Cyberbezpieczeństwo w codziennej pracy (kod: CYBER AWARENESS)

Opis i cel szkolenia

Cyberprzestępcy stosują coraz bardziej wyrafinowane metody oszustw, a phishing, wycieki danych czy ransomware to zagrożenia, które mogą dotknąć każdego użytkownika, niezależnie od jego roli w firmie, instytucji, czy nawet w domu.

Na szkoleniu dowiesz się, w przyjazny sposób i z praktycznymi przykładami: jakie są najczęstsze rodzaje ataków, jak rozpoznawać podejrzane wiadomości, tworzyć bezpieczne hasła, jak chronić komputery i urządzenia przed atakami. Opowiemy też o "socjotechnice". Nauczysz się prostych zasad, które pomogą Ci unikać cyberzagrożeń w codziennej pracy. Pokażemy również realne przykłady oszustw oraz skuteczne sposoby ochrony, abyś mógł bezpiecznie korzystać z internetu – zarówno w pracy, jak i prywatnie.

Szkolenie realizujemy zarówno w trybie **ogólnodostępnym** (każdy chętny może się zapisać, w terminach opublikowanych na stronie), jak również **na zamówienie dla grup z firm oraz instytucji**, czy to w formie interaktywnych warsztatów, czy prelekcji, również konferencyjnych, dla większych grup.

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl

Najbliższe terminy
2026-05-13 (Zdalnie)
2026-05-13 (Warszawa)
2026-06-24 (Zdalnie)
2026-06-24 (Warszawa)
2026-09-16 (Zdalnie)
2026-09-16 (Warszawa)

Czas trwania

1 dzień

Program

1. Czym jest cyberbezpieczeństwo?
   - Dlaczego cyberbezpieczeństwo jest ważne?
   - Jakie zagrożenia czyhają na zwykłych użytkowników?
   - Jakie mogą być konsekwencje nieostrożnego korzystania z internetu?
   - Jakie są podstawowe zasady bezpiecznej pracy z komputerem?
2. Hasła i logowanie – jak się zabezpieczyć?
   - Dlaczego „123456” to najgorsze hasło świata?
   - Jak tworzyć silne i unikalne (bardziej bezpieczne) hasła?
   - Menedżer haseł - bezpiecznie korzystanie w praktyce
   - Co to jest uwierzytelnianie dwuetapowe (MFA/2FA) i dlaczego warto je włączyć?
   - Czy przyszłość to logowanie bez haseł?
3. Jak nie dać się oszukać – phishing i inne pułapki
   - Zasady korzystania z Internetu
   - Portale społecznościowe - potencjalne zagrożenie
   - Poczta elektroniczna - podejrzane wiadomości i zagrożenia z tym związane;
   - Na co uważać w podejrzanych linkach? (Nie klikaj w ciemno!)
   - Jak sprawdzić, czy nadawca jest wiarygodny?
   - Przykłady udanych cyberataków i omówienie jak można było im zapobiec
4. Złośliwe oprogramowanie – jak nie paść ofiarą wirusów i ransomware?
   - Jakie są objawy infekcji?
   - Co zrobić, gdy komputer zacznie dziwnie działać?
   - Czy płacić okup, jeśli zablokują dostęp do plików?
   - Dlaczego regularny backup to najlepsze zabezpieczenie?
5. Bezpieczne korzystanie z urządzeń służbowych i prywatnych
   - Jak dbać o bezpieczeństwo laptopa i telefonu?
   - Dlaczego warto aktualizować system i aplikacje?
   - Czy antywirus nadal jest potrzebny?

   — VPN – czy warto z niego korzystać?
6. Socjotechnika – czyli jak przestępcy manipulują ludźmi
   — Fałszywe telefony i e-maile – jak nie dać się nabrać?
   — Ktoś prosi o dostęp do Twojego konta – co robić?
   — Ataki na pracowników – jak się bronić przed podszywaniem się pod szefa lub współpracowników?
7. Praktyczne wskazówki na co dzień
   — Jak bezpiecznie przesyłać i udostępniać dane?
   — Czy można klikać w reklamy w internecie?
   — Jak sprawdzić, czy strona, na której wpisujesz dane, jest bezpieczna?
   — Co robić, jeśli podejrzewasz, że padłeś ofiarą oszustwa?

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl

Przeznaczenie i wymagania

Kurs przeznaczony dla pracowników, osób prywatnych i wszystkich, którzy chcą zapoznać się z zagrożeniami jakie mogą płynąć przy korzystaniu z internetu oraz sposobami zabezpieczania się przed tymi zagrożeniami.

Od słuchaczy oczekujemy umiejętności podstawowej, codziennej obsługi komputera.

Najbliższe terminy
2026-05-13 (Zdalnie)
2026-05-13 (Warszawa)
2026-06-24 (Zdalnie)
2026-06-24 (Warszawa)
2026-09-16 (Zdalnie)
2026-09-16 (Warszawa)

Certyfikaty

Uczestnicy szkolenia otrzymują imienne certyfikaty sygnowane przez ALX.

Lokalizacje

— Warszawa – ul. Jasna 14/16A
— Zdalnie – zajęcia realizowane poprzez platformę Zoom
— Kraków – ul. św. Filipa 23
— Warsaw (English) – Jasna 14/16A
— Online (English) – your home, office or wherever you want
— na życzenie dowolne miejsce w Polsce, lub UE (zajęcia prowadzone w języku angielskim)

Cena szkolenia

790 PLN netto (VAT 23%)

W cenę szkoleń organizowanych w naszej siedzibie wliczone są:

— autorskie materiały szkoleniowe,
— indywidualne stanowisko komputerowe do pracy podczas zajęć,
— certyfikaty ukończenia szkolenia,
— drobny poczęstunek oraz ciepłe i zimne napoje,
— możliwość jednorazowego kontaktu z instruktorem (instruktorami) po szkoleniu i zadawania pytań dotyczących materiału szkolenia.

Cena szkolenia nie zawiera obiadów. Można je dokupić w cenie 35 zł netto za obiad.