Program profilaktyczny

Oszustwa telekomunikacyjne

Cele - Pokazać uczestnikom jak:

- nie dać się oszukać; korzystać z bezpiecznych linków;
- nie odbierać podejrzanych sms,
- używać sprawdzonych źródeł,
- jak rozpoznawać zainfekowane pliki

Program został podzielony na 2 części:

I. Zapobieganie

Prelekcje specjalistów do spraw cyberprzestępczości na temat zagrożeń czyhających w sieci, mający na celu uświadomienie, że Internet oprócz swoich pozytywnych aspektów jest kopalnią rzeczy, które mocno mogą zaszkodzić. Przykładowe przedstawienie sytuacji, które powinny wzbudzać czujność ludzi. Pokazanie różnych źródeł podejrzanych meili, smsów oraz stron. Omówienie sposobów zabezpieczenia się w sieci;

- **Zachowaj ostrożność jeśli otrzymasz niechciane maile, SMS-y czy telefony**, zwłaszcza jeśli kontaktujące się z Tobą osoby wykorzystują obecny kryzys i namawiają Cię do ominięcia normalnej procedury bezpieczeństwa. Napastnicy wiedzą, że często łatwiej jest oszukać człowieka niż włamać się do skomplikowanego systemu. Pamiętaj, że banki i inne organizacje nigdy nie będą Cię prosić o ujawnienie Twojego hasła.
- **Zabezpiecz swoją domową sieć internetową** - zmień domyślne hasło do sieci Wi-Fi na silne. Ogranicz liczbę urządzeń podłączonych do sieci Wi-Fi i zezwalaj tylko na zaufane urządzenia.
- **Wzmocnij swoje hasła** - pamiętaj, aby używać długich i złożonych haseł, które zawierają cyfry, litery i znaki specjalne.
- **Chroń swój sprzęt** - zaktualizuj wszystkie systemy i aplikacje, zainstaluj oprogramowanie antywirusowe i aktualizuj je.

II. Reagowanie

Przedstawienie sposobów kiedy stajemy się „ofiarami" ataków, co należy zrobić w momencie otrzymania podejrzanego telefonu, sms-a czy wiadomości. Gdzie szukać pomocy jeśli padniemy ofiarami oszustw pod przykryciem banków, przedstawienie służb udzielających pomoc np. Policji.

Przedstawienie konsekwencji prawnych, wynikających z niewłaściwego używania sieci internetowej, przedstawienie innych zagrożeń wynikających z użytkowania sieci: