Rekomendacje dla obywateli

1. Biuletyn Ouch!
   Darmowy zestaw porad bezpieczeństwa dla użytkowników komputerów: www.cert.pl/ouch
2. Artykuły z zakresu cyberbezpieczeństwa: www.cert.pl
3. Poradniki na witrynie internetowej Ministerstwa Cyfryzacji: https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo
4. Strona internetowa kampanii STÓJ. POMYŚL. POŁĄCZ. mającej na celu zwiększanie poziomu świadomości społecznej i promowanie bezpieczeństwa w cyberprzestrzeni: https://stojpomyslpolacz.pl/stp/

Zapoznaj się z poradnikiem dotyczącym bezpieczeństwa skrzynek pocztowych i kont w mediach społecznościowych oraz zastosuj się do jego rekomendacji.

Bądź wyczulony na sensacyjne informacje, w szczególności zachęcające do natychmiastowego podjęcia jakiegoś działania. Weryfikuj informacje w kilku źródłach. Upewnij się, że informacja jest prawdziwa przed podaniem jej dalej w mediach społecznościowych. Jeśli masz jakieś wątpliwości, wstrzymaj się.

Uważaj na wszelkie linki w wiadomościach mailowych i SMS-ach, zwłaszcza te sugerujące podjęcie jakiegoś działania, np. konieczność zmiany hasła, albo podejrzaną aktywność na koncie. Obserwowaliśmy w przeszłości tego typu celowane ataki na prywatne konta, gdzie celem było zdobycie informacji zawodowych.

Upewnij się, że posiadasz kopię zapasową wszystkich ważnych dla siebie plików i potrafisz je przywrócić w przypadku takiej potrzeby.

Śledź ostrzeżenia o nowych scenariuszach ataków na naszych mediach społecznościowych: Twitter, Facebook.

Zgłaszaj każdą podejrzaną aktywność przez formularz na stronie incydent.cert.pl lub mailem na cert@cert.pl. Podejrzane SMS-y prześlij bezpośrednio na numer 799 448 084. Rekomendujemy zapisanie go w kontaktach.