## Szkolenie online: Cyberbezpieczeństwo dla użytkowników końcowych [INDW02.CYBUS]

**Czas trwania:** 4 godziny

**Koszt szkolenia:** Szkolenie bezpłatne dla członków Związku Pracodawców INDORO

**Forma prowadzenia usługi:** zdalna w czasie rzeczywistym

**Cel edukacyjny:** Celem szkolenia jest dostarczenie uczestnikom wiedzy i umiejętności niezbędnych do rozpoznawania i zapobiegania cyberzagrożeniom. Uczestnicy nauczą się, jak chronić swoje dane, rozpoznawać socjotechniki oraz reagować na różne rodzaje cyberataków, co pozwoli im na bezpieczne korzystanie z komputerów i urządzeń mobilnych.

**Dla kogo:** Szkolenie jest skierowane do pracowników wszystkich szczebli, którzy regularnie korzystają z komputerów i urządzeń mobilnych w pracy oraz do osób zainteresowanych poprawą swojego poziomu wiedzy na temat cyberbezpieczeństwa.

**Dlaczego warto:** Szkolenie dostarcza aktualnej wiedzy na temat cyberzagrożeń praktycznych metod ich unikania. Uczestnicy zdobędą umiejętności niezbędne do ochrony swoich danych i urządzeń, co zwiększy bezpieczeństwo zarówno w życiu zawodowym, jak i prywatnym. Szkolenie pomaga zrozumieć, jak rozpoznawać i reagować na różne rodzaje cyberataków, co jest kluczowe w dzisiejszym cyfrowym świecie.

**Program szkolenia:**

1. Ochrona komputera:
    a. Podstawowe zasady bezpieczeństwa
    b. Filary bezpieczeństwa informatycznego
2. Wycieki danych: Jak sprawdzić, czy utraciliśmy swoje dane?
3. Bezpieczne hasło:
    a. Ogólne zasady tworzenia silnych haseł
    b. Analiza metod tworzenia haseł
    c. Korzystanie z menedżerów haseł
4. Socjotechnika - manipulacja użytkownikiem:
    a. Typowe błędy popełniane przez pracowników
    b. Omówienie prawdziwych zdarzeń i przypadków
5. Cyberzagrożenia: Na co zwracać uwagę podczas korzystania z sieci?
6. Omówienie popularnych ataków cybernetycznych: Ataki związane z mailingiem, SMS-ami, telefonami i komunikatorami internetowymi
7. Bezpieczeństwo płatności internetowych: Jak bezpiecznie przeprowadzać transakcje online?
8. Bezpieczeństwo mobilne: Ochrona urządzeń mobilnych przed zagrożeniami
9. Złośliwe oprogramowanie: Jak rozpoznawać i chronić się przed malwarem?
10. Piractwo komputerowe: Jak unikać oszustw i pirackiego oprogramowania?
11. Najważniejsze wskazówki dotyczące bezpiecznej pracy z komputerem: Praktyczne porady i zalecenia

## Planowane efekty uczenia się:

- Po szkoleniu uczestnicy będą potrafili definiować i charakteryzować najważniejsze techniki cyberataków.
- Rozpoznawać i zapobiegać zagrożeniom związanym z cyberprzestępczością.
- Podejmować odpowiednie działania w przypadku styczności z cyberatakiem.
- Rozpoznawać socjotechniki (również te stacjonarne) wykorzystywane przez cyberprzestępców.

## Wymagana wiedza/doświadczenie wstępne:

Uczestnicy powinni posiadać podstawową wiedzę z zakresu obsługi komputera i korzystania z internetu. Szkolenie jest przeznaczone dla osób, które mają już doświadczenie w pracy z komputerami i urządzeniami mobilnymi oraz w tematyce zamówień publicznych, a nie dla osób początkujących.

**Dostęp do szkolenia:** Usługa zostanie przeprowadzana na platformie online Microsoft Teams. Dostęp do szkolenia w postaci linku uczestnik otrzyma za pośrednictwem maila na 2 dni przed rozpoczęciem usługi.

## Warunki techniczne:

- Procesor dwurdzeniowy 2GHz lub lepszy (zalecany czterordzeniowy); 2GB pamięci RAM (zalecane 4GB lub więcej); System operacyjny Windows 8 (zalecany Windows 10 lub 11), Mac OS wersja 10.13 (zalecana najnowsza wersja), Linux, Chrome OS,
- Stałe szerokopasmowe łącze internetowe o prędkości min. 1,5 Mbps (zalecane 2,5 Mbps), wymagane jest korzystanie z najbardziej aktualnych oficjalnych wersji Google Chrome, Mozilla Firefox, Safari, Edge lub Opera,
- Głośniki i mikrofon,
- Kamera internetowa.

## Osoba prowadząca zajęcia:

**Jakub Kochaniak:** trener, certyfikowany audytor Microsoft, specjalizuje się w prowadzeniu szkoleń z zakresu cyberbezpieczeństwa, ochrony danych osobowych oraz bezpieczeństwa pracy w systemach informatycznych. Posiada certyfikaty audytora Microsoft i bogate doświadczenie w wykonywaniu audytów bezpieczeństwa oraz legalności oprogramowania w przedsiębiorstwach. Jego wiedza i umiejętności pomagają firmom zrozumieć i przestrzegać zasad bezpieczeństwa w systemach teleinformatycznych, co jest kluczowe dla skutecznego i bezpiecznego funkcjonowania w cyfrowym środowisku. Jakub prowadzi również konsultacje, wspierając organizacje w osiąganiu najwyższych standardów bezpieczeństwa.

## Szkolenie realizowane przy współpracy:

NT Group Systemy Informatyczne Sp. z o.o.
ul. Pomorska 65 (III piętro)
90-218 Łódź
www.ntg.pl
info@ntg.pl