Ministerstwo Cyfryzacji

PWCyber

(CYBER)SZKOLENIA
KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

Departament Cyberbezpieczeństwa

SZKOLENIE ONLINE DLA PODMIOTÓW KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA

24 marca 2026 r.
Typ 100

Nowoczesne cyberzagrożenia i metody obrony

Omnilogy Sp. z o.o.

9.45 – 10.00	**Logowanie**
10.00 – 10.05	**Zasady organizacyjne przebiegu szkolenia** *Przedstawiciel Departamentu Cyberbezpieczeństwa MC*
10.05 – 11.45	**Wprowadzenie** **Najczęściej występujące cyberzagrożenia** • Phishing i oszustwa internetowe – oszustwa przez e-mail i SMS • Złośliwe oprogramowanie (malware) • Ransomware – blokada danych • Słabe hasła i przejęcie kont • Fałszywe strony internetowe i aplikacje **Podstawowe metody ochrony – dobre praktyki** • Bezpieczne hasła i uwierzytelnianie • Aktualizacje systemów i oprogramowania • Świadomość i ostrożność użytkownika • Kopie zapasowe danych • Przykłady systemów służących ochronie przed zagrożeniami **Cyberbezpieczeństwo w administracji publicznej** **Rola pracownika i użytkownika systemów** **Podsumowanie** *Expert Omnilogy*
11.45 – 12.10	**Sesja pytań i odpowiedzi do ekspertów**