

მოდული 6 – ამოცანები: ქეისების კვლევა სხვადასხვა პროფილის სტუდენტებისთვის

ქეისი 1: მასწავლებელი (ადვილი სირთულის დონე) – ციფრული კეთილდღეობის ხელშეწყობა კლასში

სცენარი: ეკრანის დროისა და ტექნოლოგიური ჩვევების მართვა მოსწავლეებში თქვენ ხართ საშუალო სკოლის მასწავლებელი და ამჩნევთ, რომ თქვენი მოსწავლეები ხშირად გამოიყურებიან გაფანტულად, დაღლილად და მზარდად მოუსვენრად. ბევრი მათგანი აცხადებს, რომ ყოველდღიურად 7 საათზე მეტს ატარებს ეკრანებთან, მათ შორის სახლშიც. თქვენ გთხოვენ, თქვენს სწავლების პროცესში ხელი შეუწყოთ უფრო ჯანმრთელ ციფრულ ჩვევებს.

დავალებები:

- შეაფასეთ, როგორ მოქმედებს ციფრული სტრესი და ეკრანის დრო მოსწავლეებზე (ჩატარეთ არაფორმალური გამოკითხვა ან დაკვირვება).
- შეიმუშავეთ სამი სტრატეგია ან აქტივობა კლასში ციფრული ტექნოლოგიების ჯანსაღი გამოყენების წასახალისებლად.
- მიუთითეთ ინსტრუმენტები ან აპლიკაციები, რომლებსაც მოსწავლეები ეკრანის დროის მონიტორინგისა და მართვისთვის გამოიყენებენ.
- შექმენით ერთგვერდიანი გზამკვლევი ან ინფოგრაფიკა სახელწოდებით „როგორ ავიდოთ კონტროლი ჩვენს ციფრულ ცხოვრებაზე“.
- რას ისწავლიან სტუდენტები: ციფრული გადატვირთულობის ნიშნების ამოცნობა, ჯანსაღი ციფრული რუტინების განვითარება და ციფრული კეთილდღეობის პრაქტიკის გამოყენება განათლებაში.

ქეისი 2: მედლობის სტუდენტი (საშუალო სირთულის დონე) – კიბერუსაფრთხოება პერსონალური სამედიცინო მონაცემებისთვის

სცენარი: ციფრული სამედიცინო ჩანაწერების დაცვა როგორც მედლობის სტუდენტი, რომელიც კლინიკაში მუშაობთ, თქვენ გთხოვენ, დაეხმაროთ ახალ თანამშრომლებს ციფრული სამედიცინო სისტემების ათვისებაში. ბევრ თანამშრომელს ერთი და იგივე

პაროლი აქვს სხვადასხვა ანგარიშზე ან ერთმანეთში იზიარებენ შესვლის დეტალებს, რაც საფრთხეს უქმნის პაციენტის მონაცემებს. თქვენ გეკუთვნებათ დავალება, რომ გაუწიოთ მათ განათლება ჯანმრთელობის მონაცემების კიბერუსაფრთხოების საფუძვლებზე.

დავალებები:

1. გამოავლინეთ რისკები, რომლებიც უკავშირდება სუსტი პაროლების პრაქტიკას და საერთო შესვლის დეტალებს ჯანდაცვის სისტემაში.
2. შედგინეთ სია "შეიძლება/არ შეიძლება" წესებისა პაციენტის მონაცემების უსაფრთხოდ მართვისთვის.
3. შექმენით მოკლე ვიზუალური ინსტრუქცია ან პოსტერის ტიპის მასალა პაროლების მართვის საუკეთესო პრაქტიკებზე.
4. დაწერეთ მოკლე საინფორმაციო ელფოსტა ახალ თანამშრომლებისთვის, სადაც განუმარტავთ, როგორ შეიძლება ფიშინგ შეტევებმა სამედიცინო პერსონალი დააზარალოს და როგორ უნდა ამოიცნონ ისინი.

რას ისწავლიან სტუდენტები: კიბერუსაფრთხოების შესახებ ცნობიერების ამაღლება რეალურ ჯანდაცვის გარემოში, პროფესიული პასუხისმგებლობა და ციფრული ჰიგიენის ჩვევები. პაციენტის კონფიდენციალურობა უმნიშვნელოვანესია. უზრუნველყავით, რომ თქვენი კომუნიკაცია იყოს ეთიკური, პროფესიონალური და პატივისცემით სავსე.

ქეისი 3: კიბერუსაფრთხოების სტუდენტი (მაღალი სირთულის დონე) – კიბერუსაფრთხოებისა და AI-ს შესახებ ცნობიერების ხელშეწყობა სამუშაო ადგილებზე

სცენარი: თანამშრომლების განათლება უსაფრთხო ციფრული ჩვევებისა და AI-ს გამოყენების შესახებ თქვენ ხართ კიბერუსაფრთხოების ექსპერტი საშუალო ზომის კომპანიაში, რომელმაც ცოტა ხნის წინ დაიწყო AI-ზე დაფუძნებული ინსტრუმენტების გამოყენება შიდა კომუნიკაციის, კანდიდატების შერჩევისა და მომხმარებელთა მომსახურებისათვის. თუმცა ბევრი თანამშრომელი არ იცნობს ციფრული ჰიგიენის ძირითად პრინციპებს და იყენებს AI ინსტრუმენტებს რისკების გაცნობიერების გარეშე. ზოგიერთი მათგანი აზიარებს კონფიდენციურ ინფორმაციას გენერატიულ AI პლატფორმებთან, ხოლო სხვები ერთსა და იმავე პაროლს იყენებენ ყველა ანგარიშზე.

მენეჯმენტმა გთხოვთ, შექმნათ საინფორმაციო კამპანია, რომელიც გააუმჯობესებს კიბერუსაფრთხოების პრაქტიკას, გაზრდის AI-თან დაკავშირებულ რისკებზე ცნობიერებას და გააძლიერებს ციფრულ კეთილდღეობას ორგანიზაციის მასშტაბით.

დავალებები:

შეაფასეთ სამუშაო გარემოში არსებული რისკების ზონები

გამოავლინეთ სამი ძირითადი კიბერუსაფრთხოების ან კონფიდენციალურობის რისკი (მაგ., სუსტი პაროლები, ფიშინგის რისკი, AI ინსტრუმენტების არასწორი გამოყენება)

შექმენით თანამშრომელთა ცნობიერების ამაღლების რესურსი

მოამზადეთ ვიზუალური სახელმძღვანელო, ვიდეოს სცენარი ან სლაიდების პრეზენტაცია შემდეგი თემებით:

პაროლების მართვის ძირითადი პრინციპები

ფიშინგ შეტევების ამოცნობა და მათზე რეაგირება

ეთიკური და უსაფრთხო AI გამოყენება სამუშაო გარემოში

ციფრული კეთილდღეობის მარტივი რჩევები (მაგ., ეკრანის დროის შეზღუდვა)

შემოიტანეთ სამი წესის შეთავაზება სამუშაო გარემოსთვის

დაწერეთ მოკლე დოკუმენტი სახელწოდებით „ციფრული პასუხისმგებლობის პოლიტიკა“, რომელიც შეიცავს საუკეთესო პრაქტიკებს:

მონაცემთა დაცვა

ანგარიშის უსაფრთხოება

AI ინსტრუმენტების შესაბამისი გამოყენება (მაგ., არ გამოიყენოთ პირადი ან კლიენტის ინფორმაცია საჯარო AI სერვისებში)

შეაფასეთ კამპანიის შედეგი

განიხილეთ, როგორ შეიძლება კამპანიამ გააუმჯობესოს თანამშრომელთა ჩვევები და შეამციროს რისკები

შემოგთავაზეთ მონიტორინგის მეთოდი (გამოკითხვა, ციფრული ჰიგიენის ჩეკლისტი, ტესტი)

რას ისწავლიან სტუდენტები:

- კიბერუსაფრთხოების ცოდნის გამოყენება რეალურ სამუშაო გარემოში
- რისკების ეფექტური კომუნიკაცია არატექნიკურ მომხმარებლებთან
- პასუხისმგებლობის მქონე ტექნოლოგიური ქცევის ხელშეწყობა და სტრესის შემცირება დაუბალანსებელი ციფრული ჩვევებისგან

ფინალური დავალებები და მოლოდინი სტუდენტებისგან:

სტუდენტებს ეძლევათ შესაძლებლობა აირჩიონ ქეისი თავიანთი სპეციალობის მიხედვით. ისინი უნდა წარადგინონ 1–2 გვერდიანი ანგარიში, რომელიც მოიცავს:

- ეთიკური და კონფიდენციალურობის საკითხების ეტაპობრივ ანალიზს
- გამოყენებულ ინსტრუმენტებს, ქმედებებს ან გადაწყვეტილებებს
- პროფესიული კომუნიკაციის ან რეფლექსიის კომპონენტს