კიბერდანაშაული

- საქართველოს სისხლის სამართლის კოდექსით, კიბერდანაშაულად მიჩნეულია მართლსაწინააღმდეგო ქმედება, რომელიც მოიცავს იმავე კოდექსის 284-ე, 285-ე და 286-ე მუხლების დისპოზიციაში მოყვანილ ერთ-ერთ კომპონენტს მაინც და არა ნებისმიერ მართლსაწინააღმდეგო ქმედებას ჩადენილს კომპიუტერული სისტემის გამოყენებით. მაგალითად კომპიუტერულ სისტემაში უნებართვო შეღწევა (284), კომპიუტერულ სისტემაში შეღწევისათვის საჭირო პაროლის ან დაშვების კოდის უნებართვო გავრცელება (285), კომიუტერული მონაცემის უნებართვო დაზიანება (286) და სხვ. ამასთან, შესაძლოა ადგილი ჰქონდეს დანაშაულთა (მუხლთა) ერთობლიობასაც. კერძოდ, კომპიუტერულ სისტემაში უნებართვო შეღწევას და შემდგომ სხვისი მოძრავი ნივთის ფარულ დაუფლებას (სსკ-ის 284-ე და 177-ე მუხლები).
- დღესდღეობით კიბერდანაშაულის საკმაოდ გავრცელებული შემთხვევებია: ინტერნეტ თაღლითობა/ქურდობა, კომპიუტერულ სისტემასთან უნებართვო წვდომა, კომპიუტერული სისტემისა და მონაცემის უნებართვოდ გამოყენება და ა.შ.
- კიბერ დამნაშავეები ძირითადად იყენებენ სპამის მეთოდებს და სხვადასხვა მავნე პროგრამებს.
- კიბერდანაშაულის მზარდი სტატისტიკა განპირობებულია კიბერ საკითხებზე საზოგადოების დაბალი ცნობიერებით
- ინტერნეტ სივრცეშიც ხდება ისეთი დანაშაულები, როგორიცაა ქურდობა. ელექტრონული შესყიდვებისა და ელექტრონული ბანკინგის მეშვეობით, კიბერ დამნაშავეებს წვდომა მისცეს სხვა პირთა ქონებისა და ფინანსებისადმი. მათ შეუძლიათ მოიპარონ პირის საბანკო მონაცემები, დააზიანონ სხვა პირის ინფორმაცია ან პროგრამა.

კანონმდებლობა და განხორციელებული ღონისძიებები

- საქართველოში კიბერდანაშაულის დასჯადობის საკითხებს არეგულირებს სისხლის სამართლის კოდექსის (სსკ) XXXV თავი, რომლის თანახმადაც, სისხლის სამართლის პასუხისმგებლობას იწვევს კიბერსივრცეში ჩადენილი შემდეგი ქმედებები: კომპიუტერულ სისტემაში უნებართვო შეღწევა, კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის უკანონოდ გამოყენება, კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის ხელყოფა.
- მიღებულ იქნა კანონი „ინფორმაციული უსაფრთხოების შესახებ“, რომელიც აწესებს ინფორმაციული უსაფრთხოების ზოგად სტანდარტებს საჯარო და კერძო სექტორისთვის.
- შინაგან საქმეთა სამინისტროს ცენტრალური კრიმინალური პოლიციის დეპარტამენტში შეიქმნა **კიბერდანაშაულთან ბრძოლის სამმართველო,** რომელსაც ევალება კიბერ სივრცეში ჩადენილი მართლსაწინააღმდეგო ქმედებების გამოვლენა, აღკვეთა და პრევენცია.
- შსს საექსპერტო-კრიმინალისტიკური მთავარი საამმართველოს შემადგენლობაში ჩამოყალიბდა კომპიუტერულ-ციფრული ექსპერტიზის ქვეგანყოფილება.
- საქართველოს კიბერ უსაფრთხოების სტრატეგია 2013-2015 წარმოადგენს კიბერ უსაფრთხოების სფეროში სახელმწიფო პოლიტიკის განმსაზღვრელ მთავარ დოკუმენტს.
- შემუშავდა სტანდარტული ოპერაციული პროცედურები ციფრული მტკიცებულებების პირველადი მოპყრობის შესახებ. დოკუმენტები განსაზღვრავს იმ პროგრამულ უზრუნველყოფის სახეებსა და ტექნიკურ წესებს, რომლის მიხედვითაც უნდა განხორციელდეს ციფრული მტკიცებულებების დამუშავება.
- შსს აკადემიაში შემუშავდა სპეციალური ტრენინგ მოდულები, რომელიც ფარავს კიბერ დანაშაულთან დაკავშირებულ შემდეგ საკითხებს: ელექტრონული მტკიცებულებების ჩხრეკა ამოღება, კიბერ დანაშაულის საგამოძიებო ტექნიკა, კიბერ დანაშაულის სამართლებრივი ასპექტები და ა.შ.
- კიბერდანაშაულთან ბრძოლის სამმართველოს აქტიური ჩართულობით მომზადდა საკანონმდებლო ინიციატივა საქართველოს სისხლის სამართლის კოდექსის XXXV თავში შესატანი რიგი ცვლილებების შესახებ.

გახსოვდეთ!

- მუდმივად განაახლეთ თქვენი კომპიუტერი უახლესი პროგრამული უზრუნველყოფით.
- დარწმუნდით, რომ კომპიუტერი სწორად არის კონფიგურირებული. ახლად შეძენილ კომპიუტერებს შესაძლოა არ ჰქონდეთ გააქტიურებული დაცვის პროგრამა, რაც დამნაშავის სასარგებლოდ იმუშავებს.

- აირჩიეთ ძლიერი კოდი და არ გამოააშკარაოთ იგი- პაროლები ინტერნეტ სარგებლობის განუყოფელ ნაწილს წარმოადგენს, ინტერნეტ შესყიდვები და ინტერნეტ ბანკინგი შეუძლებელია მის გარეშე.
- დაიცავით თქვენი კომპიუტერი სპეციალური ანტი-ვირუსული პროგრამებით. პირველადი დამცავი მექანიზმი არის თქვენი კომპიუტერის „ფაიერვოლი“. სწორედ იგი უზრუნველყოფს შემავალი და გამავალი ინფორმაციის კონტროლს.
- ონლაინ შემოთავაზებები - ნუ აყვებით ემოციებს და ნუ მიიღებთ არარეალურად მომგებიან შემოთავაზებებს უცხო პირებისგან.
- რეგულარულად შეამოწმეთ საკრედიტო ბარათისა და ინტერნეტ ბანკინგის პირადი მონაცემები. ე.წ. ,,ტერმინალი''-თ მომსახურების ან ნივთის საფასურის გადახდის დროს ყურდღება მიაქციეთ საკრედიტო ბარათის მიმღები პირის ქმედებას და არ დაუშვათ ბარათის ფიზიკური გასვლა თქვენი ვიზუალური მეთვალყურეობის არედან.
- თავი შეიკავეთ საეჭვო ინტერნეტ საიტებზე ონლაინ გადახდებისა და საკრედიტო ბარათის მონაცემების დაფიქსირებისგან.
- ბანკომატიდან თანხის განაღდების დროს ყურადღება მიაქციეთ ხომ არ არის მასზე განთავსებული რაიმე ისეთი მოწყობილობა, რომელიც ადრე არ შეგინიშნავთ. ასეთის აღმოჩენის შემთხვევაში შეატყობინეთ შესაბამის საბანკო დაწესებულებას და პოლიციას.
- ყურადღება მიაქციეთ ბავშვების ინტერნეტში შესვლას, თვალყური ადევნეთ ვებ-გვერდებს, რომლებსაც ისინი ხშირად სტუმრობენ. აკონტროლეთ უცხო პირთა მიერ მათთან სოციალური ქსელების ან ელექტრონული ფოსტის მეშვეობით დაკავშირების მცდელობები.
- დაიცავით თქვენი პერსონალური ინფორმაცია - გამოიჩინეთ განსაკუთრებული სიფრთხილე, როდესაც აზიარებთ თქვენს პირად მონაცემებს.

თუ თქვენ გახდით კიბერ თავდასხმის მსხვერპლი ან ფლობთ ინფორმაციას კიბერდანაშაულის თაობაზე, გთხოვთ დაგვიკავშირდეთ შემდეგ საკონტაქტო მონაცემებზე:

24 საათიანი უფასო ცხელი ხაზი - 112

ტელ: 2 41 12 96, 2 41 17 67;

ელ–ფოსტა: cybercrime@mia.gov.ge