

კიბერუსაფრთხოება

მოამზადა: ნინო მარდიშვილმა



ინფორმაციულ-საკომუნიკაციო ტექნოლოგიების განვითარებამ ხელი შეუწყო მსოფლიოში ახალი გამოწვევების წარმოქმნას. ამ მეცნიერულმა მიღწევამ ბევრ უპირატესობასთან ერთად, წარმოშვა ახალი საფრთხეებიც.

დღეს, კიბერთავდასხმები წარმოადგენს საფრთხეს, რომლის წინააღმდეგაც ეროვნული უსაფრთხოების ექსპერტები ეძიებენ უფრო ეფექტურ, თანმიმდევრულ კიბერპოლიტიკას, ქმნიან სტრატეგიულ დოკუმენტებს და თავდაცვის მეთოდებს.

რა არის კიბერსივრცე?

ეს არის ელექტრონული, ვირტუალური სივრცე, რომელშიც ხდება ინფორმაციისა და მონაცემების გადაცემა და ნებისმიერი სხვა სახის კომუნიკაცია ელექტრონული საშუალებით და არა მხოლოდ კომპიუტერით. ეს შეიძლება იყოს კომპიუტერი, კომპიუტერული ქსელი, მობილური თუ სხვა ტექნიკური საშუალება, რომელიც ტექნოლოგიურად უზრუნველყოფს ინფორმაციისა და მონაცემების გადაცემას.



ინფორმაციულ-საკომუნიკაციო ტექნოლოგიების განვითარებამ მნიშვნელოვნად შეუწყო ხელი კიბერსივრცეში საფრთხეების წარმოქმნას. რაც უფრო იზრდება მობილური ტელეფონის, ციფრული აპლიკაციების და ინფორმაციები ქსელში უფრო მატულობს კომპიუტერული ვირუსები, ქსელის გათიშვა და სხვა მსგავსი პროცესები, რომელიც არასასიამოვნო და ხშირად საშიშია.

სამთავრობო, საჯარო, ფინანსური, სამხედრო ორგანიზაციები და სხვა სტრუქტურები ინახავენ დიდ რაოდენობის კონფიდენციალურ ინფორმაციას კომპიუტერებში და გადაცემენ მათ ქსელების დახმარებით სხვა კომპიუტერებს. გახშირებული კიბერშეტევების გამო, ინფორმაცია მოითხოვს დაცვას.

კიბერშეტევები და ციფრული ჯაშუშობა არის უმნიშვნელოვანესი საფრთხე ქვეყნის უსაფრთხოებისთვის.

კიბერუსაფრთხოება XXI საუკუნის ერთ-ერთი გამოწვევაა, რომელიც გულისხმობს ინფორმაციული ტექნოლოგიების უსაფრთხოებას და უზრუნველყოფს კომპიუტერების, ქსელების ინფორმაციის დაცვას გაუთვალისწინებელი წვდომისგან, შეცვლისგან ან განადგურებისგან.

რჩევები კომპიუტერული უსაფრთხოების გასაუმჯობესებლად

- ელექტრონული ფოსტის, სოციალური ქსელის და სხვა ანგარიშებისთვის არ გამოიყენოთ ადვილად დასამახსოვრებელი და გამოსაცნობი პაროლები. გამოიყენეთ პაროლი, რომელიც შეიცავს დიდ და პატარა ასოებს, სასვენ ნიშნებს, ციფრებს – ასეთი პაროლები უფრო რთულად გამოსაცნობია. არ გამოიყენოთ პაროლები, რომელიც შეიცავს დაბადების თარიღებს ან ისეთ ინფორმაციას, რომლის მოპოვება ადვილად შეიძლება. არ გამოიყენოთ ერთიდაიგივე პაროლი

სხვადასხვა ონლაინ ანგარიშებისთვის. არ უთხრათ თქვენი პაროლი არავის, არ შეინახოთ პაროლები დაუცველ დოკუმენტებში

- გამოიყენეთ ორმაგი აუთენტიფიკაციის მეთოდი-სერვისის გააქტიურების შემთხვევაში, ავტორიზაციისთვის აუცილებელი სახელის და პაროლის მოთხოვნას ემატება SMS-ით მიღებული კოდიც;
- ინტერნეტში მუშაობის დროს არ დააწკაპუნოთ საეჭვო ბმულზე ან ავტომატურად ამოვარდნილ ფანჯრებზე (Pop-Up);
- არ უპასუხოთ საეჭვო წერილს, არ გასცეთ პასუხი საეჭვო კითხვებს და არ გადახვიდეთ ფოსტაზე მოსულ საეჭვო ბმულზე;
- უფასო პროგრამების ჩამოტვირთვისას იყავით ფრთხილად, გადაამოწმეთ წყარო საიდან იწერთ პროგრამულ უზრუნველყოფას;
- განაახლეთ ოპერაციული სისტემა, პროგრამული უზრუნველყოფები;
- არ ენდოთ ისეთ უსადენო ქსელს რომელიც საჯაროდ არის გახსნილი (wi-fi);
- სოციალური ქსელის გამოყენებისას იყავით ფრთხილად, არ გამოაქვეყნოთ პირადი ინფორმაცია;
- უცნობი ვებგვერდებიდან ინფორმაციის ჩამოტვირთამდე დარწმუნდით, სანდოა თუ არა ეს ვებგვერდი;
- ბრაუზერში გახსნილი ანგარიშები(ფოსტა, სოციალური ქსელი, ინტერნეტ ბანკი და სხვა) ყოველთვის დახურეთ: „გამოსვლის“ ღილაკის საშუალებით;
- სხვა კომპიუტერზე ინტერნეტის გამოყენების შემდეგ ბრაუზერში წაშალეთ ისტორია;
- შეცვალეთ პროვაიდერის მოწოდებული პაროლი;
- გამოიყენეთ ანტივირუსი -დააყენეთ საიმედო ანტივირუსული პროგრამა;
- მობილური ტელეფონები დაიცავით პაროლის მეშვეობით, შეამოწმეთ მობილურის პარამეტრები, გადმოწერეთ აპლიკაციები მხოლოდ სანდო წყაროდან.

კომპიუტერი რა შემთხვევაში შეიძლება იყოს დაინფიცირებული?

- თუ კომპიუტერი ღიდხანს ანდომებს ოპერაციული სისტემის ჩატვირთვას და ის შენელებულად მუშაობს;
- კომპიუტერში ჩაწერილი პროგრამები არ იხსნება ან ბრძანების მიცემის გარეშე ეშვება;
- კომპიუტერში მყარი დისკი გავსებულია, მომხმარებელს კი შესაბამისი მოქმედებები არ განუხორციელებია;
- ბრაუზერის საწყისი გვერდი შეიცვალა, გარკვეულ ვებგვერდებზე შესვლა ვერ ხერხდება;
- ინტერნეტი შენელებულია;

განაახლეთ პროგრამული უზრუნველყოფა, რადგან შეიძლება თქვენი კომპიუტერი დაინფიცირებულია.

რა შეგვიძლია ვთქვათ ბავშვების შესახებ?

არსებობს კიბერსაფრთხეები, რომლებიც კონკრეტულად ბავშვებსა და თინეიჯერებზეა გათვლილი, ხანდახან ჰაკერები იყენებენ მიმზიდველ ვებგვერდებს ბავშვებში ინტერნეტის გამოწვევის მიზნით. აუხსენით ბავშვს, რომ თუ შენიშნავს ბმულს, რომელიც არასათანადო ან შეუსაბამო შინაარსის მასალას შეიცავს, აცნობოს ამის შესახებ მასწავლებელს, მშობელს. მოზარდებმა კარგად უნდა გაითავისონ, რომ გაცნობის, ახალი მეგობრების შეძენისთვის განკუთვნილი და სასაუბრო საიტები ხშირად არცთუ ისე უსაფრთხოა.

რჩევები, თუ რა უნდა იცოდნენ ბავშვებმა ინტერნეტ სივრცეში უსაფრთხოების შესახებ

1. მოიფიქრეთ ძირითადი წესები, რომლებიც განსაზღვრავენ ინტერნეტში შესვლის უფლებებს ბავშვებისთვის.

რაზე უნდა ესაუბროთ მათ:

- პერსონალური ინფორმაცია - რა უნდა გააზიარონ და რა არა;
- შესვლის სახელი (screen name) - როგორ აირჩიონ;
- პაროლები - როგორ შექმნან და მართონ;
- ფოტოები - ბავშვებმა არ უნდა განათავსონ ინტერნეტში სურათები თქვენი თანხმობის გარეშე;
- ონლაინ მეგობრები - შეახსენეთ, რომ ყველაფერი, რასაც ისინი კითხულობენ, არ არის სიმართლე. რჩევა უნდა ითხოვონ თქვენგან, სანამ ვინმესთან ონლაინ-სივრცეში დამეგობრდებიან;
- ონლაინ რეკლამები - ბავშვები უნდა მოერიდონ მშობლების თანხმობის გარეშე ყველაფერზე დაწკაპუნებას;
- ჩამოტვირთვა - ბავშვებმა უნდა იკითხონ, რამდენად შესაძლებელია რაიმე ახალი პროგრამის ჩამოტვირთვა;
- სოციალური ქსელები - დააწესეთ ასაკობრივი ზღვარი, რაც იქნება დაცვის დამატებითი დონე თქვენი შვილებისთვის;
- ძებნა - დააწესეთ შეზღუდვა იმ ვებ-გვერდებზე, რომელსაც შეუძლია ზიანი მიაყენოს თქვენს შვილებს. შეამოწმეთ რა აპლიკაციებს იყენებენ ბავშვები.

2. შეასწავლეთ მოსწავლეებს ონლაინ საფრთხეები:

შეასწავლეთ, თუ როგორ უნდა მოიქცნენ ინტერნეტში. მათ უნდა გაითავისონ საფრთხეები და ინტერნეტში „ქცევის“ წესები:

- მშობლების თანხმობის გარეშე არ გავცე პერსონალური ინფორმაცია, როგორიც არის მისამართი, ტელეფონის ნომერი, მშობლების ტელეფონის ნომრები;
- მშობლებს შევატყობინებ ნებისმიერი საექვო ფაქტის შესახებ;
- არ შევხვდები ონლაინ-მეგობარს, სანამ მშობლები არ დამრთავენ ნებას;
- ყოველთვის შევამოწმებ, რა სურათები დავდე ინტერნეტში, არ დავდებ სურათებს, რომლებიც მშობლებს არასასურველად მიაჩნიათ;
- მშობლების ნებართვის გარეშე არ ვუპასუხებ წერილებს, რადგან ისინი შეიძლება შეიცავდნენ საფრთხეს;
- მშობლების გარდა არ გავუზიარებ არავის ჩემს პაროლებს;
- ვიქნები პასუხისმგებლობის მქონე ინტერნეტ მომხმარებელი, რომელიც დაიცავს კანონს.

3. დააყენეთ საიმედო ანტივირუსული პროგრამა, მნიშვნელობა არ აქვს, შვილს საკუთარი კომპიუტერი აქვს თუ საერთო კომპიუტერს იყენებთ, ის უნდა იყოს დაცული. ბავშვებს აინტერესებთ ყოველივე ახალი, ისინი შეიძლება ენდონ ვებ-გვერდს, რომელიც საშიში ვირუსის შემცველია. უნდა ასწავლოთ, რომ არ ჩამოტვირთონ უცნობი და საექვო თამაშები.

4. აუცილებელია იქონიოთ კარგი ანტივირუსი, რომელსაც ექნება რეალურ დროში სკანირების ფუნქცია, ქსელური დაცვის ეკრანი (firewall) და ავტომატური განახლებები.

5. გამოიყენეთ ონლაინ რეჟიმში კონტროლის სპეციალური პროგრამა, რომელიც მოგცემთ საშუალებას გააკონტროლოთ ბავშვი.

უფასო ინსტრუმენტები:

- Parental Tools - <http://www.parentaltools.net/>
- DigiParent - <http://digiparent.weebly.com/>

სხვა ინსტრუმენტები (მათ შორის მობილური ტელეფონის მონიტორინგის აპლიკაციები):

<http://listoffreeware.com/list-of-best-free-parental-control-software/>
<http://www.tomsguide.com/us/best-parental-control-apps,review-2258.html>

შეჯამება:

- მარტივ ენაზე აუხსენით ბავშვებს, თუ რა არის ინფორმაციული უსაფრთხოება;
- აჩვენეთ, თუ როგორ შეიძლება გახდნენ კიბერკრიმინალების მსხვერპლი;
- ასწავლეთ, რომ უნდა იყვნენ ყურადღებით;
- ყურადღება გაამახვილეთ, თუ როგორ მუშაობს დაცვის სისტემები;
- დააყენეთ ავტომატური განახლებების სერვისი;
- შეადგინეთ საბაზისო წესები, რომლებიც განსაზღვრავენ, თუ რა შემთხვევაში და როგორ შეუძლია ბავშვს გამოიყენოს ინტერნეტი;
- შეასწავლეთ ონლაინ საფრთხეები;
- დააყენეთ კარგი ანტივირუსი;
- გამოიყენეთ მშობლების კონტროლის კომპიუტერული უზრუნველყოფა;
- მუდმივად განაახლეთ ბავშვების კომპიუტერზე პროგრამული უზრუნველყოფა;
- დაიცავით თქვენი სახლის უკაბელო ქსელი.