Szkolenie

Cyberbezpieczeństwo pracowników biurowych - kurs o bezpieczeństwie IT

Strona szkolenia | Terminy szkolenia | Rejestracja na szkolenie | Promocje

Opis szkolenia

Odkryj najnowsze techniki ochrony przed współczesnymi zagrożeniami w sieci! Nasze szkolenie z cyberbezpieczeństwa dla pracowników biurowych pozwoli Ci zdobyć wiedzę na temat najnowszych zagrożeń, technik ataków cyberprzestępczych oraz metod socjotechnicznych, które mogą Cię dotknąć podczas codziennej pracy przy komputerze.

Podczas szkolenia dowiesz się, jak chronić siebie i swoją firmę przed cyberatakami, które stają się coraz bardziej zaawansowane. Obecnie sztuczna inteligencja nie tylko pomaga w codziennych zadaniach, ale także staje się narzędziem w rękach przestępców. Nasze szkolenie pokaże Ci, jak AI jest wykorzystywana do przeprowadzania ataków i jak się przed nimi bronić.

Kurs jest zgodny z dyrektywą NIS2 i pomaga spełnić najnowsze wymogi dotyczące bezpieczeństwa sieci i informacji.

Wymagania

- Szkolenie skierowane jest do każdego pracownika w firmie bez względu na jego wiedzę i umiejętności informatyczne.

Korzyści po szkoleniu:

- Zdobycie wiedzy obejmującej bezpieczne zarządzanie miejscem pracy oraz danymi

- Zdobycie wiedzy umożliwiającej ochronę przed atakami socjotechnicznymi

Harmonogram szkolenia

1. Wprowadzenie do cyberprzestępczości: Poznaj podstawy cyberbezpieczeństwa.
2. Zorganizowane grupy cyberprzestępcze: Jak działają i dlaczego są groźne.
3. Czy cyberprzestępcy naprawdę nam zagrażają?
4. Czy jestem atrakcyjnym klientem dla cyberprzestępcy?
5. Korzyści dla cyberprzestępców: Co zyskują atakując Twoje dane?
6. Rodzaje ataków na pracowników biurowych.
7. Straty dla firmy: Skutki udanego cyberataku.
8. Sieci Botnet: Jak cyberprzestępcy przejmują komputery.
9. Skuteczne metody ochrony przed cyberatakami.
10. AI w rękach cyberprzestępców: Nowe zagrożenia z wykorzystaniem sztucznej inteligencji.
11. Spam jako niegroźny sposób na groźne ataki.
12. Czy cyberprzestępca jest zawsze anonimowy?
13. Phishing jako metoda okradania naszych kont bankowych.
14. Ataki DoS/DDoS: Zagrożenia dla instytucji.
15. Ataki 0-day: Czy istnieje sposób obrony przed nimi?
16. Opłacona faktura jako sposób przemycenia wirusa do naszego systemu.
17. Bezpieczeństwo haseł: Jak cyberprzestępcy zdobywają Twoje hasła?
18. Skanowanie kart płatniczych: Gdzie i kiedy ktoś może zeskanować Twoją kartę?
19. Ataki socjotechniczne, czyli niewinne wyłudzanie danych.
20. Kradzież tożsamości: Co? Jak? Kiedy? Gdzie?
21. Bezpieczne przekazywanie haseł współpracownikom.
22. Fizyczne bezpieczeństwo: Jak zabezpieczyć miejsce pracy.
23. Znaleziony pendrive, jako pozwolenie na atak cyberprzestępcy.
24. Zwiększenie odporności na cyberataki: Proste i skuteczne metody.
25. Sprzęt prywatny vs. firmowy: Jak zarządzać bezpieczeństwem urządzeń.

Tagi:

Adres korespondencyjny:
DAGMA Szkolenia IT | ul. Bażantów 6a/3 | Katowice (40-668)
tel. 32 793 11 80 | szkolenia@dagma.pl
szkolenia.dagma.eu

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy
Numer KRS: 0000130206, kapitał zakładowy: 75 000 zł
Numer NIP: 634-012-60-68, numer REGON: 008173852