კიბერუსაფრთხოების პრაქტიკული გზამკვლევი მასწავლებლებისთვის

სარჩევი

შესავალი 2

თავი 1. კიბერუსაფრთხოება და მისი მნიშვნელობა 3

თავი 2. კიბერსაფრთხეები 6

თავი 3. ძლიერი პაროლები და მრავალფაქტორიანი ავთენტიფიკაცია (MFA) 11

თავი 4. კიბერჰიგიენა – უსაფრთხო ციფრული ჩვევები 14

თავი 5. პერსონალური მონაცემების დაცვა 16

თავი 6. ხელოვნური ინტელექტის (AI) უსაფრთხო გამოყენება 19

თავი 7. კიბერბულინგი 21

თავი 8. კიბერინციდენტზე რეაგირება 25

კიბერჰიგიენის 10 ოქროს წესი 29

დასკვნა 30

გამოყენებული ლიტერატურა 31

სსიპ მასწავლებელთა პროფესიული განვითარების ეროვნული ცენტრი
განათლების E სახლი
2026 წელი

შესავალი

ციფრული ტექნოლოგიები თანამედროვე განათლების განუყოფელი ნაწილია. სასწავლო პროცესში ფართოდ გამოიყენება ელექტრონული ჟურნალი, ელექტრონული ფოსტა, ღრუბლოვანი საცავები, ონლაინსაკომუნიკაციო პლატფორმები, ხელოვნური ინტელექტის ინსტრუმენტები და სხვადასხვა საგანმანათლებლო ციფრული რესურსი. ამ ტექნოლოგიებმა მნიშვნელოვნად გაამარტივა სწავლა-სწავლების პროცესი, თუმცა, იმავდროულად, გაზარდა კიბერუსაფრთხოებასთან დაკავშირებული რისკებიც.

დღეს მასწავლებელი არამხოლოდ ცოდნის გამზიარებელია, არამედ მნიშვნელოვანი ციფრული ინფორმაციის მფლობელიც. ყოველდღიურ საქმიანობაში იგი ამუშავებს მოსწავლეთა, მშობლებისა და კოლეგების პერსონალურ მონაცემებს, ინახავს სასწავლო მასალებს ღრუბლოვან საცავებში, იყენებს სხვადასხვა ონლაინპლატფორმას და აქვს ელექტრონული კომუნიკაცია. სწორედ ამიტომ, კიბერუსაფრთხოების ელემენტარული ცოდნა და უსაფრთხო ციფრული ქცევა თანამედროვე პედაგოგის ერთ-ერთ აუცილებელ პროფესიულ კომპეტენციად მიიჩნევა.

კიბერუსაფრთხოების საკითხების უგულებელყოფამ შესაძლოა გამოიწვიოს პერსონალური მონაცემების გაჟონვა, ანგარიშების გატეხვა, ფინანსური ზარალი, სასწავლო მასალების დაკარგვა, დეზინფორმაციის გავრცელება და საგანმანათლებლო პროცესის შეფერხება. კიბერთავდასხმების უმეტესობა მიზანში იღებს არამხოლოდ ორგანიზაციებს, არამედ ცალკეულ მომხმარებლებსაც, რომლებიც ხშირად დაუცველები არიან უსაფრთხოების ელემენტარული წესების უგულებელყოფის გამო.

წარმოდგენილი საკითხავი მასალა განკუთვნილია ყველა საგნის მასწავლებლისთვის და მიზნად ისახავს კიბერუსაფრთხოების საბაზისო ცოდნისა და პრაქტიკული უნარების განვითარებას. მასში განხილულია: კიბერუსაფრთხოების ძირითადი ცნებები, გავრცელებული კიბერსაფრთხეები, ანგარიშებისა და პერსონალური მონაცემების დაცვის მექანიზმები,

კიბერჰიგიენის პრინციპები, ხელოვნური ინტელექტის უსაფრთხო გამოყენება, კიბერბულინგის პრევენცია და კიბერინციდენტებზე პირველადი რეაგირების ძირითადი მიდგომები.

აღნიშნული რესურსი პედაგოგებს დაეხმარება ყოველდღიური საქმიანობისას უსაფრთხო ციფრული პრაქტიკის დანერგვაში, საკუთარი და მოსწავლეთა მონაცემების დაცვაში, კიბერსაფრთეების დროულ ამოცნობასა და ინფორმირებული გადაწყვეტილებების მიღებაში.

თავი 1. კიბერუსაფრთხოება და მისი მნიშვნელობა

რა არის კიბერუსაფრთხოება?

კიბერუსაფრთხოება არის ინფორმაციული სისტემების, კომპიუტერების, მობილური მოწყობილობების, ქსელების, პროგრამული უზრუნველყოფისა და მონაცემების დაცვა უნებართვო წვდომის, დაზიანების, განადგურების, შეცვლის ან სხვა სახის კიბერსაფრთხეებისგან.

კიბერუსაფრთხოების მთავარი მიზანია ინფორმაციის **კონფიდენციალურობის**, **მთლიანობისა** და **ხელმისაწვდომობის** უზრუნველყოფა.

- **კონფიდენციალურობა (Confidentiality)** – ინფორმაცია ხელმისაწვდომია მხოლოდ იმ პირებისთვის, ვისაც ამის უფლება აქვს.
- **მთლიანობა (Integrity)** – ინფორმაცია დაცულია არასანქცირებული ცვლილებებისგან და ინარჩუნებს სიზუსტეს.
- **ხელმისაწვდომობა (Availability)** – საჭირო ინფორმაციისა და სერვისების გამოყენება შესაძლებელია შესაბამის დროს და შესაბამისი მომხმარებლებისთვის.

ეს სამი პრინციპი ცნობილია, როგორც **CIA (Confidentiality, Integrity, Availability) მოდელი,** რომელიც კიბერუსაფრთხოების ერთ-ერთი ფუნდამენტური საფუძველია.

რატომ არის კიბერუსაფრთხოება მნიშვნელოვანი მასწავლებლისთვის?

მასწავლებელი ყოველდღიურად იყენებს სხვადასხვა ციფრულ ინსტრუმენტსა და ონლაინპლატფორმას. მაგალითად:

- ელექტრონულ ფოსტას;
- ელექტრონულ ჟურნალს;
- ღრუბლოვან საცავებს (Google Drive, OneDrive და სხვა);
- ვიდეოკონფერენციის პლატფორმებს;
- სასწავლო რესურსების გაზიარების სისტემებს;
- ხელოვნური ინტელექტის ინსტრუმენტებს.

ამ პლატფორმებზე ინახება ისეთი ინფორმაცია, როგორიცაა:

- მოსწავლეთა პერსონალური მონაცემები;
- შეფასებები;
- სასწავლო მასალები;
- ტესტები;
- პროექტები;
- ფოტოები და ვიდეოები;
- სასკოლო დოკუმენტაცია.

ამ მონაცემების დაკარგვამ, შეცვლამ ან მესამე პირის ხელში აღმოჩენამ შესაძლოა სერიოზული ზიანი მიაყენოს როგორც მასწავლებელს, ისე სკოლასა და მოსწავლეებს.

რატომ ხდებიან მასწავლებლები კიბერთავდასხმების სამიზნეები?

ხშირად მცდარია წარმოდგენა, თითქოს თავდამსხმელები მხოლოდ ბანკებს ან მსხვილ კომპანიებს ესხმიან თავს. სინამდვილეში, კიბერდამნაშავეები მიზანში იღებენ ნებისმიერ მომხმარებელს, რომელსაც აქვს ღირებული ინფორმაცია ან წვდომა მნიშვნელოვან სისტემებზე.

მასწავლებლები შესაძლოა გახდნენ თავდასხმის სამიზნეები, რადგან:

- ფლობენ მოსწავლეთა პერსონალურ მონაცემებს;
- იყენებენ მრავალ ონლაინსერვისს;
- აქტიურად მუშაობენ ელექტრონულ ფოსტასთან;
- იღებენ ფაილებს სხვადასხვა წყაროდან;
- ხშირად აზიარებენ სასწავლო მასალებს;
- იყენებენ ერთსა და იმავე ანგარიშებს რამდენიმე მოწყობილობაზე.

რეალური მაგალითი

სიტუაცია

მასწავლებელმა ელექტრონულ ფოსტაზე მიიღო შეტყობინება:

„თქვენი Google Drive-ის საცავი გადაივსო. 24 საათის განმავლობაში დაადასტურეთ ანგარიში, წინააღმდეგ შემთხვევაში ყველა ფაილი წაიშლება”.

წერილს ახლავს ღილაკი **„ანგარიშის დადასტურება**”.

მასწავლებელი გადადის ბმულზე და შეჰყავს ელფოსტა და პაროლი.

რამდენიმე წუთში ვეღარ შედის საკუთარ ანგარიშზე, ხოლო თავდამსხმელი იღებს წვდომას Google Drive-ში შენახულ ყველა დოკუმენტზე.

რა უნდა გაეკეთებინა?

- შეემოწმებინა გამომგზავნის ელფოსტის მისამართი;
- არ გადასულიყო საეჭვო ბმულზე;
- პირდაპირ შესულიყო Google-ის ოფიციალურ ვებგვერდზე და იქ შეემოწმებინა შეტყობინება;
- საეჭვო წერილი წაეშალა ან აღენიშნა, როგორც ფიშინგი.

დაიმახსოვრე

- ✓ კიბერუსაფრთხოება მხოლოდ ტექნოლოგიური საკითხი არ არის — ის ყოველდღიური პროფესიული პასუხისმგებლობის ნაწილია.
- ✓ მასწავლებელი პასუხისმგებელია როგორც საკუთარი, ისე მოსწავლეთა მონაცემების უსაფრთხოებაზე.
- ✓ კიბერსაფრთხეების უმეტესობის თავიდან აცილება შესაძლებელია უსაფრთხო ციფრული ჩვევების დანერგვით.

თავი 2. კიბერსაფრთხეები

ფიშინგი, მავნე პროგრამები, სოციალური ინჟინერია, QR-ფიშინგი, გამომძალველი პროგრამები

ციფრული ტექნოლოგიების განვითარებასთან ერთად იზრდება კიბერსაფრთხეების რაოდენობა და მათი განხორციელების მეთოდებიც უფრო დახვეწილი ხდება. თავდამსხმელები ხშირად იყენებენ ადამიანის

უყურადღებობას, ნდობას ან ინფორმაციის ნაკლებობას, რის გამოც მნიშვნელოვანია, მასწავლებელმა იცოდეს ყველაზე გავრცელებული საფრთხეები და მათი ამოცნობის გზები.

2.1. ფიშინგი (Phishing)

ფიშინგი არის კიბერთავდასხმის ერთ-ერთი ყველაზე გავრცელებული ფორმა, რომლის მიზანია მომხმარებლის მოტყუებით კონფიდენციალური ინფორმაციის (მაგალითად, მომხმარებლის სახელის, პაროლის, საბანკო მონაცემების ან ერთჯერადი კოდის) მოპოვება.

თავდამსხმელები ხშირად ქმნიან ოფიციალური ორგანიზაციების, ბანკების, ონლაინპლატფორმების ან სახელმწიფო უწყებების მსგავს ელექტრონულ წერილებს, SMS-ებს ან ვებგვერდებს. შეტყობინებები, როგორც წესი, შეიცავს გადაუდებელი მოქმედების მოთხოვნას, მაგალითად:

- „თქვენი ანგარიში დაიბლოკება".
- „დაადასტურეთ თქვენი ვინაობა".
- „მიიღეთ საჩუქარი".
- „შეცვალეთ პაროლი დაუყოვნებლივ".

როგორ ამოვიცნოთ ფიშინგი?

- ყურადღებით შეამოწმეთ გამომგზავნის მისამართი;
- დააკვირდით ბმულის ნამდვილ მისამართს;
- საეჭვოა შეტყობინება, რომელიც გადაუდებელ მოქმედებას მოითხოვს;
- არ გახსნათ უცნობი დანართები!
- არ შეიყვანოთ პაროლი ბმულზე გადასვლის შემდეგ, თუ დარწმუნებული არ ხართ ვებგვერდის სანდოობაში.

პრაქტიკული მაგალითი

მასწავლებელი იღებს წერილს, რომელიც თითქოს Google Classroom-ისგან არის გამოგზავნილი, სადაც წერია, რომ ანგარიში დაიბლოკება. წერილში მოცემულ ბმულზე გადასვლის შემდეგ იხსნება Google-ის მსგავსი გვერდი, თუმცა მისი მისამართი განსხვავებულია. პაროლის შეყვანის შემთხვევაში თავდამსხმელი იღებს ანგარიშზე წვდომას.

2.2. მავნე პროგრამები (Malware)

მავნე პროგრამა არის ნებისმიერი პროგრამა, რომელიც შექმნილია კომპიუტერის, მობილური მოწყობილობის ან მონაცემების დაზიანების, მოპარვის ან არასანქცირებული კონტროლის მიზნით.

მავნე პროგრამების ძირითადი სახეებია:

- **ვირუსი (Virus)** – ვრცელდება სხვა ფაილებთან ერთად და აზიანებს სისტემას.
- **ჭია (Worm)** – დამოუკიდებლად ვრცელდება ქსელში.
- **ტროას პროგრამა (Trojan)** – თავს უსაფრთხო პროგრამად ასაღებს.
- **ჯაშუში პროგრამა (Spyware)** – აგროვებს ინფორმაციას მომხმარებლის შესახებ.
- **სარეკლამო პროგრამა (Adware)** – აჩვენებს არასასურველ რეკლამებს და ხშირად აგროვებს მონაცემებს.

როგორ დავიცვათ თავი?

- გამოიყენეთ ლიცენზირებული პროგრამები.
- რეგულარულად განაახლეთ ოპერაციული სისტემა.

- გამოიყენეთ ანტივირუსული პროგრამა.
- არ ჩამოტვირთოთ პროგრამები უცნობი წყაროებიდან.
- ფრთხილად გახსენით ელექტრონული ფოსტის დანართები.

2.3. სოციალური ინჟინერია (Social Engineering)

სოციალური ინჟინერია არის ადამიანით მანიპულირების მეთოდი, რომლის მიზანია კონფიდენციალური ინფორმაციის მოპოვება ან მომხმარებლისგან ისეთი მოქმედების შესრულება, რომელიც თავდამსხმელს აძლევს წვდომას სისტემებზე.

თავდამსხმელები ხშირად იყენებენ:

- ავტორიტეტის იმიტაციას;
- ნდობის მოპოვებას;
- შიშის გამოწვევას;
- ცნობისმოყვარეობას;
- გადაუდებლობის განცდას.

მაგალითი

მასწავლებელს ურეკავს პირი, რომელიც თავს სკოლის ტექნიკურ სპეციალისტად წარადგენს და სთხოვს პაროლის თქმას „სისტემის შემოწმებისთვის. სინამდვილეში, იგი ცდილობს ანგარიშის გატეხვას.

გახსოვდეთ: არცერთი ორგანიზაცია არ მოგთხოვთ ტელეფონით ან ელფოსტით თქვენი პაროლის გამხელას.

2.4. QR-ფიშინგი (Quishing)

QR-ფიშინგი არის თაღლითობის თანამედროვე ფორმა, როდესაც თავდამსხმელი მავნე ვებგვერდზე გადასაყვანად იყენებს QR კოდს.

ასეთი QR კოდები შეიძლება განთავსდეს:

- ელექტრონულ წერილებში;
- პლაკატებზე;
- სოციალურ ქსელებში;
- ბეჭდურ მასალებში.

QR კოდის სკანირების შემდეგ მომხმარებელი ხვდება ყალბ ვებგვერდზე, სადაც სთხოვენ პაროლის ან საბანკო მონაცემების შეყვანას.

რეკომენდაციები

- დაასკანერეთ მხოლოდ სანდო QR კოდები.
- გადაამოწმეთ გახსნილი ვებგვერდის მისამართი.
- არ შეიყვანოთ პერსონალური ინფორმაცია უცნობ გვერდებზე.

2.5. გამომძალველი პროგრამები (Ransomware)

გამომძალველი პროგრამა (Ransomware) შიფრავს კომპიუტერში არსებულ ფაილებს და მათ გასახსნელად მომხმარებელს თანხის გადახდას სთხოვს.

ყველაზე ხშირად ზიანდება:

- დოკუმენტები;
- ფოტოები;

- პრეზენტაციები;
- სასწავლო რესურსები.

როგორ ავიცილოთ თავიდან?

- რეგულარულად შექმენით სარეზერვო ასლები.
- არ გახსნათ საეჭვო დანართები.
- მუდმივად განაახლეთ პროგრამები.
- გამოიყენეთ ანტივირუსი.

დაიმახსოვრე

✓ ფიშინგის მთავარი იარაღი მომხმარებლის მოტყუებაა.

✓ მავნე პროგრამები ყველაზე ხშირად ვრცელდება დაუცველი პროგრამებისა და ელფოსტის მეშვეობით.

✓ არასოდეს გაამჟღავნოთ პაროლი ტელეფონით ან ელექტრონული ფოსტით.

✓ QR კოდის სკანირებამდე დარწმუნდით მის სანდოობაში.

✓ სარეზერვო ასლები საუკეთესო დაცვაა მონაცემების დაკარგვისგან.

თავი 3. ძლიერი პაროლები და მრავალფაქტორიანი ავთენტიფიკაცია (MFA)

მომხმარებლის ანგარიშის უსაფრთხოების ერთ-ერთი ყველაზე მნიშვნელოვანი ელემენტი ძლიერი პაროლია. მიუხედავად ამისა, კიბერინციდენტების დიდი ნაწილი კვლავ სუსტი ან განმეორებით გამოყენებული პაროლების შედეგია.

როგორი უნდა იყოს ძლიერი პაროლი?

ძლიერი პაროლი:

- შეიცავს მინიმუმ **12–16 სიმბოლოს**;
- აერთიანებს დიდ და პატარა ასოებს, ციფრებსა და სპეციალურ სიმბოლოებს;
- არ შეიცავს პირად ინფორმაციას (დაბადების თარიღი, სახელი, ტელეფონის ნომერი);
- უნიკალურია თითოეული ანგარიშისთვის.

არ გამოიყენოთ

❌ 12345678

❌ password

❌ qwerty

❌ საქართველო123

❌ Nino2025

გამოიყენეთ პაროლური ფრაზა

პაროლური ფრაზა შედგება რამდენიმე ერთმანეთთან დაუკავშირებელი სიტყვისა და დამატებითი სიმბოლოებისგან.

მაგალითად:

Mze!Tetri#Sakheli_2026

ასეთი პაროლი გაცილებით რთულია გამოსაცნობად და მარტივია დასამახსოვრებლად.

პაროლების მენეჯერი

ბევრი ანგარიშის არსებობის პირობებში ყველა პაროლის დამახსოვრება რთულია. ამ მიზნით გამოიყენება **პაროლების მენეჯერი**, რომელიც უსაფრთხოდ ინახავს პაროლებს და საჭიროების შემთხვევაში ავტომატურად ავსებს მათ.

პაროლების მენეჯერის გამოყენების უპირატესობებია:

- უნიკალური პაროლების შექმნა;
- უსაფრთხო შენახვა;
- სწრაფი ავტორიზაცია;
- პაროლების სინქრონიზაცია სხვადასხვა მოწყობილობაზე.

მრავალფაქტორიანი ავთენტიფიკაცია (MFA)

მრავალფაქტორიანი ავთენტიფიკაცია (Multi-Factor Authentication – MFA) ნიშნავს, რომ ანგარიშზე შესვლისას მომხმარებელი ადასტურებს საკუთარ ვინაობას ორი ან მეტი დამოუკიდებელი ფაქტორის გამოყენებით.

ეს შეიძლება იყოს:

- პაროლი;
- ავტორიზაციის აპლიკაციით გენერირებული კოდი;
- უსაფრთხოების გასაღები;
- ბიომეტრიული მონაცემები (თითის ანაბეჭდი, სახის ამოცნობა).

MFA მნიშვნელოვნად ამცირებს ანგარიშის გატეხვის რისკს, რადგან პაროლის მოპოვება თავდამსხმელისთვის საკმარისი აღარ არის.

დაიმახსოვრე

✓ თითოეული ანგარიშისთვის გამოიყენეთ განსხვავებული პაროლი.

✓ გამოიყენეთ პაროლების მენეჯერი.

✓ ჩართეთ მრავალფაქტორიანი ავთენტიფიკაცია ყველა მნიშვნელოვან ანგარიშზე.

თავი 4. კიბერჰიგიენა – უსაფრთხო ციფრული ჩვევები

კიბერჰიგიენა გულისხმობს ყოველდღიურ პრაქტიკას, რომელიც ამცირებს კიბერსაფრთხეების ალბათობას და უზრუნველყოფს მონაცემებისა და მოწყობილობების დაცვას.

პროგრამებისა და ოპერაციული სისტემის განახლება

პროგრამების განახლება მხოლოდ ახალი ფუნქციების დამატებას არ ემსახურება. განახლებები ხშირად ასწორებს უსაფრთხოების ხარვეზებს, რომლებიც შესაძლოა თავდამსხმელებმა გამოიყენონ.

რეკომენდაცია: ჩართეთ ავტომატური განახლებები.

სარეზერვო ასლები (Backup)

მნიშვნელოვანი ფაილების დაკარგვის თავიდან ასაცილებლად აუცილებელია მათი რეგულარული კოპირების შექმნა.

სარეზერვო ასლები შეიძლება ინახებოდეს:

- გარე მყარ დისკზე;
- ღრუბლოვან საცავში;
- სკოლის სერვერზე (თუ ასეთი არსებობს).

უსაფრთხო Wi-Fi

საჯარო Wi-Fi ქსელები ხშირად არასაკმარისად არის დაცული.

რეკომენდებულია:

- გამოიყენოთ მხოლოდ სანდო ქსელები;
- არ შეასრულოთ მნიშვნელოვანი ოპერაციები დაუცველ ქსელში;
- საჭიროების შემთხვევაში გამოიყენოთ VPN.

ეკრანის "ჩაკეტვა"

სამუშაო ადგილის დატოვებისას ყოველთვის ჩაკეტეთ კომპიუტერი.

ეს განსაკუთრებით მნიშვნელოვანია სკოლაში, სადაც ერთ მოწყობილობასთან შესაძლოა რამდენიმე ადამიანი მივიდეს.

USB მოწყობილობების უსაფრთხო გამოყენება

USB მეხსიერება შესაძლოა შეიცავდეს მავნე პროგრამებს.

უსაფრთხოების მიზნით:

- გამოიყენეთ მხოლოდ სანდო მოწყობილობები;
- სკანირება ჩაუტარეთ ანტივირუსით;
- არ შეაერთოთ უცნობი USB მოწყობილობები.

პროგრამების ლიცენზირებული გამოყენება

არალიცენზირებული პროგრამები ხშირად შეიცავს უსაფრთხოების რისკებს და შესაძლოა მავნე კოდიც კი.

გამოიყენეთ მხოლოდ ოფიციალური წყაროებიდან ჩამოტვირთული პროგრამები.

დაიმახსოვრეთ:

✓ რეგულარულად განაახლეთ პროგრამები.

✓ შექმენით სარეზერვო ასლები.

✓ გამოიყენეთ უსაფრთხო Wi-Fi.

✓ ყოველთვის ჩაკეტეთ კომპიუტერი სამუშაო ადგილის დატოვებისას.

✓ ფრთხილად გამოიყენეთ USB მოწყობილობები.

✓ ჩამოტვირთეთ პროგრამები მხოლოდ სანდო წყაროებიდან.

თავი 5. პერსონალური მონაცემების დაცვა

5.1. რა არის პერსონალური მონაცემი?

პერსონალური მონაცემი არის ნებისმიერი ინფორმაცია, რომლის საშუალებითაც შესაძლებელია პირის პირდაპირ ან არაპირდაპირ იდენტიფიცირება.

პერსონალურ მონაცემებს მიეკუთვნება:

- სახელი და გვარი;
- პირადი ნომერი;
- დაბადების თარიღი;
- საცხოვრებელი მისამართი;
- ტელეფონის ნომერი;

- ელექტრონული ფოსტის მისამართი;
- ფოტო და ვიდეომასალა;
- მოსწავლის აკადემიური მოსწრება;
- ჯანმრთელობის შესახებ ინფორმაცია;
- IP მისამართი და სხვა ელექტრონული იდენტიფიკატორები.

საგანმანათლებლო დაწესებულებაში ყოველდღიურად მუშავდება მოსწავლეების, მშობლებისა და თანამშრომლების პერსონალური მონაცემები. ამიტომ მათი დაცვა არამხოლოდ ეთიკური, არამედ სამართლებრივი ვალდებულებაც არის.

5.2. რატომ არის მნიშვნელოვანი პერსონალური მონაცემების დაცვა?

პერსონალური მონაცემების არასათანადო დამუშავებამ შეიძლება გამოიწვიოს:

- პირადი ცხოვრების ხელყოფა;
- ფინანსური ან რეპუტაციული ზიანი;
- მონაცემების უკანონო გავრცელება;
- პიროვნების იდენტობის მითვისება;
- ნდობის დაკარგვა სკოლის მიმართ.

მასწავლებელს განსაკუთრებული პასუხისმგებლობა ეკისრება, რადგან მას აქვს წვდომა მოსწავლეთა პირად ინფორმაციაზე.

5.3. პერსონალური მონაცემების დამუშავების ძირითადი პრინციპები

მონაცემების დამუშავებისას მნიშვნელოვანია შემდეგი პრინციპების დაცვა:

- მონაცემები უნდა შეგროვდეს მხოლოდ კანონიერი მიზნით;

- დამუშავდეს მხოლოდ საჭირო მოცულობით;
- იყოს ზუსტი და განახლებული;
- ინახებოდეს უსაფრთხოდ;
- ხელმისაწვდომი იყოს მხოლოდ უფლებამოსილი პირებისთვის;
- აღარ ინახებოდეს იმაზე დიდხანს, ვიდრე ეს აუცილებელია.

5.4. უსაფრთხო პრაქტიკა სკოლაში

მასწავლებელმა უნდა დაიცვას შემდეგი წესები:

- არ გააზიაროს მოსწავლეთა მონაცემები მესამე პირებთან შესაბამისი საფუძვლის გარეშე;
- არ გააგზავნოს კონფიდენციალური ინფორმაცია დაუცველი არხებით;
- გამოიყენოს პაროლით დაცული მოწყობილობები;
- "ჩაკეტოს" კომპიუტერი სამუშაო ადგილის დატოვებისას;
- არ დატოვოს დაბეჭდილი დოკუმენტები ყველასთვის ხელმისაწვდომ ადგილას.

5.5. პრაქტიკული მაგალითი

სიტუაცია

მასწავლებელმა მოსწავლის შეფასება შეცდომით გაუგზავნა სხვა მშობელს.

შედეგი

- მოსწავლეთა შეფასება გახდა ხელმისაწვდომი სხვა პირისთვის;
- დაირღვა პერსონალური მონაცემების კონფიდენციალურობა.

როგორ უნდა მოქცეულიყო?

- ინფორმაცია გაეზიარებინა მხოლოდ უფლებამოსილი პირებისთვის.

დაიმახსოვრე

✓ მოსწავლის ინფორმაცია კონფიდენციალურია.

✓ გააზიარეთ მხოლოდ აუცილებელი მონაცემები.

✓ ყოველთვის გადაამოწმეთ, ვის უგზავნით ინფორმაციას.

✓ გამოიყენეთ უსაფრთხო პლატფორმები მონაცემების შესანახად და გასაზიარებლად.

თავი 6. ხელოვნური ინტელექტის (AI) უსაფრთხო გამოყენება

6.1. ხელოვნური ინტელექტი განათლებაში

ხელოვნური ინტელექტი (Artificial Intelligence – AI) სულ უფრო ფართოდ გამოიყენება სასწავლო პროცესში. მასწავლებლები AI ინსტრუმენტებს იყენებენ სასწავლო მასალების, ტესტების, პრეზენტაციების, შეფასების კრიტერიუმებისა და სხვა რესურსების მოსამზადებლად.

AI მნიშვნელოვნად ამარტივებს სამუშაო პროცესს, თუმცა მისი გამოყენება კიბერუსაფრთხოების და ეთიკურ რისკებთან არის დაკავშირებული.

6.2. რა რისკებს შეიცავს AI-ის გამოყენება?

AI სისტემაში შეყვანილი ინფორმაცია შეიძლება:

- დამუშავდეს სისტემის მიერ;
- შეინახოს გარკვეული პერიოდის განმავლობაში (სერვისის პირობებიდან გამომდინარე);

- უნდა გამოიყენებოდეს მოდელის გაუმჯობესებისთვის, თუ ის არ არის გამორთული.

ამიტომ მომხმარებელმა განსაკუთრებული ყურადღება უნდა მიაქციოს იმ ინფორმაციას, რომელსაც AI სისტემაში ათავსებს.

6.3. რა ინფორმაცია არ უნდა ავტვირთოთ AI სისტემებში?

არასოდეს ატვირთოთ:

- მოსწავლეთა პირადი მონაცემები;
- პირადი ნომრები;
- შეფასებების ბაზები;
- ჯანმრთელობის ინფორმაცია;
- პაროლები;
- ფინანსური ინფორმაცია;
- სკოლის შიდა კონფიდენციალური დოკუმენტები.

სასწავლო მაგალითების შექმნისას გამოიყენეთ გამოგონილი ან ანონიმიზებული მონაცემები.

6.4. AI-ის პასუხისმგებლიანი გამოყენება

ხელოვნური ინტელექტის მიერ შექმნილი პასუხები ყოველთვის არ არის ზუსტი.

ამიტომ აუცილებელია:

- გადაამოწმოთ ფაქტობრივი ინფორმაცია;
- გადაამოწმოთ წყაროები;
- არ დაეყრდნოთ AI-ს, როგორც ერთადერთ ავტორიტეტულ წყაროს;

- დაიცვათ საავტორო უფლებები;
- მიუთითოთ გამოყენებული წყაროები საჭიროების შემთხვევაში.

6.5. პრაქტიკული მაგალითი

სიტუაცია

მასწავლებელმა AI სისტემაში ჩატვირთა მოსწავლეთა სრული სია შეფასებებთან ერთად, რათა ავტომატურად მიეღო ანალიზი.

სწორი მიდგომა

მონაცემები უნდა ყოფილიყო ანონიმიზებული (მაგალითად: მოსწავლე A, მოსწავლე B), ან გამოყენებული უნდა ყოფილიყო მხოლოდ გამოგონილი მაგალითები.

დაიმახსოვრე

✓ AI არის დამხმარე ინსტრუმენტი და არა საბოლოო გადაწყვეტილების მიმღები.

✓ არ ატვირთოთ კონფიდენციალური ინფორმაცია.

✓ ყოველთვის გადაამოწმეთ AI-ის მიერ მოწოდებული ინფორმაცია.

✓ გამოიყენეთ AI ეთიკურად და პასუხისმგებლობით.

თავი 7. კიბერბულინგი

7.1. რა არის კიბერბულინგი?

კიბერბულინგი არის ციფრული ტექნოლოგიების გამოყენებით განხორციელებული მიზანმიმართული, განმეორებითი და მავნე ქმედება, რომელიც მიზნად ისახავს სხვა ადამიანის დამცირებას, დაშინებას, შეურაცხყოფას ან დაზიანებას.

კიბერბულინგი შეიძლება განხორციელდეს:

- სოციალურ ქსელებში;
- მესენჯერებში;
- ონლაინთამაშებში;
- ელექტრონული ფოსტით;
- ფორუმებსა და კომენტარებში.

7.2. კიბერბულინგის ძირითადი ფორმები

ყველაზე გავრცელებულია:

- შეურაცხმყოფელი შეტყობინებები;
- ცილისწამება;
- ყალბი პროფილების შექმნა;
- პირადი ფოტოების ან ვიდეოების გავრცელება;
- მუქარა;
- ჯგუფიდან განზრახ გამორიცხვა;
- სიძულვილის ენის გამოყენება.

7.3. როგორ ამოვიცნოთ კიბერბულინგი?

მასწავლებელმა ყურადღება უნდა მიაქციოს შემდეგ ნიშნებს:

- მოსწავლე უარს ამბობს ონლაინაქტივობებზე;
- უეცრად იცვლება მისი ქცევა;
- შფოთავს შეტყობინებების მიღებისას;
- ერიდება თანატოლებთან ურთიერთობას;
- უქვეითდება აკადემიური შედეგები.

7.4. როგორ უნდა იმოქმედოს მასწავლებელმა?

კიბერბულინგის აღმოჩენის შემთხვევაში:

1. მშვიდად მოუსმინეთ მოსწავლეს.
2. არ დაადანაშაულოთ დაზარალებული.
3. შეინახეთ მტკიცებულებები (სქრინშოთები, შეტყობინებები, ბმულები).
4. აცნობეთ სკოლის ადმინისტრაციას.
5. საჭიროების შემთხვევაში ჩართეთ მშობელი.
6. დაიცავით კონფიდენციალურობა.
7. საჭიროების შემთხვევაში მიმართეთ შესაბამის სპეციალისტებს.

7.5. პრევენცია

კიბერბულინგის პრევენციისთვის მნიშვნელოვანია:

- მოსწავლეებთან რეგულარული საუბარი ციფრულ ეთიკაზე;

- უსაფრთხო ონლაინქცევის სწავლება;
- კონფიდენციალურობის პარამეტრების სწორად გამოყენება;
- პოზიტიური ონლაინკომუნიკაციის წახალისება;
- სკოლაში შესაბამისი წესებისა და რეაგირების მექანიზმების არსებობა.

პრაქტიკული მაგალითი

მოსწავლემ მასწავლებელს აცნობა, რომ კლასელებმა სოციალურ ქსელში შექმნეს ჯგუფი, სადაც მის ფოტოს შეურაცხმყოფელი კომენტარები დაურთეს.

სწორი რეაგირება

- შეინახეთ სქრინშოთები;
- აცნობეთ ადმინისტრაციას;
- ჩართეთ მშობლები;
- დაეხმარეთ მოსწავლეს ემოციური მხარდაჭერის მიღებაში;
- იმოქმედეთ სკოლის შიდა რეგულაციების შესაბამისად.

დაიმახსოვრე

✓ კიბერბულინგი ისეთივე სერიოზული პრობლემაა, როგორც ბულინგი რეალურ გარემოში.

✓ მტკიცებულებების შენახვა მნიშვნელოვანია შემდგომი რეაგირებისთვის.

✓ ნუ უპასუხებთ აგრესიას აგრესიით.

✓ მასწავლებლის დროულმა რეაგირებამ შეიძლება თავიდან აიცილოს სერიოზული შედეგები.

თავი 8. კიბერინციდენტზე რეაგირება

8.1. რა არის კიბერინციდენტი?

კიბერინციდენტი არის ნებისმიერი მოვლენა, რომელიც საფრთხეს უქმნის ინფორმაციული სისტემების, მონაცემების ან ციფრული სერვისების უსაფრთხოებას. კიბერინციდენტმა შესაძლოა გამოიწვიოს მონაცემების დაკარგვა, ანგარიშზე უნებართვო წვდომა, მავნე პროგრამის გავრცელება ან სისტემის მუშაობის შეფერხება.

სკოლაში კიბერინციდენტის მაგალითებია:

- მასწავლებლის ან მოსწავლის ანგარიშის გატეხვა;
- ფიშინგშეტყობინებაზე რეაგირება;
- მავნე პროგრამით კომპიუტერის დაინფიცირება;
- სასწავლო მასალების ან პერსონალური მონაცემების დაკარგვა;
- ღრუბლოვან საცავზე უნებართვო წვდომა;
- სასკოლო ელფოსტის არასანქცირებული გამოყენება.

კიბერინციდენტის შემთხვევაში სწრაფი და სწორი რეაგირება მნიშვნელოვნად ამცირებს შესაძლო ზიანს.

8.2. როგორ ამოვიცნოთ კიბერინციდენტი?

ყურადღება უნდა მიაქციოთ შემდეგ ნიშნებს:

- პაროლი აღარ მუშაობს, მიუხედავად იმისა, რომ სწორად შეგყავთ;

- ანგარიშიდან იგზავნება შეტყობინებები, რომლებიც თქვენ არ გაგიგზავნიათ;
- კომპიუტერი ან მობილური მოწყობილობა მოულოდნელად ნელდება;
- ჩნდება უცნობი პროგრამები ან ფანჯრები;
- ფაილები გაქრა, შეიცვალა ან აღარ იხსნება;
- ბრაუზერში ხშირად იხსნება არასასურველი გვერდები;
- იღებთ შეტყობინებას უცნობი მოწყობილობიდან ანგარიშზე შესვლის შესახებ.

8.3. როგორ უნდა მოვიქცეთ კიბერინციდენტის დროს?

ინციდენტის აღმოჩენისთანავე იმოქმედეთ შემდეგი თანმიმდევრობით:

1. შეინარჩუნეთ სიმშვიდე

პანიკა ხშირად იწვევს არასწორ გადაწყვეტილებებს. პირველ რიგში, შეაფასეთ სიტუაცია.

2. შეცვალეთ პაროლი

თუ ეჭვი გაქვთ, რომ თქვენი ანგარიში კომპრომეტირებულია, დაუყოვნებლივ შეცვალეთ პაროლი.

- შექმენით ახალი, ძლიერი და უნიკალური პაროლი;
- არ გამოიყენოთ ძველი პაროლი ან მისი მცირედ შეცვლილი ვერსია.

3. გათიშეთ ყველა აქტიური სესია

ბევრი ონლაინსერვისი საშუალებას გაძლევთ დაასრულოთ ყველა აქტიური სესია. ეს მნიშვნელოვანია, რადგან შესაძლოა თავდამსხმელი კვლავ შესული იყოს თქვენს ანგარიშში.

4. ჩართეთ მრავალფაქტორიანი ავთენტიფიკაცია (MFA)

თუ აქამდე არ გქონდათ გააქტიურებული, ჩართეთ MFA. ეს მნიშვნელოვნად ამცირებს ანგარიშის ხელახლა კომპრომეტირების რისკს.

5. შეამოწმეთ მოწყობილობა

განაახლეთ ანტივირუსი და ჩაატარეთ სისტემის სრული სკანირება. საჭიროების შემთხვევაში მიმართეთ ინფორმაციული ტექნოლოგიების სპეციალისტს.

6. აცნობეთ სკოლის ადმინისტრაციას

თუ ინციდენტი დაკავშირებულია სასკოლო ანგარიშებთან, მოსწავლეთა მონაცემებთან ან სასწავლო სისტემებთან, დაუყოვნებლივ აცნობეთ სკოლის ადმინისტრაციას ან პასუხისმგებელ პირს.

7. აღადგინეთ მონაცემები

თუ ფაილები დაზიანდა ან წაიშალა, გამოიყენეთ წინასწარ შექმნილი სარეზერვო ასლები.

8. შეინახეთ მტკიცებულებები

არ წაშალოთ საეჭვო შეტყობინებები, ელექტრონული წერილები ან ეკრანის ანაბეჭდები (სქრინშოთები). ისინი შესაძლოა მნიშვნელოვანი იყოს ინციდენტის გამოძიებისთვის.

8.4. როგორ ავიცილოთ თავიდან კიბერინციდენტები?

საუკეთესო გზა კიბერინციდენტებთან გასამკლავებლად მათი პრევენციაა.

რეკომენდებულია:

- რეგულარულად განაახლოთ პროგრამები;
- გამოიყენოთ ძლიერი პაროლები;
- ჩართოთ მრავალფაქტორიანი ავთენტიფიკაცია;
- არ გახსნათ საეჭვო ბმულები და ფაილები;
- რეგულარულად შექმნათ სარეზერვო ასლები;
- მუდმივად იზრუნოთ კიბერჰიგიენაზე.

პრაქტიკული მაგალითი

სიტუაცია

მასწავლებელმა მიიღო შეტყობინება, რომ მის Google ანგარიშზე უცხო ქვეყნიდან განხორციელდა შესვლა.

სწორი რეაგირება

- დაუყოვნებლივ შეცვალა პაროლი;
- დაასრულა ყველა აქტიური სესია;
- ჩართო მრავალფაქტორიანი ავთენტიფიკაცია;
- გადაამოწმა უსაფრთხოების პარამეტრები;
- აცნობა სკოლის ადმინისტრაციას, რადგან ანგარიში გამოიყენებოდა სასწავლო პროცესში.

დაიმახსოვრე

✓ კიბერინციდენტის დროს სწრაფი რეაგირება ამცირებს ზიანს.

✓ შეცვალეთ პაროლი და გათიშეთ ყველა აქტიური სესია.

✓ შეინახეთ მტკიცებულებები.

✓ საჭიროების შემთხვევაში აცნობეთ სკოლის ადმინისტრაციას.

✓ გამოიყენეთ სარეზერვო ასლები მონაცემების აღსადგენად.

კიბერჰიგიენის 10 ოქროს წესი

კიბერუსაფრთხოება იწყება ყოველდღიური, პასუხისმგებლობიანი ქცევით. ქვემოთ მოცემული წესების დაცვა მნიშვნელოვნად ამცირებს კიბერსაფრთხეების ალბათობას.

1. **გამოიყენეთ ძლიერი და უნიკალური პაროლები.**
   თითოეული ანგარიშისთვის შექმენით განსხვავებული, რთულად გამოსაცნობი პაროლი.

2. **ჩართეთ მრავალფაქტორიანი ავთენტიფიკაცია (MFA).**
   დამატებითი ავტორიზაცია მნიშვნელოვნად ზრდის ანგარიშის უსაფრთხოებას.

3. **ყოველთვის გადაამოწმეთ ბმულები და გამომგზავნი.**
   ფრთხილად იყავით ელექტრონულ წერილებთან, SMS-ებთან და QR კოდებთან.

4. **რეგულარულად განაახლეთ პროგრამები და ოპერაციული სისტემა.**
   განახლებები ასწორებს უსაფრთხოების ხარვეზებს.

5. **შექმენით სარეზერვო ასლები (Backup).**
   მნიშვნელოვანი მონაცემები შეინახეთ უსაფრთხო ადგილას.

6. **დაიცავით პერსონალური მონაცემები.**
   გააზიარეთ მხოლოდ აუცილებელი ინფორმაცია და მხოლოდ უფლებამოსილ პირებთან.

7. **გამოიყენეთ მხოლოდ ლიცენზირებული და სანდო პროგრამები.**
   ჩამოტვირთეთ პროგრამები მხოლოდ ოფიციალური წყაროებიდან.

8. **ფრთხილად იყავით საჯარო Wi-Fi ქსელების გამოყენებისას.**
   მოერიდეთ კონფიდენციალური ინფორმაციის გადაცემას დაუცველი ქსელებით.

9. **არ გახსნათ საეჭვო ფაილები და დანართები.**
   უცნობი გამომგზავნისგან მიღებული ფაილები შესაძლოა მავნე პროგრამას შეიცავდეს.

10. **იმოქმედეთ სწრაფად კიბერინციდენტის შემთხვევაში.**
    შეცვალეთ პაროლი, შეწყვიტეთ აქტიური სესიები, შეინახეთ მტკიცებულებები და საჭიროების შემთხვევაში აცნობეთ პასუხისმგებელ პირებს.

დასკვნა

ციფრული ტექნოლოგიები მნიშვნელოვან შესაძლებლობებს ქმნის სწავლებისა და სწავლის პროცესში, თუმცა მათი უსაფრთხო გამოყენება მოითხოვს პასუხისმგებლობიან დამოკიდებულებასა და შესაბამის ცოდნას. თანამედროვე მასწავლებელი მხოლოდ საგნობრივი ცოდნის გამზიარებელი აღარ არის — ის ასევე ქმნის უსაფრთხო ციფრულ გარემოს, სადაც დაცულია მოსწავლეთა ინტერესები, პერსონალური მონაცემები და სასწავლო რესურსები.

კიბერუსაფრთხოება არ ეფუძნება მხოლოდ ტექნიკურ საშუალებებს. მისი საფუძველია ყოველდღიური უსაფრთხო ჩვევები: ძლიერი პაროლების გამოყენება, მრავალფაქტორიანი ავთენტიფიკაციის ჩართვა, პროგრამების

რეგულარული განახლება, პერსონალური მონაცემების დაცვა, ინფორმაციის კრიტიკული შეფასება და კიბერსაფრთხეებზე დროული რეაგირება.

ამ საკითხავ მასალაში წარმოდგენილი რეკომენდაციები და პრაქტიკული მაგალითები დაეხმარება მასწავლებლებს უსაფრთხო ციფრული გარემოს შექმნასა და პროფესიულ საქმიანობაში კიბერუსაფრთხოების პრინციპების ეფექტიანად დანერგვაში. უსაფრთხო ციფრული კულტურის განვითარება თითოეული ჩვენგანის პასუხისმგებლობაა და მისი დაცვა განათლების ხარისხის, ნდობისა და მოსწავლეთა კეთილდღეობის მნიშვნელოვანი წინაპირობაა.

გამოყენებული ლიტერატურა:

- ციფრული მოქალაქეობის პროგრამა „იყავი ინტერნეტ გენიოსი“ (Be Internet Awesome – Google). საგანმანათლებლო რესურსები ონლაინ უსაფრთხოების, ციფრული მოქალაქეობისა და პასუხისმგებლიანი ქცევის შესახებ. https://beinternetawesome.withgoogle.com/ka_ge
- Microsoft Security – Security Documentation and Best Practices. კიბერუსაფრთხოების, მონაცემთა დაცვისა და უსაფრთხო ციფრული პრაქტიკის სახელმძღვანელო რესურსები. https://www.microsoft.com/security
- UNESCO – Digital Learning and Online Safety. ციფრული განათლებისა და ონლაინ უსაფრთხოების საკითხებთან დაკავშირებული საერთაშორისო რესურსები. https://www.unesco.org/en/digital-education