Cyberzagrożenia - spersonalizowane oszustwa

Cyberprzestępcy w dalszym ciągu poszukują nowych, kreatywnych sposobów oszukiwania ludzi. Na popularności zyskuje nowy rodzaj tzw. spersonalizowanego oszustwa. Przestępcy wyszukują lub nabywają informacje o milionach osób, wykorzystując zdobyte dane do przeprowadzenia ataku.

Najczęściej jest to mail zawierający groźbę wysyłaną na losowe adresy mailowe osób, których dane kontaktowe (mail i hasło) zostały upublicznione w wyniku wycieku danych z różnych serwisów lub są dostępne publicznie.

Wszystkie podejrzane wiadomości a także sms-y można zgłaszać do CERT.PL poprzez stronę:
https://incydent.cert.pl/#!/lang=pl

Polecamy zapoznanie się również z zaufaną stroną internetową https://haveibeenpwned.com/, na której można bezpiecznie sprawdzić, czy mail oraz powiązane z nim hasło w przeszłości nie uległy upublicznieniu.

Odpowiednia złożoność haseł może zabezpieczyć przed ich odgadnięciem oraz wykorzystaniem przez przestępców. Zachęcamy do zapoznania się z bazą wiedzy na temat haseł: https://cert.pl/hasla/

Dodatkowo zachęcamy do zapoznania się z biuletynem OUCH! “Spersonalizowane oszustwa”, dostępnym na stronie: https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltf02c8355723d094a/6047b17f5aedc043351b6f7d/201902-OUCH-February-Polish-FINAL.pdf, w którym jest opisywany ten rodzaj oszustwa.

Zachęcamy do obserwowania CERT Polska w mediach społecznościowych:
-Facebook: https://facebook.com/CERT.Polska/
-Twitter: https://twitter.com/CERT_Polska/
gdzie umieszczane są ostrzeżenia przed aktywnymi oszustwami.