

## **Uważaj na oszustów, podających się za pracownika Twojego banku lub znanej Ci firmy**

**Mnożą się sposoby wyłudzenia i nieuprawnionego wykorzystania skradzionych danych. Metod, jakimi posługują się złodzieje danych jest bardzo wiele. Do jednych z bardziej niebezpiecznych sposobów oszustów należą chwytły socjotechniczne. To, co je łączy, to element zaskoczenia oraz bazowanie na ludzkiej naiwności lub nieuwadze.**

Zwykle przestępcy internetowi działają w bardzo podobny sposób. Każde z przestępstw bazuje na nawiązaniu relacji z potencjalną ofiarą. Zazwyczaj będzie to wiadomość SMS albo mail, ale także poprzez różnego rodzaju media społecznościowe i komunikatory. Powszechne są również oszukańcze połączenia i rozmowy telefoniczne.

Przestępca nawiązuje bliski i przekonujący kontakt z ofiarą, namawiając do podania danych, np. do wykonania przelewu lub dokonania transakcji kartowej. Wszystkie szczegóły są zmyślane: przestępcy podają fikcyjne uzasadnienie, fikcyjne kwoty zobowiązań, nieistniejące dane odbiorcy.

### **Ekspert BIK zaobserwował zwiększoną aktywność telefoniczną oszustów podszywających się pod rozmaite instytucje zaufania publicznego w celu zebrania danych personalnych.**

Rozmowy mogą trwać długo, przestępcy przełączają rozmowę do innych „konsultantów”, żeby stworzyć pozory prawdziwego kontaktu np. z bankiem. Rozmówca jest zmanipulowany, zaczyna wierzyć, że jego pieniądze są w niebezpieczeństwie. Często zdarza się, że jest nakłaniany do zainstalowania na swoim komputerze lub smartfonie aplikacji, która zwiększy bezpieczeństwo pieniędzy. W rzeczywistości ten program czy aplikacja umożliwi oszustom przejście kontroli nad telefonem lub komputerem ofiary.

### **Nie daj się nabrać, zwróć uwagę kto naprawdę do Ciebie dzwoni**

Motywy działania złodziei są te same - mają one na celu uzyskanie korzyści finansowych. Lepiej więc nie wdawać się w dyskusję z nieznanymi. Taka łatwowierność może wiele kosztować. Oto wybrane porady, jak nie dać się oszukać

- Nigdy nie kontynuuj podejrzanych rozmów - jeśli masz wątpliwości co do wiarygodności osoby, która dzwoni – natychmiast rozłącz się, a następnie zadzwoń na oficjalną infolinię firmy, aby potwierdzić czy faktycznie jej pracownik kontaktował się z Tobą. Nie oddzwaniaj odruchowo na nieznany numer – to niebezpieczeństwo przekierowania do krajów egzotycznych - za takie połączenie nasz operator komórkowy pobierze podwyższoną opłatę. Nie odpisuj anonimowym nadawcom, nie klikaj w linki podsuwane zarówno w mailach, jak i w wiadomościach sms - w pośpiechu można przenieść się na fałszywą stronę, a to już krok od utraty danych lub wprost pieniędzy;
- Nigdy nie instaluj żadnych aplikacji, jeśli namawia Cię do tego osoba, która sama do Ciebie zadzwoniła;
- Pamiętaj, pracownik BIK, Związku Banków Polskich, Twojego banku NIGDY nie pyta się o login i hasło do logowania na Twoje konto w banku, nie prosi o pełny numer Twojej karty, jej daty ważności oraz kod CVV2/CVC2, ani nie namawia do zainstalowania aplikacji na Twoim komputerze lub smartfonie;
- Nigdy nie wiadomo, kiedy i skąd nasze dane zostaną skradzione, dlatego miej włączone Alerty BIK – ostrzeżenia sms, które otrzymasz, gdy ktoś na Twoje dane zaciąga kredyt, pożyczkę, umowę z operatorem telekomunikacyjnym, dokonuje zakupów na raty.