



H2B GROUP
SPÓŁKA Z
OGRA NICZONĄ
ODPOWIEDZIALNOŚ
CIĄ
★★★★★ 4,8 / 5
38 ocen

Bądź bezpieczny w sieci - wprowadzenie do podstaw cyberbezpieczeństwa w prowadzeniu biznesu i życiu osobistym - szkolenie (ONLINE - forma zdalna)

Numer usługi 2025/05/28/168043/2776147

2 950,00 PLN brutto
2 398,37 PLN netto
245,83 PLN brutto/h
199,86 PLN netto/h

📍 zdalna w czasie rzeczywistym

🏠 Usługa szkoleniowa

🕒 12 h

📅 18.09.2025 do 19.09.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikatory projektów	Kierunek - Rozwój
Grupa docelowa usługi	Szkolenie jest skierowane do firm MŚP oraz osób fizycznych zainteresowanych wiedzą z obszaru Cyberbezpieczeństwa - w tym przedsiębiorców, managerów zarządzających, urzędników oraz pracowników działów administracji, księgowości, sprzedaży, HR, rekrutacji, IT, marketingu, logistyki, a także entuzjastów ochrony danych i bezpieczeństwa, którzy chcą podnieść swoje kwalifikacje oraz nabyć podstawowe umiejętności w zakresie bezpieczeństwa cyfrowego. Szkolenie jest przeznaczone przede wszystkim dla osób chcących rozwijać się zawodowo oraz odnosić sukcesy zawodowe poprzez pracę nad samym sobą.
Minimalna liczba uczestników	4
Maksymalna liczba uczestników	40
Data zakończenia rekrutacji	15-09-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	12
Podstawa uzyskania wpisu do BUR	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Usługa opracowana została na podstawie rzeczywistych doświadczeń projektowych i przygotowuje do samodzielnego stosowania technik ochrony danych za sprawą nabycia fundamentalnej wiedzy teoretycznej i praktycznej z zakresu cyberbezpieczeństwa.

Każdy uczestnik zostanie poddany pre-testowi sprawdzającemu poziom wiedzy oraz post-testowi sprawdzającemu nabyte w czasie usługi kompetencje.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wiedza: Posługuje się wiedzą na temat cyberbezpieczeństwa	Definiuje podstawowe pojęcia i koncepcje związane ze cyberbezpieczeństwem	Test teoretyczny
	Rozróżnia podstawowe typy ataków oraz ich motywacje	Test teoretyczny
	Wskazuje potencjalne skutki kradzieży tożsamości	Test teoretyczny
	Charakteryzuje role polityki bezpieczeństwa informacji	Test teoretyczny
	Wymienia elementy składające się na bezpieczeństwo fizyczne	Test teoretyczny
	Wymienia przykłady naruszeń RODO	Test teoretyczny
Umiejętności: Korzysta z dobrych praktyk i zasad bezpieczeństwa danych	Generuje silne i bezpieczne hasła	Test teoretyczny
	Generuje szyfrowane pliki na nośnikach	Test teoretyczny
	Analizuje incydenty bezpieczeństwa	Test teoretyczny
	Rozpoznaje ataki phishingowe	Test teoretyczny
	Formułuje metody zapamiętywania złożonych haseł	Test teoretyczny

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

Krótki opis usługi:

Usługa ma na celu zapoznanie uczestników z podstawami cyberbezpieczeństwa, ze szczególnym uwzględnieniem metod ochrony przed cyberatakami, oszustwami i utratą prywatności. Uczestnicy poznają podstawowe zagadnienia cyberbezpieczeństwa, typologię ataków i stojącą za nimi motywację, a także potencjalne skutki. Usługa zapewni solidne fundamenty teoretyczne i praktyczne do dalszego zgłębiania tematyki oraz praktyczne techniki przeciwdziałania.

Podczas usługi zostaną zaprezentowane główne zasady ochrony, aby uczestnicy mogli szybko wdrożyć je w swoich organizacjach i życiu prywatnym. To wyjątkowa okazja, by zrozumieć jak praktycznie podnieść swoje bezpieczeństwo w sieci.

Ramowy program usługi:

Szkolenie jest skierowane do firm MŚP oraz osób fizycznych zainteresowanych wiedzą z obszaru Cyberbezpieczeństwa - w tym przedsiębiorców, managerów zarządzających, urzędników oraz pracowników działów administracji, księgowości, sprzedaży, HR, rekrutacji, IT, marketingu, logistyki, a także entuzjastów ochrony danych i bezpieczeństwa, którzy chcą podnieść swoje kwalifikacje oraz nabyć podstawowe umiejętności w zakresie bezpieczeństwa cyfrowego. Szkolenie jest przeznaczone przede wszystkim dla osób chcących rozwijać się zawodowo oraz odnosić sukcesy zawodowe poprzez pracę nad samym sobą.

Poniżej prezentujemy szczegółowy program usługi:

Dzień 1 - Bezpieczeństwo informacji (1 spotkanie online w dniu 18.09.2025 od 8:00 do 13:00 - 5h)

1. Wprowadzenie do cyberbezpieczeństwa

- Podstawowe zagadnienia, Triada CIA
- Rodzaje atakujących i ich motywy
- Skutki cyberataków dla biznesu oraz dla osób prywatnych

2. Ochrona danych osobowych wg RODO

- Przypomnienie najważniejszych zasad
- Prawa osób, których dane dotyczą
- Przykłady naruszeń RODO i wnioski z nich płynące

3. Kradzież tożsamości

- Skutki kradzieży tożsamości
- Przykłady kradzieży tożsamości
- Zapobieganie i działania po incydencie

4. Rola pracowników w bezpieczeństwie informacji

- Jak działania pracowników wpływają na bezpieczeństwo organizacji
- Pozytywne i negatywne postawy pracowników w kontekście cyberbezpieczeństwa
- Najważniejsze zasady cyberhigieny

5. Polityka bezpieczeństwa informacji w firmie

- Czym jest ten dokument i jaka jest jego rola w organizacji
- Co zawiera Polityka bezpieczeństwa informacji
- Jakie wymagania stawia wobec pracowników

6. Bezpieczeństwo fizyczne

- Czym jest bezpieczeństwo fizyczne i dlaczego jest ważne
- Jaka jest jego rola w budowaniu cyberbezpieczeństwa organizacji
- Jakie elementy składają się na bezpieczeństwo fizyczne

Dzień 2 - Bezpieczne funkcjonowanie w świecie cyberzagrożeń (1 spotkanie online w dniu 19.09.2025 od 8:00 do 13:00 -5h)

7. Bezpieczne korzystanie z Internetu

- Przegląd różnych rodzajów cyberzagrożeń
- Działania niebezpieczne w sieci
- Dobre praktyki w korzystaniu z Internetu

8. Zasady tworzenia silnych haseł

- Cechy silnego i bezpiecznego hasła
- Metody zapamiętywania złożonych haseł
- Dobre i złe praktyki w zakresie haseł

9. Reagowanie na incydenty bezpieczeństwa

- Czym jest incydent bezpieczeństwa
- Rodzaje incydentów bezpieczeństwa
- Zasady prawidłowej reakcji na incydent

10. Zasady bezpiecznego korzystania ze służbowego sprzętu komputerowego

- Bezpieczne logowanie, zasada czystego ekranu
- Znaczenie regularnych aktualizacji oprogramowania
- Szyfrowanie plików na nośnikach danych

11. Phishing i inne ataki socjotechniczne

- Mechanizmy działania i cele ataków
- Rodzaje phishingu
- Zasady unikania ataków phishingowych

Q&A - konsultacje, pytania, problemy

Na koniec szkolenia Uczestnicy otrzymują materiały szkoleniowe wraz z instrukcjami do narzędzi omawianych na zajęciach. Materiały szkoleniowe będą przesyłane do uczestników za pomocą poczty e-mail.

Efekty kształcenia zostaną sprawdzone za pomocą przeprowadzonych pre- i post-testów uczestników (informacja zwrotna, krótka ocena).

Rozliczeniu podlega 160 godzin szkoleniowych usługi. Usługa prowadzona jest w trybie godzin zegarowych (godzina szkolenia = 60 minut), przerwy wliczają się w czas trwania usługi.

Walidacja usługi - w zakresie spełnienia celu edukacyjnego będzie przeprowadzony post-test po zakończeniu usługi.

Harmonogram

Liczba przedmiotów/zajęć: 21

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 21 Zasady obowiązujące na szkoleniu. Omówienie agendy i organizacji pierwszego dnia szkolenia (wykład)	Grzegorz Strupczewski	18-09-2025	08:00	08:10	00:10
2 z 21 Pre-test wykonywany za pomocą narzędzi cyfrowych (test)	-	18-09-2025	08:10	08:25	00:15
3 z 21 Wprowadzenie do cyberbezpieczeństwa (wykład)	Grzegorz Strupczewski	18-09-2025	08:25	09:25	01:00
4 z 21 Ochrona danych osobowych wg RODO (wykład)	Grzegorz Strupczewski	18-09-2025	09:25	10:25	01:00
5 z 21 Przerwa	Grzegorz Strupczewski	18-09-2025	10:25	10:40	00:15
6 z 21 Kradzież tożsamości (wykład)	Grzegorz Strupczewski	18-09-2025	10:40	11:40	01:00
7 z 21 Rola pracowników w bezpieczeństwie informacji (wykład)	Grzegorz Strupczewski	18-09-2025	11:40	12:10	00:30
8 z 21 Polityka bezpieczeństwa informacji w firmie (wykład)	Grzegorz Strupczewski	18-09-2025	12:10	12:40	00:30
9 z 21 Przerwa	Grzegorz Strupczewski	18-09-2025	12:40	12:55	00:15
10 z 21 Bezpieczeństwo fizyczne (wykład)	Grzegorz Strupczewski	18-09-2025	12:55	13:45	00:50

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
11 z 21 Q&A (rozmowa na żywo)	Grzegorz Strupczewski	18-09-2025	13:45	14:00	00:15
12 z 21 Omówienie agendy i organizacji drugiego dnia szkolenia (wykład)	Grzegorz Strupczewski	19-09-2025	08:00	08:10	00:10
13 z 21 Bezpieczne korzystanie z Internetu (wykład)	Grzegorz Strupczewski	19-09-2025	08:10	09:10	01:00
14 z 21 Zasady tworzenia silnych haseł (wykład)	Grzegorz Strupczewski	19-09-2025	09:10	10:10	01:00
15 z 21 Przerwa	Grzegorz Strupczewski	19-09-2025	10:10	10:25	00:15
16 z 21 Reagowanie na incydenty bezpieczeństwa (wykład)	Grzegorz Strupczewski	19-09-2025	10:25	11:25	01:00
17 z 21 Zasady bezpiecznego korzystania ze służbowego sprzętu komputerowego (wykład)	Grzegorz Strupczewski	19-09-2025	11:25	12:25	01:00
18 z 21 Przerwa	Grzegorz Strupczewski	19-09-2025	12:25	12:40	00:15
19 z 21 Phishing i inne ataki socjotechniczne (wykład)	Grzegorz Strupczewski	19-09-2025	12:40	13:40	01:00
20 z 21 Post-test wykonywany za pomocą narzędzi cyfrowych (test)	-	19-09-2025	13:40	13:50	00:10

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
21 z 21 Q&A - konsultacje, pytania, problemy (rozmowa na żywo)	Grzegorz Strupczewski	19-09-2025	13:50	14:00	00:10

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 950,00 PLN
Koszt przypadający na 1 uczestnika netto	2 398,37 PLN
Koszt osobogodziny brutto	245,83 PLN
Koszt osobogodziny netto	199,86 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Grzegorz Strupczewski

Grzegorz Strupczewski to specjalista w zakresie cyberbezpieczeństwa i zarządzania ryzykiem cyfrowym, profesor Uniwersytetu Ekonomicznego w Krakowie. Posiada wieloletnie doświadczenie w prowadzeniu szkoleń, warsztatów i wykładów z zakresu ochrony przed cyberzagrożeniami, adresowanych zarówno do instytucji finansowych, administracji publicznej, jak i sektora prywatnego. Dodatkowo pracuje jako menadżer ds. usług cyberbezpieczeństwa w firmie z branży IT odpowiadając za tworzenie i koordynację wdrażania polityk bezpieczeństwa informacji w różnych organizacjach. Jako praktyk i naukowiec, skutecznie łączy wiedzę teoretyczną z realiami rynkowymi. Jego ekspercka wiedza, poparta licznymi publikacjami naukowymi i praktyką dydaktyczną, czyni go cenionym trenerem w dziedzinie cyberbezpieczeństwa.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy usługi, po jej zakończeniu, otrzymują:

- Opracowane materiały zagadnień poruszanych w trakcie usługi wraz z listą artykułów i prac naukowych pozwalających na pogłębienie wiedzy przekazanej w trakcie usługi
- Certyfikat ukończenia szkolenia potwierdzający uzyskane kompetencje

Warunki uczestnictwa

- Podstawowa znajomość obsługi komputera
- Dostęp do komputera z internetem i kamerą
- Zainteresowanie tematyką ochrony danych

Warunki techniczne

Usługa zostanie przeprowadzona na platformie Google Meet. Link do spotkania zostanie przesłany uczestnikom drogą e-mail najpóźniej dzień przed rozpoczęciem Usługi.

Podstawowe minimalne wymagania sprzętowe:

Aby skorzystać z usługi online, potrzebny jest komputer ze stabilnym łączem internetowym i bez blokad firmowych. Zalecana minimalna prędkość pobierania danych: 10 Mb/s oraz prędkość wysyłania: 5 Mb/s. Twój komputer powinien posiadać minimum:

- najnowszą wersję przeglądarki internetowej (Edge lub Chrome),
- 2-rdzeniowy procesor 1,6 GHz lub szybszy,
- pamięć 4 GB pamięci RAM (wersja 32-bitowa – 2 GB),
- jeżeli chcesz zadawać pytania głosowo, konieczny jest mikrofon. Dodatkowo, wszyscy mogą zadawać pytania za pośrednictwem chatu online.

Dodatkowe wymagania:

- Konto na platformie google (do spotkania)

Kontakt



Robert Forreiter

E-mail bur@h2b-group.com

Telefon (+48) 531 033 437