



Opis przedmiotu zamówienia

Podstawowe szkolenia lub dostęp do platform szkoleniowych budujące świadomość cyberzagrożeń i sposobów ochrony dla pracowników JST.

Cel szkolenia: Celem szkolenia z zakresu cyberzagrożeń jest zwiększenie świadomości uczestników na temat potencjalnych niebezpieczeństw w cyberprzestrzeni oraz wyposażenie ich w praktyczne umiejętności niezbędne do ochrony danych i systemów informatycznych.

Grupa docelowa: Pracownicy Urzędu Gminy Zbuczyn oraz 8 jednostek organizacyjnych

Tryb szkolenia: online lub dostęp do platformy szkoleniowej

Liczba uczestników: 50 osób

Wykonawca zapewni szkolenie w co najmniej dwóch terminach lub dostęp do platformy szkoleniowej przez okres co najmniej 30 dni.

Liczba godzin szkoleniowych: minimum 3 h (przez godzinę Zamawiający rozumie 45 minut)

Salę szkoleniową: nie dotyczy

Catering podczas szkoleń: nie dotyczy

Materiały szkoleniowe: po stronie Wykonawcy w formie elektronicznej

Dokumentacja szkolenia:

Ponadto Wykonawca zobowiązany jest do:

- zapewnienia każdemu uczestnikowi imiennego certyfikatu/zaświadczenia potwierdzającego ukończenie szkolenia,
- prowadzenia listy obecności (podpisy/logi),
- oznaczenia wszelkich materiałów, prezentacji i innych dokumentów opracowanych na potrzeby szkolenia zgodnie z wymaganiami regulaminu konkursu „Cyberbezpieczny Samorząd”, umowy o powierzenie grantu oraz wniosku o dofinansowanie.

Program szkolenia powinien obejmować co najmniej następujące zagadnienia:

1. Data Leak – czym jest i jakie zagrożenia niesie;
2. Polityka haseł – praktyczne podejście i narzędzia wspomagające;
3. Socjotechniki – podstawowe definicje i przykłady użycia;
4. Phishing / Spoofing – nigdy nie wiesz kto jest po drugiej stronie;
5. Vhishing / ID Call Hijacking – telefony też nie są w pełni bezpieczne;
6. Metadane – czyli dane o danych;
7. Web Archive – Internet nie zapomina;
8. Pliki Cookies – czym są popularne „ciasteczka”;
9. Zagrożenia związane z nieznanym sprzętem – jak nieznaną pendrive może zaszkodzić całej instytucji;
10. Ataki Bruteforce / Ataki Słownikowe – podstawowe metody łamania haseł;
11. Spear Phishing – wszystko co „powiesz” (w sieci) może zostać użyte przeciwko Tobie;
12. Krótkie przypomnienie szkolenia pn: „Podstawy cyberbezpieczeństwa”;
13. Podsumowanie ostatnich lat w cyberbezpieczeństwie;



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



14. AI - krótkie wprowadzenie do sztucznej inteligencji i przykłady jak może być wykorzystywana przeciwko nam;
15. BinB i inne bardziej zaawansowane podszywanie się;
16. Cała prawda o VPNach - czym są, co zapewniają a czego nie;
17. Kody QR;
18. MitM - nie tylko WiFi można podsłuchiwać;
19. Uwaga na WhatsAppa;
20. Fałszywe aplikacje na telefon.