

Program szkolenia:

E-obywatel – E bezpieczeństwo (24 godziny zegarowe)

Cele szkolenia „E-obywatel – E bezpieczeństwo”

Cel główny:

Uczestnicy nabędą wiedzę i umiejętności niezbędne do bezpiecznego korzystania z internetu, ochrony danych osobowych, rozpoznawania zagrożeń cyfrowych oraz stosowania praktyk zwiększających bezpieczeństwo w sieci.

Cele szczegółowe:

Uczestnik po szkoleniu:

- rozpoznaje podstawowe zagrożenia w sieci (phishing, malware, spam, socjotechnika),
- zna zasady tworzenia silnych haseł i bezpiecznego logowania,
- potrafi korzystać z narzędzi ochrony danych (VPN, antywirus, firewall),
- rozumie znaczenie RODO i ochrony danych osobowych,
- potrafi bezpiecznie korzystać z mediów społecznościowych i komunikatorów,
- zna zasady bezpiecznego korzystania z urządzeń mobilnych i sieci publicznych,
- potrafi zastosować zasady higieny cyfrowej,
- umie korzystać z profilu zaufanego.

Materiały dla trenera:

- Komputery/laptopy/tablety z dostępem do Internetu
- Rzutnik/projektor
- Prezentacja multimedialna
- Test wstępny i końcowy
- Formularze do ćwiczeń praktycznych

Przebieg zajęć:

Informacje podstawowe	Cele sesji	Przebieg	Materiały i linki do zajęć	Uwagi
------------------------------	-------------------	-----------------	-----------------------------------	--------------

<p>Moduł 1: Wprowadzenie do e-bezpieczeństwa (3h)</p>	<p>Zapoznanie uczestników z podstawowymi pojęciami i zagrożeniami w sieci.</p>	<ul style="list-style-type: none"> • Prezentacja multimedialna • Dyskusja moderowana • Quiz wstępny 	<ul style="list-style-type: none"> • Prezentacja Powerpoint • Test wstępny • Tablica/flipchart 	<ul style="list-style-type: none"> • Zachęcić uczestników do dzielenia się własnymi doświadczeniami z zagrożeniami online.
<p>Moduł 2 Profil zaufany – teoria i praktyka (2,5h)</p>	<p>Poznanie funkcji profilu zaufanego i jego zastosowań, zapoznanie z opcją incognito w przeglądarce.</p>	<p>Pokaz zakładania profilu, ćwiczenia logowania i podpisu</p>	<p>https://pz.gov.pl, instrukcja PDF</p>	<p>Wymagany dostęp do Internetu i konta bankowego, Trener musi zwrócić szczególną uwagę na bezpieczne korzystanie z publicznych urządzeń. Najlepiej korzystać ze swoich urządzeń.</p>
<p>Moduł 3: Higiena cyfrowa i bezpieczeństwo (3h)</p>	<p>Rozpoznawanie zagrożeń i ochrona danych osobowych</p>	<p>Wykład, analiza przypadków. Uczestnicy zapoznają się w grupach z prezentacją o zasadach higieny cyfrowej i wykonują quiz.</p>	<p>Materiały PDF, przykłady phishingu</p>	<p>Możliwość pracy w grupach</p>

<p>Moduł 4: Ochrona danych osobowych (2,5h)</p>	<p>Zasady ochrony danych osobowych zgodnie z RODO. Bezpieczne udostępnianie informacji w sieci.</p>	<p>Analiza przypadków</p>	<p>https://uodo.gov.pl/ https://www.gov.pl/web/cyfryzacja/ochrona-danych-osobowych https://gdpr.pl/</p>	
<p>Moduł 5: Bezpieczne hasła i logowanie (3h)</p>	<p>Nauka tworzenia silnych haseł i stosowania uwierzytelniania a dwuskładnikowego.</p>	<ul style="list-style-type: none"> • Prezentacja zasad tworzenia haseł • Ćwiczenia: generowanie haseł • Demonstracja 2FA 	<ul style="list-style-type: none"> • Generator haseł online • Prezentacja • Karty ćwiczeń 	<ul style="list-style-type: none"> • Pokazać różnice między słabym a silnym hasłem na przykładach.

<p>Moduł 6: Rozpoznawanie zagrożeń (phishing, malware, spam) (3h)</p>	<p>Umiejętność identyfikacji i reagowania na zagrożenia cyfrowe.</p>	<ul style="list-style-type: none"> • Analiza fałszywych wiadomości e-mail • Ćwiczenia: rozpoznawanie phishingu • Prezentacja typów malware 	<ul style="list-style-type: none"> • Przykładowe e-maile • Prezentacja • Karty ćwiczeń 	<ul style="list-style-type: none"> • Uczestnicy mogą przynieść własne przykłady podejrzanych wiadomości.
<p>Moduł 7: Narzędzia ochrony (VPN, firewall, antywirus) (2h)</p>	<p>Poznanie narzędzi zwiększających bezpieczeństwo w sieci.</p>	<p>Demonstracja działania VPN</p> <p>Omówienie funkcji firewalla</p> <p>Ćwiczenia: instalacja i konfiguracja antywirusa</p>	<p>Prezentacja</p> <p>Instrukcje instalacji</p>	<p>Zapewnić dostęp do bezpłatnych wersji programów ochronnych.</p>

<p>Moduł 8: Bezpieczne korzystanie z mediów społecznościowych (3h)</p>	<p>Świadome i bezpieczne korzystanie z serwisów społecznościowych.</p>	<ul style="list-style-type: none"> • Analiza ustawień prywatności • Ćwiczenia: konfiguracja konta • Dyskusja: zagrożenia w social media 	<ul style="list-style-type: none"> • Przykłady ustawień prywatności • Karty ćwiczeń • Prezentacja 	<p>Warto omówić konkretne przypadki naruszeń prywatności</p>
<p>Moduł 7: Urządzenia mobilne i sieci publiczne (1.5h)</p>	<p>Bezpieczne korzystanie z smartfonów, tabletów i Wi-Fi.</p>	<ul style="list-style-type: none"> • Prezentacja zagrożeń mobilnych • Ćwiczenia: konfiguracja zabezpieczeń • Symulacja ataku przez publiczne Wi-Fi 	<ul style="list-style-type: none"> • Smartfony/tablety uczestników • Prezentacja • Karty ćwiczeń 	<ul style="list-style-type: none"> • Pokazać aplikacje zwiększające bezpieczeństwo mobilne.

Podsumowanie i test końcowy (0,5 h)	Utrwalenie wiedzy i ocena efektów szkolenia	Powtórka, test wiedzy, omówienie wyników	Test papierowy lub online, formularz ewaluacyjny	Możliwość zadawania pytań końcowych
---	---	--	--	-------------------------------------