

შ.პ.ს. კავკასიის ბიზნესის სკოლა

ტექნოლოგიური ტრენინგი პედაგოგებისთვის

მოსწავლეები: ლია ძველაია

პროექტის თემა: კიბერუსაფრთხოება; კიბერჰიგიენა

საგაკვეთილო პროექტი IX კლასის მოსწავლეებისთვის სადამრიგებლო საათის ფარგლებში

პროექტის იდეა: კიბერუსაფრთხოების პროექტი მიზნად ისახავს მოსწავლეების ინფორმირებულობას კიბერუსაფრთხოების საკითხებზე და მათი ცოდნის გაუმჯობესებას ონლაინ სივრცეში უსაფრთხოების პრინციპების დაცვაზე.

პროექტის აქტუალობა: დღევანდელ ციფრულ ეპოქაში კიბერუსაფრთხოება უმნიშვნელოვანესი საკითხია. ტექნოლოგიაზე და ინტერნეტზე ზრდადი ნდობა აუცილებელს ხდის ჩვენი ციფრული აქტივების და პირადი ინფორმაციის დაცვას კიბერუსაფრთხოებისგან. ეს პროექტი გვიჩვენებს კიბერუსაფრთხოების მნიშვნელობას, ხშირ საფრთხეებს და საუკეთესო პრაქტიკას უსაფრთხო ონლაინ გარემოს უზრუნველსაყოფად.

პროექტის მიზანი:

- ✓ მოსწავლეებში ცნობიერების ამაღლება კიბერუსაფრთხოების საფრთხეების შესახებ.
- ✓ ონლაინ უსაფრთხოების წესების და პრინციპების გაცნობა.
- ✓ პრაქტიკული უნარების განვითარება, რათა მოსწავლეებმა შეძლონ დაიცვან საკუთარი თავი და პირადი მონაცემები ონლაინ სივრცეში.

პროექტის შედეგი: პროექტის დასრულების შემდეგ, მოსწავლეები შეძლებენ:

- ✓ ამოიცნონ და გაუმკლავდნენ კიბერუსაფრთხოების საფრთხეებს.
- ✓ დაიცვან პირადი მონაცემები და პაროლები.
- ✓ გამოიყენონ უსაფრთხოების პრინციპები სოციალურ ქსელებსა და სხვა ონლაინ პლატფორმებზე.

რესურსები:

- ✓ **ონლაინ რესურსი:** Power Point; Ionline.ge; scratch; <https://haveibeenpwned.com/>; [Wheel of Names | Random name picker](#)
- ✓ **მატერიალური რესურსი:** პროექტორი, დინამიკი, დაფა, ფლაჰჩარტი, მარკერები, პლანშეტები ან ტელეფონები, ყუთი რომელშიც მოთავსებული იქნება სხვადასხვა სიტუაციური მაგალითები.

ხანგრძლივობა : 2 აკადემიური საათი

პროექტის დიზაინი/თანმიმდევრობა:

აქრივობა1. მოსწავლეთა ინტერესის და ჩართულობის გაზრდის მიზნით შეხვედრას დავინწყებ დისკუსიით და დავუსვამ შეკითხვას: „ რატომ გვჭირდება ინტერნეტი?“ და „რა საფრთხეებს შესაძლებელია გადავანყდეთ კიბერსივრცეში?“

აქტივობა2. გამოვიყენებ აქტივობას - „გონებრივი იერიში“ რომ დავადგინო მოსწავლეთა წინარე ცოდნა , რა იციან ჯერ კიბერუსაფრთხოების და შემდეგ კიბერჰიგიენის შესახებ? მოსწავლეთა პასუხებს ჩამოვწერთ ფლაჰჩარტზე.

აქტივობა 3. მოსწავლეებს ვესაუბრები და Power Point-ში აწყობილი პრეზენტაციის მიხედვით ვუხსნი კიბერუსაფრთხოების და კიბერჰიგიენის შესახებ.

აქტივობა 4. ფიშინგის და ქარდინგის უკეთ აღსაქმელად ვათამაშებ თამაშებს Ionline.ge - გამოცენებით. და განვიხილავთ მაგალითებს.

აქტივობა 5. დავეკითხები ხომ არ შეუძლიათ გაიხსენონ ფიშინგის ან ქარდინგის რაიმე პრეცედენტი; მოვუყვები ჩემს პირად მაგალითს თუ როგორ ჩამომეჭრა ანგარიშიდან თანხა ისე რომ ბარათი საფულეში მქონდა, მასცემდეგ რაც ბენზინგასამართ სადგურზე მივანოდე ჩემი ბარათი თანხის გადასახდელად. და ვთხოვ იმსჯელონ რომელი კიბერდანაშაულის მსხვერპლი აღმოვჩნდი და რა იყო ჩემი შეცდომა.

აქტივობა 6. როლური თამაში. მოსწავლეებს დავყოფ 4 კაციან ჯგუფებად და ვთხოვ ამოიღონ ყუთში წინასწარ მოთავსებული სიტუაციები და ელ.რესურსის Scratch- ით შექმნან მოკლე ანიმაციები. მსხვერპლი ყვება ამბავს. ერთერთი გამოკვეთს პრობლემას და დანარჩენები აძლევენ რჩევებს. შექმნილ ანიმაციებს წავიკითხავთ და ვიმსჯელებთ.

აქტივობა 7. იმისთვის რომ გადავამოწმოთ თუ რამდენად დაცული და უდაფრთხო პაროლი აქვთ მოსწავლეებს შევთავაზებ შემდეგ აქტივობას თავიანთი გაჯეტების მეშვეობით გადავიდნენ ბმულზე „ How Secure is my password“ და შეამოწმონ რამდენი დრო შეიძლება დაჭირდეს კომპიუტერს რო გატეხოს მათი პაროლი.

აქტივობა 8. <https://haveibeenpwned.com> - ბმულის გამოყენებით შევამოწმებთ ყოფილა თუ არა მცდელობა მათი გვერდის გატეხვისა.

აქტივობა 9. [Wheel of Names | Random name picker](#)-ს გამოვიყენებ რომ შეძლონ მოსწავლეებმა გაარჩიონ მოცემული პაროლი სუსტია თუ ძლიერი და როგორ შეიძლება გავაძლიეროთ სუსტი პაროლი.