Szkolenie

Cyberbezpieczeństwo 2024 - Szkolenie ochronne przed współczesnymi atakami sieciowymi

Strona szkolenia | Terminy szkolenia | Rejestracja na szkolenie | Promocje

Opis szkolenia

Szkolenie ochronne przed współczesnymi atakami sieciowymi. Szkolenie zaznajamia uczestnika z najnowszymi zagrożeniami, technikami ataków cyberprzestępczych oraz metodami socjotechnicznymi, ukierunkowanymi na osoby pracujące na co dzień przed komputerem.

Podczas szkolenia uczestnicy zapoznają się z najnowszymi trendami jakimi kierują się cyberprzestępcy. Każdego dnia powstają nowe formy ataku na nieświadomych użytkowników Internetu. Dzięki uświadamianiu jesteśmy coraz bardziej odporni na cyberataki. Możemy powiedzieć, że rok 2023 jest rokiem sztucznej inteligencji, która uczy i bawi, a także pomaga przestępcom. Dzięki naszemu szkoleniu słuchacze dowiedzą się w jaki sposób AI wykonuje polecenia przestępców dzięki którym łatwiej im dostać się do naszych pieniędzy lub co gorsza tożsamości.

Harmonogram szkolenia

1. Co to jest cyberprzestępczość?
2. Opis funkcjonowania zorganizowanych grup cyberprzestępczych
3. Czy naprawdę nam zagrażają?
4. Czy jestem atrakcyjnym „klientem” dla cyberprzestępcy?
5. Jakie zyski może mieć cyberprzestępca atakując moje dane?
6. Straty wynikające z udanego ataku na firmę
7. Rodzaje ataków skierowane w pracowników biurowych

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
KRS pod numerem 0000130206, kapitał zakładowy 75 000 zł
Numer NIP 634-012-60-68, numer REGON: 008173852
DAGMA Sp. z o.o. posiada status dużego przedsiębiorcy
w rozumieniu art. 4c ustawy o przeciwdziałaniu nadmiernym
opóźnieniom w transakcjach handlowych.

8. Jak cyberprzestępca dołącza nasz komputer do sieci Botnet?
9. Jak się przed tym bronić?
10. Sztuczna inteligencja w służbie cyberprzestępców
11. Spam jako niegroźny sposób na groźne ataki
12. Czy przestępca jest zawsze anonimowy?
13. Kampanie Phishingowe jako metoda okradania naszych kont bankowych
14. Opłacalność ataków DoS/DDoS wymierzonych w naszą instytucję
15. Groźne ataki 0-day – czy istnieje sposób obrony przed nimi
16. Opłacona FV jako sposób przemycenia wirusa do naszego systemu
17. Skąd cyberprzestępca zna moje hasło?
18. Skanowanie kart płatniczych – gdzie i kiedy ktoś zeskanował moja kartę
19. Ataki socjotechniczne, czyli niewinne „wyłudzanie” danych
20. Kradzież tożsamości – Co? Jak? Gdzie? Kiedy?
21. Przekazywanie haseł dostępowych współpracownikom
22. Fizyczne bezpieczeństwo miejsca pracy
23. Znaleziony pendrive na parkingu jako pozwolenie na atak dla cyberprzestępcy
24. Jak łatwo zwiększyć odporność na cyberataki?
25. Sprzęt prywatny a sprzęt firmowy
26. Sesja pytań i odpowiedzi

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
KRS pod numerem 0000130206, kapitał zakładowy 75 000 zł
Numer NIP 634-012-60-68, numer REGON: 008173852
DAGMA Sp. z o.o. posiada status dużego przedsiębiorcy
w rozumieniu art. 4c ustawy o przeciwdziałaniu nadmiernym
opóźnieniom w transakcjach handlowych.