CORE
Avast & AVG Distributor

CORE Arkadiusz Stanoszek
ul. Wolności 109a
41-500 Chorzów
NIP: PL6271341058

Alior Bank S.A: 42 2490 0005 0000 4500 9503 7991
tel: +48 32 246 94 94
email: biuro@core.link | pomoc@core.link
https://core.link

Bezpieczeństwo w sieci – oszustwa z wykorzystaniem telefonu

Smishing

1. To rodzaj phishingu rozprzestrzenianego za pomocą wiadomości SMS, skąd wzięła się jego nazwa (SMS + phishing = SMiShing).
2. Oszuści chcą w ten sposób wyłudzić od ofiar wrażliwe dane, takie jak numery karty płatniczej, dowodu osobistego czy dane logowania do bankowości internetowej.
3. Cyberprzestępcy zaszywają w wiadomości link prowadzący do fałszywej strony, np. imitującej witrynę banku.
4. Oszuści mogą też wyłudzać pieniądze, podsyłając link do płatności w celu rzekomego uregulowania zaległych należności.
5. Popularne są wiadomości z prośbą o dopłatę do przesyłki kurierskiej, informacje o nieuregulowanym rachunku czy blokadzie konta bankowego.
6. Nie klikaj w otrzymywane w ten sposób linki, nie reaguj na prośby o wpłatę, ani nie odpisuj na wiadomości smishingowe.

Spoofing telefoniczny

1. Cyberprzestępcy mogą podszyć się pod wybrany numer telefonu, udając np. przedstawiciela banku.
2. Chcą w ten sposób wyłudzić wrażliwe dane, takie jak imię i nazwisko czy numer PESEL.
3. Bądź podejrzliwy podczas rozmów telefonicznych. Nie zdradzaj nikomu danych do logowania do banku i nie instaluj dodatkowego oprogramowania, jeśli zostaniesz o to poproszony.

Duplikat SIM i kradzież numeru

1. Oszust wyrabia duplikat karty SIM ofiary w salonie operatora, identyfikując się np. podrobionym dokumentem tożsamości.
2. Loguje się na konto bankowe ofiary i zleca przelew na dużą kwotę. Operację autoryzuje kodem SMS, który otrzymał na wyrobiony duplikat karty.
3. Ofiara już wcześniej musi być na celowniku oszustów. Pozyskali oni bowiem dane logowania do bankowości, a także informacje służące do wyrobienia fałszywego dokumentu tożsamości.

CORE Arkadiusz Stanoszek
ul. Wolności 109a
41-500 Chorzów
NIP: PL6271341058

Alior Bank S.A: 42 2490 0005 0000 4500 9503 7991
tel: +48 32 246 94 94
email: biuro@core.link | pomoc@core.link
https://core.link

4. Monitoruj kartę SIM. Jeśli nagle przestanie działać, może to oznaczać, że ktoś wyrobił jej duplikat. Zweryfikuj operację u operatora i poinformuj bank o możliwym oszustwie.
5. Używaj innego numeru telefonu do obsługi konta bankowego – takiego, który nie jest udostępniony w internetowych bazach, np. w KRS.

Połączenia z zagranicznych numerów telefonów

1. Oszustwo polega na wykonaniu krótkiego połączenia na numer ofiary. Oszuści liczą, że ofiara oddzwoni na zagraniczny numer, nacinając się tym samym na wysokie opłaty.
2. Nie oddzwaniaj na nieznane numery. Weryfikuj też numer kierunkowy – w przypadku Polski jest to +48.

Stalkerware – szpieg w telefonie

1. Stalkerware to oprogramowanie, które pozwala śledzić każdy ruch użytkownika na jego telefonie. Aby je zainstalować, wystarczy fizyczny dostęp do smartfona.
2. Osoba szpiegująca może widzieć aktualną lokalizację ofiary, jej wiadomości, komunikatory, zdjęcia, filmy i pliki, a także podsłuchiwać rozmowy telefoniczne.
3. Aby się chronić, zabezpiecz fizyczny dostęp do swojego telefonu blokadą ekranu i nie zostawiaj urządzenia bez opieki.
4. Zainstaluj oprogramowanie antywirusowe (np. Avast Mobile Security), monitoruj zużycie baterii, transfer danych i przejrzyj uprawnienia aplikacji.

Oszustwa na WhatsAppie

1. Ofiarą może być osoba sprzedająca coś na portalu aukcyjnym. Oszust kontaktuje się ze sprzedawcą i informuje, że opłacił zamówienie. Przesyła fałszywy link do firmy kurierskiej, twierdząc, że można tam odebrać pieniądze. W rzeczywistości sprzedający udostępnia wrażliwe dane oszustowi.
2. Oszustwa te mogą przybierać różne warianty, ale mają wspólny mianownik – chęć rozliczenia płatności/przesyłki poza serwisem aukcyjnym.
3. Oszuści wykorzystują też Booking.com. Kontaktują się na WhatsAppie z osobą, która złożyła rezerwację. Informują, że jest problem z płatnością kartą i należy ją autoryzować. Jeśli przekażesz dane karty przez komunikator, narazisz się na utratę pieniędzy.
4. Aby uchronić się przed takimi oszustwami, nie koresponduj z zainteresowanymi poza oficjalnymi kanałami. Ogranicz się do portali aukcyjnych czy platform do rezerwacji noclegów.