Ostrzeżenie o próbach wyłudzenia danych lub oszustwach polegających na instalowaniu przestępczego oprogramowania poprzez kliknięcie w linki lub za pomocą technik socjotechnicznych

W ostatnich miesiącach coraz częściej obserwujemy w Polsce ataki teleinformatyczne z użyciem telefonu lub internetu na osoby fizyczne, których celem jest pozyskanie danych dostępowych do kont bankowych, poprzez techniki manipulacyjne lub znane wcześniej ataki na urządzenia (komputer, smartfon) osób fizycznych. Informacje o skutecznych lub nieskutecznych próbach wyłudzeń danych dostępowych (loginu i hasła) do kont bankowych, ale także danych osobowych (Pesel, nr dok. tożsamości, itp.), pojawiają się także bardzo często w przestrzeni publicznej w programach telewizyjnych, radiowych oraz w prasie krajowej i lokalnej.

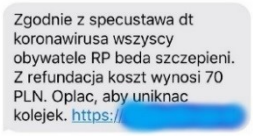
Celem przestępstwa jest zawsze albo pozyskanie poufnych informacji ofiary i/lub nakłonienie ofiary do wykonania określonych czynności (np. zainstalowania aplikacji dającej przestępcom zdalny dostęp do komputera czy telefonu komórkowego ofiary, wykonania przelewu, podanie adresu, nr konta, nr dowodu osobistego, itp.). Wykonując te czynności Klient naraża się na przejęcie kontroli nad urządzeniem i kontrolowanie go przez przestępców.

Cały atak jest zawsze precyzyjnie przygotowany i oparty o techniki manipulacji, zmierzające do wywarcia presji na rozmówcę, która ma na celu ujawnienie danych osobistych. Wiarygodność oszustów zwiększa fakt, że w celu uwiarygodnienia kontaktu, przestępcy potrafią na telefonie ofiary wyświetlić numer telefonu lub nazwę zaufanej instytucji, zaufanej osoby, ale także członka rodziny Klienta. Najczęściej są to próby wyłudzeń: na policjanta, na infolinię banku, na numer telefonu oddziału banku, na wnuczka, na ZUS, na firmę telekomunikacyjną, na dostawcę energii elektrycznej, na firmę ubezpieczeniową, na firmę kurierską, itp. Ze względu na wyświetlający się numer telefonu znanej instytucji odbiorca połączenia jest na początku całkowicie przekonany, że rozmawia z pracownikiem banku lub inną, godną zaufania, osobą.

KDBS Bank regularnie edukuje Klientów, poprzez: publikowanie pakietu informacji dotyczących bezpieczeństwa bankowania przez Internet przy uruchamianiu kanałów zdalnych, wysyłanie wiadomości na skrzynki mailowe oraz przez bankowość internetową i mobilną (do Klientów którzy wyrazili zgodę na otrzymywanie wiadomości od Banku). Regularnie także publikujemy informacje o zasadach cyberbezpieczeństwa, zarówno na stronie internetowej Banku, pod adresem: https://kdbs.com.pl/ostrzezenie-dla-klientow-kdbs-bank, jak również na odbiornikach telewizji bankowej w placówkach Banku. Szczegółowy wykaz rodzajów ataków socjotechnicznych na osoby fizyczne znajduje się nie tylko na stronach KDBS, ale także na stronie Związku Banków Polskich w zakładce: https://zbp.pl/dla-klientow/bezpieczne-bankowanie/Aktualnosci.

Zapobiegając takim sytuacjom w przyszłości, uprzejmie przypominamy, żeby:

1. Chronić swoje dane osobowe, w tym dowód osobisty i nr Pesel, poprzez nie publikowanie adresów w mediach społecznościowych, nie tracenie kontaktu wzrokowego z dowodem osobistym czy kartą płatniczą w momencie ich używania. Wszystkie te dane nie powinny być ujawniane, ponieważ rodzą potencjalne ryzyko ich wykorzystania przez przestępców.
2. Nie ujawniać prywatnych danych osobom dzwoniącym, nawet jeżeli na telefonie wyświetla się numer telefonu znanej instytucji, jak policji, infolinii banku, ZUS, czy gminy.
3. Nie ufać nieznanemu rozmówcy, który chce, aby podać poufne dane (w szczególności hasła, numery kart płatniczych, numery PIN), np. pod pretekstem: rozpracowania grupy przestępczej (tzw. metoda „na policjanta") lub sprawdzenia konta, potwierdzenia przelewu czy zwrotu środków (tzw. metoda „na pracownika banku").
4. Nie klikać w żadne linki, które znajdują się w przychodzących sms-ach, nawet, jeżeli instytucja która sms-a przysłała jest powszechnie znana. Kliknięcie w link może spowodować zainstalowanie w telefonie niebezpiecznego oprogramowania, które może ułatwić atak w przyszłości. Poniżej przykład SMS-a podszywającego się pod ministerstwo zdrowia, w związku z Covid:



   SMS-y z linkiem mogą przychodzić od firm kurierskich, Poczty Polskiej, sklepów internetowych, OLX, Vinted, allegro, innych znanych instytucji, ale również od osób które, posiadają nas w swoich kontaktach telefonicznych.
5. Nie klikać w linki zawarte w poczcie e-mailowej i nie odpowiadać na takie maile.
6. Uważać na fałszywe strony internetowe znanych sprzedawców artykułów konsumpcyjnych.
7. Nie przelewać środków pieniężnych na prośbę obcych nieznanych osób, na ich konta bankowe, nawet jeżeli byłoby to tylko przelanie środków w wysokości 1 zł.
8. Uważać na zbyt korzystne oferty sprzedaży dóbr konsumpcyjnych ogłaszane, w szczególności, na darmowych platformach i w mediach społecznościowych.
9. Uważać przy sprzedaży swoich własnych rzeczy (ubrań, sprzętu elektronicznego, innych) na darmowych portalach internetowych. Na prośby o: uwierzytelnienie pobranej aplikacji poprzez logowanie do bankowości internetowej lub kliknięcie w link wysłany przez nabywcę, natychmiast rozłączyć się i zgłosić na infolinię lub do placówki Banku. **Często niezbędne jest natychmiastowe zablokowanie konta bankowości elektronicznej i aplikacji mobilnej, co można zrobić poprzez infolinię Banku pod nr tel. 800-888-888.**
10. Nie skanować nieznanych kodów QR. To, że kod jest naklejony na urządzeniu, drzwiach zaufanej instytucji nie oznacza równocześnie, że jest to kod któremu możemy zaufać.
11. Nie przekazywać kodu BLIK obcej osobie.

12. Nie przekazywać danych karty bankowej, ani kodów 3D Secure, ponieważ mogą zostać użyte w Internecie. Dotyczy to również przekazywania takich danych dzieciom, wnukom, itp. które często nieświadomie padają ofiarą oszustów internetowych.
13. Nie ujawniać numeru konta bankowego, chyba, że znamy osobę i jej ufamy.
14. Chronić urządzenia osobiste jak: telefon komórkowy, tablet czy komputer, płatnym oprogramowaniem antywirusowym. Na bieżąco aktualizować systemy operacyjne w tych urządzeniach.
15. **W przypadku gdy rozmówca straszy, że zniknęły z konta bankowego środki finansowe lub że jest właśnie wykonywany przelew środków na inne konto (scenariusze takich rozmów są różne, ale zwykle polegają na straszeniu Klienta utratą pieniędzy z konta bankowego), absolutnie nie dawać wiary takim informacjom, natychmiast rozłączyć się i niezwłocznie, osobiście lub z użyciem innego telefonu skontaktować się z Bankiem (oddziałem lub infolinią**).

Prosimy, aby zachować daleko idącą czujność wobec każdej rozmowy, dotyczącej podania danych osobistych, szczególnie w sytuacji formułowania przez rozmówcę nietypowych scenariuszy czy zdarzeń, które wywołują silne emocje u odbierającego telefon. W takiej sytuacji należy natychmiast przerwać rozmowę.

Prosimy być pewnym, że bank, policjant, ZUS, firma kurierska, zakład energetyczny czy inna instytucja **nie zadzwoni sama do Klienta** (nawet jeżeli na ekranie wyświetla się prawdziwy numer telefonu tych instytucji), **żeby prosić o podanie**: prywatnego loginu i hasła do bankowości, danych dowodu osobistego, miejsca zamieszkania, Pesel, itp., **jak również nie poprosi o wypłacenie, czy przelanie środków z konta bankowego. Tym bardziej nikt z Banku nie poprosi o zainstalowanie na komputerze lub komórce programu lub kliknięcie w link przesłany sms-em.**

Jeszcze raz przypominamy, w razie jakichkolwiek wątpliwości, na przyszłość zawsze może Pani/Pan w każdej chwili zgłosić się osobiście lub telefonicznie do pracownika jednostki Banku, który posłuży wiedzą i wsparciem.

W razie wątpliwości, proszę kontaktować się z Dyrektorem Oddziału lub Anną Małas – Pełnomocnikiem Zarządu ds. Bezpieczeństwa Informacji tel. do kontaktu 54/253-21-51 lub tel. kom. 507-702-724.

Z poważaniem

Kujawsko-Dobrzyński
Bank Spółdzielczy