

EDU HEZO

Katalog szkoleń



all of
security

KATALOG SZKOLEŃ:

	Tytuł	Czas (min)	Opis/Desc
bezpieczeństwo poczty email	Bezpieczeństwo poczty e-mail	20	Dowiedz się, jak rozpoznawać wiadomości wyłudające informacje, niebezpieczne załączniki i inne oszustwa związane z wiadomościami e-mail.
	Narzędzia ochrony wiadomości e-mail	15	Naucz się rozpoznawać wiadomości phishingowe z oznakowanymi adresami URL.
	Bezpieczeństwo poczty e-mail na urządzeniach mobilnych	10	Unikaj wiadomości phishingowych na urządzeniach mobilnych
	Unikanie niebezpiecznych załączników	9	Zidentyfikuj niebezpieczne załączniki e-mail i unikaj ich
	Ataki z użyciem złośliwego oprogramowania	10	Skutki ataku z użyciem złośliwego oprogramowania mogą być katastrofalne. W tym module skupimy się na tym, czym jest złośliwe oprogramowanie, jak można je przesyłać na urządzenia i jak uniknąć ataku z użyciem złośliwego oprogramowania.
	Email Attack Methods: Business Email Compromise	3	This video training will help you understand security risks regarding Business Email Compromise (BEC).
bezpieczeństwo pracy	Bezpieczeństwo urządzeń przenośnych	5	Z tego szkolenia video dowiesz się, jak chronić dane, funkcje i komunikację na urządzeniach przenośnych.
	Bezpieczeństwo poza biurem	15	Unikaj najczęstszych błędów dotyczących bezpieczeństwa danych w domu i w podróży.
	Bezpieczeństwo urządzeń przenośnych	22	Korzystaj z zabezpieczeń fizycznych i technicznych zapewniających ochronę urządzeń oraz danych.
	Podstawy bezpieczeństwa fizycznego	2	Cyberbezpieczeństwo nie polega tylko na aktualizowaniu oprogramowania i unikaniu szkodliwych wiadomości czy witryn. Aby chronić dane i urządzenia, potrzebujemy skutecznych nawyków bezpieczeństwa fizycznego, wykraczających poza cyberprzestrzeń. Należy o nich wiedzieć i je właściwie stosować.
	Podstawy bezpieczeństwa: przetwarzanie danych i bezpieczeństwo	2	Kurs Podstawy bezpieczeństwa dostarcza podstawowych informacji na temat koncepcji związanych z przetwarzaniem danych i bezpieczeństwem.
	Podstawy bezpieczeństwa: zagrożenia wewnętrzne	2	Kurs Podstawy bezpieczeństwa dostarcza podstawowych informacji na temat koncepcji związanych z zagrożeniami wewnętrznymi.
	Podstawy bezpieczeństwa: bezpieczeństwo fizyczne i praca zdalna	2	Kurs Podstawy bezpieczeństwa dostarcza podstawowych informacji na temat koncepcji związanych z bezpieczeństwem fizycznym i pracą zdalną.
	Bezpieczeństwo w miejscu pracy w praktyce	14	Ćwicz stosowanie najlepszych praktyk w zakresie bezpieczeństwa biurowego zgodnie z prawdopodobnymi scenariuszami, obejmującymi aspekty z zakresu inżynierii społecznej, zagrożeń wewnątrz firmy i techniki shoulder surfing.
	Zagrożenia wewnętrzne	9	Ucz się na podstawie rzeczywistych sytuacji i odkrywaj działania, które pomogą Ci zminimalizować zagrożenie.
	Podsumowanie zagrożeń wewnętrznych	12	Rozpoznawaj zagrożenia wewnętrzne i opanuj najlepsze praktyki w zakresie ochrony przed zagrożeniami.
	Bezpieczeństwo fizyczne	14	Naucz się jak zapewnić bezpieczeństwo fizyczne danych i aktywów.
	Bezpieczeństwo urządzeń USB	9	Podczas używania nośników USB chroń siebie, dane i system.
	Niezamierzone zagrożenia wewnętrzne	10	Zapoznaj się ze scenariuszami ilustrującymi codzienne czynności pracowników, które stwarzają niezamierzone zagrożenia, zapobiegaj im lub ograniczaj ich skutki.

	Tytuł	Czas (min)	Opis/Desc
bezpieczeństwo w internecie	Przeglądanie internetu: Rozpoznawanie zagrożeń (początkujący)	2	Zawartość online może być szkodliwa. W końcu każdy może stworzyć witrynę i hostować treść cyfrową w sieci – także przestępcy. Każdy może kupić domenę dostępną w rejestrze domen. Nie istnieje zbyt wiele ograniczeń. W tym module opisano sygnały ostrzegawcze, na które należy zwracać uwagę.
	Unikanie niebezpiecznych linków	9	Rozpoznawaj typowe oszustwa mailowe i unikaj niebezpiecznych linków
	Mądre posługiwanie się mediami społecznościowymi	2	W mediach społecznościowych nie dziwi nas, że jesteśmy zasypywani prośbami o zawarcie znajomości, wzięcie udziału w ankiecie lub odwiedzenie nowej strony internetowej. Ale musimy zachować ostrożność wobec osób i treści, i wiedzieć, co zrobić, gdy zauważymy coś podejrzanego.
	Bezpieczniejsze przeglądanie Internetu	23	Korzystaj bezpiecznie z Internetu, unikając ryzykownych zachowań i częstych pułapek
	Podstawy wiedzy na temat adresów URL	18	Zapoznaj się z różnymi częściami adresu URL i pytaniami, które należy zadać podczas jego analizy.
dane osobowe	URL Fundamentals	16	Learn the different parts of a URL and what questions to ask when reviewing one.
	Podstawy ochrony danych osobowych	16	Chroń swoje poufne dane, a także poufne dane dotyczące Twojego pracodawcy i klientów.
	Dane osobowe w praktyce	11	Możliwość pracy przy pomocy zestawu scenariuszy. Zobacz, w jaki sposób najlepsze praktyki zdobyte dzięki „Podstawowym zasadom dotyczącym danych osobowych” wpływają na decyzje podejmowane w świecie rzeczywistym.
	Dane osobowe w praktyce cz.2	10	Dowiedz się, jak stosować najlepsze praktyki w pracy z danymi osobowymi.
phishing	Wprowadzenie do phishingu	19	Uniknąć niebezpieczeństw związanych z pocztą e-mail i oszustw phishingowych
	Rozpoznawanie ataków phishingowych: wykrywanie sygnałów ostrzegawczych (początkujący)	2	Zagrożenie atakami phishingowymi nie zniknie, dlatego należy poznać chociaż niektóre oznaki takich działań, aby zachować bezpieczeństwo w pracy i w domu. W tym module wyjaśniono, na co zwracać uwagę.
	Phishing wprowadzanych danych	8	Naucz się, jak rozpoznawać oszustwa mające na celu pozyskanie wrażliwych informacji lub danych osobowych oraz jak ich unikać.
	Prekursor phishingu	9	Dowiedz się, jak oszuści wykorzystują phishingowe wiadomości e-mail do kradzieży poufnych informacji i czego należy szukać w podejrzanym wiadomościach e-mail.
	Ataki typu spear phishing	12	Rozpoznaj zagrożenia spear phishingowe i uniknij ich
regulacje prawne	Podstawy bezpieczeństwa – zarząd	15	Po pomyślnym ukończeniu tego modułu będziesz w stanie zmniejszyć ryzyko związane z naruszeniem firmowego e-maila, naruszeniem konta e-mail i ekspozycją danych.
	Podstawy bezpieczeństwa – zarząd cz.2	17	Po pomyślnym ukończeniu tego modułu będziesz w stanie zmniejszyć ryzyko związane z naruszeniem firmowego e-maila, naruszeniem konta e-mail i ekspozycją danych.
	Informacje ogólne o RODO	14	Dowiedz się, jak europejskie Rozporządzenie o Ochronie Danych Osobowych wpływa na ochronę danych osobowych.
	Praca zdalna: Rozpoznawanie ryzyka	2	Koncepcja „miejsca pracy” uległa w ostatnich latach przekształceniu. Technologia pozwala wielu ludziom pracować dziś z dowolnego miejsca. Praca zdalna stanowi jednak okazję dla cyberprzestępców do wymierzenia ataku w pracownika lub jego firmę.
	RODO w praktyce	22	Naucz się stosować pojęcia przedstawione w RODO w codziennych sytuacjach i decyzjach.

	Tytuł	Czas (min)	Opis/Desc
regulacje prawne	Dane publiczne a dane niepubliczne	2	Niektóre rodzaje informacji są bardziej wrażliwe od innych. Organizacje korzystają z różnego nazewnictwa do oznaczenia rodzajów takich danych. Zasadniczo dane organizacji można jednak podzielić na dwie grupy: publiczne i niepubliczne. Należy znać różnicę między tymi rodzajami danych i wiedzieć, jak się nimi posługiwać.
	Anti-Fraud and Bribery	12	Understanding the different types of fraud and bribery that can occur is crucial to preventing incidents. This course helps educate users on what fraud and bribery means, as well as how to recognize the key elements and warning signs. End-users will take part in a practical real-life scenario and be provided with guidance on what to do if they suspect a fraud or bribery incident.
	PCI DSS	12	The Payment Card Industry Data Security Standard is administered by the PCI Security Standards Council to prevent payment card fraud and increase the security of confidential payment card information. It is a global data security standard that all organisations, of any size, must adhere to in order to accept payment cards. This course will help employees understand what PCI DSS is, how it protects financial and personal information, and their specific responsibilities in order to comply with PCI DSS and keep payment data secure.
	HIPAA Overview	12	Omówienie wymagań prawnych Health Insurance Portability and Accountability Act (HIPAA)
socjotechnika	Prekursor phishingu	5	Dowiedz się, jak oszuści wykorzystują phishingowe wiadomości e-mail do kradzieży poufnych informacji i czego należy szukać w podejrzanych wiadomościach e-mail.
	Inżynieria społeczna: Wiele metod, wiele motywów	2	Manipulacja emocjonalna i taktyki zwodzenia znane jako „inżynieria społeczna” są powszechne w cyberatakach. W tym module omówiono kilka typowych ataków inżynierów społecznych.
	Socjotechnika	19	Rozpoznawaj ataki socjotechniczne i ich unikaj
	Podstawy zapewniania bezpieczeństwa	17	Rozpoznawaj kwestie związane z bezpieczeństwem w codziennych czynnościach zawodowych i osobistych.
	Zasady dotyczące haseł	7	Naucz się, jak tworzyć hasła zgodne z zasadami obowiązującymi w twojej firmie.
	Uwierzytelnianie wielopoziomowe	6	Poznaj najlepsze praktyki w zakresie stosowania uwierzytelniania wielopoziomowego, dzięki czemu zyskasz dodatkowy poziom zabezpieczeń dla swoich kont.
	Więcej niż hasło	11	Zastosuj coś więcej niż hasło. Dowiedz się, jak używać kodów PIN i wyrażeń hasłowych w celu zabezpieczenia swoich kont i urządzeń.
	Zarządzanie hasłami	13	Dowiedz się, jakie są najlepsze praktyki w zakresie bezpiecznego zarządzania hasłami.
	Bezpieczne portale społecznościowe	16	Dowiedz się, jak bezpiecznie i odpowiedzialnie korzystać z serwisów społecznościowych.

Skontaktuj się z nami
edu@myHEZO.pl | myHEZO.pl/edu



Katalog szkoleń



all of
security