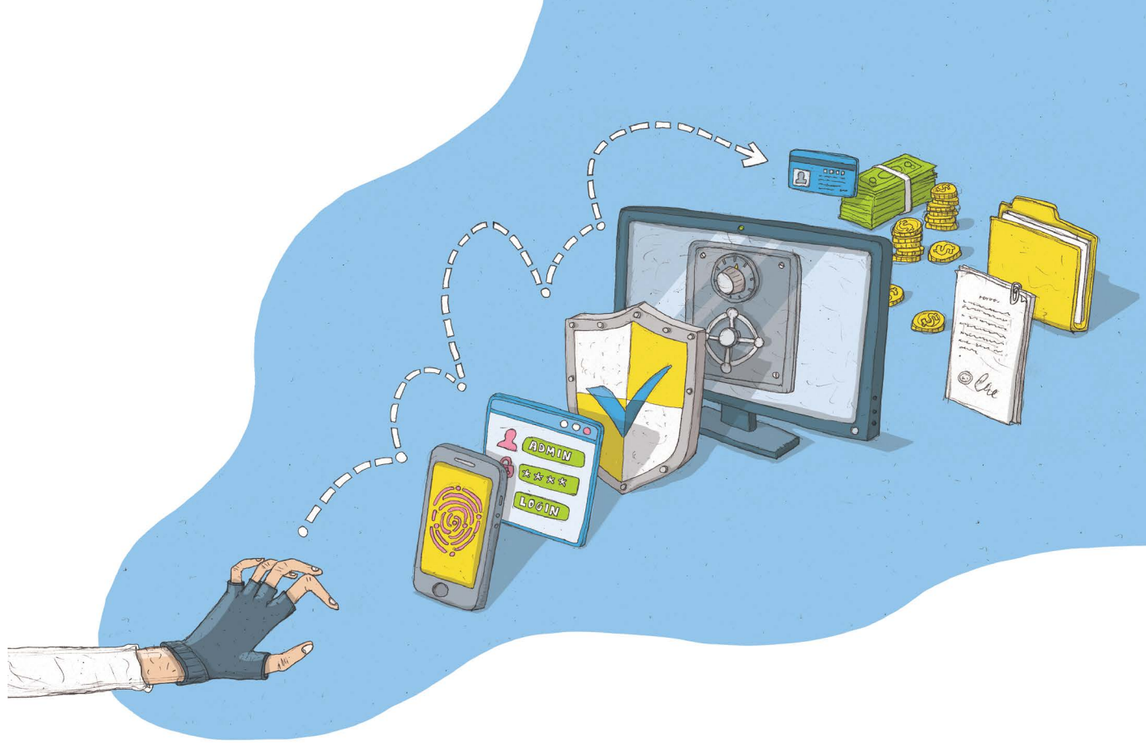
გრაფიკული ორგანიზატორი: ***კიბერდანაშაული***

გავრცელებული კიბერდანაშაული

კიბერდანაშაულის თავიდან არიდების გზები

კიბერდანაშაულით გამოწვეული საფრთხეები





რა საფრთხეებს გვიქმნის კიბერდანაშაული?

კიბერდანაშაულის ჩადენის შემთხვევაში, შესაძლოა, დამნაშავის ხელში აღმოჩნდეს ისეთი ინფორმაცია, რომელიც შეიძლება უკავშირდებოდეს:

- პიროვნების პერსონალურ მონაცემებს
- პიროვნების პირად ცხოვრებას

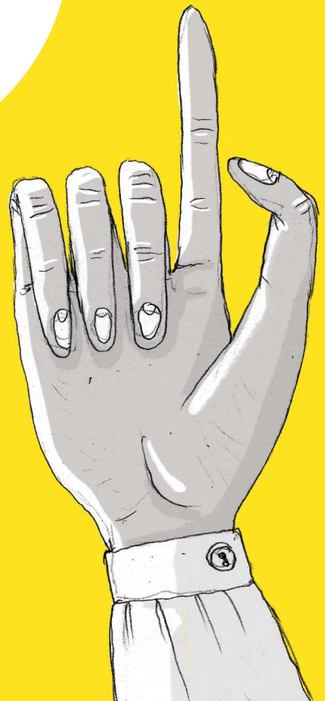
პერსონალური მონაცემი არის ნებისმიერი მონაცემი, რომელიც უკავშირდება იდენტიფიცირებად ან იდენტიფიცირებულ ფიზიკურ პირს, მაგალითად: სახელი, გვარი, პირადი ნომერი, ***საბანკო ინფორმაცია,*** ტელეფონის ნომერი, ელ-ფოსტა, ინფორმაცია მის საკუთრებაში არსებული ქონების შესახებ ან სხვა მონაცემი, რომლითაც შესაძლებელია პირის პირდაპირი ან არაპირდაპირი გზით იდენტიფიცირება, კერძოდ, საიდენტიფიკაციო ნომრით, ფიზიკური, ფსიქოლოგიური, ეკონომიკური, კულტურული ან სოციალური მახასიათებლებით.

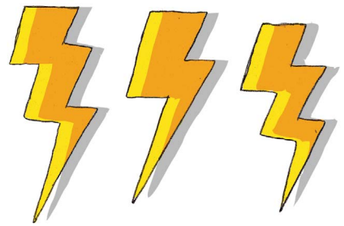
სხვა სიტყვებით რომ ვთქვათ, პერსონალური მონაცემები არის ჩვენ შესახებ არსებული ინფორმაცია, რომლითაც შესაძლებელია ჩვენი იდენტიფიცირება.

ყურადღება გავამახვილოთ:

პირადი ცხოვრების ამსახველი ინფორმაცია შეიძლება იყოს სურათი, აუდიო/ვიდეო ჩანაწერი, მიმოწერა, პირადი ჩანაწერები ან სხვა, რომელიც შეიცავს ადამიანის პირადი ცხოვრების ამსახველ ცნობებს.

საბანკო ინფორმაციაში იგულისხმება პიროვნების საკუთრებაში არსებული ინტერნეტბანკი და საბანკო პლასტიკურ ბარათზე მითითებული ინფორმაცია: სახელი და გვარი, საბანკო პლასტიკური ბარათის ნომერი, მისი მოქმედების ვადა, CVC კოდი და მაგნიტური ველი (ბარათის უკანა მხარეს არსებული მუქი ფერის ზოლი), რომელზეც ინფორმაცია დატანილია ელექტრონულად.

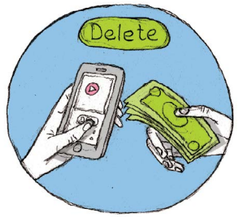




რისთვის სჭირდება დამნაშავეს სხვა ადამიანის პერსონალური მონაცემები და პირადი ცხოვრების ამსახველი ინფორმაცია?

ამ მონაცემების საშუალებით დამნაშავეს ადვილად შეუძლია:

- მიიღოს ფინანსური სარგებელი;
- შანტაჟის[1] ან მუქარის გზით აიძულოს პიროვნება, განახორციელოს ან თავი შეიკავოს რაიმე ქცევის განხორციელებისგან მისი ნების საწინააღმდეგოდ და დამნაშავის სასარგებლოდ.



იძულება - ადამიანის ნება-სურვილის საწინააღმდეგო ფიზიკური ან ფსიქოლოგიური იძულება, შეასრულოს ან არ შეასრულოს მოქმედება, რომლის განხორციელება ან რომლისგან თავის შეკავება მისი უფლებაა.

მუქარა - სიცოცხლის მოსპობის ან ჯანმრთელობის დაზიანების ანდა ქონების განადგურების მუქარა, როდესაც იმას, ვისაც ემუქრებიან, გაუჩნდა მუქარის საფუძვლიანი შიში.

[1] შანტაჟი არ არის სისხლის სამართლის კოდექსით გათვალისწინებული დანაშაული, მისი თანასწორი ქმედებაა გამოძალვა, იძულება და მუქარა, რომელიც საქ. სსკ-შია გათვალისწინებული. თუმცა სისხლის სამართლის კოდექსშიც მრავლადაა მოცემული დანაშაულის შემადგენელ ქმედებად შანტაჟი. მაგ: მუხლი 253. პროსტიტუციაში ჩაბმა 1. პროსტიტუციაში ჩაბმა ძალადობით, ძალადობის ან ქონების განადგურების მუქარით, შანტაჟით ან მოტყუებით. ვინაიდან დამნაშავემ უნებართვოდ შეაღწია სხვის კომპიუტერულ სისტემაში (ინტერნეტბანკი არის კომპიუტერული სისტემა), სახეზე გვაქვს კიბერდანაშაული, ხოლო სხვისი ანგარიშიდან თანხის საკუთარ ანგარიშზე გადარიცხვა არის ქურდობა.

ქვემოთ მოყვანილ მაგალითებში კარგად ჩანს როგორც კიბერდანაშაულის, ასევე კიბერმეთოდებით ჩადენილი დანაშაულის მოტივები:

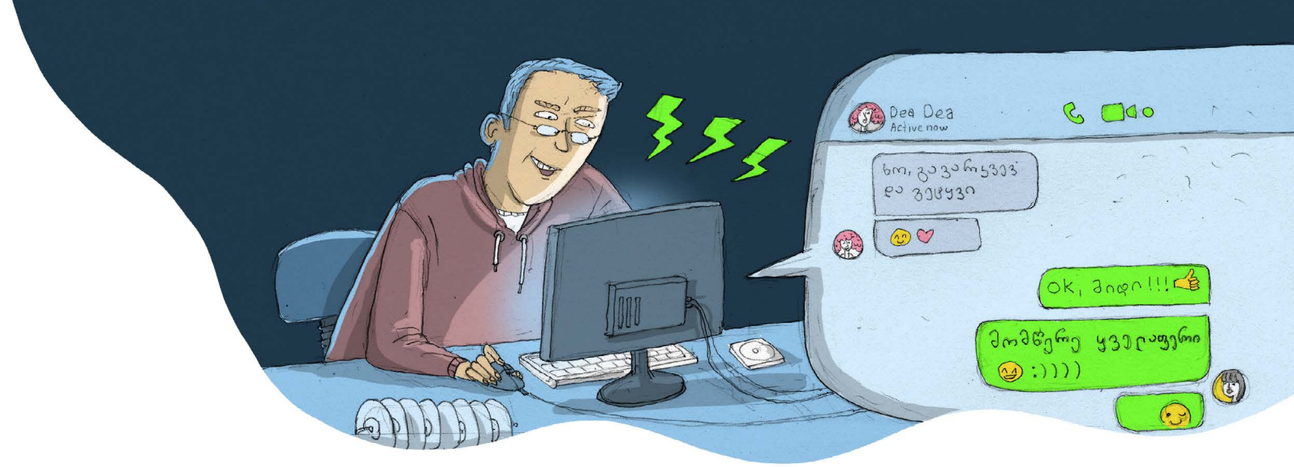
მაგალითი 1.

დამნაშავემ დაინახა, ინტერნეტბანკში შესასვლელად როგორ აკრიფა მისმა თანამშრომელმა კომპიუტერში ავტორიზაციის პარამეტრები - სახელი და პაროლი. დამნაშავემ ეს მონაცემები დაიმახსოვრა, მოგვიანებით თავად გახსნა ინტენეტბანკის გვერდი, აკრიფა მისი თანამშრომლის სახელი და პაროლი, შეაღწია საბანკო ანგარიშზე და იქ არსებული 100 ლარი თავის ანგარიშზე გადარიცხა.

ვინაიდან დამნაშავემ უნებართვოდ შეაღწია სხვის კომპიუტერულ სისტემაში (ინტერნეტბანკი არის კომპიუტერული სისტემა) სახეზე გვაქვს კიბერდანაშაული, ხოლო სხვისი ანგარიშიდან თანხის საკუთარ ანგარიშზე გადარიცხვა არის ქურდობა.

მაგალითი 2.

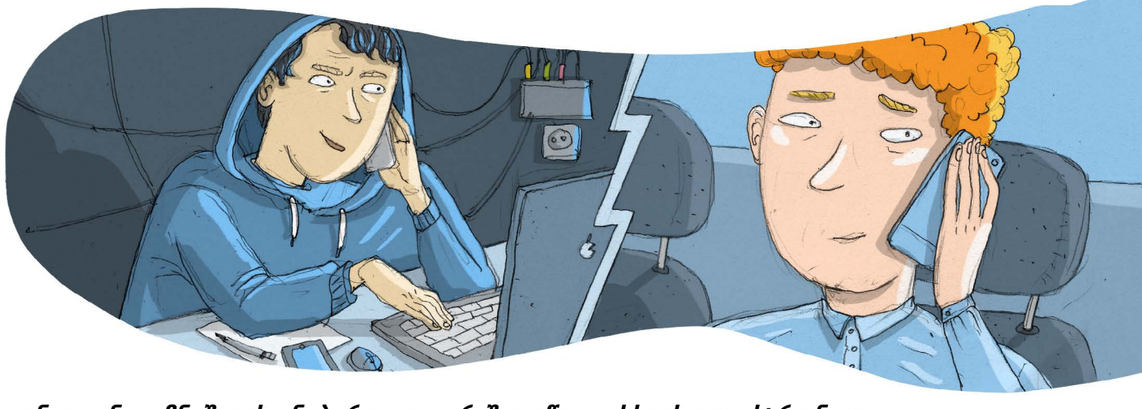
დამნაშავეს შექმნილი ჰქონდა ე.წ. „ფიშინგ“ გვერდი („ფიშინგის“ განმარტება იხ. მომდევნო ქვეთავში), რისი საშუალებითაც ერთ-ერთი სოციალური ქსელის მომხმარებლის ავტორიზაციის პარამეტრები მოიპოვა - კერძოდ, სახელი და პაროლი. შემდეგ, კომპიუტერისა და აღნიშნული ავტორიზაციის პარამეტრების გამოყენებით, შეაღწია მოცემული მომხმარებლის სოციალური ქსელის გვერდზე (კომპიუტერული სისტემა) და მისი სახელით მიმოწერა აწარმოა მომხმარებლის მეგობრებთან.



ვინაიდან დამნაშავემ უნებართვოდ შეაღწია სხვის კომპიუტერულ სისტემაში (სოციალური ქსელის გვერდზე), ადგილი აქვს კიბერდანაშაულს.

მაგალითი 3.

დამნაშავე ელექტრონული ფოსტით დაუკავშირდა პიროვნებას მისი კლასელი გიორგის სახელით და მოატყუა, რომ ახლა იმყოფება მეზობელ ქვეყანაში, დაკარგა როგორც ტელეფონი, ასევე პირადი დოკუმენტაცია და გარკვეული პირობების გამო, ახალი ელექტრონული ფოსტის გახსნა დასჭირდა. წერილში იგი მას დახმარებას და გარკვეული თანხის კონკრეტულ ანგარიშზე გადაგზავნას სთხოვდა. ადრესატი ამ სიცრუეს წამოეგო, დაიჯერა, რომ ნამდვილად მისი კლასელი წერდა და დამნაშავეს თანხა გადაურიცხა.



ვინაიდან დამნაშავეს უნებართვოდ არ შეუღწევია სხვის ელექტრონულ ფოსტაზე და თაღლითურად, თანხის მოტყუებით დაუფლების მიზნით, შექმნა ახალი ელექტრონული ფოსტა, ეს დანაშაული კვალიფიცირდება როგორც თაღლითობა, ხოლო დანაშაულის ჩადენის მეთოდად გამოყენებულია კიბერმეთოდები ანუ ინტერნეტი, როგორც კომუნიკაციის საშუალება.

კიბერდანაშაულს საკმაოდ ხშირად არასრულწლოვნები ჩადიან. მათი ნაწილის მიზანი კომპიუტერულ სისტემაში შენახული ინფორმაციის (ფოტოსურათი, პირადი მომოწერა) დაუფლებაა, ნაწილის კი - ფინანსური სარგებელი (საბანკო ანგარიშზე, ელექტრონულ საფულეზე შესვლა და თანხის ქურდობა), ხოლო ნაწილს მხოლოდ თავისი შესაძლებლობის გამოცდა სურს და სხვა მიზანი არ ამოძრავებს.

უმეტეს შემთხვევაში არასრულწლოვანთა უმრავლესობას არ ჰგონია, რომ სხვის კომპიუტერულ სისტემაში უნებართვო შეღწევით ან სხვა მსგავსი სახის უკანონო ქმედებით დანაშაულს ჩადის, **თუმცა კანონის არცოდნა პასუხისმგებლობისგან არავის ათავისუფლებს.** ყველა მოქალაქე ვალდებულია, იცოდეს კანონი და პატივი სცეს კანონით დაცულ სამართლებრივ სიკეთეს.

რა ხერხებით ხდება ადამიანის პერსონალური მონაცემებისა და პირადი ცხოვრების ამსახველი ინფორმაციის მოპოვება, ანუ კიბერდანაშაულის ჩადენა?

კიბერდამნაშავეები ინტერნეტ სივრცეში ხშირად ცდილობენ მომხმარებელთა მოტყუებას, ქმნიან სოციალური ქსელების, ელექტრონული ფოსტებისა და კომუნიკაციისთვის საჭირო სხვა რეალური ვებგვერდების მსგავს გვერდებს. ამის შემდეგ კი, უკავშირდებიან ამ ვებგვერდების რეალური მომხმარებლის მეგობრებს, ვითომდა, არიან მათი მეგობრები და ფულადი თანხის გადარიცხვას სთხოვენ მათ; ან მათთან პირადი ცხოვრების შესახებ საუბრობენ და მოპოვებულ ინფორმაციას მოტყუებული მომხმარებლის საწინააღმდეგოდ იყენებენ. ასევე, მრავლადაა ე.წ. ყალბი გვერდები, რომლებიც ჩვენი, ანუ მომხმარებლის გვერდის ავტორიზაციის პარამეტრებს ან საბანკო რეკვიზიტებს იმახსოვრებენ.

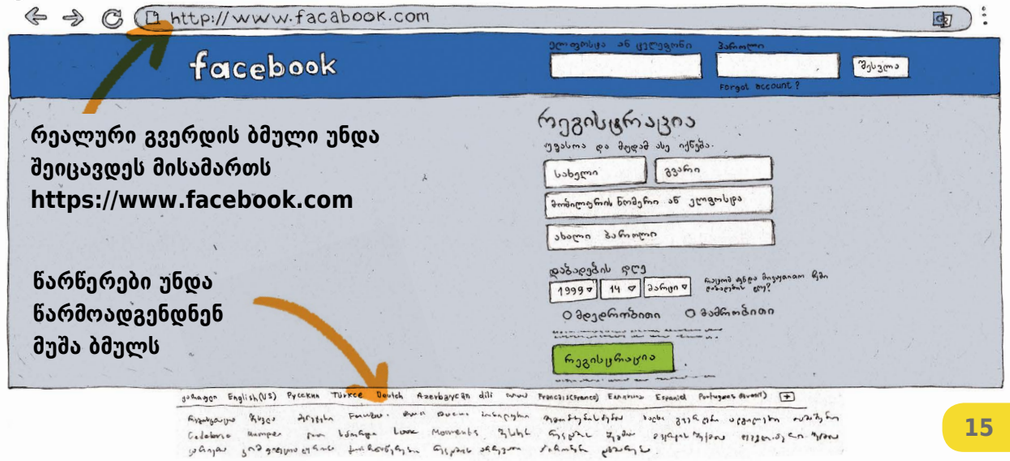
პერსონალური და საბანკო მონაცემების შესახებ ინფორმაციის მოპოვება შესაძლებელია სხვადასხვაგვარი ხერხებით, თუმცა საქართველოში ყველაზე გავრცელებული კიბერდანაშაული ***„ფიშინგის“ (phishing), „ქარდინგისა“ (carding) და ვებგვერდებზე თავდასხმის*** (უნებართვო შეღწევის, მონაცემების წაშლის, შეცვლის და სხვ.) გზით ხორციელდება. განვიხილოთ თითოეული მათგანი.

ფიშინგი

„ფიშინიგი“ არის მსხვერპლის ავტორიზაციის პარამეტრების ან მსგავსი ტიპის მონაცემების მოტყუებით მოპოვება, რაც დამნაშავეს მის პირად გვერდზე უნებართვოდ შეღწევის შესაძლებლობას აძლევს.

კიბერსივრცეში სხვადასხვა სოციალური ქსელებისა თუ მომხმარებლის გვერდებზე შესასვლელად საჭიროა ავტორიზაციის პარამეტრების - კერძოდ, მომხმარებლის სახელისა და პაროლის მითითება (მაგ: facebook.com-ზე შესასვლელად შესაბამის ველებში მომხმარებლის სახელი და პაროლი უნდა მივუთითოთ). „ფიშინგის“ დროს ე.წ. ჰაკერი ქმნის, მაგალითად, სოციალური ქსელის მიმსგავსებულ ვებგვერდს, რომელიც რეალური გვერდის თითქმის ზუსტი ასლია, თუმცა მათ შორის განსხვავებაც არის (იხ. სურათი 1 და 2). ყალბი გვერდის შემქმნელის მიზანია მომხმარებლის შეცდომაში შეყვანა, თითქოს ის ნამდვილ გვერდზეა შესული. მოტყუებული მომხმარებელი გვერდზე შესასვლელად ავტორიზაციის პარამეტრებს უთითებს, თუმცა, სინამდვილეში, მითითებული მომხმარებლის სახელი და პაროლი ყალბი გვერდის შემქმნელს ეგზავნება, თავად კი, ვერ შედის გვერდზე, რასაც გვერდის გაუმართავად მუშაობას აბრალებს. ამგვარად, მომხმარებელი ვერც კი ხვდება, რომ აღნიშნული ქმედებით, ფაქტობრივად, გადასცა თავისი სახელი და პაროლი უცნობ ადამიანს, რომელსაც ნებისმიერ დროს უნებართვოდ შეუძლია შეაღწიოს მის პირად გვერდზე.

საზოგადოებაში ხშირად მოვისმენთ გამოთქმას, რომ მომხმარებელს „გაუტეხეს“ ესა თუ ის გვერდი. ზემოთ თქმულიდან გამომდინარე ნათელია, რომ ეს არასწორი შეხედულებაა, რადგან ამ შემთხვევაში ხდება არა „გატეხვა“, არამედ ავტორიზაციის პარამეტრების მოპოვება ვებგვერდზე უნებართვოდ შეღწევის მიზნით. ე.წ. „გატეხვა“ რომ შესაძლებელი იყოს (იგულისხმება არა რომელიმე მომხმარებლის გვერდის „გატეხვა“, არამედ მთლიანად სოციალური ქსელის), არცერთ სოციალურ ქსელს არ ექნებოდა ის პოპულარობა, რაც მათ გააჩნია.



მაგალითად, ე.წ. ჰაკერმა სოციალურ ქსელში დადო სკანდალური განცხადება, რომლითაც ინტერნეტმომხმარებელთა უმრავლესობა დაინტერესდა. განცხადების სრულად სანახავად საჭირო იყო ბმულზე ე.წ. ლინკზე გადასვლა. ინტერნეტმომხმარებლების მიერ ბმულზე გადასვლის შემდეგ ეკრანზე გამოდიოდა ფანჯარა, სადაც გამოსახული იყო სოციალური ქსელის ავტორიზაციის გვერდი. იქმნებოდა წარმოდგენა, რომ მომხმარებელი „გვერდმა გამოაგდო“ და უკან დასაბრუნებლად შესაბამის ველებში სახელსა და პაროლს უთითებდა. შემდეგ აჭერდა შესვლის (Enter) ღილაკს და ბრუნდებოდა სოციალური ქსელის თავის გვერდზე. სინამდვილეში, ამ დროს „ფიშინგის“ შემქმნელს ეგზავნებოდა მომხმარებლის სახელი და პაროლი, უნებართვოდ აღწევდა მომხმარებლის გვერდზე, ცვლიდა პაროლს და გვერდიდან „აგდებდა“ რეალურ მომხმარებელს, რის შემდეგაც რეალური მომხმარებელი საკუთარ გვერდზე წვდომას კარგავდა.

მეორე მაგალითი ეხება 2016 წლის ნოემბერში პერსონალურ მონაცემთა დაცვის ინსპექტორის მიერ გამოქვეყნებულ გაფრთხილებას მოქალაქეებისადმი. გაფრთხილება შეეხებოდა ინტერნეტ სივრცეში გამოჩენილ ახალ ვებგვერდს - „შეამოწმე შენი მონაცემები,“ რომელიც მოქალაქეებს სთავაზობდა იმის შემოწმებას, დავირუსებულია თუ არა მათი ანგარიში.

გამაფრთხილებელი განაცხადი:

ჰაკერი - პირი, რომელიც კომპიუტერული სისტემის მეშვეობით არალეგალურად მოიპოვებს წვდომას სხვა პიროვნების ან დაწესებულების კომპიუტერულ მონაცემებზე.

„პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი გაფრთხილებთ, არ შეასრულოთ ამ საიტის ინსტრუქციები, რადგან მისი მიზანი, დიდი ალბათობით, თქვენი საბანკო მონაცემების შეგროვება და საკუთარი ინტერესებისთვის გამოყენებაა. ვებგვერდი ცდილობს დაგარწმუნოთ, რომ მათ ბაზაში მილიონზე მეტი დავირუსებული ანგარიშია და მათ შორის შეიძლება თქვენიც იყოს. ამის შესამოწმებლად კი თქვენგან ითხოვს სახელის და გვარის, საბანკო ბარათის ნომრის, მისი მოქმედების ვადის და CVC კოდის შეყვანას. ამ მონაცემების გამოყენებით თაღლითებმა, შესაძლოა, სხვადასხვა სახის ზიანი მოგაყენონ, მაგალითად, თქვენს ნაცვლად იყიდონ ნივთები ონლაინ მაღაზიებში."

წყარო: ***http://liberali.ge/news/view/26131/ar-miutitot-sabanko-monatsemebi--personalur-monatsemta-datsvis-inspeqtorisgafrtkhileba***

ქარდინგი

„ქარდინგი“ არის საბანკო პლასტიკური ბარათის მონაცემების მოპოვება („ფიშინგით“, „სკიმერით“, „ქარდ რიდერით“ და ა.შ.) და შემდგომ ამ ინფორმაციის გაყიდვა ან გამოყენება ფინანსური სარგებლის მიღების მიზნით.

თანამედროვე სამყაროში ფიზიკური ფულადი ერთეულის ბრუნვა შეიცვალა ელექტრონული ფულადი ბრუნვით, შესაბამისად, მომსახურეობის ან პროდუქციის შესაძენად, ხშირ შემთხვევაში, გადახდის ფორმად შეგვიძლია, ავირჩიოთ უნაღდო ანგარიშსწორება და ფიზიკურად ფულის თან ქონა აღარ არის საჭირო. აქტიურად ხდება საბანკო სერვისების გამოყენება საბანკო პლასტიკური ბარათის მეშვეობით, თუმცა ბევრ ჩვენგანს ვერც წარმოუდგენია, რომ საბანკო პლასტიკური ბარათის გამოყენება, შესაძლებელია, საფრთხის შემცველი იყოს და მატერიალური ზიანი მოგვადგეს. არსებობს მრავალი ტიპის საბანკო ბარათი. მათგან ყველაზე გავრცელებულია სამი ტიპის ბარათი:

1. **სადებეტო ანუ სახელფასო ბარათი** - ბარათი, რომელიც მფლობელს საშუალებას აძლევს, ემიტენტსა და ბარათის მფლობელს შორის გაფორმებული ხელშეკრულების საფუძველზე განკარგოს მის საბარათე ანგარიშზე არსებული თანხები, ასევე ისარგებლოს ოვერდრაფტით;

2. **საკრედიტო ბარათი - ბარათი**, რომელიც ემიტენტთან გაფორმებული ხელშეკრულების პირობების შესაბამისად, ბარათის მფლობელს საშუალებას აძლევს, ოპერაციები მოახდინოს ემიტენტის მიერ მინიჭებული საკრედიტო ხაზის ფარგლებში;

3. **წინასწარი გადახდის ბარათი - ბარათი**, რომელიც არ საჭიროებს ბარათის მფლობელის ან ბარათის შემძენის სახელზე საბარათე ანგარიშის გახსნას. აღნიშნული ბარათით ოპერაციები მხოლოდ წინასწარ ჩარიცხული თანხის ფარგლებში სრულდება.

გარდა ამისა, არსებობს პერსონიფიცირებული და არაპერსონიფიცირებული საბანკო პლასტიკური ბარათები. პერსონიფიცირებულია, რომელზეც ასახულია მომხმარებლის სახელი (შესაძლოა, მხოლოდ ინიციალი) და გვარი, ხოლო არაპერსონიფიცირებულია, რომელზეც არ არის ასახული მომხმარებლის სახელი ან/და გვარი. თუმცა, უმრავლეს საბანკო პლასტიკურ ბარათს გააჩნია მაგნიტური ველი

(პლასტიკური ბარათის უკანა მხარეს არსებული მოშავო ფერის ზოლი), პლასტიკური ბარათის ნომერი, მოქმედების ვადა და ე.წ. CVC კოდი. აღნიშნული მონაცემების სხვის ხელში აღმოჩენის შემთხვევაში შესაძლებელია, საბანკო პლასტიკური ბარათის ფიზიკურად არქონის მიუხედავად, მოხდეს საბანკო ანგარიშიდან მოხსნა ან ინტერნეტ სივრცეში პროდუქციის შეძენა.

მაგალითად, ერთ-ერთ რესტორანში მას შემდეგ, რაც კლიენტმა შეკვეთილი კერძების გადახდა საბანკო პლასტიკური ბარათით დააპირა, მიმტანმა მას მოატყუა, რომ საბანკო ტერმინალს გარკვეული ტექნიკური ხარვეზები ჰქონდა, ამიტომ ტერმინალი ფიქსირებული იყო სხვა ოთახში და მოტანა არ შეეძლო. ამ მიზეზით მიმტანმა კლინეტს სთხოვა, მისთვის გადაეცა ბარათი, რომელსაც თანხის ჩამოჭრის შემდეგ უკან დაუბრუნებდა. კლიენტი მას ენდო და თავისი საბანკო პლასტიკური ბარათი გადასცა. მიმტანმა ბარათი სხვა ოთახში შეიტანა, კლიენტისგან მალულად ფოტო გადაუღო, შემდეგ ტერმინალის საშუალებით კლიენტის მიერ დახარჯული თანხა ჩამოაჭრა და ქვითართან ერთად უკან დაუბრუნა. კლიენტი ვერაფერს მიხვდა, თუმცა, რესტორნის მიმტანმა მისი საბანკო პლასტიკური ბარათის მონაცემების გამოყენებით რამდენჯერმე შეიძინა სხვადასხვა ნივთი ინტერნეტში.

საბანკო პლასტიკური ბარათის მონაცემების დამახსოვრება შესაძლებელია საბანკო ტერმინალების გამოყენების დროსაც, თუ ტერმინალზე დამნაშავე დამატებით მოწყობილობას ჩააშენებს. დანაშაულის ამ ფორმას „სქიმინგი“ ეწოდება. „სქიმინგის“ დროს დამნაშავეები სხვადასხვა ხერხს იყენებენ, მაგალითად, ე.წ. ბანკომატებზე ამონტაჟებენ სხვადასხვა სახის მოწყობილობებს, რომელიც იმახსოვრებს საბანკო პლასტიკური ბარათის მონაცემებს და მათი გადატანა სხვა საბანკო პლასტიკურ ბარათზე ხდება (იხ. სურათი 3). შედეგად, ყალბი საბანკო პლასტიკური ბარათი, რომელზეც ნამდვილი საბანკო პლასტიკური ბარათის მონაცემებია გადატანილი, ყოველგვარი დაბრკოლების გარეშე შეიძლება გამოიყენონ სხვა პირის ანგარიშიდან თანხის მოსახსნელად.

ვებგვერდებზე თავდასხმა

ინტერნეტში მრავლადაა პოპულარული და არაპოპულარული ვებგვერდები, რომელიც კიბერდამნაშავეთა სამიზნეს წარმოადგენს. სწორედ ვებგვერდებზე უნებართვო შეღწევის გზით აღწევენ კიბერდამნაშავეები სხვადასხვა მიზანს, როგორიცაა, მაგალითად: ვებგვერდზე რეგისტრირებულ მომხმარებელთა მონაცემების დაუფლება ან სხვადასხვა შინაარსის გამოსახულებების განთავსება ტექსტისა თუ ფოტოსურათის სახით. ვინაიდან ინტერნეტის მომხმარებელთა უმრავლესობა ერთი და იგივე მომხმარებლის სახელითა და პაროლითაა რეგისტრირებული სხვადასხვა ვებგვერდებზე, დამნაშავეებს შეუძლიათ უკანონოდ მოპოვებული მომხმარებლის სახელისა და პაროლის გამოყენებით ყველა ამ ვებგვერდზე შევიდნენ და სასურველ ინფორმაციას დაეუფლონ ან მატერიალური სარგებელი მიიღონ.

მაგალითი

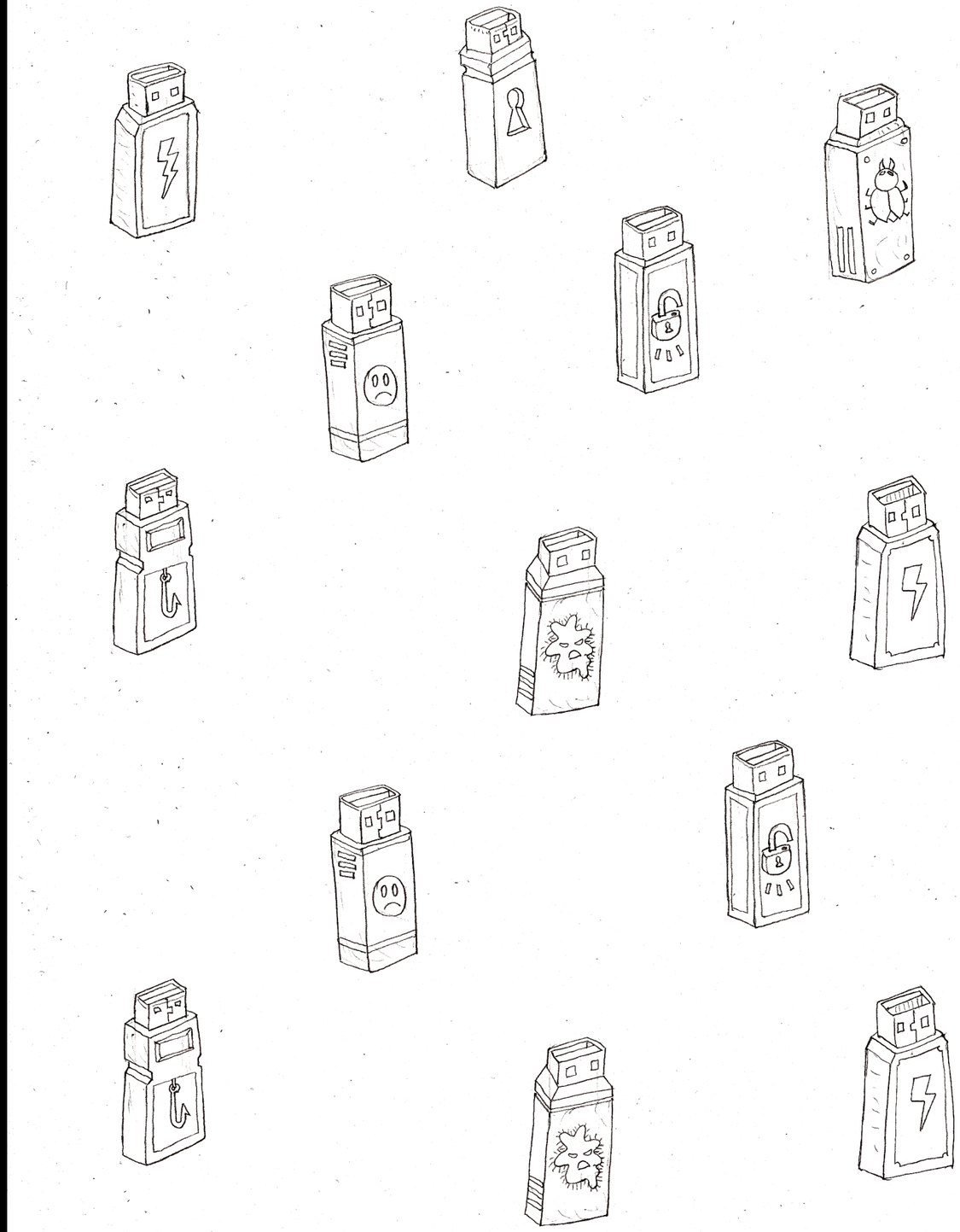
ერთ-ერთ პოპულარულ ვებგვერდზე, რომელზეც ინტერნეტის მეშვეობით პროდუქციის შეძენა შეიძლებოდა, აუცილებელი პირობა იყო ვებგვერდზე რეგისტრაციის გავლა.

აღნიშნულ ვებგვერდს ძალიან მალე კონკურენტები გამოუჩნდა, რის გამოც მისი პოპულარობა სულ უფრო შემცირდა, საბოლოოდ კი, მასზე პროდუქციის გაყიდვა შეწყდა. შექმნილი ვითარებიდან გამომდინარე, ვებგვერდს მფლობელებისგან სათანადო ყურადღება აღარ ექცეოდა, რის გამოც იგი მარტივად გახდა კიბერთავდასხმის მსხვრპლი. კერძოდ, დამნაშავემ შეაღწია ვებგვერდზე, წაშალა იქ განთავსებული სურათები და განათავსა წარწერა “HACKED“; ამავდროულად, წვდომა მოიპოვა ვებგვერდის მონაცემთა ბაზაზე, სადაც რეგისტრირებული მომხმარებლების ავტორიზაციის პარამეტრები (სახელი და პაროლი) იყო მითითებული.

დამნაშავემ გაიაზრა, რომ მომხმარებლების ნაწილს სხვადასხვა ვებგვერდზე რეგისტრაციის დროს, შესაძლოა, ერთი და იგივე მომხმარებლის სახელი და პაროლი გამოეყენებინა. ამიტომ იგი შეეცადა, მოპოვებული მომხმარებლების ავტორიზაციის პარამეტრების საშუალებით, ეს მომხმარებლები სხვადასხვა ვებგვერდზე მოეძია და მათ პირად გვერდებზე შეეღწია, რაც წარმატებით გამოუვიდა - სოციალური ქსელის facebook.com-ის გვერდზე ავტორიზაციისთვის მომხმარებელთა ნაწილი იმავე მომხმარებლის სახელსა და პაროლს იყენებდა, რომლის მოპოვებაც დამნაშავემ შეძლო.

აღნიშნულ მომხმარებელთა ვებგვერდზე შეღწევის შემდეგ, დამნაშავემ ისინი სოციალურ ქსელში facebook.com მის მიერ შექმნილ ჯგუფში დაამატა, რომელსაც რეკლამის განსათავსებლად იყენებდა და ამგვარად გაზარდა ჯგუფის მომხმარებელთა რაოდენობა.

hacked



შემთხვევების განხილვა

ქვემოთ მოცემულია:

• კანონმდებლობის ის მუხლები, რომლებიც არეგულირებს კიბერდანაშაულს;
• შემთხვევები, რომელთა მსგავს შემთხვევებსაც რეალურად ჰქონდა ადგილი, თუმცა, მოქმედი პირების სახელები და პიროვნების მაიდენტიფიცირებელი სხვა დეტალები შეცვლილია.

ინსტრუქცია ჯგუფური სამუშაოსთვის:

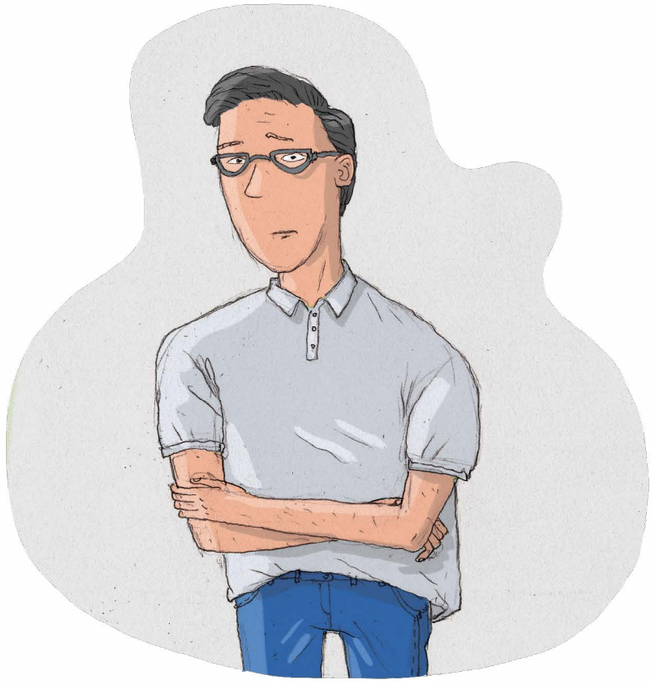
შექმენით მცირე ჯგუფები თანაკლასელებთან ერთად, გაეცანით მოცემულ შემთხვევებს და უპასუხეთ ქვემოთ დასმულ კითხვებს:

• თქვენ მიერ განხილულ შემთხვევაში ადგილი აქვს კიბერდანაშაულს თუ კიბერ მეთოდებით ჩადენილ დანაშაულს?
• კონკრეტულად, რა დანაშაულს აქვს ადგილი?
• რა საფრთხის წინაშე აღმოჩნდა მსხვერპლი?
• საქართველოს სისხლის სამართლის კოდექსის რომელი მუხლით/მუხლებით რეგულირდება ეს დანაშაული?

შემთხვევების განხილვის შემდეგ თითოეულმა ჯგუფმა მოკლედ წარმოადგინეთ თქვენი მოსაზრება ქვემოთ მოცემული ცხრილის დახმარებით

ცხრილი 1

შემთხვევის N	დანაშაულის ტიპი (კიბერდანაშაული თუ კიბერ მეთოდებით ჩადენილი დანაშაული?)	გამოკვეთილი დანაშაული	საფრთხე, რომელიც იქმნება მსხვერპლისთვის	სისხლის სამართლის კოდექსის შესაბამისი მუხლი



შემთხვევა N1

გიორგის ბავშვობიდან აინტერესებდა კომპიუტერული ტექნოლოგიები და ინტერნეტ სივრცეში ხშირად ეძებდა სიახლეებსა თუ სხვადასხვა სახის ინფორმაციებს კომპიუტერული ტექნოლოგიების სტრუქტურისა და მოწყობის შესახებ. ეტაპობრივად მან ვებგვერდის შექმნაც შეძლო დამოუკიდებლად და დაინტერესდა, რამდენად იყო დაცული მისი გვერდი ჰაკერული თავდასხმისაგან. ამ მიზნით მოიძია ინფორმაცია, თუ როგორ და რა ხერხებით მუშაობენ ჰაკერები. შემდეგ კი ახლად ნასწავლი ჰაკერული ტექნიკის გამოყენება მან რეალურ ვებგვერდზე სცადა და თანმიმდევრობით შეასრულა ჰაკერთა მოქმედებები, რათა დარწმუნებულიყო, რამდენად რეალური იყო ეს ტექნიკა და რამდენად კარგად გამოუვიდოდა თავად იგივეს გაკეთება.

აღმოჩნდა, რომ მან მართლაც შეძლო ერთ-ერთ ვებგვერდზე უნებართვო შესვლა, რის შემდეგაც გვერდზე არსებული ინფორმაცია წაშალა და, ამგვარად, გვერდის ადმინისტრატორებმა მასზე წვდომა დაკარგეს. დაზარალებულმა კომპანიამ დახმარებისათვის საქართველოს შინაგან საქმეთა სამინისტროს მიმართა.

კიბერშეტევის ამსახველი ინფორმაციის გაანალიზებით დანაულის ჩამდენი დადგინდა, რომელმაც განაცხადა, რომ მხოლოდ საკუთარი შესაძლებლობების გამოცდა უნდოდა, სხვა რაიმე ზიანის მიყენების განზრახვა არ ჰქონია და არც ის იცოდა, რომ აღნიშნული ქმედებით დანაშაულს სჩადიოდა.

შემთხვევა N2

17 წლის გოგამ facebook-ის ყალბი გვერდი შექმნა და მისი მისამართი თავისივე თანასკოლელს, 16 წლის თამთას გაუგზავნა. თამთამ გოგასგან გამოგზავნილი მისამართი მიიღო, გადავიდა მასზე და ავტორიზაციაც გაიარა (მიუთითა მომხმარებლის სახელი და პაროლი). შედეგად, გოგა თამთას facebook-ის ავტორიზაციის პარამეტრებს დაეუფლა, შემდეგ კი მისგან მალულად შეაღწია თამთას გვერდზე და ყველა პირადი მიმოწერა წაიკითხა, რომელიც არა მხოლოდ თამთას, არამედ მისი მეგობრების შესახებ პირად ინფორმაციასაც შეიცავდა. მიმოწერები გოგამ ფოტოების სახით შეინახა.

ამის შემდეგ გოგამ თამთას მიმოწერის ამსახველი ფოტოები და შეტყობინება გაუგზავნა, რომლითაც გოგონას თავისი შიშველი ფოტოების გაგზავნას სთხოვდა, წინააღმდეგ შემთხვევაში, მის პირად მიმოწერებს გაასაჯაროებდა.

შემთხვევა N3

თამუნაზე შეყვარებულმა ლაშამ, გადაწყვიტა, მისი ნებართვის გარეშე შესულიყო თამუნას გვერდზე სოციალურ ქსელში facebook.com მომხმარებლის სახელისა და პაროლის მოპოვების მიზნით. ამისათვის მან თავის პერსონალურ კომპიუტერში სპეციალური პროგრამა ჩაწერა, რომელიც კლავიატურაზე აკრეფილ ინფორმაციას იმახსოვრებდა.

ერთხელაც, ლაშას სახლში სტუმრად ყოფნის დროს, თამუნამ ლაშას კომპიუტერით გახსნა facebook.com-ის საკუთარი გვერდი, რისთვისაც, რა თქმა უნდა, ავტორიზაციის გვერდზე შესაბამისი მომხმარებლის სახელი და პაროლი მიუთითა.

მოგვიანებით, კომპიუტერში ჩაწერილი სპეციალური პროგრამის დახმარებით, თამუნას პირად გვერდზე ავტორიზაციის სახელი და პაროლი ლაშასთვის ხელმისაწვდომი გახდა და მან მომხმარებლის სახელისა და პაროლის მოპოვება შეძლო. შემდეგ კი ნებართვის გარეშე შევიდა შეყვარებულის პირად გვერდზე, თუმცა, არ იცოდა, რომ თამუნას უსაფრთხოების პარამეტრები ჰქონდა გააქტიურებული. შედეგად, გოგონამ საკუთარ მობილურ ტელეფონზე ინფორმაცია მიიღო მის გვერდზე შესვლის შესახებ.

თამუნამ დახმარებისათვის შსს სამინისტროს მიმართა. გამოძიებით დადგინდა, თუ საიდან, როდის და ვის მიერ მოხდა თამუნას გვერდზე შესვლა. ლაშას განმარტებით, მან არ იცოდა, რომ მის მიერ ჩადენილი ქმედება დანაშაული იყო და საკუთარი ქცევის მიზეზად ეჭვიანობა დაასახელა.

შემთხვევა N4

დამნაშავეების ჯგუფმა, რომელთაც სურდათ, დანაშაული ისე ჩაედინათ, რომ თავად არავის მოხვედროდნენ თვალში, საქმეში არასრულწლოვნების გამოყენება გადაწყვიტა. ამ მიზნით ჯგუფის ერთერთი წევრი, 36 წლის ლია სოციალურ ქსელში 19 წლის ოთოს სახელით დარეგისტრირდა, შექმნილ გვერდზე განათავსა უცხოელი თინეიჯერის პირადი გვერდიდან ჩამოტვირთული ფოტოები და იმავე სოციალური ქსელის საშუალებით, გაცნობის მიზნით, 14 წლის ნუცას დაუკავშირდა. ნუცაც დაეთანხმა ვირტუალურ სივრცეში მეგობრობის თხოვნას.

„ოთო“ თითქმის ყოველ დღე ეხმიანებოდა ნუცას, ეკითხებოდა თუ როგორ ჩაიარა სკოლაში დღემ, როგორ გაერთო მეგობრებთან ერთად, რა ფილმის ყურებას აპირებდა და სხვა მსგავსი თემები. თანდათან „ოთომ“ ნუცასთან პირად მიმოწერაში საკმაოდ „გულახდილი“ საუბარი დაიწყო საკუთარ ცხოვრებაზე, პრობლემებზე, სამომავლო გეგმებზე, რითაც ნუცას ნდობა დაიმსახურა და გულის გადაშლის სურვილი მასაც გაუჩინა. მალე „ოთომ“ საკმაოდ ბევრი ინფორმაცია შეიტყო ნუცას პირადი ცხოვრების, მისი სუსტი მხარეებისა და მის ოჯახში არსებული პრობლემების შესახებ.

ერთ დღესაც, ნუცამ „ოთოსგან“ მისთვის მოულოდნელად, სრულიად განსხვავებული შინაარსის წერილი მიიღო. წერილით „ოთო“ მისგან ისეთი ქმედების შესრულებას მოითხოვდა, რომელიც დანაშაულის ნიშნებს შეიცავდა. „ოთო“ ნუცას ემუქრებოდა, თუ ნუცა მოთხოვნის შესრულებაზე უარს ეტყოდა, იგი მათ მიმოწერას ნუცას ყველა მეგობარს გაუზიარებდა და ნუცას პირადი და ოჯახური ცხოვრების დეტალები ყველასთვის ცნობილი გახდებოდა. თავზარდაცემულმა ნუცამ მოთხოვნის შესრულება გადაწყვიტა. თუმცა, სიტუაცია სულ უფრო და უფრო გართულდა, რადგან „ოთო“ მას ახალ-ახალ დავალებებს აძლევდა, რომელთაგან ზოგიერთი შედარებით უწყინარი, ზოგი კი საფრთხისა და დანაშაულის ნიშნების შემცველი იყო.

გარკვეული დროის შემდეგ ნუცამ „ოთოს“ მისწერა, რომ მისთვის არ ჰქონდა მნიშვნელობა, გასაჯაროვდებოდა თუ არა მათი მიმოწერა და ამიტომ მისი მოთხოვნების შესრულებას აღარ აპირებდა.

დამნაშავეთა ჯგუფმა ნუცას კიდევ უფრო დაშინება გადაწყვიტა და „ოთოს“ სახელით კვლავ გაუგზავნეს წერილი, რომლითაც ნუცას ოჯახის წევრებისთვის ზიანის მიყენებით დაემუქრნენ. სინამდვილეში ისინი ამის გაკეთებას არ აპირებდნენ, რადგან კარგად იცოდნენ, რომ მსგავსი რამ სერიოზული დანაშაულია და ციხეში აღმოჩნდებოდნენ, მაგრამ მათ მუქარამ ნუცაზე იმოქმედა - მიცემული დავალებების უსიტყვოდ შესრულების გარდა გოგონა სხვა გამოსავალს ვეღარ ხედავდა, რადგან არ სურდა, მისი შეცდომის გამო ოჯახის წევრებისთვის საფრთხე შეექმნა.

ნუცას პოლიციისთვის არ მიუმართავს, რადგან თუ ამას იზამდა, „ოთო“ მისი ოჯახის წევრებისთვის კიდევ უფრო დიდი ზიანის მიყენებით ემუქრებოდა.

კანონმდებლობა, რომელიც ამ სფეროს არეგულირებს / როგორ ისჯება კიბერდამნაშავე?

საქართველოს სისხლის სამართლის კოდექსის **XXXV** თავი კიბერდანაშაულს ეთმობა და **284**-ე, **285**-ე და **286**-ე მუხლებს მოიცავს:

მუხლი 284. კომპიუტერულ სისტემაში უნებართვო შეღწევა

1. კომპიუტერულ სისტემაში უნებართვო შეღწევა, – ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ანდა თავისუფლების აღკვეთით იმავე ვადით.

2. იგივე ქმედება:
ა) წინასწარი შეთანხმებით ჯგუფის მიერ;
ბ) სამსახურებრივი მდგომარეობის გამოყენებით;
გ) არაერთგზის;
დ) რამაც მნიშვნელოვანი ზიანი გამოიწვია, – ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ანდა თავისუფლების აღკვეთით ვადით ორიდან ხუთ წლამდე.

შენიშვნა:

1. კომპიუტერული სისტემა არის ნებისმიერი მექანიზმი ან ერთმანეთთან დაკავშირებულ მექანიზმთა ჯგუფი, რომელიც პროგრამის მეშვეობით, ავტომატურად ამუშავებს მონაცემებს (მათ შორის, პერსონალური კომპიუტერი, ნებისმიერი მოწყობილობა მიკროპროცესორით, აგრეთვე, მობილური ტელეფონი).

2. კომპიუტერული მონაცემი არის კომპიუტერულ სისტემაში დამუშავებისათვის ხელსაყრელი ნებისმიერი ფორმით გამოსახული ინფორმაცია, მათ შორის, პროგრამა, რომელიც კომპიუტერული სისტემის ფუნქციონირებას უზრუნველყოფს.

3. უნებართვო გულისხმობს უკანონოს, აგრეთვე, იმ შემთხვევას, როდესაც უფლების მფლობელს პირდაპირ ან არაპირდაპირ არ გადაუცია უფლება ქმედების ჩამდენი პირისათვის.

4. ამ თავში მნიშვნელოვნად ითვლება 2000 ლარზე მეტი ოდენობის ზიანი.

5. ამ მუხლით გათვალისწინებული ქმედებისათვის იურიდიული პირი ისჯება ჯარიმით, საქმიანობის უფლების ჩამორთმევით ან ლიკვიდაციითა და ჯარიმით.

მუხლი 285. კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის უკანონოდ გამოყენება

1. კომპიუტერული პროგრამის ან/და სხვა მოწყობილობის, აგრეთვე, კომპიუტერულ სისტემაში შეღწევისათვის საჭირო პაროლის, დაშვების კოდის ან სხვა მსგავსი მონაცემის უნებართვო დამზადება, შენახვა, გაყიდვა, გავრცელება ან ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა ამ თავითა და ამ კოდექსის 158-ე ან 159-ე მუხლით გათვალისწინებული დანაშაულის ჩადენის გამო, – ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ან/და თავისუფლების აღკვეთით ვადით სამ წლამდე.

2. ამ მუხლის პირველი ნაწილით გათვალისწინებული ქმედება:
ა) წინასწარი შეთანხმებით ჯგუფის მიერ;
ბ) სამსახურებრივი მდგომარეობის გამოყენებით;

გ) არაერთგზის;
დ) რამაც მნიშვნელოვანი ზიანი გამოიწვია, – ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ან/და თავისუფლების აღკვეთით ვადით სამიდან ექვს წლამდე.

შენიშვნა: ამ მუხლით გათვალისწინებული ქმედებისათვის იურიდიული პირი ისჯება ჯარიმით, საქმიანობის უფლების ჩამორთმევით ან ლიკვიდაციითა და ჯარიმით.

მუხლი 286. კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის ხელყოფა

1. კომპიუტერული მონაცემის უნებართვო დაზიანება, წაშლა, შეცვლა ან დაფარვა, – ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ან/და თავისუფლების აღკვეთით იმავე ვადით.

2. ამ მუხლის პირველი ნაწილით გათვალისწინებული ქმედება, აგრეთვე, კომპიუტერული მონაცემის უნებართვო ჩასმა ან გადაცემა, რამაც კომპიუტერული სისტემის ფუნქციონირების განზრახ მნიშვნელოვანი შეფერხება გამოიწვია, – ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ან/და თავისუფლების აღკვეთით ვადით სამ წლამდე.

3. ამ მუხლის პირველი ან მე-2 ნაწილით გათვალისწინებული ქმედება:

ა) წინასწარი შეთანხმებით ჯგუფის მიერ;
ბ) სამსახურებრივი მდგომარეობის გამოყენებით;
გ) არაერთგზის;
დ) რამაც მნიშვნელოვანი ზიანი გამოიწვია, – ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ანდა თავისუფლების აღკვეთით ვადით სამიდან ხუთ წლამდე.

შენიშვნა: ამ მუხლით გათვალისწინებული ქმედებისათვის იურიდიული პირი ისჯება ჯარიმით, საქმიანობის უფლების ჩამორთმევით ან ლიკვიდაციითა და ჯარიმით.

გარდა ამისა, ყურადღება შეიძლება გამახვილდეს საქართველოს სისხლის სამართლის კოდექსის 150-ე, 157-ე, 158-ე და 159-ე მუხლებზეც, ვინაიდან ეს მუხლები ზოგჯერ კავშირშია კიბერდანაშაულთან ან კიბერმეთოდებით ჩადენილ დანაშაულთან.

მუხლი 150. იძულება

1. ადამიანისათვის ქმედების თავისუფლების უკანონო შეზღუდვა, ე.ი. მისი ფიზიკური ან ფსიქიკური იძულება, შეასრულოს ან არ შეასრულოს მოქმედება, რომლის განხორციელება ან რომლისაგან თავის შეკავება მის უფლებას წარმოადგენს, ანდა საკუთარ თავზე განიცადოს თავისი ნება-სურვილის საწინააღმდეგო ზემოქმედება, – ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ერთ წლამდე ანდა თავისუფლების აღკვეთით იმავე ვადით.

[1. ადამიანისათვის ქმედების თავისუფლების უკანონო შეზღუდვა, ე.ი. მისი ფიზიკური ან ფსიქიკური იძულება, შეასრულოს ან არ შეასრულოს მოქმედება, რომლის შესრულება ან რომლის შესრულებისაგან თავის შეკავება მისი უფლებაა, ანდა საკუთარ თავზე განიცადოს თავისი ნება-სურვილის საწინააღმდეგო ზემოქმედება, – ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ერთ წლამდე ან შინაპატიმრობით ვადით ექვსი თვიდან ორ წლამდე ანდა თავისუფლების აღკვეთით ვადით ერთ წლამდე. (ამოქმედდეს 2018 წლის 1 იანვრიდან)]

2. იგივე ქმედება, ჩადენილი:

ა) დამნაშავისათვის წინასწარი შეცნობით არასრულწლოვნის, უმწეო მდგომარეობში მყოფის, შეზღუდული შესაძლებლობის მქონე პირის ან ორსული ქალის მიმართ;
ბ) ჯგუფურად;
გ) არაერთგზის, – ისჯება გამასწორებელი სამუშაოთი ვადით ორ წლამდე ან თავისუფლების აღკვეთით ვადით თვრამეტ თვემდე.

მუხლი 157. პირადი ცხოვრების აძსახველი ინფორმაციის ან პერსონალური მონაცემების ხელყოფა

1. პირადი ცხოვრების ამსახველი ინფორმაციის ან პერსონალური მონაცემების უკანონოდ მოპოვება, შენახვა, გამოყენება, გავრცელება ან ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა, რამაც მნიშვნელოვანი ზიანი გამოიწვია, — ისჯება ჯარიმით ანდა გამასწორებელი სამუშაოთი ვადით ორ წლამდე ანდა თავისუფლების აღკვეთით ვადით სამ წლამდე.

2. პირადი ცხოვრების ამსახველი ინფორმაციის ან პერსონალური მონაცემების უკანონოდ გამოყენება ან/და გავრცელება ამა თუ იმ ხერხით გავრცელებული ნაწარმოების, ინტერნეტის, მათ შორის, სოციალური ქსელის, მასობრივი მაუწყებლობის ან სხვა საჯარო გამოსვლის მეშვეობით, რამაც მნიშვნელოვანი ზიანი გამოიწვია, — ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ანდა თავისუფლების აღკვეთით ვადით ოთხ წლამდე.

3. ამ მუხლის პირველი ან მე-2 ნაწილით გათვალისწინებული ქმედება, ჩადენილი:
ა) ანგარებით;
ბ) არაერთგზის, – ისჯება ჯარიმით ან თავისუფლების შეზღუდვით ვადით ხუთ წლამდე ანდა თავისუფლების აღკვეთით იმავე ვადით.

[3. ამ მუხლის პირველი ან მე-2 ნაწილით გათვალისწინებული ქმედება, ჩადენილი:

ა) ანგარებით;
ბ) არაერთგზის, – ისჯება ჯარიმით ან თავისუფლების აღკვეთით ვადით ხუთ წლამდე (ამოქმედდეს 2018 წლის 1 იანვრიდან)].

4. ამ მუხლის პირველი, მე-2 ან მე-3 ნაწილით გათვალისწინებული ქმედება, ჩადენილი იმ პირის მიერ, რომელსაც სამსახურებრივი მდგომარეობის, პროფესიული საქმიანობის ან სხვა გარემოების გამო ევალებოდა ამ ინფორმაციის ან მონაცემების დაცვა ან რომელმაც აღნიშნული ქმედება ჩაიდინა სამსახურებრივი მდგომარეობის გამოყენებით, – ისჯება თავისუფლების აღკვეთით ვადით ოთხიდან შვიდ წლამდე, თანამდებობის დაკავების ან საქმიანობის უფლების ჩამორთმევით ვადით სამ წლამდე ან უამისოდ.

შენიშვნა: 1.ამ მუხლის პირველი ნაწილით გათვალისწინებული დანაშაულისათვის (მოპოვება, შენახვა) სისხლისსამართლებრივი პასუხისმგებლობა არ დაეკისრება პირს, რომელმაც ამ მუხლის პირველი ნაწილით გათვალისწინებული მოპოვებული/შენახული ინფორმაცია საგამოძიებო ორგანოებს გადასცა და ჩადენილი/მოსალოდნელი სხვა დანაშაულებრივი ქმედების შესახებ ინფორმაცია ამ გზით მიაწოდა.

2.ამ მუხლით გათვალისწინებული ქმედებისათვის იურიდიული პირი ისჯება ჯარიმით, საქმიანობის უფლების ჩამორთმევით ან ლიკვიდაციითა და ჯარიმით.

მუხლი 158. კერძო კომუნიკაციის საიდუმლოების დარღვევა

1. კერძო საუბრის უნებართვო ჩაწერა ან მიყურადება, აგრეთვე, კომპიუტერულ სისტემაში ან სისტემიდან კერძო კომუნიკაციისას გადაცემული კომპიუტერული მონაცემის ან ამგვარი მონაცემის მატარებელი ელექტრომაგნიტური ტალღების უნებართვო მოპოვება ტექნიკური საშუალების გამოყენებით ან კერძო კომუნიკაციის ჩანაწერის, ტექნიკური საშუალებით მოპოვებული ინფორმაციის ან კომპიუტერული მონაცემის უკანონოდ შენახვა, – ისჯება ჯარიმით ან თავისუფლების შეზღუდვით ვადით ორიდან ოთხ წლამდე ანდა თავისუფლების აღკვეთით იმავე ვადით.

2. კერძო კომუნიკაციის ჩანაწერის, ტექნიკური საშუალებით მოპოვებული ინფორმაციის ან კომპიუტერული მონაცემის უკანონოდ გამოყენება, გავრცელება ან ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა, – ისჯება ჯარიმით ან თავისუფლების შეზღუდვით ვადით ორიდან ხუთ წლამდე ანდა თავისუფლების აღკვეთით იმავე ვადით.

[1. კერძო საუბრის უნებართვო ჩაწერა ან მიყურადება, აგრეთვე, კომპიუტერულ სისტემაში ან სისტემიდან კერძო კომუნიკაციისას გადაცემული კომპიუტერული მონაცემის ან ამგვარი მონაცემის მატარებელი ელექტრომაგნიტური ტალღების უნებართვო მოპოვება ტექნიკური საშუალების გამოყენებით ან კერძო კომუნიკაციის ჩანაწერის, ტექნიკური საშუალებით მოპოვებული ინფორმაციის ან კომპიუტერული მონაცემის უკანონოდ შენახვა, – ისჯება ჯარიმით ან თავისუფლების აღკვეთით ვადით ორიდან ოთხ წლამდე.

2. კერძო კომუნიკაციის ჩანაწერის, ტექნიკური საშუალებით მოპოვებული ინფორმაციის ან კომპიუტერული მონაცემის უკანონოდ გამოყენება, გავრცელება ან ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა, – ისჯება ჯარიმით ან თავისუფლების აღკვეთით ვადით ორიდან ხუთ წლამდე (ამოქმედდეს 2018 წლის 1 იანვრიდან)].

3. ამ მუხლის პირველი ან მე-2 ნაწილით გათვალისწინებული ქმედება, ჩადენილი:
ა) ანგარებით;
ბ) არაერთგზის, – ისჯება თავისუფლების აღკვეთით ვადით სამიდან ექვს წლამდე.

4. ამ მუხლის პირველი, მე-2 ან მე-3 ნაწილით გათვალისწინებული ქმედება:
ა) რამაც მნიშვნელოვანი ზიანი გამოიწვია;
ბ) ჩადენილი სამსახურებრივი მდგომარეობის გამოყენებით, – ისჯება თავისუფლების აღკვეთით ვადით სამიდან შვიდ წლამდე, თანამდებობის დაკავების ან საქმიანობის უფლების ჩამორთმევით ვადით სამ წლამდე.

შენიშვნა:

1. ამ მუხლის მიზნებისათვის „კომპიუტერული მონაცემი“, „კომპიუტერული სისტემა“ და „უნებართვო“ განიმარტება ამ კოდექსის XXXV თავით გათვალისწინებული განმარტებების შესაბამისად.

2. ამ მუხლის პირველი ნაწილით გათვალისწინებული დანაშაულისათვის სისხლისსამართლებრივი პასუხისმგებლობა არ დაეკისრება პირს, რომელმაც ამ მუხლის პირველი ნაწილით გათვალისწინებული მოპოვებული/შენახული ინფორმაცია საგამოძიებო ორგანოებს გადასცა და ჩადენილი/მოსალოდნელი სხვა დანაშაულებრივი ქმედების შესახებ ინფორმაცია ამ გზით მიაწოდა.
3. ამ მუხლით გათვალისწინებული ქმედებისათვის იურიდიული პირი ისჯება ჯარიმით, საქმიანობის უფლების ჩამორთმევით ან ლიკვიდაციითა და ჯარიმით.

მუხლი 159. პირადი მიმოწერის, ტელეფონით საუბრის ან სხვაგვარი ხერხით შეტყობინების საიდუმლოების დარღვევა

1. პირადი მიმოწერის ან საფოსტო გზავნილის, ტელეფონით ან სხვა ტექნიკური საშუალებით საუბრის ჩანაწერის ან ტელეგრაფით, კომპიუტერული სისტემით,

ფაქსით ან სხვა ტექნიკური საშუალებით მიღებული ან გადაცემული შეტყობინების უკანონოდ მოპოვება, გახსნა, შინაარსის გაცნობა ან შენახვა, – ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ანდა თავისუფლების აღკვეთით ვადით სამ წლამდე.

2. პირადი მიმოწერის ან საფოსტო გზავნილის, ტელეფონით ან სხვა ტექნიკური საშუალებით საუბრის ჩანაწერის ან ტელეგრაფით, კომპიუტერული სისტემით, ფაქსით ან სხვა ტექნიკური საშუალებით მიღებული ან გადაცემული შეტყობინების უკანონოდ გამოყენება, გავრცელება ან ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა, – ისჯება თავისუფლების აღკვეთით ვადით ორიდან ხუთ წლამდე.

3. ამ მუხლის პირველი ან მე-2 ნაწილით გათვალისწინებული ქმედება, ჩადენილი: ა) ანგარებით; ბ) არაერთგზის, – ისჯება თავისუფლების აღკვეთით ვადით სამიდან ექვს წლამდე.

4. ამ მუხლის პირველი, მე-2 ან მე-3 ნაწილით გათვალისწინებული ქმედება:

ა) რამაც მნიშვნელოვანი ზიანი გამოიწვია;

ბ) ჩადენილი სამსახურებრივი მდგომარეობის გამოყენებით, – ისჯება თავისუფლების აღკვეთით ვადით სამიდან შვიდ წლამდე, თანამდებობის დაკავების ან საქმიანობის უფლების ჩამორთმევით ვადით სამ წლამდე.

შენიშვნა:

1. ამ მუხლის პირველი ნაწილით გათვალისწინებული დანაშაულისათვის სისხლისსამართლებრივი პასუხისმგებლობა არ დაეკისრება პირს, რომელმაც ამ მუხლის პირველი ნაწილით გათვალისწინებული მოპოვებული/შენახული ინფორმაცია საგამოძიებო ორგანოებს გადასცა და ჩადენილი/მოსალოდნელი სხვა დანაშაულებრივი ქმედების შესახებ ინფორმაცია ამ გზით მიაწოდა.

2. ამ მუხლით გათვალისწინებული ქმედებისათვის იურიდიული პირი ისჯება ჯარიმით, საქმიანობის უფლების ჩამორთმევით ან ლიკვიდაციითა და ჯარიმით.

როგორ დავიცვათ თავი კიბერდანაშაულით გამოწვეული საფრთხეებისაგან?

რასაკვირველია, კიბერდანაშაულის შემთხვევებისა და მასშტაბების ზრდასთან ერთად, შესაბამისი სახელმწიფო სტრუქტურები კიბერდანაშაულთან ბრძოლის მექანიზმებზეც მუშაობენ.

კიბერდანაშაულთან ბრძოლის ერთ-ერთ მექანიზმად თავად ინტერნეტ სივრცის მომხმარებელთა ინფორმირებულობა განიხილება. კიბერდამნაშავისთვის პიროვნების პერსონალური მონაცემები თუ პირადი ცხოვრების ამსახველი ინფორმაცია ხელმისაწვდომი ხშირად იმის გამო ხდება, რომ ადამიანები ამ ინფორმაციას თავად განათავსებენ ინტერნეტსივრცეში ინტერნეტის მოხმარების დროს. განვიხილოთ, როგორ დავიცვათ თავი კიბერსივრცეში არსებული სხვადასხვა საფრთხეებისგან:

პერსონალური მონაცემების უსაფრთხოება

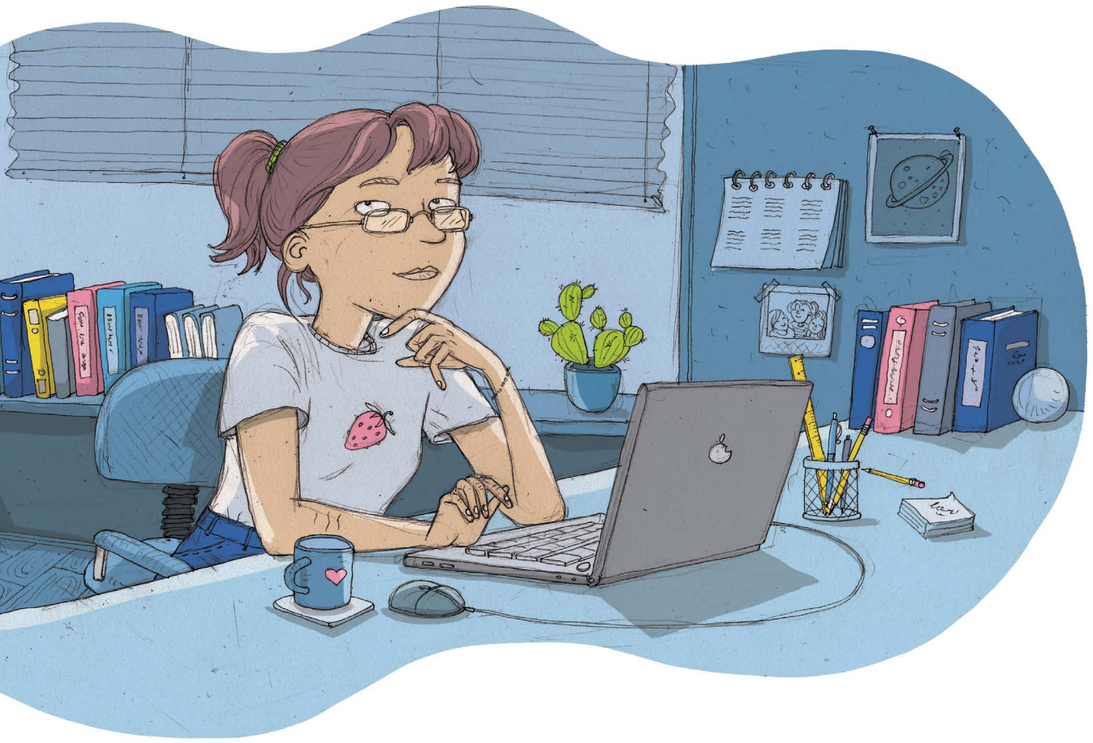
პერსონალური მონაცემების სხვა პირის მიერ დაუფლების შემთხვევაში, შესაძლებელია, კონკრეტული პიროვნების საზიანოდ მისი გამოყენება. ამიტომ არის მნიშვნელოვანი, რომ მაქსიმალურად მოვუფრთხილდეთ ჩვენს პერსონალურ ინფორმაციას და ღია, საჯარო წყაროებში მის განთავსებას მოვერიდოთ.

პერსონალური მონაცემების შესახებ ზოგიერთ ინფორმაციას თავად პიროვნება უთითებს, მაგალითად, სოციალურ ქსელებში დარეგისტრირებისას. სოციალური ქსელების საშუალებით ხდება ადამიანების გაცნობა, მათ შორის ურთიერთობების დაწყება ან აღდგენა, მეგობრებთან და ახლობლებთან ყოველდღიური ურთიერთობების შენარჩუნება. რა თქმა უნდა, ამაში ცუდი არაფერია. თუმცა, როგორც უკვე აღინიშნა, სოციალური ქსელები გარკვეულ საფრთხეებსაც შეიცავს.

ამიტომ მომხმარებელმა უნდა გაითვალისწინოს, რა სახის უსაფრთხოების პარამეტრები გააჩნია კონკრეტულ სოციალურ ქსელს და მხოლოდ აღნიშნულის შესწავლის შემდეგ ისარგებლოს მისით.

არის ისეთი შემთხვევებიც, როდესაც ზოგიერთი ვებგვერდი თავადვე მიუთითებს, რომ მომხმარებლის პირადი ინფორმაციის უსაფრთხოებაზე პასუხისმგებლობას არ იღებს, თუმცა, მომხმარებელი დაუდევრობას იჩენს და მაინც რეგისტრირდება ამ ვებგვრდზე.

არსებობს ისეთი ვებგვერდებიც, რომელზე დარეგისტრირებისასაც მომხმარებელს პირადი ინფორმაციის მითითება მოეთხოვება, თუმცა, ვებგვერდი არა რომელიმე სანდო და საერთაშორისოდ აღიარებული, არამედ ნაკლებად ცნობილი კომპანიების



ან, თუნდაც, ნებისმიერი კერძო პირის მიერ არის შექმნილი. მსგავსი ვებგვერდების „უსაფრთხოების პირობებში“ შეიძლება მითითებულიც კი იყოს, რომ მომხმარებლის შესახებ პირადი ინფორმაცია დაცულია, მაგრამ მომხმარებელი უნდა დაფიქრდეს, რამდენად სანდო შეიძლება იყოს ეს დაპირება და რა იურიდიული ბერკეტები გააჩნია იმისათვის, რომ ამ პირობების დარღვევის შემთხვევაში იურიდიული პასუხისმგებლობა ვებგვერდის შემქმნელს დააკისროს.

ამ კითხვებზე პასუხის გაცემის ერთ-ერთი გზა იმ ინფორმაციის გაცნობაა, თუ რა შეფასებებს აკეთებენ აღნიშნული ვებგვერდის შესახებ სხვა ინტერნეტმომხმარებლები და ექსპერტები.

პერსონალური მონაცემების დაცვასთან დაკავშირებული რისკების თავიდან ასაცილებლად, დღეის მდგომარეობით, მრავლადაა ორმაგი ავტორიზაციის მქონე ვებგვერდები, რაც 100% დაცულს ხდის მომხმარებლის გვერდს და მასზე შეღწევა სხვა პირების მიერ მომხმარებლის ნებართვის ან მისი დაუდევარი ქმედების გარეშე შეუძლებელია. მაგალითად, სოციალურ ქსელს facebook.com გააჩნია ფუნქცია, რომლის გააქტიურების შემთხვევაშიც, ვებგვერდზე შესასვლელად, მომხმარებლის ავტორიზაციის პარამეტრების - სახელისა და პაროლის მითითების გარდა, საჭიროა მობილურ ტელეფონზე მიღებული ერთჯერადი კოდის მითითებაც.

გარდა ამისა, მნიშვნელოვანია ვიცოდეთ, რომ სხვადასხვა ვებგვერდზე რეგისტრაციისას სხვადასხვა პაროლი გამოვიყენოთ. ეს ამცირებს რისკს, რომ დამნაშავის ხელში აღმოჩნდეს არა მხოლოდ რომელიმე ერთ, არამედ სხვადასხვა პირად გვერდებზე პიროვნების შესახებ არსებული ინფორმაცია.

თავად პაროლი იმისათვის, რომ ის ჩაითვალოს დაცულ პაროლად, არ უნდა იყოს ძალიან მოკლე, უნდა შედგებოდეს განსხვავებული სიმბოლოებისგან, არ უნდა შეიცავდეს მომხმარებლის ან მისი ახლობლების სახელს ან გვარს, დაბადების თარიღს ან პიროვნების საიდენტიფიკაციო სხვა რაიმე ინფორმაციას. დაუცველი პაროლის ნიმუში: gochajojua17.
დაცული პაროლის შესაქმნელად შემდეგი სტრატეგიების გამოყენება შეიძლება:

• მოიფიქრეთ რაიმე ფრაზა და ჩასვით სხვადასხვა სიმბოლოები ამ ფრაზის სიტყვებს შორის. მაგალითად, თუ ავიღებთ ფრაზას: ეს არის ჩემი კალამი, შეგვიძლია, მივიღოთ შემდეგი სახის პაროლი: es*aris@chemi^kalami;

• მოიფიქრეთ რაიმე ფრაზა და პაროლის შესაქმნელად ამ ფრაზის პირველი ასოები გამოიყენეთ. მაგალითად, ფრაზისგან: „თავისუფალი ის არის, ვინც არასოდეს იტყუება”, მივიღებთ შემდეგი სახის პაროლს: tiavai;

• გააერთიანეთ ისეთი სიტყვები და ციფრები, რომლებსაც ერთმანეთთან კავშირი არ აქვს. მაგალითად, შეიძლება გამოიყენოთ თქვენი დაბადების თარიღი (პირობითად, 1 მარტი, 2005 წელი), შემდეგ ნებისმიერი სიტყვა, ბოლოს კი ჯონი დეპის დაბადების თარიღი (9 ივნისი, 1963 წელი): 01032005amindi09061963.

საბანკო მონაცემების უსაფრთხოება

საბანაკო მონაცემები პირდაპირ კავშირშია ჩვენს მატერიალურ კეთილდღეობასთან და მისი დაცვა არანაკლებ მნიშვნელოვანია, რათა აღნიშნული მონაცემები უცნობ პირებთან არ აღმოჩნდეს და თავიდან ავიცილოთ მატერიალური ზიანი.

შესაბამისად, უნდა გვახსოვდეს, რომ არ გადავცეთ ჩვენი საბანკო პლასტიკური ბარათის მონაცემები სხვას; ასევე, არ გადავცეთ სხვას თავად ბარათი. როდესაც თანხას ტერმინალის საშუალებით ვიხდით, საბანკო პლასტიკური ბარათის გამოყენება მხოლოდ ჩვენი თანდასწრებით უნდა მოხდეს.

დღეისათვის საბანკო სისტემაშიც არსებობს საკმოდ დაცული, ორმაგი ავტორიზაციის ვებგვერდები, რომელიც ჩვენს საბანკო მონაცემებს უფრო დაცულს ხდის. მაგალითად, ელექტრონულ საფულეზე შესასვლელად, მომხმარებელმა მომხმარებლის სახელისა და პაროლის გარდა, მითითებულ ველში უნდა ჩაწეროს მის მობილურ ტელეფონზე ავტომატურად გამოგზავნილი ერთჯერადი კოდი.

პირადი ცხოვრების ამსახველი ინფორმაციის უსაფრთხოება

პირადი ცხოვრების ამსახველი ინფორმაცია შეიძლება იყოს სურათი, ვიდეო, მიმოწერა ან სხვა, რომელიც ჩვენი პირადი ცხოვრების ამსახველ ცნობებს შეიცავს. შესაბამისად, მაქსიმალურად უნდა შევეცადოთ, რომ აღნიშნული ინფორმაცია არა მხოლოდ არ განვათავსოთ ინტერნეტის საჯარო სივრცეში, არამედ დაცულად შევინახოთ იგი, რათა უცნობი პირების ხელში არ აღმოჩნდეს და მომავალში ჩვენი შანტაჟის (რაიმე ქმედების განხორციელების ან განხორციელებისაგან თავის შეკავების მოთხოვნა ჩვენი ნების საწინააღმდეგოდ) შესაძლებლობა არ მივცეთ ვინმეს.

უნდა გვახსოვდეს, რომ ინტერნეტის მოხმარებისას, ჩვენ მიერ მითითებული პერსონალური და პირადი ცხოვრების ამსახველი ინფორმაცია ინახება ამა თუ იმ სერვერზე (ტექნიკური მოწყობილობა), ასევე, გარკვეულწილად, იმ მოწყობილობაზე, საიდანაც ეს ინფორმაცია იგზავნება. იმ შემთხვევაში, თუ აღნიშნული მოწყობილობები ვინმესთვის ხელმისაწვდომი გახდება, ჩვენი ინფორმაციის დაცულობას შეექმნება

საფრთხე.
ჩვენ მიერ განხილულ მე-4 შემთხვევაში პირადი ცხოვრების შესახებ ინფორმაცია მიმოწერის გზით თავად ნუცამ გასცა. ზოგადად, ადამიანების უმრავლესობა ნდობას იმსახურებს. ასე რომ არ იყოს, ადამიანთა თანაცხოვრება შეუძლებელი იქნებოდა და მსოფლიო ერთ დიდ ბრძოლის ველს დაემსგავსებოდა. შესაბამისად, თუ ჩვენ სხვა პიროვნების მიმართ ნდობა გვიჩნდება, ეს კარგია, მაგრამ უნდა გვახსოვდეს, რომ ვირტუალური სოციალური სივრცე ბევრ სხვადასხვა საფრთხეს შეიცავს. ერთ-ერთი საფრთხე კი სწორედ უცნობ ადამიანებთან კონტაქტმა შეიძლება მოიტანოს.

ამიტომ, ვიდრე მათთან დაახლოებას გადავწყვეტთ, საჭიროა გადავამოწმოთ, რამდენად რეალურია მათ მიერ მოწოდებული ინფორმაცია; ნამდვილად ის პიროვნებები არიან თუ არა, რომლებადაც თავს ასაღებენ და მათი ქცევის რეალურ მოტივებში დავრწმუნდეთ.

ამისათვის, თუ სოციალური ქსელის საშუალებით თქვენთან დამეგობრებას უცნობი ადამიანი ცდილობს:

1. კარგად დაფიქრდით, ვიდრე დამეგობრებაზე მის თხოვნას დაეთანხმებით;

2. დაუსვით კითხვები: რატომ სურს თქვენთან დამეგობრება? როგორ გაიგო თქვენი არსებობის შესახებ? გყავთ თუ არა საერთო ნაცნობები? თუ კი, კონკრეტულად ვინ? თუ საერთო ნაცნობები დაგისახელათ, გადაამოწმეთ მათთან, ნამდვილად იცნობენ თუ არა ამ პიროვნებას პირადად. თუ აღმოაჩენთ, რომ ნამდვილად გაკავშირებთ საერთო ნაცნობები, შეგიძლიათ დაიმეგობროთ, თუ არა - მაშინ უარი თქვით მასთან კონტაქტზე.

უნდა გვახსოვდეს: მაშინაც კი, თუ მისი მეგობრების სიაში ბევრი ადამიანია, ეს სრულიად არ ნიშნავს, რომ ეს პიროვნება რეალურია. ყალბი გვერდის მფლობელები, შეცდომაში შეყვანის გზით, ხშირად უმეგობრდებიან ერთ ისეთ კონკრეტულ პიროვნებას, რომელიც სოციალურ ქსელში პოპულარობით სარგებლობს და ბევრი მეგობარი ჰყავს. მასთან დამეგობრების შემდეგ კი მის მეგობრებთან დამეგობრებას ცდილობენ.

მაგალითად, პიროვნებას, რომელიც საგანმანათლებლო საქმიანობას ეწევა და მუშაობის პროცესში ძალიან ბევრ ადამიანს ხვდება, სოციალური ქსელის საშუალებით უკავშირდება ყალბი გვერდის მფლობელი, რომელმაც მისი საქმიანობის შესახებ

წინასწარ მოაგროვა ინფორმაცია. ამ პიროვნებას ატყუებს, რომ მის მიერ ჩატარებულ საგანმანათლებლო ღონისძიებას ესწრებოდა, რომლითაც აღფრთოვანებული დარჩა და ახლა მასთან დამეგობრება სურს. აღნიშნული პიროვნება იჯერებს ტყუილს, უხერხულად გრძნობს თავს, უარი უთხრას მეგობრობის შემოთავაზებაზე და თავისი მეგობრების სიაში ამატებს მას. ამის შემდეგ, ყალბი გვერდის მფლობელი ამ პიროვნების სხვა მეგობარს უკავშირდება და ახალი ტყუილის გამოგონებით მასაც სთხოვს დამეგობრებას. მეგობარი, ვინაიდან ხედავს, რომ მათ საერთო მეგობარი ჰყავთ, უფრო ადვილად ტყუვდება და მეგობრებში იმატებს. ყალბი გვერდის შემქმნელი კი იგივე მეთოდებით კვლავაც აგრძელებს საკუთარი მეგობრების სიის გაზრდას. შემდეგ კი მათთან მეგობრობას სხვადასხვა დანაშაულის ჩასადენად იყენებს.

შანტაჟისა და მუქარისაგან თავის დაცვა

როდესაც შანტაჟისა და მუქარის შესახებ ვსაუბრობთ, უნდა გვახსოვდეს, რომ ეს სერიოზული დანაშაულია, დანაშაულთან ბრძოლა კი პოლიციის მოვალეობაა. ჩვეულებრივ მოქალაქეს, როგორც წესი, ძალა არ შესწევს, დანაშაულს სამართალდამცველების დახმარების გარეშე გაუმკლავდეს.

თუ თქვენ დაიწყებთ იმ პირის მითითებების შესრულებას, რომელიც შანტაჟს გიწყობთ ან გემუქრებათ, მაშინ ის თქვენს სისუსტეს და დაუცველობას იგრძნობს, აუცილებლად გაეზრდება მოთხოვნები და სულ უფრო და უფრო აუტანელი გახდება.

ხშირად იმ ადამიანებს, რომლებიც ვინმეს აშანტაჟებენ ან ემუქრებიან, რეალური ზიანის მიყენების ძალა არ შესწევთ ან არც კი აპირებენ მსგავსი დანაშაულის ჩადენას, რადგან მძიმე დანაშაულის ჩადენით ცხოვრების გართულება არ სურთ. სამაგიეროდ, მათი ძლიერი მხარე ადამიანის ფსიქოლოგიის ცოდნა და მისი სისუსტეების გამოყენებაა - მათ ზუსტად იციან, როგორ, რა გზებით, რა სიტყვებით იმოქმედონ ამა თუ იმ კონკრეტულ ადამიანზე. როდესაც მსხვერპლი ასეთი „შეტევის“ წინაშე მარტოა, წინააღმდეგობის გაწევა და გონივრული გამოსავლის მოძებნა უჭირს.

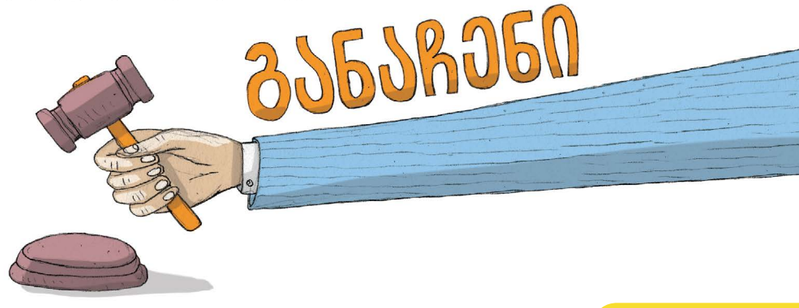
ამიტომ თუ ვინმე ცდილობს, რაიმე ქცევის შესრულება ან არშესრულება გაიძულოთ შანტაჟის ან მუქარის გზით, აუცილებლად აცნობეთ მშობლებს, მასწავლებელს, თქვენთვის სანდო სხვა პიროვნებას ან პირდაპირ პოლიციას. პოლიციელებმა იციან, როგორ დაეხმარონ ადამიანებს მსგავს შემთხვევაში, რადგან მათ ამისათვის სპეციალური განათლება აქვთ მიღებული.

ამასთანავე, შეეცადეთ, მოაგროვოთ ყველა ფაქტი, რომელიც დამნაშავის მხრიდან მოწყობილ შანტაჟსა და მუქარას მოწმობს. გადაუღეთ ფოტო დამნაშავის მიერ მოწერილ ყველა წერილს და ეს ფოტოები მატერიალური სახით შეინახეთ საიმედო ადგილას, პოლიციისათვის მათ გადაცემამდე.

რომელი სახელმწიფო უწყებებია ჩართული კიბერდანაშაულის გამოძიების პროცესში და რა ფუნქციები აქვთ მათ?

კიბერდანაშაულის გამოძიება იურიდიული განათლების გარდა ტექნიკური საკითხების ცოდნასაც მოითხოვს, რისთვისაც შსს კიბერდანაშაულის სამმართველოში 2 სპეციალური განყოფილება ფუნქციონირებს. მათ შემადგენლობაში შედიან საქმის მწარმოებელი გამომძიებლები და გამომძიებლები, რომლებსაც საკმარისი ტექნიკური ცოდნა გააჩნიათ. საქმის გამოძიება ორივე განყოფილების ერთობლივი ჩართულობით ხდება. კიბერტერორიზმის შემთხვევაში კი საქმეს სახელმწიფო უსაფრთხოების სამსახური იძიებს.

მას შემდეგ, რაც კონკრეტულ ფაქტზე გამოძიება დაიწყება და დანაშაულის ჩამდენი პირი გამოიკვეთება, ჩადენილი ქმედებისათვის ბრალი წარედგინება მას და სისხლის სამართლის საქმე პროკურატურაში გაიგზავნება. პროკურატურიდან საქმე სასამართლოში გადადის, სადაც მოსამართლე წარმოდგენილ მტკიცებულებებზე დაყრდნობით განიხილავს, ჩაიდინა თუ არა დანაშაული ბრალდებულმა და გამამართლებელი ან გამამტყუნებელი განაჩენი გამოაქვს.



რა მექანიზმები არსებობს კიბერდანაშაულის მსხვერპლთა დასახმარებლად?

საქართველოს შინაგან საქმეთა სამინისტროში, კერძოდ, ცენტრალური კრიმინალური პოლიციის დეპარტამენტში ფუნქციონირებს სპეციალიზირებული დანაყოფი - კიბერდანაშაულთან ბრძოლის სამმართველო, რომელიც კიბერდანაშაულის საქმეებს იძიებს. ამ განყოფილებასთან დაკავშირება ქვემოთ მითითებული ტელეფონის ნომრების საშუალებით ხდება:

2 41 12 96;
2 41 17 67;
112 - უფასო ცხელი ხაზი 24 საათის განმავლობაში;
ელ–ფოსტა: cybercrime@mia.gov.ge

გარდა ამისა, მოქალაქეს შეუძლია, აღნიშნულ სამმართველოს განცხადებით მიმართოს შემდეგ მისამართზე: ქ.თბილისი, გულუას ქ N10.

სამართალდამცავი ორგანო არა მხოლოდ დანაშაულის ჩამდენი პირის დადგენასა და კანონით გათვალისწინებული სხვა ღონისძიებების გატარებას შეეცდება, არამედ - მოქალაქის დარღვეული უფლებების აღდგენასაც. მაგალითად, შეიძლება, მოქალაქეს წვდომა დაუბრუნდეს მომხმარებლის დაკარგულ გვერდზე; ასევე, აღკვეთოს მომავალში დანაშაულებრივი გზით მოპოვებული პერსონალური მონაცემებისა თუ პირადი ცხოვრების ამსახველი ინფორმაციის გავრცელება; დაუბრუნოს მატერიალური ღირებულების მქონდე ნივთები, როგორიცაა: ფული, ძვირფასი ლითონი და სხვ.

შეამოწმე შენი თავი

თქვენ უკვე ბევრი გაიგეთ კიბერდანაშაულის, მასთან ბრძოლისა და, ზოგადად, კიბერდანაშაულისგან თავდაცვის მექანიზმების შესახებ.

გადაამოწმეთ, რა იცოდით ამ თემასთან დაკავშირებით და რა გაიგეთ ახალი? ამისათვის, დაუბრუნდით იმავე აქტივობას, რაც ამ გაკვეთილის დასაწყისში გააკეთეთ - ხელმეორედ გადახაზეთ თქვენს სამუშაო რვეულებში იგივე გრაფიკული ორგანიზატორი და იმავე კითხვებს უპასუხეთ.

საშინაო დავალება

ფიქრი განაგრძეთ კიბერდანაშაულის თემაზე; შეეცადეთ, განხილული საკითხები გონებაში შეაჯამოთ და შეასრულეთ საშინაო დავალებები.

ქვემოთ მოცემულია სამი დავალება.

მოცემულ კითხვებზე პასუხის გაცემა დაგეხმარებათ, დარწმუნდეთ, თუ რამდენად კარგად გაიაზრეთ განხილული საკითხები. იმ შემთხვევაში, თუ რომელიმე კითხვაზე პასუხი არ გექნებათ, განმარტებებისთვის მომდევნო გაკვეთილზე მასწავლებელს მიმართეთ.

დავალება

1. უპასუხეთ კითხვებს:

• რატომ არის მნიშვნელოვანი უსაფრთხოებაზე ზრუნვა ინტერნეტის გამოყენებისას?

• რა გზებით არის შესაძლებელი კიბერდანაშაულისგან თავის დაცვა? დაფიქრდი, როგორ უკავშირდება ეს შენს კომპიუტერს, ტელეფონს ან ინტერნეტ ქსელში ჩართულ სხვა ელექტრონულ მოწყობილობას?

• რატომ არის მნიშვნელოვანი „ძლიერი“ პაროლის გამოყენება ვებგვერდებზე რეგისტრაციისას?

• რისი გაკეთება შეგიძლია შენი სკოლის მასშტაბით იმისათვის, რომ აამაღლო თანატოლების ცნობიერება კიბერდანაშაულისგან თავის დაცვის მიზნით?

დავალება

2. „ორმაგი ჩანაწერების დღიური“

დახაზეთ ორსვეტიანი ცხრილი, როგორც ეს მოცემულია ქვემოთ. ცხრილის პირველ სვეტში ჩაწერეთ ფაქტები, ტერმინები, განმარტებები ან ნაწყვეტები შესასწავლი მასალიდან. მეორე სვეტში კი ჩამოაყალიბეთ ამ ფაქტის/ტერმინის/განმარტების/ნაწყვეტის შესახებ თქვენი პირადი დამოკიდებულებები, შეხედულებები, მოსაზრებები ან კითხვები.

ცხრილის მარცხენა სვეტში ჩაწერეთ ერთი ან ორი ფაქტი, ტერმინი, განმარტება, რომლებმაც თქვენი განსაკუთრებული ყურადღება მიიქცია. მარჯვენა სვეტში კი - მათთან დაკავშირებით თქვენი კითხვები, მოსაზრებები, დამოკიდებულებები, ემოციები. მოსაზრებების არგუმენტირებისათვის შეგიძლიათ მოიყვანოთ ცხოვრებისეული მაგალითებიც.

ცხრილი 2. ორმაგი ჩანაწერების დღიური

სახელი, გვარი:	თარიღი:
ფაქტი/ტერმინი/განმარტება/ნაწყვეტი	ჩემი დამოკიდებულება/შეხედულება/მოსაზრება/კითხვა

დავალება

3. „ორი ჭეშმარიტი და ერთი მცდარი დებულება.“

დაწერეთ 2 ჭეშმარიტი და 1 მცდარი დებულება კიბერდანაშაულის შესახებ.

.....

.....

.....

ლექსიკონი

ემიტენტი - იურიდიული პირი: ბანკი, დაწესებულება, სახელმწიფო ცენტრალური ან ადგილობრივი ხელისუფლების მმართველობის ორგანო, რომელიც მიმოქცევაში უშვებს ფასიან ქაღალდებს და ამ ფასიანი ქაღალდების მფლობელების მიმართ გარკვეულ ვალდებულებებს კისრულობს (სამოქალაქო განათლების ლექსიკონი).

მუქარა - სიცოცხლის მოსპობის ან ჯანმრთელობის დაზიანების, ანდა ქონების განადგურების მუქარა, როდესაც იმას, ვისაც ემუქრებიან, გაუჩნდა მუქარის საფუძვლიანი შიში(CIVIL ენციკლოპედიური ლექსიკონი).

კიბერდანაშაული - ნებისმიერი მართლსაწინააღმდეგო ქმედება, რომელიც ჩადენილია კომპიუტერული სისტემის გამოყენებით კიბერსივრცეში და კომპიუტერული სისტემის ფუნქციონირებასა და კომპიუტერული მონაცემების დაცულობას ხელყოფს.

კომპიუტერული სისტემა - ნებისმიერი მექანიზმი ან ერთმანეთთან დაკავშირებულ მექანიზმთა ჯგუფი, რომელიც პროგრამის მეშვეობით ან ავტომატურად ამუშავებს მონაცემებს (მაგ: პერსონალური კომპიუტერი, ლეპტოპი, პლანშეტური კომპიუტერი, მობილური ტელეფონი სმარტფონი და ნებისმიერი მოწყობილობა მიკროპროცესორით) (საქართველოს სისხლის სამართლის საპროცესო კოდექსის მე-3 მუხლის 27-ე ნაწილი).

კიბერმეთოდებით ჩადენილი დანაშაული - დანაშაულის ჩამდენი არ ჩადის კიბერდანაშაულს, ჩადის სხვა დანაშაულს (მაგალითად: თაღლითობა, გამოძალვა და ა.შ.) და კომუნიკაციის მეთოდად ინტერნეტს (კიბერსივრცეს) იყენებს.

პერსონალური მონაცემი - ნებისმიერი მონაცემი, რომელიც უკავშირდება იდენტიფიცირებად ან იდენტიფიცირებულ ფიზიკურ პირს, მაგალითად: სახელი, გვარი, პირადი ნომერი, საბანკო ინფორმაცია, ტელეფონის ნომერი, ელ-ფოსტა, ინფორმაცია მის საკუთრებაში არსებული ქონების შესახებ ან სხვა მონაცემი, რომლითაც შესაძლებელია პირის პირდაპირი ან არაპირდაპირი გზით იდენტიფიცირება, კერძოდ: საიდენტიფიკაციო ნომრით, ფიზიკური, ფსიქოლოგიური, ეკონომიკური, კულტურული ან სოციალური მახასიათებლებით (საქართველოს კანონი პერსონალურ მონაცემთა დაცვის შესახებ, მუხლი 2).

საბანკო ინფორმაცია - პიროვნების საკუთრებაში არსებული ინტერნეტბანკი და საბანკო პლასტიკურ ბარათზე მითითებული ინფორმაცია: სახელი და გვარი, საბანკო პლასტიკური ბარათის ნომერი, მისი მოქმედების ვადა, CVC კოდი და მაგნიტური

ველი (ბარათის უკანა მხარეს არსებული მუქი ფერის ზოლი), რომელზეც ინფორმაცია დატანილია ელექტრონულად.

პირადი ცხოვრების ამსახველი ინფორმაცია - სურათი, აუდიო/ვიდეო ჩანაწერი, მიმოწერა, პირადი ჩანაწერები ან სხვა, რომელიც შეიცავს ადამიანის პირადი ცხოვრების ამსახველ ცნობებს.

ჰაკერი - პირი, რომელიც კომპიუტერული სისტემის მეშვეობით არალეგალურად მოიპოვებს წვდომას სხვა პიროვნების ან დაწესებულების კომპიუტერულ მონაცემებზე.

ფიშინგი - დამნაშავის მიერ მოტყუებით მსხვერპლის კომპიუტერული მონაცემების დაუფლება.

ქარდინგი - დამნაშავის მიერ საბანკო ბარათების ან სხვა საბანკო მონაცემების მოპოვება (ფიშინგით, სკიმერით, ქარდ რიდერით და ა.შ.) და შემდგომ ამ ინფორმაციის გაყიდვა ან გამოყენება ფინანსური სარგებლის მიღების მიზნით.

იძულება - ადამიანის ნება-სურვილის საწინააღმდეგო ფიზიკური ან ფსიქოლოგიური იძულება, შეასრულოს ან არ შეასრულოს მოქმედება, რომლის განხორციელება ან რომლისგან თავის შეკავება მისი უფლებაა.

შენიშვნების გვერდი

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

გამოყენებული ლიტერატურა

1. საქართველოს სისხლის სამართლის კოდექსი;

2. საქართველოს ეროვნული ბანკის პრეზიდენტის ბრძანება საგადასახადო ბარათების შესახებ დებულების დამტკიცების თაობაზე. №38/04 2011 წლის 16 მაისი, ქ. თბილისი.

3. https://matsne.gov.ge/ka/document/view/1561437?publication=18

4. https://personaldata.ge/ge/for-public-bodies/ra-aris-personaluri-monatsemi

5. http://www.nplg.gov.ge/gwdict/index.php?a=term&d=4&t=4418

6. http://www.nplg.gov.ge/gwdict/index.php?a=term&d=5&t=4075

7. http://www.nplg.gov.ge/gwdict/index.php?a=term&d=6&t=17034

8. http://liberali.ge/news/view/26131/ar-miutitot-sabanko-monatsemebi--personalur-monatsemta-datsvisinspeqtoris-gafrtkhileba

9. https://www.inverse.com/article/34507-is-sarahah-safe-snapchat-anonymous-messaging-bullying

10. http://www.alertboot.com/blog/blogs/endpoint_security/archive/2010/09/16/information-security-whatis-a-weak-password.aspx

11. http://cyber.kvira.ge/

12. მ. ხუნძაყიშვილი "განმავითარებელი შეფასება და დიფერენცირებული სწავლება. " თბილისი. 2018 წ.