კიბერუსაფრთხოებასთან დაკავშირებული სახელმძღვანელო მშობლებისათვის

უსაფრთხოების თემაზე საუბარი ბავშვებთან ისეთივე მარტივია, როგორც მოზრდილ ადამიანებთან, რადგანაც ბავშვებს, ისევე როგორც ზრდასრულებს არ სურთ აღმოჩნდნენ მოტყუებულ მდგომარეობაში. უბრალოდ უნდა ავუხსნათ მათ, რომ არსებობენ ადამიანები, რომლებიც ცდილობენ სარგებლის მიღებას სხვების მოტყუების, მათი კუთვნილი ინფორმაციის ან ფულის მითვისების გზით. საჭიროა განვუმარტოთ ბავშვებს, რომ ყველაფერი ისე არ არის, როგორც ერთი შეხედვით ჩანს - ამიტომ, მნიშვნელოვანია დაფიქრება ყოველი ონლაინ-ქმედების განხორციელებამდე. არ მივცეთ ზემოხსენებულ საუბარს ერთჯერადი სახე, არამედ დავუბრუნდეთ მას დროდადრო, ვკითხოთ ბავშვს რაიმე საეჭვო ხომ არ შეუნიშნავს ბოლო პერიოდში. თქვენმა შვილებმა შესაძლოა იმაზე გაცილებით მეტი იცოდნენ კიბერუსაფრთხოების შესახებ, ვიდრე თქვენ ფიქრობთ.

ბავშვების შესახებ

არსებობს უსაფრთხოებასთან დაკავშირებული საფრთხეები, რომლებიც კონკრეტულად ბავშვებსა და თინეიჯერებზეა გათვლილი, თუმცა საფრთხეების უმეტესი ნაწილი გათვლილია პოტენციურ მსხვერპლზე, ასაკის გათვალისწინების გარეშე. ხანდახან ჰაკერები იყენებენ მიმზიდველ ვებ-გვერდებს ბავშვებში ინტერესის გამოწვევის მიზნით, მაგალითად „ფან-კლუბებს“, YouTube-ს, Instagram-ს და ა.შ; და გამომდინარე იქიდან, რომ მოზრდილი ადამიანებისთვისაც კი რთული განსასხვავებელია ოფიციალური და ყალბი ვებ-გვერდები, ბავშვები, რომელთაც ჯერ არ აქვთ ჩამოყალიბებული კრიტიკული აზროვნების უნარ-ჩვევები რათქმაუნდა გაცილებით ძნელი იქნება განსხვავების აღმოჩენა.

• **ბავშვებს უყვართ ვიდეოები.** საფრთხის შემცველი ბმულები დიდი ალბათობით შესაძლოა განთავსებული იყოს ისეთ პოპულარულ ვიდეო-პორტალებზე, როგორიცაა მაგალითად YouTube. აუხსენით თქვენს შვილს, რომ თუ შენიშნავს ბმულს, რომელიც არასათანადო ან შეუსაბამო შინაარსის მასალას შეიცავს, გაცნობოთ ამის შესახებ. თუ ისინი წააწყდნენ ყალბ ვებ-

გვერდს, სავარაუდოდ მოახდინეს მისი იგნორირება, რადგანაც მსგავსი ვებ-გვერდები საკმაოდ ჭკვიანურადაა შეფუთული კიბერკრიმინალების მიერ. მოზარდებმა კარგად უნდა გაითავისონ, რომ გაცნობის, ახალი მეგობრების შეძენისთვის განკუთვნილი და საჭორაო საიტები ხშირად არცთუ ისე უსაფრთხოა.

• **ბავშვები ხშირად იყენებენ ოჯახის კომპიუტერს.** გამომდინარე იქიდან, რომ ბავშვებს არ გააჩნიათ საკუთარი საკრედიტო ბარათები, თქვენ შესაძლოა იფიქროთ, რომ ისინი დაცულნი არიან ფინანსური დანაშაულებების მსხვერპლის სტატუსისგან, მაგრამ თუკი ბავშვები და მშობლები საერთო კომპიუტერს იყენებენ, მათი ონლაინ-აქტივობები მათ შორის ონლაინ-შოპინგი, მშობლების მიერ სახლის კომპიუტერით განხორციელებული საბანკო თუ სამსახურთან დაკავშირებული საქმიანობა ცალსახად ახდენს გავლენას სხვებზე; და მშობლებმა აუცილებლად უნდა იცოდნენ, თუკი შვილებმა შეამოწმეს ბრაუზერის ისტორია, ისინი შეძლებენ იგივე ვებ-გვერდებზე შესვლას, რომლებიც მათი მშობლების მიერ იქნა გამოყენებული სახლის კომპიუტერის მეშვეობით.

• **ბავშვები შეიძლება დიდი გულშემატკივრები იყვნენ.** მოზარდების მსგავსად და ხშირად უფრო მეტადაც კი, ბავშვებს და თინეიჯერებს შეუძლიათ გულშემატკივრობა - "გულშემატკივართა საიტები" და ჩატით საუბარი საყვარელ ცნობილ ადამიანებთან ან ადამიანებზე. არსებობს უამრავი ვარსკვლავის საიტი, რომლებსაც მართავს თვითონ ცნობილი ადამიანი ან გასართობი ამბების გამომცემელი ორგანიზაცია. თუმცა აუცილებელია ზედმეტი სიფრთხილის გამოჩენა ისეთ საიტებზე შესვლისას, რომლებიც შესაძლოა მოხვდნენ ძიების შედეგებში, თუმცა რეალურად არ მიეკუთვნებოდნენ ვარსკვლავებს. ასეთი ვებ-გვერდები როგორც წესი ძიების შედეგების ქვედა ზღვარზე ხვდებიან.

• **ბავშვები სოციალურები არიან.** არსებობს სოციალური მიზეზი, რის გამოც ბავშვებზე ხდება ჰაკერული შეტევა. ერთ-ერთი ფორმაა ბავშვის პაროლის გამოყენებით მის სოციალურ ანგარიშზე შესვლა და უხერხული შინაარსის შეტყობინებებისა თუ გამოსახულებების გაზიარება, სპამის გავრცელება ან ისეთი ბმულების დაპოსტვა, რომლებიც შესაძლოა შეიცავდეს მავნე კოდს. ასწავლეთ შვილებს **არ გაუზიაროთ პაროლები თუნდაც უახლოეს მეგობრებს და ყოველთვის დახუროთ ანგარიშები,** როდესაც ისინი გამოიყენებენ საჯარო გამოყენების კომპიუტერს, როგორიცაა სკოლაში და საჯარო ბიბლიოთეკებში განთავსებული კომპიუტერები. ბრაუზერი „იმახსოვრებს“ პაროლებს, თუ არ იყენებთ ბრაუზერის რეჟიმს „პირადი“ ან „ინკოგნიტო“, ან არ შლით ისტორიას მისი გამოყენების შემდეგ.

• **ბავშვების ID ბარათები ღირებული სამიზნეა ქურდებისთვის.** ზოგჯერ სამიზნე ხდება ბავშვის პირადობის მოწმობა - სადაც მითითებულია დეტალური ინფორმაცია მათ შესახებ (მაგალითად, სახელი, მისამართი და სოციალური დაცვის ნომერი), რათა მიიღონ კრედიტი ან ჩაიდინონ დანაშაული ბავშვის სახელით. ბავშვები არიან კარგი სამიზნე იმიტომ, რომ აქვთ ყველაზე სრულყოფილი საკრედიტო (მათ არასდროს ჰქონიათ ნასესხები ფული, შესაბამისად არასდროს დაუგვიანიათ გადახდა) ისტორია და ამ ფაქტის გამოვლენაც იქნება შეუძლებელი მანამ, სანამ მოზრდილ ასაკში თვითონ არ მიმართავენ ბანკს სტუდენტური სესხის ან საკრედიტო ბარათის ასაღებად.

მობილურ მოწყობილობებთან დაკავშირებული უსაფრთხოება

ბავშვებსა და მოზარდებს უყვართ ყველა ფუნქცია, რასაც მათ სმარტფონი და ტაბლეტი სთავაზობთ, დაწყებული თამაშებით და დასრულებული ფოტოს გაზიარებით. არსებობს ასობით ათასი აპლიკაცია სმარტფონებისა და ტაბლეტებისთვის, თუმცა ყველა მათგანი არ მიეკუთვნება სანდო რეპუტაციის მქონე მომწოდებელს. სანამ ბავშვებს მისცემთ აპლიკაციის ჩამოტვირთვის უფლებას, დარწმუნდით, რომ მათ (და თქვენც) იციან, რისთვის არის განკუთვნილი აპლიკაცია, რა ინფორმაციას აგროვებს და რაში იყენებს ამ მონაცემებს. აპლიკაციებისთვის იშვიათობას არ წარმოადგენს მომხმარებლის ადგილმდებარეობის იდენტიფიკაცია და ისეთი დეტალების დადგენაც კი, როგორიცაა ასაკი და სქესი.

• **დაიცავით ტელეფონი პაროლის მეშვეობით.** თითქმის ყველა ტელეფონის დაბლოკვა შეიძლება მარტივი რიცხვითი კოდით, პაროლით ან ანაბეჭდით, რომელთა გარეშეც საგანგებო სამსახურების გარდა ვერავისთან დაკავშირებას ვერ შეძლებთ. ამ მეთოდით შეძლებთ თქვენს ტელეფონში შენახული ინფორმაციის დაცვას არასანქცირებული ზარებისგან და მოახდენთ ცუდი ზრახვების მქონე ადამიანების მიერ თქვენი ტელეფონის გამოყენებით უხერხული შეტყობინებების ან კომენტარების გაკეთების პრევენციას.

• **შეამოწმეთ თქვენი ტელეფონის პარამეტრები.** სმარტფონებს გააჩნიათ კონფიდენციალურობის და უსაფრთხოების პარამეტრები, რომელთა მეშვებითაც კონტროლდება კონკრეტულ ინფორმაციასთან ხელმისაწვდომობა, მაგალითად: რომელი აპლიკაციის მეშვეობით ხდება თქვენი კონტაქტების, კალენდარისა და ადგილმდებარეობის მართვა. ყურადღებით დააკვირდით პარამეტრებს და შეცვალეთ ისინი საჭიროების შემთხვევაში.

• **გამოიჩინეთ სიფრთხილე სერვისების შესყიდვისას.** მიუხედავად იმისა, რომ არსებობს ბევრი უფასო ლეგიტიმური პროგრამა, რომელიც კანონიერად აკისრებს მომხმარებელს გადასახადს განახლებისთვის, თამაშების მომდევნო დონეზე გადასვლისთვის, თამაშების გმირებისთვის დამატებითი უნარების შეძენისთვის, ასევე არსებობს არალეგიტიმური აპლიკაციები, რომლებიც ცდილობენ მომხმარებლის შეცდომაში შეყვანას და მათთვის გარკვეული სერვისების მიყიდვას. ლეგიტიმური აპლიკაციის შემთხვევაშიც კი ბავშვმა უნდა იცოდეს, როდის შეიძლება ან როდის არ არის მიზანშეწონილი აპლიკაციის ან მის მიერ შემოთავაზებული სერვისების შესყიდვა. ნებისმიერი აპლიკაციის ჩამოტვირთვა შეთანხმებული უნდა იყოს მშობელთან.

• **შეარჩიეთ ლეგიტიმური აპლიკაციები.** ხშირია შემთხვევები, როდესაც კრიმინალები ავრცელებენ აპლიკაციებს მომხმარებლისგან პირადი ინფორმაციის არასანქცირებულად მითვისების მიზნით. არსებობს ასევე ლეგიტიმური აპლიკაციის ჰაკერების მიერ ხელში ჩაგდების რისკიც. გამოსავალი არის ჩამოტვირთოთ აპლიკაციები მხოლოდ ავტორიტეტული “app store”-დან - სასურველია გაეცნოთ რეიტინგებსა და შეფასებებს. ყველაზე მეტ ინფორმაციას ბავშვები მეგობრებისგან იღებენ და აუცილებელია შევახსენოთ მათ, რომ გარდა მეგობრებისა, საჭიროა აპლიკაციის რეიტინგსა და ჩამოტვირთვის რაოდენობაზე ყურადღების გამახვილება. თუ შეგექმნათ ეჭვის საფუძველი და აპლიკაცია უკვე გადმოწერილი გაქვთ, წაშალეთ დაუყოვნებლივ.

- **გამოიყენეთ „geolocation“ დიდი სიფრთხილით.** ეს მნიშვნელოვანია მობილური მოწყობილობის ყველა მომხმარებლისათვის. "Pew Internet Research“-ის ბოლო კვლევაზე დაყრდნობით თინეიჯერების 46%-ს (გოგონების 59%-ს) გამორთული აქვს ადგილმდებარეობის განმსაზღვრელი ფუნქცია. ზოგიერთი სერვისი, მაგალითად სანავიგაციო სისტემები და პროგრამები ეხმარება მშობლებს შვილების ადგილმდებარეობის კონტროლში მათი უსაფრთხოების მიზნით, თუმცა ყველა აპლიკაცია ამ ფუნქციის გააქტიურებას არ საჭიროებს (ზოგიერთი მას საკუთარი მარკეტინგული მიზნებისათვის იყენებს). შეგიძლიათ გამორთოთ „geolocation“ ფუნქცია ტელეფონში, მაგრამ ხშირად უფრო მართებულია მისი გათიშვა მხოლოდ კონკრეტული აპლიკაციებისათვის. ასე რომ გადახედეთ ბავშვის მიერ ხშირად გამოყენებადი აპლიკაციების პარამეტრებს და თუ რომელიმე მათგანს ჩართული აქვს ადგილმდებარეობის დადგენის ფუნქცია, რაც თქვენთვის მიუღებელია, გამორთეთ ფუნქცია ან წაშალეთ აპლიკაცია.

შემაჯამებელი მოსაზრებები

ტექნოლოგია და მასთან დაკავშირებული რისკები მზარდი და განვითარებადია, როდესაც ახალი და მასშტაბური ტექნოლოგია შემოდის, მილიონობით ადამიანი აპირებს მის გამოყენებას, მათგან მცირე რაოდენობის ხალხი - ბოროტი მიზნებით. მსგავსი ინტერესების მქონე ადამიანები მაქსიმალურად შეეცდებიან მათ ხელთ არსებული როგორც სოციალური, ისე ტექნიკური ბერკეტების გამოყენებას მიზნის მისაღწევად. როგორც უსაფრთხოების ექსპერტები ცდილობენ განავითარონ საკუთარი უნარ-ჩვევები და შესაძლებლობები, იგივე წარმატებით ვითარდებიან კიბერკრიმინალებიც. ეს ყოველთვის იქნება „კატა-თაგვობანა“-ს ტიპის თამაში და უსაფრთხოებასთან დაკავშირებულ საფრთხეებსაც სავარაუდოდ კიდევ დიდხანს ვერ გავექცევით.

გარდა თქვენს მიერ გამოყენებული ტექნოლოგიური საშუალებებისა, გაცილებით სანდო დაცვაა **კრიტიკული აზროვნება** - აღქმა მაგალითად იმისა, რომ რამდენიმე წამიანი შეჩერება ბმულზე დაკლიკების, აპლიკაციის ჩამოტვირთვის, პაროლის ან პირადი ინფორმაციის შეყვანის შედეგების შესაფასებლად მნიშვნელოვანია. თუ ვინმე თქვენი ოჯახის წევრებს შორის უშვებს შეცდომას, შეეცადეთ არ მოახდინოთ მწვავე რეაგირება. მშვიდად შეაფასეთ, თუ რა იყო არასწორი და შეეცადეთ დახმარებას, თავი აარიდეთ „ბრალის წაყენებას“. გაითვალისწინეთ, რომ არსებობს უამრავი დიდი კომპანია და სამთავრობო უწყება, რომლებიც გახდნენ ჰაკერული თავდასხმის მსხვერპლი.

რისკების არსებობა არ ნიშნავს იმას, რომ აღარ უნდა გამოიყენოთ ტექნოლოგიური საშუალებები ან აუკრძალოთ ბავშვს მათთან მიახლოება. თუმცა აუცილებლობას წარმოადგენს რისკების შემცირებაზე ზრუნვა და დაშვებული შეცდომების საკუთარი ძალებით გამოსწორების უნარების გამომუშავება. როგორც სხვა დანარჩენ საკითხებთან მიმართებაში, ჩვენ ტექნოლოგიასთან დაკავშირებული შესაძლო რისკების მინიმუმამდე დაყვანაც შეგვიძლია საღი აზროვნების მეშვეობით და გაფრთხილებებისთვის ყურადღების მიქცევით. უსაფრთხოებასთან დაკავშირებული რისკები დიდი პრობლემაა, თუმცა თანამედროვე ტექნოლოგიებით მიღებულ სარგებელს ცხოვრების შეცვლა შეუძლია.