PROGRAM SZKOLENIA

TYTUŁ SZKOLENIA: Zapobieganie zagrożeniom z obszaru cyberbezpieczeństwa - podstawowe zasady pracy w urzędzie.

GRUPA DOCELOWA: członkowie korpusu służby cywilnej ze wszystkich urzędów.

CEL GŁÓWNY: Zapoznanie uczestników z zagrożeniami, jakie płyną z cyberprzestrzeni oraz z metodami ochrony przed nimi.

EFEKTY SZKOLENIA: Uczestnicy po ukończeniu szkolenia:

- rozumieją podstawowe zagadnienia związane z cyberbezpieczeństwem;
- rozumieją, jakie znaczenie ma skuteczna ochrona przed cyberzagrożeniami w pracy w administracji;
- znają metody ustawiania bezpiecznego hasła, bezpiecznego korzystania ze skrzynki mailowej;
- potrafią rozróżnić maile, które mogą być potencjalnie niebezpieczne;
- wiedzą, gdzie szukać pomocy i jak zareagować w momencie podejrzenia lub zidentyfikowania zagrożenia w cybeprzestrzeni;
- znają narzędzia wspomagające ochronę w sieci dla użytkownika indywidualnego, tj. manager haseł, klucz zabezpieczający.

METODY DYDAKTYCZNE: wykład, dyskusja moderowana, praca indywidualna, praca w grupach, ćwiczenia

ŚRODKI DYDAKTYCZNE: prezentacja multimedialna, ćwiczenia, instrukcje, filmy, pre- i post-test

LICZBA GODZIN DYDAKTYCZNYCH: 6

Zadanie przed szkoleniem

Przed szkoleniem prosimy o obejrzenie materiału filmowego z wykładu na TED https://www.ted.com/talks/gary_kovacs_tracking_our_online_trackers/transcript (film ma możliwość włączenia napisów w języku polskim). Instrukcja w oddzielnym pliku

Lp.	Temat (części szkolenia)	Metoda dydaktyczna	Czas (godziny dydaktyczne /min)	Uwagi (środki dydaktyczne)
1.	• Omówienie agendy szkolenia i spraw organizacyjnych • Zapoznanie uczestników z technicznymi aspektami szkolenia • Przedstawienie się uczestników • Pre-test • Odniesienie się do zadania przedszkoleniowego • Cyberbezpieczeństwo czyli co? • Ramy prawne cyberbezpieczeństwa w Unii Europejskiej i w Polsce • Instytucje odpowiedzialne za bezpieczeństwo w sieci	Praca indywidualna Dyskusja moderowana Wykład	1 godz. dyd.	Pre-test Prezentacja multimedialna
2.	• Rodzaje zagrożeń w internecie • Techniki manipulacji i wyłudzania informacji	Wykład Dyskusja moderowana	1 godz. dyd.	Prezentacja multimedialna Mapa interaktywna

3.	• Inżynieria społeczna jako podstawa do przeprowadzenia cyberataku • Dane osobowe w sieci, czyli czego nie publikować • Bezpieczni w mediach społecznościowych	Wykład Dyskusja moderowana Praca indywidualna	1 godz. dyd.	Prezentacja multimedialna Film Ćwiczenia
4.	• Dezinformacja jako cyberzagrożenie • Jednostki administracji państwowej oraz europejskiej zwalczające fake newsy	Wykład Praca indywidualna	20 minut	Prezentacja multimedialna Ćwiczenia
5.	• Ważna rola skrzynki e-mail – jak dbać o bezpieczeństwo • Stwórz bezpieczne hasło - kluczowe techniki • Bezpieczny e-mail a ataki phishingowe	Wykład Praca indywidualna	40 minut	Prezentacja multimedialna Ćwiczenia
6.	• Bezpieczne zakupy w sieci oraz bezpieczne płatności • Postępowanie w cyberincydencie	Wykład Praca w grupach	1 godz. dyd.	Prezentacja multimedialna Ćwiczenia w grupie
7.	• Bezpieczne aplikacje wspierające prywatność (kopie danych, odzyskiwanie danych, manager haseł) • Instalacja wtyczek do przeglądarki wspierających anonimowość w sieci – indywidualna praca uczestników • Wirtualna sieć prywatna	Wykład Praca indywidualna	30 minut	Prezentacja multimedialna Ćwiczenia Post-test

Zadanie po szkoleniu

W CELU UTWARLENIA WIEDZY PROSIMYO PRZECZYTANIE PORADNIKA

„Jak chronić się przed cyberatakami”? Poradnik do pobrania pod adresem https://www.gov.pl/attachment/18b1b36f-b49a-4a20-bdfe-1037ffdea885