Możliwość dofinansowania

Comarch SA

4,5 / 5

1 038 ocen

Cyberbezpieczeństwo - Podstawy bezpiecznego poruszania się po sieci oraz rozpoznawania i unikania niebezpieczeństw

Numer usługi 2026/04/20/7733/3499570

zdalna w czasie rzeczywistym

Usługa szkoleniowa

8 h

06.05.2026 do 06.05.2026

1 230,00 PLN brutto

1 000,00 PLN netto

153,75 PLN brutto/h

125,00 PLN netto/h

118,13 PLN cena rynkowa

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Programowanie
Identyfikatory projektów	Małopolski Pociąg do kariery, Kierunek - Rozwój, Nowy start w Małopolsce z EURESEM, Zachodniopomorskie Bony Szkoleniowe, Regionalny Fundusz Szkoleniowy II
Grupa docelowa usługi	Profil uczestnika: Kurs jest skierowany m.in. do: • początkujących pracowników IT • przedsiębiorców chcących poznać ryzyka braku inwestycji w cyberbezpieczeństwo • właścicieli i administratorów stron internetowych, sklepów internetowych • analityków biznesowych, kierowników projektów • osób prywatnych chcących poszerzyć swoją wiedzę z zakresu cyberbezpieczeństwa Szkolenie jest skierowane do osób zarówno początkujących jak i posiadających podstawową wiedzę z zakresu cyberbezpieczeństwa, którą dzięki szkoleniu będą mogli poszerzyć i uporządkować. Przygotowanie uczestnika: • Szkolenie nie wymaga od uczestników specjalistycznego przygotowania ani posiadania technicznej wiedzy. **Czas trwania kursu wynosi 8 godzin lekcyjnych, godzina lekcyjna to 45 minut.** **Usługa jest dedykowana dla uczestników projektu Małopolski pociąg do kariery**
Minimalna liczba uczestników	4
Maksymalna liczba uczestników	12

Data zakończenia rekrutacji	29-04-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	8
Podstawa uzyskania wpisu do BUR	Znak Jakości Małopolskich Standardów Usług Edukacyjno-Szkoleniowych (MSUES) - wersja 2.0

Cel

Cel edukacyjny

Celem szkolenia jest przekazanie uczestnikom wiedzy na temat podstaw bezpiecznego korzystania z internetu zarówno w pracy jak i prywatnie. Uczestnik w trakcie szkolenia nauczy się w jaki sposób rozpoznawać podstawowe ataki, próby wyłudzenia, jak poprawić swoje bezpieczeństwo oraz jakie narzędzia wspomagające ten cel można stosować.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Identyfikuje potencjalne zagrożenia w cyberprzestrzeni oraz szybko rozpoznaje ataki socjotechniczne kierowane w jego stronę.	1. Bezbłędnie wskazuje złośliwe elementy i cechy charakterystyczne fałszywej wiadomości e-mail (phishing) lub SMS (smishing) na podstawie zaprezentowanego studium przypadku. 2. Wymienia i klasyfikuje aktualne zagrożenia czyhające na użytkowników sieci, zagrażające poufności danych firmowych i prywatnych.	Test teoretyczny z wynikiem generowanym automatycznie
Zabezpiecza urządzenia końcowe, z których korzysta na co dzień, oraz w bezpieczny sposób przechowuje poufne dane i poświadczenia logowania.	1. Wdraża podstawowe zasady higieny cyfrowej, konfigurując ustawienia prywatności, blokadę ekranu i mechanizmy aktualizacji na wybranym urządzeniu (smartfon/komputer). 2. Generuje silne, unikalne hasło i bezpiecznie zapisuje je w skonfigurowanym przez siebie menedżerze haseł.	Test teoretyczny z wynikiem generowanym automatycznie
Wdraża i obsługuje mechanizmy wieloskładnikowego uwierzytelniania (MFA) oraz fizyczne klucze zabezpieczeń.	1. Konfiguruje dwuetapowe logowanie (2FA) do wybranej usługi internetowej przy użyciu aplikacji autentykującej (np. Google Authenticator) lub przypina do konta sprzętowy klucz kryptograficzny (np. YubiKey).	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Reaguje prawidłowo w przypadku incydentów bezpieczeństwa i wycieków danych oraz skutecznie weryfikuje informacje o nowych zagrożeniach w rzetelnych źródłach.	1. Podejmuje właściwe kroki zaradcze (np. zmiana poświadczeń, blokada kart, natychmiastowe zgłoszenie do działu IT/CERT) w przypadku symulowanej sytuacji naruszenia bezpieczeństwa lub wycieku bazy danych. 2. Wyszukuje oficjalne ostrzeżenia o zagrożeniach cyfrowych na stronach zweryfikowanych i zaufanych instytucji (np. CERT Polska), potrafiąc oddzielić fakty od dezinformacji (fake news).	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

1.Usługa jest realizowana w godzinach lekcyjnych, tj. za godzinę usługi szkoleniowej rozumie się 45 minut, łącznie 8 godzin lekcyjnych.

Planowane przerwy w trakcie zajęć: 10:30-10:45, 13:00-13:30, 14:45-15:00. Przerwy nie są wliczone w godziny zajęć usługi. Liczba godzin zajęć praktycznych: 4 godzin lekcyjnych , liczba godzin zajęć teoretycznych: 4 godzin lekcyjnych, w tym test 10 min.

Wykładowca ma prawo zmienić godziny przerw, jeśli wymaga tego proces dydaktyczny (np. rozpoczęte ćwiczenie) lub na życzenie większości uczestników kursu (zmęczenie, większa trudność treści kształcenia).

Grupa docelowa:

Szkolenie skierowane jest do każdego użytkownika urządzeń mobilnych i komputerów podłączonych do internetu we współczesnym świecie. W szczególności dla osób pracujących na stanowiskach, które wymagają operacji na danych poufnych.

Kurs jest skierowany m.in. do:

- początkujących pracowników IT
- przedsiębiorców chcących poznać ryzyka braku inwestycji w cyberbezpieczeństwo
- właścicieli i administratorów stron internetowych, sklepów internetowych
- analityków biznesowych, kierowników projektów
- osób prywatnych chcących poszerzyć swoją wiedzę z zakresu cyberbezpieczeństwa

Szkolenie jest skierowane do osób zarówno początkujących jak i posiadających podstawową wiedzę z zakresu cyberbezpieczeństwa, którą dzięki szkoleniu będą mogli poszerzyć i uporządkować.

Przygotowanie uczestników

- Szkolenie nie wymaga od uczestników specjalistycznego przygotowania ani posiadania technicznej wiedzy.

Szczegółowy program szkolenia

Wprowadzenie do cyberbezpieczeństwa

- Czym jest i jakie znaczenie ma cyberbezpieczeństwo
- Higiena pracy z komputerem
- Konsekwencje braku zachowania podstawowych zabezpieczeń

Bezpieczeństwo haseł i kont użytkownika

- Słabe mechanizmy uwierzytelniania w oparciu o hasła
- Jak i gdzie przechowywać hasła
- Jak sprawdzić czy nasze hasło jest bezpieczne
- MFA i 2FA - czym jest i czy go potrzebujesz?
- Przyszłość - passwordless

Bezpieczeństwo danych

- Szyfrowanie dysków
- Jak bezpiecznie przesyłać/udostępniać dane poufne
- Jak chronić się przed wyciekami

Phishing

- Jak rozpoznać - przykłady z życia
- Jak się chronić i reagować

Malware i ransomware

- Jak rozpoznać - przykłady z życia
- Jak reagować - czy płacić okup?
- Jak zapobiegać - dlaczego backup jest taki ważny
- Przykłady z życia

Inne zagrożenia

- Socjotechnika – ataki personalizowane
- Insider
- MITM
- Koparki kryptowalut

Bezpieczeństwo urządzeń mobilnych

Ochrona przed zagrożeniami

- Antywirus
- Aktualizacje
- VPN
- Backup (Two is one, one is none)

Podsumowanie

Metoda realizacji

Forma szkolenia ma na celu przedstawienie w sposób atrakcyjny i interesujący wiedzy i technik związanych ze zwiększeniem poziomu cyberbezpieczeństwa w życiu prywatnym i zawodowym.

Szkolenie będzie realizowane w formie:

- części teoretycznej w postaci prezentacji,
- części praktycznej realizowanej naprzemiennie z częścią teoretyczną w postaci
  - praktycznych i intuicyjnych ćwiczeń polegających m.in. na rozpoznaniu phishingu i tworzeniu „mocnych haseł”
  - burzy mózgów – np. znalezieniu najlepszego sposobu zabezpieczenia swoich danych
  - dyskusji z uczestnikami
  - analizy przypadków (case studies) z życia prywatnego i zawodowego uczestników
  - quizów i ankiet.

Harmonogram

Liczba przedmiotów/zajęć: 0

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Jeżeli korzystasz z dofinansowania w wysokości co najmniej 70% przysługuje Tobie zwolnienie z podatku VAT

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	1 230,00 PLN
Koszt przypadający na 1 uczestnika netto	1 000,00 PLN
Koszt osobogodziny brutto	153,75 PLN
Koszt osobogodziny netto	125,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Agnieszka Sagan

od 18 lat związana z firmą Comarch, gdzie obecnie pełni funkcję Kierownika Działu Asysty Technicznej Comarch BPM. Odpowiadm za całokształt wsparcia merytorycznego dla tej aplikacji, zarządzając zespołem specjalistów i dbając o najwyższą jakość obsługi klienta. W swojej pracy koncentruje się na skutecznym rozwiązywaniu wyzwań biznesowych oraz zapewnieniu stabilnego działania procesów u naszych użytkowników.
Od 7 lat aktywnie prowadzi szkolenia z zakresu aplikacji Comarch BPM. Dzięki codziennemu kierowaniu działem asysty posiada unikalną wiedzę o realnych potrzebach i problemach użytkowników. W procesie szkoleniowym kładzie nacisk na praktykę i konkretne scenariusze biznesowe, ucząc, jak optymalnie wykorzystać Comarch BPM do usprawnienia i automatyzacji codziennej pracy.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały w postaci skryptu w wersji elektronicznej albo papierowej

Warunki uczestnictwa

Warunkiem skorzystania ze szkolenia jest dokonanie równolegle rejestracji na kurs na stronie www.comarch.pl/szkolenia w formie:

- elektronicznego zamówienia szkolenia (przycisk "Zamów" przy wybranym temacie i terminie). Opcja ta dotyczy osób fizycznych oraz firm/instytucji

albo

- poprzez uzupełnienie i odesłanie na adres szkolenia@comarch.pl tradycyjnego formularza zgłoszeniowego który jest dostępny na stronie www.comarch.pl/szkolenia (przycisk "Pobierz formularz zgłoszeniowy"). Opcja ta dotyczy wyłącznie firm/Instytucji.

W obu przypadkach przy dokonaniu zgłoszenia prosimy o informacje dotyczącą projektu z którego dofinansowania korzysta Uczestnik.

Informacje dodatkowe

Szkolenie zakończone jest testem wiedzy z zakresu tematycznego omawianego na szkoleniu.

Szkolenie może być zwolnione z VAT-u w zależności od rodzaju dofinasowania

Zawarto umowę z WUP Kraków na rozliczanie Usług z wykorzystaniem elektronicznych bonów szkoleniowych w ramach projektu „Małopolski Pociąg do Kariery” i "Małopolskie Bony Rozwojowe Plus"

Szkolenie może być nagrywane /rejestrowane w celu kontroli/audytu zgodnie z Regulaminem Świadczenia Usług Szkoleniowych Organizatora.

Zawarto umowę z WUP w Toruniu w ramach Projektu Kierunek – Rozwój.

Uczestnicy szkolenia otrzymają materiały szkoleniowe w wersji elektronicznej albo papierowej.

Planowana przerwa: –obiadowa 30 min plus 2 kawowe po 15 minut.

Wykładowca ma prawo zmienić godziny przerw, jeśli wymaga tego proces dydaktyczny (np. rozpoczęte ćwiczenie) lub na życzenie większości uczestników kursu (zmęczenie, większa trudność treści kształcenia).

Warunki techniczne

Wymagania techniczne:

- Komputer / laptop ze stałym dostępem do Internetu (Szybkość pobierania/przesyłania: minimalna 2 Mb/s / 128 kb/s; zalecana 4 Mb/s / 512 kb/s
- przeglądarka internetowa – zalecane: Google Chrome, Mozilla Firefox, Microsoft Edge
- słuchawki lub dobrej jakości głośniki
- mikrofon

Zalecane

- dodatkowy monitor
- kamera (w przypadku komputerów stacjonarnych)
- spokojne miejsce, odizolowane od zewnętrznych czynników rozpraszających
- podstawowa znajomość języka angielskiego (do sprawnego poruszania się po platformie zdalnej)

Informacje dodatkowe

Szkolenie Zdalne prowadzone jest w czasie rzeczywistymi i transmitowane za pomocą kanału internetowego z wykorzystaniem systemu ZOOM, który umożliwia komunikację głosową oraz wideo z Uczestnikami przebywających w dowolnym miejscu ze sprawnie działającym stałym łączem internetowym. Każdy z uczestników szkolenia otrzymuje przed szkoleniem link dostarczony w wiadomości mailowej z informacjami dotyczącymi szkolenia zdalnego. Link umożliwiający uczestnictwo w spotkaniu jest ważny do momentu zakończenia szkolenia.

Szkolenie zakończone jest testem wiedzy z zakresu tematycznego omawianego na szkoleniu.

Szkolenie może być nagrywane /rejestrowane w celu kontroli/audytu zgodnie z Regulaminem Świadczenia Usług Szkoleniowych Organizatora.

Uczestnicy szkolenia otrzymają materiały szkoleniowe w wersji elektronicznej.

Cena kursu na stronie www.comarch.pl/szkolenia może różnić się znacząco od ceny podanej w Bazie Usług Rozwojowych. Dla klientów którzy przy zgłoszeniu na www.comarch.pl/szkolenia (albo przy pobranym z tej strony formularzu zgłoszeniowym) podadzą numer usługi z BUR i dokonają równoległej rejestracji obowiązuje cena z BUR.

Kontakt

Aneta Lewkowska

E-mail aneta.lewkowska@comarch.pl
Telefon (+48) 12 6877 811