

## PROGRAM SZKOLENIA

**TYTUŁ WEBINARU:** Cyberbezpieczeństwo – podstawy bezpiecznego korzystania z Internetu i komputera 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:** Uczestnik po szkoleniu:

- rozumie podstawowe zagadnienia związane z cyberbezpieczeństwem;
- rozumie, jakie znaczenie ma skuteczna ochrona przed cyberzagrożeniami w pracy w administracji;
- zna metody ustawiania bezpiecznego hasła, bezpiecznego korzystania ze skrzynki mailowej oraz z przeglądarek internetowych na sprzęcie komputerowym oraz urządzeniach mobilnych;
- wie, gdzie szukać pomocy i jak zareagować w momencie podejrzenia lub zidentyfikowania zagrożenia w cyberprzestrzeni;
- rozumie ważność tworzenia kopii zapasowych i odzyskiwania danych.

**METODY DYDAKTYCZNE:** wykład

**ŚRODKI DYDAKTYCZNE:** prezentacja multimedialna

**LICZBA GODZIN DYDAKTYCZNYCH:** 2

<b>Lp.</b>	<b>Temat (części szkolenia)</b>	<b>Czas (min)</b>
1.	<ul style="list-style-type: none"><li>• Rodzaje zagrożeń w sieci – od wirusów po wyłudzenie danych</li></ul>	30 min
2.	<ul style="list-style-type: none"><li>• Ślad cyfrowy i dane osobowe w sieci</li><li>• Bezpieczni w mediach społecznościowych</li></ul>	15 min
3.	<ul style="list-style-type: none"><li>• Bezpieczne e-maile oraz bezpieczne hasło</li></ul>	15 min
4.	<ul style="list-style-type: none"><li>• Kopie zapasowe i odzyskiwanie danych</li></ul>	10 min
5.	<ul style="list-style-type: none"><li>• Ramy prawne cyberbezpieczeństwa w Unii Europejskiej i w Polsce</li><li>• Instytucje odpowiedzialne za bezpieczeństwo w sieci</li><li>• Postępowanie w cyberincydencie – co, gdzie i komu zgłaszać</li></ul>	20 min