Security Awareness

Bezpieczny pracownik w sieci

Zespół Edukacji i Szkoleń Akademii NASK

www.akademia.nask.pl
szkolenia@nask.pl

NASK

NASK akademia

Oferta szkoleń specjalistycznych

Naukowa i Akademicka Sieć Komputerowa
jest państwowym instytutem badawczym prowadzącym działalność badawczo-rozwojową w zakresie opracowywania rozwiązań zwiększających efektywność i bezpieczeństwo sieci teleinformatycznych. Jako operator telekomunikacyjny NASK oferuje innowacyjne rozwiązania teleinformatyczne dla klientów finansowych, biznesowych, administracji i nauki.

Akademia NASK realizuje działalność edukacyjną i popularyzatorską Instytutu. Prowadzi m. in. unikatowe szkolenia z tematyki cyberbezpieczeństwa ICT oraz zagrożeń dzieci i młodzieży w internecie.

Zespół Edukacji i Szkoleń Akademii NASK jest działem Akademii NASK, który zajmuje się edukacją i szkoleniem w zakresie bezpieczeństwa w sieci, wykorzystywaniem nowoczesnych technologii i multimediów w dydaktyce, rozwijaniem kompetencji w zakresie technologii oraz budowaniem świadomości na temat zagrożeń internetowych.

W naszej **ofercie** znajdą Państwo **interesujące kursy i szkolenia**, które prowadzą **wysoko wyspecjalizowani** pracownicy i **eksperci** w dziedzinie telekomunikacji. Zakres tematyczny ustalany jest zgodnie z zapotrzebowaniem merytorycznym klienta i pod konkretną grupę słuchaczy. Każdego traktujemy indywidualnie, badamy jego potrzeby tak, aby przekazać najbardziej aktualną wiedzę.

Serdecznie zapraszamy do kontaktu.

Zespół Edukacji i Szkoleń
Akademii NASK

www.akademia.nask.pl
szkolenia@nask.pl

NASK

NASK akademia

Security Awareness
Bezpieczny pracownik w sieci

Pracownicy stanowią największy
zasób i kapitał firmy. Wnoszą swoje kompetencje
i zaangażowanie w rozwój instytucji. Jednocześnie mogą być
też najbardziej wrażliwym elementem jej bezpieczeństwa i najsłabszym
ogniwem w łańcuchu zabezpieczeń przed cyberprzestępcami.

Brak wiedzy i niska świadomość osób korzystających w pracy z komputerów są najczęstszą przyczyną incydentów naruszenia bezpieczeństwa informatycznego firmy takich, jak utrata ważnych danych, wyciek poufnych informacji finansowych, ujawnienie danych osobowych klientów, itp.

O szkoleniu

Celem szkolenia jest zwiększenie bezpieczeństwa organizacji poprzez podnoszenie poziomu kompetencji pracowników w zakresie bezpieczeństwa IT, w szczególności w zakresie ochrony danych, informacji i wiedzy na temat zagrożeń sieciowych oraz inżynierii społecznej – socjotechniki stosowanej w naruszeniach bezpieczeństwa sieci.

Szkolenie ma za zadanie nauczyć pracowników, jak korzystać z urządzeń ICT – komputera, smartphonów i innych urządzeń teleinformatycznych, tak aby nie narażać danych firmy na ataki cyberprzestępców.

W ramach szkolenia omawiane są najważniejsze obszary związane z cyberbezpieczeństwem:

- Świadomość zagrożeń - rozumienia na jakie niebezpieczeństwa narażeni są pracownicy korzystający z komputerów i urządzeń mobilnych podpiętych do sieci LAN i internetu
- Umiejętność rozpoznawania zagrożeń i właściwego reagowania, w tym informowania o zdarzeniach i podejmowania decyzji w sposób przemyślany, zgodnie z zasadami bezpieczeństwa
- Bezpieczne korzystanie z nowoczesnych technologii w pracy i domu
- Obowiązek ochrony informacji i zabezpieczania środowiska pracy
- Odpowiedzialność za utrzymanie bezpieczeństwa informacji i reputacji instytucji oraz zaufania klientów

Korzyści ze szkolenia

- Podniesienie kwalifikacji pracowników
- Ochrona firmy przed stratami finansowymi i wizerunkowymi
- Zapobieganie utracie ważnych danych
- Unikanie niekontrolowanych wycieków informacji do konkurencji
- Budowanie wizerunku firmy jako godnej zaufania i dbającej o bezpieczeństwo klientów

Adresaci szkolenia

Pracownicy korzystający na co dzień z komputera podpiętego do sieci LAN i Internet

Zakres wymagań dla uczestników szkolenia

Aby wziąć udział w szkoleniu nie potrzeba specjalistycznej wiedzy z zakresu technologii ICT. Wystarczy umiejętność podstawowej obsługi komputera, przeglądarki internetowej oraz poczty elektronicznej.

Zakres tematyczny

- Zagrożenia w cyberprzestrzeni dla pracownika oraz dla zasobów organizacji – obecne trendy
- Socjotechniczne mechanizmy działania cyberprzestępców
- Dobre praktyki zabezpieczania się przed poszczególnymi zagrożeniami, w tym budowania skutecznych haseł, tworzenia kopii bezpieczeństwa
- Rozpoznawanie złośliwego oprogramowania i innych ataków na banki oraz reagowanie na pojawiające się niebezpieczeństwa
- Omówienie obowiązku ochrony informacji i zabezpieczania środowiska pracy z podkreśleniem indywidualnej odpowiedzialności za utrzymanie bezpieczeństwa informacji i reputacji instytucji oraz zaufania klientów
- Konsekwencje ataku na instytucję
- Przykładowe narzędzia pomocne w obronie przed atakami
- Przenoszenie się zagrożeń pomiędzy obszarem prywatnym a służbowym
- Profilaktyka bezpiecznego korzystania z Internetu oraz sieci LAN

W ramach poszczególnych obszarów, w trakcie szkolenia będą przedstawiane miedzy innymi takie zagadnienia, jak:

- Ty też jesteś celem. Ludzkie słabości i emocje – naturalne reakcje ludzkie w obliczu współczesnych zagrożeń
- Czym jest złośliwe oprogramowanie?
- Bezpieczeństwo haseł (min. bezpieczne i silne hasła, systemy zarządzania hasłami, dwustopniowe uwierzytelnianie)
- Socjotechnika on-line, Phishing i Spear Phishing czyli oszustwa w e-mailach i mediach społecznościowych
- Bezpieczeństwo i prywatność w przeglądarkach
- Pracownik w podróży i praca zdalna
- Fałszywe strony i oszustwa w bankowości internetowej

Czas trwania i forma zajęć

Czas trwania szkolenia to 6 godzin. Zajęcia prowadzone są w formie interaktywnych wykładów i warsztatów. Całość szkolenia kończy się testem sprawdzającym, a uczestnicy otrzymują zaświadczenia o ukończeniu szkolenia.

Prowadzący

Wojciech Wrzesień i Piotr Bisialski

Trenerami prowadzącymi szkolenie są eksperci NASK od wielu lat realizujący projekty związane z różnorodnymi aspektami bezpieczeństwa IT.
Bogate doświadczenie trenerów NASK w prowadzeniu szkoleń gwarantuje wysoki poziom merytoryczny szkolenia, wprowadzanie teoretycznych i praktycznych zagadnień w sposób przystępny i dopasowany do potrzeb oraz poziomu zaawansowania słuchaczy.
Aktywny sposób prowadzenia zajęć umożliwia uczestnikom pełne zaangażowanie się w tematykę szkolenia i zdobywanie nowych kompetencji w oparciu o osobiste doświadczenia.