Możliwość dofinansowania

Cyberbezpieczeństwo w pracy biurowej – usługa szkoleniowa

Numer usługi 2026/01/23/161638/3278315

8 610,00 PLN brutto
7 000,00 PLN netto
195,68 PLN brutto/h
159,09 PLN netto/h

KORYCKI & GRACZYK CONSULTING GROUP SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

4,9 / 5

541 ocen

zdalna w czasie rzeczywistym
Usługa szkoleniowa
44 h
23.02.2026 do 27.02.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	• Pracownicy biurowi, administracja, sekretariaty, recepcje, kancelarie, działy kadr, księgowości, obsługi klienta, back-office itp. • Pracownicy jednostek administracji publicznej oraz firm prywatnych przetwarzający dane i informacje (w tym dane osobowe). • Osoby przygotowujące się do pracy na stanowiskach administracyjnych. • pracownicy i/lub właściciele pracujący z komputerem, Internetem oraz urządzeniami mobilnymi • pracownicy z sektora MSP
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	22-02-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	44
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Usługa „Cyberbezpieczeństwo w pracy biurowej – usługa szkoleniowa” przygotowuje do zwiększenia świadomości i kompetencji uczestników w zakresie cyberbezpieczeństwa oraz higieny w sieci poprzez rozwijanie rozumienia oraz praktycznego stosowania najlepszych praktyk i strategii obrony przed zagrożeniami cybernetycznymi w środowisku zawodowym na stanowiskach biurowych.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Omawia podstawowe pojęcia związane z cyberbezpieczeństwem i higieną w sieci, takie jak malware, phishing, bezpieczne hasła i szyfrowanie danych.	Uczestnik poprawnie definiuje wymienione pojęcia i opisuje ich znaczenie w kontekście bezpieczeństwa sieciowego.	Test teoretyczny z wynikiem generowanym automatycznie
Charakteryzuje różne typy zagrożeń cyfrowych oraz metody ich rozpoznawania.	Uczestnik wymienia i opisuje co najmniej trzy różne typy zagrożeń, podając przykłady oraz sposoby ich identyfikacji.	Test teoretyczny z wynikiem generowanym automatycznie
Definiuje znaczenie aktualizacji oprogramowania w kontekście zabezpieczeń cyfrowych.	Uczestnik wyjaśnia, dlaczego regularne aktualizacje oprogramowania są kluczowe dla zachowania bezpieczeństwa systemów i danych.	Test teoretyczny z wynikiem generowanym automatycznie
Stosuje praktyki tworzenia i zarządzania bezpiecznymi hasłami.	Uczestnik demonstruje umiejętność tworzenia silnych haseł i korzystania z menedżerów haseł do ich przechowywania.	Test teoretyczny z wynikiem generowanym automatycznie
Identyfikuje i reaguj na próby phishingu i inne oszustwa internetowe.	Uczestnik poprawnie identyfikuje fałszywe wiadomości e-mail i strony internetowe oraz zna procedury reagowania na te zagrożenia.	Test teoretyczny z wynikiem generowanym automatycznie
Stosuje zasady bezpiecznego korzystania z sieci publicznych i prywatnych.	Uczestnik potrafi skonfigurować bezpieczne połączenie sieciowe i stosuje praktyki ochrony prywatności podczas korzystania z sieci publicznych.	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

TAK

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Dzień 1:

1. wprowadzenie do szkolenia
2. audyt cyberbezpieczeństwa
3. istota i podstawowe terminy w zakresie cyberbezpieczeństwa
4. podstawy prawne cyberbezpieczeństwa i zalecenia ENISA
5. najpopularniejsze ataki cybernetyczne

Dzień 2:

1. ćwiczenie: phishing
2. przestępstwa finansowe w przestrzeni cyfrowej
3. zasady ustalania haseł zgodnie z obecnymi standardami bezpieczeństwa cyfrowego
4. jak działa i jak wybrać menadżera haseł?
5. dlaczego tak często hakerzy łamią hasła?
6. dlaczego samo hasło nie wystarczy? Autoryzacja dwuskładnikowa w praktyce

Dzień 3:

1. szyfrowanie plików,folderów i pendrive'ów w praktyce
2. jak chronić dane osobowe zgodnie z RODO?
3. zastrzeż swój PESEL
4. jak robić backup danych?

Dzień 4:

1. dlaczego warto korzystać z„chmury”?
2. wykorzystywanie AI przez cyberprzestępców – jak nie dać się nabrać?
3. jak zabezpieczyć swój sprzęt i prywatność? Programy antywirusowe, firewall, tryb incognito, cookies, VPN
4. co o nas wiedzą? - socjotechniki wykorzystywane przez hakerów
5. co zrobić, gdy zostanę zaatakowany? Procedura formalna i komunikacyjna

Dzień 5:

1. jak wzmocnić kulturę cyberbezpieczeństwa w organizacji?
2. jak rodzą się fake newsy przez wykorzystywanie narzędzi AI?
3. ćwiczenie grupowe: symulacje ataków cybernetycznych
4. narzędzia i programy wzmacniające bezpieczeństwo cyfrowe
5. Podsumowanie
6. Test teoretyczny z wynikiem generowanym automatycznie - walidacja

1) Godziny i forma

Szkolenie odbywa się w godzinach dydaktycznych (1 godz. = 45 minut), łącznie **44 godziny dydaktyczne**. Usługa realizowana jest zdalnie, w czasie rzeczywistym, na platformie **Google Meet**. Przerwy nie są wliczane do czasu szkolenia. Grupy: **1–15 osób**.

2) Metoda prowadzenia

Zajęcia prowadzone są metodami **interaktywnymi i aktywizującymi**: krótkie wprowadzenia trenera, studia przypadków, ćwiczenia indywidualne, quizy on-line, dyskusje moderowane, praca na checklistach i prostych procedurach.

3) Grupa docelowa. Usługa skierowana jest do:

- pracowników biurowych, administracji, sekretariatów, recepcji, kancelarii, działów kadr, księgowości, obsługi klienta, back-office itp.,
- pracowników jednostek administracji publicznej oraz firm prywatnych przetwarzających dane i informacje (w tym dane osobowe),
- osób przygotowujących się do pracy na stanowiskach administracyjnych.

4) Cel edukacyjny. Usługa „Cyberbezpieczeństwo w pracy biurowej – usługa szkoleniowa" przygotowuje do zwiększenia świadomości i kompetencji uczestników w zakresie cyberbezpieczeństwa oraz higieny w sieci poprzez rozwijanie rozumienia oraz praktycznego stosowania najlepszych praktyk i strategii obrony przed zagrożeniami cybernetycznymi w środowisku zawodowym na stanowiskach biurowych.

5) Walidacja – kryteria ogólne

Ocena efektów uczenia się prowadzona jest za pośrednictwem standaryzowanego testu dostępnego online, którego wynik generowany jest automatycznie przez system, bez udziału człowieka. Mechanizm walidacji działa niezależnie od procesu szkoleniowego (nie jest obsługiwany przez trenera ani zespół prowadzący), co zapewnia rozdzielność obu procesów. Test ma z góry określone progi zaliczeniowe, a wyniki wraz z metadanymi (data/godzina, czas trwania, identyfikator uczestnika) są archiwizowane w systemie, a informacja o rezultacie udostępniana jest uczestnikowi niezwłocznie. Tym samym warunek rozdzielności procesów szkolenia i walidacji pozostaje zachowany. Test składa się z dwudziestu pytań jednokrotnego wyboru (cztery warianty odpowiedzi). Uczestnik rozwiązuje test w programie Google Forms, oświadczając o niekorzystaniu z pomocy dydaktycznych przy jego rozwiązywaniu. Każde pytanie punktowane jest po jeden punkt. Nie ma punktów ujemnych.

Uczestnik otrzyma zaświadczenie po spełnieniu dwóch warunków:

- frekwencja co najmniej **80% czasu szkolenia** (bez przerw) oraz
- wynik walidacji na poziomie minimum **80%** (test teoretyczny z wynikiem generowanym automatycznie)

6) Charakter usługi (VAT)

Szkolenie stanowi usługę **kształcenia zawodowego** w rozumieniu art. 43 ust. 1 pkt 29 ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług, tj. nauczanie pozostające w bezpośrednim związku z branżą i zawodem pracowników biurowych i administracji oraz służące uzyskaniu lub uaktualnieniu wiedzy do celów zawodowych, zgodnie z definicją przyjętą w rozporządzeniu wykonawczym Rady UE nr 282/2011.

7) Minimalne wymagania: Uczestnicy nie muszą posiadać doświadczenia, wiedzy ani umiejętności w zakresie bezpieczeństwa cyfrowego.

Harmonogram

Liczba przedmiotów/zajęć: 36

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 36 wprowadzenie do szkolenia – wideokonferencja	Marta Schneider	23-02-2026	08:00	09:00	01:00
2 z 36 audyt cyberbezpieczeństwa – współdzielenie ekranu	Marta Schneider	23-02-2026	09:00	10:00	01:00
3 z 36 Przerwa	Marta Schneider	23-02-2026	10:00	10:30	00:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
4 z 36 istota i podstawowe terminy w zakresie cyberbezpieczeństwa – wideokonferencja	Marta Schneider	23-02-2026	10:30	11:30	01:00
5 z 36 podstawy prawne cyberbezpieczeństwa i zalecenia ENISA – wideokonferencja	Marta Schneider	23-02-2026	11:30	12:30	01:00
6 z 36 Przerwa	Marta Schneider	23-02-2026	12:30	13:00	00:30
7 z 36 najpopularniejsze ataki cybernetyczne – współdzielenie ekranu	Marta Schneider	23-02-2026	13:00	15:45	02:45
8 z 36 ćwiczenie: phishing	Marta Schneider	24-02-2026	08:00	09:00	01:00
9 z 36 przestępstwa finansowe w przestrzeni cyfrowej – wideokonferencja	Marta Schneider	24-02-2026	09:00	10:00	01:00
10 z 36 Przerwa	Marta Schneider	24-02-2026	10:00	10:30	00:30
11 z 36 zasady ustalania haseł zgodnie z obecnymi standardami bezpieczeństwa cyfrowego – wideokonferencja	Marta Schneider	24-02-2026	10:30	11:30	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
12 z 36 jak działa i jak wybrać menadżera haseł? – współdzielenie ekranu	Marta Schneider	24-02-2026	11:30	12:30	01:00
13 z 36 Przerwa	Marta Schneider	24-02-2026	12:30	13:00	00:30
14 z 36 dlaczego tak często hakerzy łamią hasła? – wideokonferencja	Marta Schneider	24-02-2026	13:00	15:45	02:45
15 z 36 dlaczego samo hasło nie wystarczy? Autoryzacja dwuskładnikowa w praktyce – ćwiczenia	Marta Schneider	25-02-2026	08:00	09:00	01:00
16 z 36 szyfrowanie plików,folderów i pendrive'ów w praktyce – współdzielenie ekranu	Marta Schneider	25-02-2026	09:00	10:00	01:00
17 z 36 Przerwa	Marta Schneider	25-02-2026	10:00	10:30	00:30
18 z 36 jak chronić dane osobowe zgodnie z RODO? – wideokonferencja	Marta Schneider	25-02-2026	10:30	11:30	01:00
19 z 36 zastrzeż swój PESEL – współdzielenie ekranu	Marta Schneider	25-02-2026	11:30	12:30	01:00
20 z 36 Przerwa	Marta Schneider	25-02-2026	12:30	13:00	00:30
21 z 36 jak robić backup danych? – ćwiczenia	Marta Schneider	25-02-2026	13:00	15:45	02:45

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
22 z 36 dlaczego warto korzystać z„chmury”? – wideokonferencja	Marta Schneider	26-02-2026	08:00	09:00	01:00
23 z 36 wykorzystywanie AI przez cyberprzestępców – jak nie dać się nabrać? – ćwiczenia	Marta Schneider	26-02-2026	09:00	10:00	01:00
24 z 36 Przerwa	Marta Schneider	26-02-2026	10:00	10:30	00:30
25 z 36 jak zabezpieczyć swój sprzęt i prywatność? Programy antywirusowe, firewall, tryb incognito, cookies, VPN – współdzielenie ekranu	Marta Schneider	26-02-2026	10:30	11:30	01:00
26 z 36 co o nas wiedzą? - socjotechniki wykorzystywane przez hakerów – wideokonferencja	Marta Schneider	26-02-2026	11:30	12:30	01:00
27 z 36 Przerwa	Marta Schneider	26-02-2026	12:30	13:00	00:30
28 z 36 co zrobić, gdy zostanę zaatakowany? Procedura formalna i komunikacyjna – ćwiczenia	Marta Schneider	26-02-2026	13:00	15:45	02:45
29 z 36 jak wzmocnić kulturę cyberbezpieczeństwa w organizacji? – chat	DOMINIK HAMERA	27-02-2026	08:00	09:00	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
30 z 36 jak rodzą się fake newsy przez wykorzystywanie narzędzi AI? – wideokonferencja	DOMINIK HAMERA	27-02-2026	09:00	10:00	01:00
31 z 36 Przerwa	DOMINIK HAMERA	27-02-2026	10:00	10:30	00:30
32 z 36 ćwiczenie: symulacje ataków cybernetycznych	DOMINIK HAMERA	27-02-2026	10:30	11:30	01:00
33 z 36 narzędzia i programy wzmacniające bezpieczeństwo cyfrowe – wideokonferencja	DOMINIK HAMERA	27-02-2026	11:30	12:30	01:00
34 z 36 Przerwa	DOMINIK HAMERA	27-02-2026	12:30	13:00	00:30
35 z 36 Podsumowanie – chat	DOMINIK HAMERA	27-02-2026	13:00	14:00	01:00
36 z 36 Test teoretyczny z wynikiem generowanym automatycznie - walidacja	DOMINIK HAMERA	27-02-2026	14:00	15:00	01:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	8 610,00 PLN
Koszt przypadający na 1 uczestnika netto	7 000,00 PLN

Koszt osobogodziny brutto	195,68 PLN
Koszt osobogodziny netto	159,09 PLN

Prowadzący

Liczba prowadzących: 2

1 z 2

DOMINIK HAMERA

Posiada 9 lat doświadczenia w pozyskiwaniu funduszy. Firma, którą prowadzi pozyskała ponad 100 000 000 zł dla swoich klientów. Specjalizuje się w doradztwie biznesowym, unijnym, w zakresie pozyskiwania funduszy zewnętrznych, zarządzaniu, procesami motywacyjnymi. Prowadzi szkolenia z indywidualne oraz grupowe m.in. „Motywacja pracowników w zarządzaniu zespołem" „Zarządzanie procesami w biznesie" „Budowanie motywacji i zaangażowania pracowników" „Pozyskiwanie funduszy unijnych", „Automotywacja pracowników".
Od ponad 8 lat prowadzi przedsiębiorstwo doradcze w zakresie pozyskiwania funduszy unijnych, zarządzania strategicznego w firmie. Zajmuje się oceną i kontroli systemu organizacji procesów zachodzących w firmie.
Posiada wykształcenie wyższe zdobyte na AWF Warszawa, kierunek wychowanie fizyczne, specjalizacja menedżer. Współpracuje z Ministerstwem Sportu i Turystyki.
Przeprowadził ponad 1000 godzin szkoleń dla firm z sektora MŚP oraz organizacji pozarządowych. Współpracuje z podmiotami ekonomii społecznej. Prowadzi diagnozy potrzeb rozwojowych oraz szkoleniowych. Prowadzi szkolenia dla właścicieli firm oraz kadry kierowniczej z zarządzania strategicznego w firmie, zarządzania procesami oraz motywacyjne.

2 z 2

Marta Schneider

Marta Schneider – ekspertka w dziedzinie cyberbezpieczeństwa i higieny cyfrowej, trenerka kompetencji miękkich oraz przywództwa z ponad 1500 godzinami przeprowadzonych szkoleń w ostatnich pięciu latach. W tym ponad 250 godzin poświęciła na szkolenia z zakresu cyberbezpieczeństwa, higieny w sieci oraz zaawansowanych technik ochrony przed zagrożeniami cyfrowymi, rozwijając u uczestników zarówno świadomość zagrożeń, jak i praktyczne nawyki bezpiecznego korzystania z technologii.

Specjalizuje się w łączeniu perspektywy bezpieczeństwa cyfrowego z rozwojem liderów i zespołów. 350 godzin szkoleń z przywództwa, budowania zespołów i umiejętności menedżerskich wykorzystuje do tego, by pokazywać, jak liderzy mogą realnie wzmacniać kulturę cyberbezpieczeństwa w organizacji – od zarządzania ryzykiem, przez kształtowanie postaw pracowników, po wdrażanie prostych, ale skutecznych procedur bezpieczeństwa.

Absolwentka socjologii (specjalność: praca socjalna) Uniwersytetu im. Adama Mickiewicza w Poznaniu, wyróżniona stypendium rektora za najwyższą średnią. Łączy wiedzę z socjologii, psychologii rozwoju człowieka i zarządzania konfliktem z praktyką w obszarze cyberbezpieczeństwa, przekładając ją na mierzalne rezultaty biznesowe oraz wzrost dojrzałości cyfrowej organizacji.

Posiada liczne certyfikaty z zakresu cyberbezpieczeństwa, które potwierdzają jej kompetencje w

obszarze ochrony informacji, bezpiecznej pracy w środowiskach cyfrowych oraz budowania kultury bezpieczeństwa w organizacjach.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały zostaną przesłane drogą mailową w formacie pdf. Uczestnik otrzyma:

1. skrypty

2. materiały video

Warunki uczestnictwa

Ukończony 18 rok życia.

Informacje dodatkowe

1. Jeśli szkolenie będzie dofinansowane ze środków publicznych w **co najmniej 70%,** będzie **zwolnione przedmiotowo z podatku VAT** (podstawa prawna: par. 3 ust. 1 pkt 14 *Rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień* (t.j. Dz. U. z 2023 r. poz. 955 z późn. zm.)).
2. Usługa rozwojowa nie jest świadczona przez podmiot pełniący funkcję Operatora lub Partnera Operatora w danym projekcie PSF lub w którymkolwiek Regionalnym Programie lub FERS albo przez podmiot powiązany z Operatorem lub Partnerem kapitałowo lub osobowo.

Warunki techniczne

1. **Platforma komunikacyjna** – Google Meet.

2. **Wymagania sprzętowe:**

- komputer z aktualnym systemem (Windows 10 lub nowszy / macOS 12 lub nowszy / aktualna dystrybucja Linux),
- aktualna przeglądarka (Chrome/Edge/Firefox/Safari – co najmniej dwie ostatnie wersje),
- stabilne łącze internetowe o przepustowości min. 10 Mb/s (pobieranie) i 2 Mb/s (wysyłanie),
- sprawna kamera komputerowa i mikrofon,
- sprawne słuchawki/ głośniki.

1. **Okres ważności linku:** od godziny zegarowej przed godziną rozpoczęcia szkolenia w dniu pierwszym do godziny zegarowej po zakończeniu szkolenia w dniu ostatnim.

Kontakt

WOJCIECH GRACZYK

E-mail wojciech.graczyk@korycki-graczyk.pl
Telefon (+48) 698 291 420