uniseco®

SECURITY AWARENESS

bezpieczny pracownik w cyberprzestrzeni

Szkolenie uświadamia uczestnika, jak w prosty sposób - korzystając z narzędzi takich jak poczta elektroniczna, media społecznościowe – można narazić siebie i swoich współpracowników na atak hakerski.

Akademia Bezpieczeństwa UNISECO nauczy zabezpieczania komputerów i telefonów, ochrony kont bankowych, a także zabezpieczy pracowników przed uleganiem socjotechnikom, stosowanym przez cyberprzestępców. Uczestnicy szkolenia poznają mechanizmy ataków w sieci, na które narażony jest każdy z nas.

Poznaj zawartość naszego szkolenia:

Lekcja 1

Bezpieczeństwo informacji – wprowadzenie.

- Omówienie zagadnień: bezpieczeństwo informacji, zarządzanie bezpieczeństwem.
- Triada bezpieczeństwa: poufność, dostępność, integralność.
- Wprowadzenie do systemu zarządzania bezpieczeństwem informacji.

Lekcja 2

Czym jest phishing i jak wykorzystywany jest do ataku na użytkownika?

- Czym jest phishing i jakie są jego odmiany?
- Przykłady ataków phishingowych – studium przypadków.
- Ochrona przed phishingiem.

Lekcja 3

Internet - zasady bezpiecznego surfowania po stronach WWW.

- Bezpieczne korzystanie z przeglądarek.
- Przykłady niepożądanych wtyczek i aplikacji webowych.
- Zasady i ograniczenia w dostępie do Internetu.

Lekcja 4

Portale społecznościowe - zagrożenie czy też szansa?

- Przykłady oszustw stosowane na portalach społecznościowych - studium przypadków.
- Wizerunek organizacji i własny w sieci – dlaczego należy zwracać uwagę na umieszczane tam informacje.
- 10 zasad świadomego korzystania z portali społecznościowych.

Lekcja 5

Poczta elektroniczna - zasady korzystania i ograniczenia.

- Firmowa poczta elektroniczna – zasady korzystania.
- Skąd biorą się ograniczenia w korzystaniu z poczty elektronicznej.
- Pojęcie SPAM i podstawy prawne.

Lekcja 6

"Sezamie otwórz się" czyli wszystko o hasłach.

- Idea kontroli dostępu: identyfikacja, uwierzytelnianie, autoryzacja.
- Obowiązki użytkowników mających dostęp do systemów teleinformatycznych.
- Zakazy i nakazy dotyczące tworzenia, zapisywania i zapamiętywania haseł.
- Ataki na hasła: online i offline.
- Menedżery haseł – zaszyfrowane sejfy.

Lekcja 7

Socjotechnika - czyli po co łamać hasła jak można o nie poprosić użytkownika.

- Scenariusze ataków socjotechnicznych – studium przypadków.
- Zasady ochrony przed atakami socjotechnicznymi.

Lekcja 8

Jak poprawnie zabezpieczyć sprzęt mobilny.

- Systemy Mobile Device Management.
- Możliwe reakcje w przypadku kradzieży i zagubienia sprzętu mobilnego.
- Zasady bezpiecznej pracy na urządzeniach przenośnych wpływające na bezpieczeństwo danych.

Lekcja 9

Prawne aspekty i konsekwencje lekceważenia zasad bezpieczeństwa informacji.

- Elementy Kodeksu Karnego odnoszące się do naruszenia i łamania zasad bezpieczeństwa informacji „Przestępstwa przeciwko ochronie informacji”.
- Elementy Ustawy o Ochronie Danych Osobowych, o Prawach Autorskich i Prawach Pokrewnych.
- Wizerunek organizacji w sieci – aspekty prawne.
- Stalking i cyberstalking.

Lekcja 10

Bezpieczeństwo płatności elektronicznych.

- Jakie metody wykorzystują cyberprzestępcy, by zdobyć Twoje pieniądze.
- Na co zwracać uwagę przy korzystaniu z bankowości elektronicznej.
- Jakie przestępstwa wiążą się z płatnościami on-line i przy wykorzystaniu kart płatniczych.

Lekcja 11

Ransomware – co to jest i dlaczego to taki poważny problem?

- Ransomware i jak to wygląda w praktyce na przykładzie ostatniego cyberataku WannaCry.
- Jakie są dobre praktyki w zakresie tworzenia kopii zapasowych danych.
- Rzeczywiste przykłady cyberataków na firmy i instytucje.

Lekcja 12

Zabezpieczenie fizyczne dokumentacji, sprzętu IT i pomieszczeń.

- Ryzyka w zakresie braku zabezpieczenia dokumentacji przetwarzanej w organizacji, a także najlepsze sposoby jej zabezpieczania.
- Sposoby uzyskania nieautoryzowanego dostępu do komputerów oraz ryzyka związane z brakiem zabezpieczenia pomieszczeń, a także skutki z tym związane.
- Omówienie zagadnień na temat systemów wspomagających zabezpieczenia w warstwie fizycznej.

Lekcja 13

Cyberprzestępcy atakują

- Nowe zagrożenia i sposób ochrony przed nimi.

Lekcja 14

Menedżer haseł

- Analiza i praktyczne wykorzystanie menedżerów haseł.
- Na co należy zwrócić uwagę przy wyborze odpowiedniego menedżera haseł.

Lekcja 15

Uważaj by nie zostać „mułem finansowym”

- Głównym celem przestępców jest szybko zarobić duże pieniądze... Jeśli są sprytni to jeszcze ważniejsze dla nich jest wynalezienie sposobu, by nie pozostawić po sobie śladu lub ślad prowadził do kogoś innego.
- „Muły pieniężne” to funkcjonujące w rzeczywistości pojęcie i dotyczy osób, które najczęściej kompletnie nieświadomie, zostały zwerbowane przez organizacje przestępcze do prania pieniędzy. Osoby stające się mułami finansowymi kuszone są obietnicą łatwych pieniędzy później mają naprawdę duże problemy.

Lekcja 16

Bezprzewodowe życie

- Moduł odnosi się do najnowszych zagrożeń ale też wyjaśnia cele, sposoby zabezpieczeń i ochrony sieci, bez których nie wyobrażamy już sobie teraz życia, a więc sieci bezprzewodowych.

Lekcja 17

Praca zdalna - jak zrealizować ją bezpiecznie?

- Epidemia koronawirusa (COVID-19) spowodowała, że wiele organizacji stanęło przed decyzją wysłania większości pracowników na przymusową pracę zdalną. To zupełnie nowe wyzwanie dla wielu organizacji. Jak sobie z tym poradzić postaramy się o tym opowiedzieć w tym module.

Lekcja 18

Vishing… co to jest?

- Czyli skrót od Voice phishing to kolejna metoda oszustw bankowych. Tym razem złodzieje wykorzystują telefony, by wyłudzić od przypadkowych osób sekretne dane. Na czym to dokładnie polega? Jak nie dać się oszukać?

UNISECO Sp. z o.o. ul. Niemierzyńska 17a, 71-441 Szczecin,

telefon: 795 696 995 e-mail: biuro@uniseco.pl **www.uniseco.pl**