Ataki socjotechniczne

Ataki spersonalizowane

Wraz ze wzrostem przypadków naruszenia ochrony danych cyberprzestępcom łatwiej jest znaleźć lub kupić duże zbiory danych osobowych w sieci. Używają ich następnie, by personalizować ataki socjotechniczne, przez co e-maile, SMS-y lub rozmowy telefoniczne są znacznie bardziej skuteczne.

Przestępcy używają twoich danych osobowych, próbując cię zastraszyć lub zmusić do wykonania ich poleceń. Cyberprzestępca może na przykład pobrać twoje hasło podczas twej wizyty na przejętej stronie internetowej, po czym użyć tej informacji, aby oszukać cię, że włamał się do twojego komputera.

To naturalne, że się boisz, gdy przestępca ma twoje dane osobowe.

Wiedza, że takie e-maile lub rozmowy telefoniczne to przekręt, może ułatwić ci ich identyfikację. Częste oznaki ataku spersonalizowanego to:

Wykorzystywanie twoich danych osobowych – takich jak imię i nazwisko, używane w przeszłości hasła, numery telefonów, miejsca pracy czy inne szczegóły – które można znaleźć w sieci.

Wykorzystywanie emocji – takich jak strach, nagła potrzeba czy wstyd – aby pchnąć cię do popełnienia błędu.

Żądanie płatności taką metodą jak bitcoin czy inne kryptowaluty.

Jeśli otrzymasz podejrzany e-mail, zachowaj spokój – im pilniejsza wiadomość, tym prawdopodobniejsze oszustwo. Spróbuj przeszukać Internet, by sprawdzić, czy inne osoby zgłosiły podobne ataki. W końcu zdrowy rozsądek stanowi najlepszą obronę.

SSA-1906FS001

This factsheet is published by example.
For more information, please contact us at:

security@example.org