Wektor Wiedzy
Kierunek Twojego rozwoju.

Kurs cyberbezpieczeństwa oraz pracy zdalnej w działach księgowości

Dlaczego ten kurs jest dla Ciebie

Grupa docelowa:

Szkolenie ma na celu zwiększenie komfortu pracy osób zatrudnionych w działach finansowo-księgowych oraz kadrowych w panującej wirtualnej rzeczywistości. Rok 2020 znacznie zmienił wymogi dotyczące realizacji zadań zawodowych. W wielu przedsiębiorstwach praca zdalna stała się koniecznością, pokazując również korzyści z takiego rozwiązania. Jednak, aby sprawnie oraz bezpiecznie funkcjonować w sieci realizując odpowiedzialne zadania, jakie należą do omawianych działów, konieczna jest znajomość systemów umożliwiających sprawną komunikację n odległość oraz świadomość na temat zagrożeń związanych z cyberprzestępczością.

Cel kształcenia:

- Sprawna komunikacja zespołowa oraz możliwość realizacji spotkań sprzedażowych za pośrednictwem MS Teams
- Doskonały przepływ informacji dzięki platformie Ms sharepoint
- Publikowanie formularzy MS Forms
- Zamieszczanie prezentacji MS Sway
- Zarządzanie zadaniami w MS Planner
- Firmowe archiwum online na dysku OneDrive
- Znajomość bezpiecznego poruszania w sieci oraz dobre praktyki pracy w ramach cyberbezpieczeństwa

Wymagania techniczne dla uczestników:

- Posiadanie narzędzi z głośnikami (laptop, komputer stacjonarny z głośnikami lub podłączenie słuchawek).
- Zalecane używanie mikrofonu na zajęciach, gdyż w ten sposób łatwiej skomunikować się
- Trenerem w razie wystąpienia wątpliwości przy rozwiązywaniu zadań,
- Zalecane jest korzystanie podczas zajęć z dwóch monitorów, gdyż ułatwi to samodzielną pracę na zadaniach.

Więcej informacji na temat szkolenia znajdziesz na: https://wektorwiedzy.pl

Program kursu:

Moduł I: Bezpieczeństwo informacji – aktualne zagrożenia cyberprzestępczością

Temat 1: Podstawy Bezpieczeństwa teleinformatycznego i klasyfikacji zagrożeń

1. **Podstawy bezpieczeństwa teleinformatycznego**

   - Co to jest cyberbezpieczeństwo - definicja cyberprzestrzeni i cyberbezpieczeństwa, dlaczego to jest ważne
   - Aktualność problemu bezpieczeństwa teleinformatycznego
   - Ryzyko i zarządzanie ryzykiem - co to jest ryzyko, podstawowe pojęcia i zasady zarządzania ryzykiem
   - Polityka bezpieczeństwa - czym jest w organizacji polityka bezpieczeństwa i jaka jest jej rola
   - Incydenty bezpieczeństwa - co należy rozumieć jako incydent bezpieczeństwa i jak z nim postępować
   - Normy i standardy bezpieczeństwa - powszechnie stosowane rozwiązania, norma ISO27001

2. **Ataki „na człowieka" tzw. SOCJOTECHNIKA (stosowane techniki manipulacji)**

   - Ataki socjotechniczne - techniki manipulacji wykorzystywane przez cyberprzestępców
   - Sposoby - pod jakimi pretekstami wyłudza się firmowe dokumenty
   - Wykrywanie - jak rozpoznać, że jest się celem ataku socjotechnicznego
   - Reakcja - jak prawidłowo reagować na ataki socjotechniczne
   - Jak i skąd atakujący zbierają dane na twój temat
   - Miejsca, w których zostawiamy swoje dane świadomie i nieświadomie - jak świadomie udostępniać informacji w sieci.

3. **Klasyfikacja zagrożeń dla sieci teleinformatycznej i ich źródeł**

   - Podatności sieci teleinformatycznej na ataki
   - Sposoby atakowania sieci, rodzaje włamań sieciowych, rodzaje ataków sieciowych
   - Podatność na ataki w związku z przelewami i bankowością

4. **Monitorowanie incydentów bezpieczeństwa teleinformatycznego**

   - Diagnozowanie incydentów
   - Zbieranie danych dotyczących incydentów
   - Analiza danych dotyczących incydentów podejmowanie działań naprawczych

Temat 2: Organizacyjne i techniczne środki bezpieczeństwa teleinformatycznego

1. **Mechanizmy ochrony przed zagrożeniami bezpieczeństwa sieci teleinformatycznej**

   - Narzędzia i aplikacje do zabezpieczania sieci
   - Zabezpieczenia danych finansowych
   - Systemy wykrywania włamań i ataków
   - Zapory sieciowe
   - Bezpieczna konfiguracja narzędzi do zarządzania i monitorowania urządzeń sieciowych

2. **Metody i środki ochrony informacji**

   - Bezpieczeństwo fizyczne
   - Bezpieczeństwo finansowo-kadrowe
   - Bezpieczeństwo programowe
   - Podstawowe zasady ochrony komputerów służbowych
   - Kopie zapasowe
   - Polityka stosowania rozwiązań kryptograficznych i szyfrowanie informacji przedsięwzięcia organizacyjne
   - Zarządzanie uprawnieniami użytkowników systemów informatycznych, kontrola dostępu

3. **Atak „na komputery" - demonstracje wraz z objaśnieniem metod ochrony**

   - Przegląd aktualnych ataków komputerowych wykorzystywanych przez cyberprzestępców, typowe błędy zabezpieczeń wykorzystywane przez atakujących
   - Ataki przez sieci bezprzewodowe (WiFi, Bluetooth, NFC)
   - Ataki przez pocztę e-mail (fałszywe e-maile)
   - Ataki przez strony WWW - jak nie dać się zainfekować, fałszywe strony
   - Ataki przez komunikatory (Skype, Facebook)
   - Ataki przez telefon (fałszywe SMS-y, przekierowania rozmów, itp.)
   - Ataki APT, phishing, smishing, spear-phishing, pharming, spoofing, spam, spim, scam

4. **Cyberprzestępczość - najpowszechniejsze rodzaje ataków i zagrożeń – praktyczne case study przypadków**

   - Phishing i inne odmiany ataków socjotechnicznych
     Pozostałe zagrożenia dla bezpieczeństwa sieci teleinformatycznej
   - Cracking
   - Sniffing
   - Metoda salami
   - Fałszywe powiadomienia z mediów społecznościowych
   - Oszustwo na „nigeryjskiego księcia"
   - Skimming

Temat 3: Cyberbezpieczeństwo i systemy bezpieczeństwa teleinformatycznego

1. **Organizacja bezpiecznej sieci teleinformatycznej i bezpieczeństwa informacji – rozwiązania systemowe i wymagania prawne w Polsce**

   - Norma ISO 27001:2017
   - Rozporządzenie o Ochronie Danych Osobowych

- Rozporządzenie o Krajowych Ramach Interoperacyjności
- projektowanie bezpiecznej sieci teleinformatycznej
  narzędzia do weryfikacji bezpieczeństwa teleinformatycznego

2. **Dobre praktyki związane z bezpiecznym wykorzystaniem firmowych zasobów**

- Polityka haseł, zarządzanie dostępem i tożsamością - jakie hasło jest bezpieczne, jak nim zarządzać, zasady udzielania dostępu do zasobów informacyjnych
- Bezpieczeństwo fizyczne - urządzenia, nośniki danych, dokumenty, „czyste biurko"
- Bezpieczeństwo danych osobowych kadrowych
- Bezpieczna praca z urządzeniami mobilnymi (smartfon, tablet, laptop)
- Problem aktualnego oprogramowania i kopii zapasowych
- Bezpieczna praca z pakietem biurowym Microsoft Office
- Bezpieczna praca z programem pocztowym
- Bezpieczna praca z przeglądarką internetową
- Zastosowanie technik kryptograficznych (szyfrowanie, certyfikaty)

3. **Aspekty prawne**

- Odpowiedzialność pracownika przed pracodawcą za ujawnienie informacji
- Nieautoryzowane użycie systemów komputerowych
- Rażące zaniedbania związane z wykorzystywaniem sprzętu komputerowego
- Dane osobowe i dane wrażliwe
- Jakie działania związane z cyberatakami kwalifikowane są jako przestępstwa?
- Jakie kary grożą za popełnianie cyberprzestępstw?
- Jakie prawa ma ofiara, która padła ofiarą cyberprzestępstwa?
- Nieautoryzowane użycie komputera.

Moduł II: Narzędzia wspomagające pracę pracowników księgowości i kadr - Office 365

Temat 1: Zapoznanie z Microsoft Teams- praca ze spotkaniami

1. Wstęp do programu Microsoft Teams

- Praca z przeglądarką, aplikacją i aplikacją mobilną, przechowywanie danych na chmurze
- Przydatne skróty klawiaturowe, Statusy
- Tworzenie zespołów i kanałów, współpraca w czasie rzeczywistym w ramach plików Word, Excel, Power Point i innych,

2. Praca w zespole

- Tworzenie zespołów,
- Tworzenie kanałów
- Rozmowy indywidualne i grupowe
- Zapraszanie uczestników spoza organizacji
- Publikowanie plików
- Zarządzanie zadaniami w MS Planner
- Publikowanie formularzy MS Forms

- Zamieszczanie prezentacji MS Sway
- Wzmianki @

3. Rozmowy wideo

- Dodawanie uczestników
- Udzielanie głosu
- Tworzenie notatek
- Rejestrowanie rozmowy
- Udostępnianie plików
- Udostępnianie ekranu

Temat 2: Szczegóły Microsoft Teams - praca z plikami (SharePoint i uprawnienia w SharePoint)

1. SharePoint- Firmowy Intranet- bezproblemowy przepływ informacji wewnątrz organizacji.

Umożliwia tworzenie zabezpieczonych witryn internetowych służących do przechowywania, organizowania i udostępniania informacji z dowolnego urządzenia z dostępem do Internetu. Jeśli wielu współpracowników wnosi dane, które potrzebujemy zgromadzić w jednym miejscu łatwo udostępniamy dokument i każda osoba, która otrzyma uprawnienia może w czasie rzeczywistym edytować plik. Istnieje również możliwość udostepnienia samego widoku dla konkretnego użytkownika, bez możliwości edycji pliku.

- Wersjonowanie plików
- Udostępnianie plików współpracownikom i gościom
- Tworzenie list programu SharePoint
- Praca ze stronami
- Uprawnienia

Temat 3: Omówienie OneDrive, synchronizacja plików, rozwiniecie wiadomości o aplikacji SharePoint

1. OneDrive- osobisty magazyn plików, nawet 1 TB przestrzeni dyskowej.

Dostęp do plików „na żądanie” bez konieczności przechowywania ich na urządzeniu, co pozwala na przyspieszenie komputera czy innych urządzeń. OneDrive na rynku wyróżnia pełna funkcjonalność ze środowiskiem Microsoft Office, umożliwia pracę na pełnych wersjach programu Word, Excel czy Power Point.

- Przekazywanie plików do magazynu. Dane są szyfrowane podczas przesyłania
- Udostępnianie dokumentów innym użytkownikom
- Synchronizacja danych