თავდაცვის ინსტიტუციური აღმშენებლობის სკოლა
კურსების კატალოგი

კიბერუსაფრთხოების საბაზისო კურსი

მიზანი:

კიბერუსაფრთხოების საკითხებზე კურსის მონაწილეთა ცნობიერების ამაღლება, კიბერსივრციდან მომდინარე საფრთხეების შესახებ საბაზისო ცოდნის მიწოდება, პოტენციური კიბერშეტევის თავიდან ასაცილებლად.

განსახილველი საკითხები:

- კიბერუსაფრთხოება და მისი არსი, კიბერუსაფრთხოების მნიშვნელობა; ინფორმაციული უსაფრთხოების ასპექტები, კიბერაქტორები საქართველოში;
- მავნე პროგრამული უზრუნველყოფა და მისი ტიპები, ფიშინგი, ფინანსური თაღლითობები (სქიმინგი, ვიშინგი, ქარდინგი);
- ელ-ფოსტის უსაფრთხოება;
- უსაფრთხო ვებ-ბრაუზინგი, სოციალური ქსელის უსაფრთხოება, სმარტფონის უსაფრთხოება, მოწყობილობის დაინფიცირების ნიშნები;
- კიბერშეტევები საქართველოს წინააღმდეგ.

სასწავლო ამოცანები:

- მავნე პროგრამული უზრუნველყოფისა და მათი შესაძლებლობების შესახებ საბაზისო ცოდნის მიწოდება, რაც მას შესაძლებლობას მისცემს მეტი წარმატებით დაიცვას საკუთარი ელ-ფოსტის, სმარტფონისა და სოციალური ქსელის უსაფრთხოება;
- ელ. მოწყობილობის დაინფიცირების ნიშნების აღმოჩენა და შემდგომი რეაგირების მიზნით მითითებების პრაქტიკაში გამოყენება.

კურსის შედეგად განვითარებული უნარები:

- კიბერჰიგიენის უნარები (მავნე შიგთავსის მქონე წერილის აღმოჩენა, საეჭვო გვერდის ამოცნობა, კიბერშეტევის ასპექტების ამოცნობა).

სწავლების ფორმა: დისტანციური სწავლება/სემინარი.

სწავლების მეთოდოლოგია:

☒შემთხვევების ანალიზი

☒სალექციო კურსი

☒შემაჯამებელი დისკუსია

სამიზნე აუდიტორია: თავდაცვისა და უსაფრთხოების სექტორის სპეციალისტები, შუა რგოლის მენეჯერები.

კურსის ხანგრძლივობა: 1 დღე.
მონაწილეთა რაოდენობა: 25.
სწავლების ენა: ქართული.
კოდი: SSOPM9-2021.