

Wcześniej czy później ...
każdy zostanie zhakowany!
czy moja firma jest na to przygotowana?

CYBERBEZPIECZNY PRACOWNIK



cyberbezpieczny.pl

CEL SZKOLENIA:

Celem tego szkolenia jest **przygotowanie każdego pracownika** – użytkownika dowolnego urządzenia podłączonego do Internetu - **do swobodnego i bezpiecznego poruszania się w cyberprzestrzeni**, realizując każdego dnia swoje obowiązki oraz pasje.

Podniesiemy świadomość każdego uczestnika szkolenia odnośnie cyber zagrożeń w każdej organizacji, sposobów i metod **cyberataków**, jak również przekażemy dobre praktyki dotyczące obszaru bezpieczeństwa informacji w organizacji.

W trakcie szkolenia zaprezentujemy **praktyczne przykłady cyberataków**, szczególnie z zastosowaniem metod socjotechnicznych. **Po tym szkoleniu całkowicie zmieni się Twoja świadomość!**

JAKĄ WIEDZĘ ZDOBĘDZIESZ:

- W jaki sposób działają i atakują nas cyberprzestępcy
- W jaki sposób chronić się przed atakami **cyberprzestępców w domu i w biurze**
- W jaki sposób wykrywać i reagować na ataki typu **phishing, vishing, smishing, spoofing**
- W jaki sposób wykrywać i reagować na ataki typu **ransomware**
- W jaki sposób wykrywać i reagować na ataki typu **spoofing**
- W jaki sposób wykrywać i reagować na **ataki socjotechniczne**
- W jaki sposób bezpiecznie korzystać ze **smartfona**
- W jaki sposób bezpiecznie korzystać z **aplikacji biurowych, poczty e-mail czy komunikatora**
- W jaki sposób bezpiecznie przeglądać **strony internetowe**
- W jaki sposób bezpiecznie zarządzać swoimi **hasłami**
- W jaki sposób rozróżnić fałszywe **domeny internetowe**
- W jaki sposób **chronić dane** na urządzeniach połączonych z internetem
- W jaki sposób bezpiecznie **pracować zdalnie**
- W jaki sposób bezpiecznie korzystać z **sieci bezprzewodowych**
- Informacje prywatne i służbowe – jaka jest różnica?

KTO POWINIEN UCZESTNICZYĆ W TYM SZKOLENIU:

- Każdy kto posiada **jakikolwiek urządzenie połączone z Internetem**
- Każdy kto korzysta z **poczty elektronicznej**
- Każdy kto przegląda **strony internetowe**
- Każdy kto korzysta z **dowolnych aplikacji**
- Każdy kto **kupuje lub sprzedaje** w sieci
- Każdy kto ma dostęp do **informacji poufnych**
- Każdy kto pracuje (**w biurze lub zdalnie**)
- Każdy kto ma **inteligentny dom**
- Każdy kto klika w **linki**
- Każdy kto ma **dzieci**
- Każdy kto ma **konto** w banku
- Każdy **pracownik, manager, prezes czy członek zarządu**
- Każdy tata, mama, dziecko, wujek, ciocia, babcia i dziadek!
- słowem ... **każdy użytkownik Internetu!**

DLACZEGO | cyberbezpieczny.pl

Cyberbezpieczeństwo to proces. To szkolenie to prawdziwe kompendium wiedzy! Od początku do końca zorientowane na **praktycznych codziennych przykładach z życia wziętych**. Materiał oparty jest na solidnym, wieloletnim doświadczeniu, zdobytym w obszarach bezpieczeństwa informacji i cyberbezpieczeństwa.

Wszystkie informacje zostaną przekazane w sposób łatwy i zrozumiały **dla każdego**. Każdy z uczestników szkolenia nauczy się i zrozumie, **jak rozpoznać cyberatak i jak sobie z nim poradzić**. Naprawdę każdy!

Szkolenie oparte jest na rekomendacjach ENISA - Agencji Unii Europejskiej ds. Cyberbezpieczeństwa, działającej na rzecz osiągnięcia wysokiego ogólnego poziomu cyberbezpieczeństwa w całej Europie, koncentrując się na realnych przykładach cyberataków oraz rzeczywistych sytuacjach życiowych.

CO ZYSKASZ?

Wykwalifikowaną kadrę pracowników, świadomych aktualnych cyber zagrożeń, dzięki którym Twoja firma będzie miała szansę obronić się przed cyberatakami, **a dane w Twojej firmie będą bezpieczne.**

- INTERNET
- LIVE CHAT
- MEDIA
- PHOTOS
- VIDEOS
- MUSIC



cyberbezpieczny.pl

TEMATY SZKOLENIA

1. Cyberbezpieczeństwo – zaczynamy

- 👉 Budujemy świadomość! Poznaj swojego wroga!
- 👉 Dlaczego dzisiaj mówimy o cyberbezpieczeństwie i dlaczego to takie ważne?
- 👉 Kim jest cyberprzestępca i dlaczego jest tak niebezpieczny?
- 👉 Kradzież danych, uszkodzona infrastruktura, zablokowane urządzenia i systemy – czy to możliwe?

2. Etapy, czyli cyberatak krok po kroku

- 👉 Atak = Motywacja (Cel) + Metoda + Podatność
- 👉 Dlaczego nikt z nas nie może czuć się bezpieczny?
- 👉 W jaki sposób cyberprzestępcy przygotowują się do cyberataków i jaka jest nasza rola?
- 👉 Jakie informacje potrzebują do ataku cyberprzestępcy i w jaki sposób je zdobywają?
- 👉 (Nieświadomy) Pracownik – największe zagrożenie dla danych firmowych?
- 👉 Kto i kiedy nas zaatakuje?

TEMATY SZKOLENIA

3. Typy cyberataków

Obecnie na świecie występuje wiele odmian cyberataków. Jeżeli jesteśmy tego **świadomi**, łatwiej nam będzie chronić przed nimi nasze dane i systemy. W tym miejscu dokładnie omówimy najczęstsze typy cyberataków, które mogą dotknąć **każdą osobę lub firmę**, w każdej chwili.

- 👉 Ataki na pracownika - świadomy (cyber)pracownik! (wszystko co MUSISZ wiedzieć!)
- 👉 Ataki z wykorzystaniem metod socjotechnicznych (dasz im wszystko to, o co cię poproszą)
- 👉 Ataki z wykorzystaniem poczty e-mail (Phishing, Spoofing, kradzież tożsamości, BEC)
- 👉 Ataki z wykorzystaniem stron www (domeny, Phishing, certyfikaty, przeglądarka internetowa)
- 👉 Ataki z wykorzystaniem smartfonów (SMSishing, Vishing, Spyware)
- 👉 Ataki z wykorzystaniem oprogramowania szpiegującego (Spyware)
- 👉 Ataki z wykorzystaniem komunikatorów (Messenger, WhatsApp, Signal)
- 👉 Ataki z wykorzystaniem mediów społecznościowych (Phishing, Kradzież tożsamości)
- 👉 Ataki z wykorzystaniem złośliwego oprogramowania (na co musimy zwrócić uwagę)
- 👉 Ataki z wykorzystaniem nośników USB (ulubione narzędzie cyberprzestępców)
- 👉 Ataki z wykorzystaniem IoT (SmartTV, lodówka, żarówka inteligentna)
- 👉 Ataki z wykorzystaniem sklepów online (OLX, Allegro, Vinted)
- 👉 Ataki z wykorzystaniem bankomatów (Skimming)
- 👉 Ataki z wykorzystaniem sieci BOTNET (Denial-of-Service, Malware, Spam)



TEMATY SZKOLENIA

4. Złośliwe oprogramowanie (malware)

- 👉 W jaki sposób cyberprzestępcy przejmują nasze komputery i smartfony?
- 👉 Jak rozpoznać czy moje urządzenie jest zainfekowane złośliwym oprogramowaniem?
- 👉 Jak usunąć złośliwe oprogramowanie? Jak się zabezpieczyć na przyszłość?

- 👉 Wirusy, robaki, konie trojańskie
- 👉 Ransomware (oprogramowanie szyfrujące pliki)
- 👉 Spyware (oprogramowanie szpiegujące)
- 👉 Adware (niechciane reklamy)
- 👉 Keyloggers (oprogramowanie do wykradania m.in. haseł)
- 👉 Rootkit (ukryte aplikacje, pozwalające zarządzać całym systemem)
- 👉 Rogue Anti-Spyware (nie daj się nabrać!)
- 👉 Cryptojacking (koparka kryptowaluty)
- 👉 Denial-of-Service (koniec mojego businessu?)
- 👉 Zero-Day Exploit
- 👉 Watering Hole
- 👉 Dark Web, Deep Web – ukryte zasoby Internetu

Liczba ataków rośnie! Jak się bronić? Dowiesz się podczas szkolenia.

TEMATY SZKOLENIA

5. Bezpieczeństwo moich urządzeń (router, komputer, laptop, smartfon, tablet, dyski)

- 👉 **Router** – drzwi do mojego wirtualnego świata – 5 kroków bezpiecznej konfiguracji
- 👉 Router – Bezpieczeństwo sieci domowej

- 👉 **Smartfon** – furtka do naszych danych!
- 👉 Smartfon – kto ma dostęp do mikrofonu? Jak się chronić przed podsłuchem?
- 👉 Smartfon – bezpieczna instalacja aplikacji, rekomendacje
- 👉 Smartfon – czy grożą mi wirusy?
- 👉 Smartfon – dlaczego cyberprzestępcy potrzebują mojego smartfona?
- 👉 Smartfon – bezpieczna konfiguracja i użytkowanie
- 👉 Smartfon – bezpieczne korzystanie z łączności bezprzewodowej (Wi-Fi, GPS, Bluetooth)
- 👉 **Laptop** – bezpieczna konfiguracja
- 👉 Laptop – szyfrowanie dysku, czy potrzebne?
- 👉 Laptop – ochrona przed wirusami i zagrożeniami
- 👉 Laptop – w ile sekund można zhakować zabezpieczonego Windowsa
- 👉 Laptop – kontrola aplikacji

- 👉 **Botnet** - czy mój komputer lub smartfon jest naprawdę mój?
- 👉 **IoT (Internet Rzeczy)** – cyberatak, czyli kto ma kontrolę nad twoim domem?
- 👉 **Nośniki USB** – ulubione narzędzie cyberprzestępców
- 👉 **Kopie zapasowe!**
- 👉 Dlaczego warto szyfrować dysk twardy na komputerze?



TEMATY SZKOLENIA

6. Bezpieczeństwo danych

- 👉 W jaki sposób cyberprzestępcy **wykradają nasze dane?**
- 👉 W jaki sposób cyberprzestępcy gromadzą dane na nasz temat (FB, LinkedIn, Google)?
- 👉 Jak nie narazić siebie oraz firmy na ataki? **Na co zwrócić uwagę rodzinie i znajomym?**
- 👉 **Tokeny U2F** – jak skutecznie zabezpieczyć się przed Phishingiem i przejęciem konta?
- 👉 **VPN** – jak skutecznie chronić prywatność i tożsamość online?
- 👉 Jak sprawdzić czy link lub załączony plik jest **bezpieczny?**
- 👉 Co o tobie wie Facebook, Google, TikTok?
- 👉 **Szyfrowanie danych** poufnych - w jaki sposób i kiedy?
- 👉 Metadane, dlaczego są tak ważne?
- 👉 Czy moje dane wyciekły? Gdzie mogę to sprawdzić?
- 👉 **Wyciek danych**. Co teraz? Gdzie i w jaki sposób zgłosić?
- 👉 Prawo do bycia zapomnianym, jak to zrobić?

7. Metody socjotechniczne – jakie informacje przekazemy

- 👉 Dane karty kredytowej
- 👉 Dane logowania do systemów
- 👉 PESEL i datę urodzenia
- 👉 Dane osobiste, wykształcenie, firma, stanowisko
- 👉 Dane dotyczące narzędzi bezpieczeństwa wykorzystywanych w firmie
- 👉 Dane na temat systemów operacyjnych i aplikacji
- 👉 Dane na temat konfiguracji sieci komputerowych
- 👉 **Adresy IP i nazwy serwerów**
- 👉 **i wiele wiele innych ... ☺**

Jak temu zapobiec? Dowiesz się podczas szkolenia.

TEMATY SZKOLENIA

8. (cyber)Bezpieczny pracownik

- ← **PAMIĘTAJ! Wystarczy że klikniesz tylko raz!**
- ← Jak zadbać o siebie w cyberprzestrzeni?
- ← Czy lubię dużo mówić i czy to jest niebezpieczne?
- ← Ile informacji na temat mojego miejsca pracy wrzucam publicznie do sieci?
- ← Dlaczego warto ukryć swój adres IP?
- ← Domeny internetowe – jak bezpiecznie korzystać?
- ← Dostęp do prywatnej poczty e-mail lub mediów społecznościowych z sieci firmowej?
- ← Kliknąć w **linki**? O co tutaj chodzi i jak to naprawdę działa?
- ← **Podszywanie się** pod pracowników działów IT/InfoSec – jak reagować?
- ← Bezpieczna salka konferencyjna? Czy ktoś nas **podstuchuje**?
- ← Klient prosi o **pilny** przelew? Jak rozpoznać cyberatak?
- ← Czy dostanę w sieci coś za darmo?
- ← Dezinformacja (**fake news**) – jak wpływa na działanie pracownika?
- ← Klasyfikacja informacji – dlaczego jest tak ważna?
- ← Jak przetwarzać i zabezpieczyć **dane wrażliwe**?
- ← Program antywirusowy? To za mało!
- ← Rozmowy rekrutacyjne w firmie – **co wspólnego mają z cyberatakiem**?
- ← Wydruki, na co powinienem zwrócić uwagę
- ← Kopie zapasowe
- ← **Awareness**

TEMATY SZKOLENIA

9. Bezpieczna zdalna praca (WFA – Work from Anywhere)

Cyberprzestępcy zdali sobie sprawę, że phishing jest wciąż skuteczną metodą ataku, a **pracownicy są bramą do danych firmowych**. Ataki na pracowników zdalnych będą coraz liczniejsze i coraz bardziej wyrafinowane. Coraz więcej cyberprzestępców stara się dostać do danych biznesowych i systemów wykorzystując luki bezpieczeństwa pracowników pracujących z domu. **Jak się obronić?**

- 👉 Przygotowanie miejsca do (cyber)bezpiecznej zdalnej pracy – **5 kroków**
- 👉 Dostęp do zasobów organizacji (VPN)
- 👉 W jaki sposób zabezpieczyć się przed wyciekiem danych
- 👉 Cyberbezpieczna praca w miejscach publicznych (**hotel, kawiarnia, pociąg**)
- 👉 Cyberbezpieczna praca z narzędziami do komunikacji (**komunikatory, Zoom, Skype, Teams**)
- 👉 Cyberbezpieczna **telekonferencja**
- 👉 Bezpieczeństwo **informacji poufnych**
- 👉 ETM (Electronic Transportable Media) – **bezpieczny transfer danych** na nośnikach danych (pendrive, CD)

10. Bezpieczeństwo aplikacji

- 👉 **Aplikacje** – jak bezpiecznie instalować i używać
- 👉 Aplikacje – do czego dajemy dostęp i co dalej mogą robić?
- 👉 **Komunikatory** – który wybrać i jakie dane udostępniamy?
- 👉 Google – co wie na mój temat? Czy naprawdę wszystko?
- 👉 Google Play – Trojany to codzienność. Jak je rozpoznać?
- 👉 **Przeglądarki internetowe** – czym się różnią? którą wybrać?
- 👉 Programy antywirusowe – który wybrać i dlaczego?

TEMATY SZKOLENIA

11. Incydenty cyberbezpieczeństwa (Cyber security incident response)

- 👉 **Zhakowali mnie! Co dalej? Jak odzyskać konto?**
- 👉 **Cyberatak i co dalej?**
- 👉 Co powinna zawierać **instrukcja dla pracownika?**
- 👉 **Zgłaszanie incydentów** – kiedy i kogo powinniśmy poinformować o cyberataku
- 👉 Operator usług kluczowych -> obowiązki opisane w Ustawie o krajowym systemie cyberbezpieczeństwa
- 👉 Zaangażowanie IODO, jaki i kiedy komunikat do klientów?
- 👉 **Jak odzyskać dane?**
- 👉 **System Zarządzania Bezpieczeństwem Informacji** w organizacji
- 👉 Normy i standardy z zakresu bezpieczeństwa informacji i bezpieczeństwa IT

12. Kopia zapasowa (Backup)

- 👉 Kopia zapasowa to jeden z najważniejszych elementów systemu zabezpieczeń.
- 👉 Gdzie przechowywane są dane z telefonu
- 👉 Tworzenie kopii zapasowych smartfona lub karty SIM oraz przywracanie tych kontaktów
- 👉 Na co naprawdę zwrócić uwagę i w jaki sposób wykonywać kopie danych.

Zapraszamy do kontaktu:



cyberbezpieczny.pl



502 702 004



info@cyberbezpieczny.pl