Urząd Ochrony Konkurencji i Konsumentów

STRACISZ DANE, STRACISZ PIENIĄDZE! – JAK NIE PAŚĆ OFIARĄ OSZUSTÓW

- **Prezes UOKiK Tomasz Chróstny w kampanii „Stracisz dane, stracisz pieniądze!" ostrzega konsumentów.**
- **Podejrzane SMS-y zawierające linki do płatności, dopłaty do przesyłek czy namowy do pobrania aplikacji. Kontakt telefoniczny i podawanie się ze pracownika banku, policji lub urzędu. Wszystko to w atmosferze presji oraz zagrożenia, bez czasu na zastanowienie i obiektywną ocenę sytuacji.**
- **Uwaga! UOKiK, eksperci i media - które już włączyły się w kampanię - alarmują: to może być próba wyłudzenia danych.**

[Warszawa, 14 grudnia 2022 r.] - *Konsument odbiera połączenia telefoniczne, SMS-y albo maile z linkiem do płatności. Do tego dochodzą strach o utratę pieniędzy, ponaglanie do jak najszybszego działania, podania danych. UOKiK w kampanii „Stracisz dane, stracisz pieniądze!" przypomina, że należy stosować zasadę ograniczonego zaufania przy udostępnianiu danych. Ostrzegamy przed groźbą utraty pieniędzy po podaniu przez konsumenta np. loginu i hasła do konta czy wejściu na podejrzaną stronę internetową. Utrata danych może prowadzić do kradzieży oszczędności całego życia. Każdy może paść ofiarą cyberoszustów, dlatego tak ważne jest jak najszersze informowanie konsumentów o zagrożeniach* – mówi Tomasz Chróstny, Prezes Urzędu Ochrony Konkurencji i Konsumentów.

Aby nie wpaść w pułapki zastawiane przez cyberprzestępców, UOKiK przygotował w ramach kampanii „Stracisz dane, stracisz pieniądze" dwa spoty. Od 5 grudnia są nieodpłatnie emitowane w mediach publicznych w oparciu o art. 31 c ustawy o ochronie konkurencji i konsumentów, a także przez nadawców komercyjnych - Radio ESKA, RMF FM, Radio ZET, Radio Centrum Rzeszów, Radio Kraków i Radio Olsztyn, którzy zgodzili się na wsparcie kampanii bez pobierania wynagrodzenia.

Spoty kampanii są dostępne na stronie Stracisz dane, stracisz pieniądze!. W materiałach pokazane są wybrane sytuacje, w których może dojść do wyłudzenia danych i kradzieży pieniędzy. Warto też odwiedzić strony uokik.gov.pl oraz finanse.uokik.gov.pl. Są tam dostępne między innymi - przygotowane przez UOKiK i Biuro Rzecznika Finansowego - odpowiedzi na najczęściej zadawane pytania dotyczące nieautoryzowanych transakcji: zakładka FAQ - finanse.uokik.gov.pl/faq/

- Przestępcy nieustannie udoskonalają sposoby oszustw. Obserwujemy z roku na rok coraz więcej prób wyłudzeń. Dotyczy to nie tylko fałszywych stron znanych instytucji (phishing), ale także wysyłania SMS-ów oraz wykonywania połączeń, technicznie podając się za kogoś innego (spoofing) – odbiorcy wyświetla się numer infolinii banku, zamiast prawdziwego numeru, z którego pochodzi połączenie. Skalę zjawiska pokazują nasze dane. W 2021 roku liczba zgłoszonych incydentów, polegających na próbie kradzieży danych, wzrosła trzykrotnie w porównaniu do poprzedniego roku. Realizując ataki, oszuści wykorzystują narzędzia zdalnego dostępu do pulpitu, niedoskonałości w budowie sieci telekomunikacyjnej, ale przede wszystkim proste sztuczki socjotechniczne, takie jak zastraszanie i zmuszanie do działania w pośpiechu - mówi Szymon Sidoruk, Analityk Zagrożeń, CERT Polska.

Kradzież danych przyjmuje różne formy, nieustannie się one zmieniają. Do najczęściej spotykanych należą:

1. **Podawanie się za pracownika banku, odwoływanie do cenionych instytucji – policji, urzędów**

Oszuści kontaktują się z klientami banków w różny sposób, najczęściej telefonicznie. Ich celem jest wyłudzenie pieniędzy. Przedstawiają się jako pracownicy banku, policji czy też instytucji finansowej. Zwykle informują o konieczności szybkich działań w celu ochrony środków na koncie lub możliwości otrzymania dodatkowych pieniędzy. Nakłaniają do podania loginu i hasła do konta. Zachęcają do zainstalowania oprogramowania, pozwalającego na zdalny dostęp do pulpitu w celu wykonania przelewu na konto, gdzie środki konsumenta będą rzekomo bezpieczne. Przestępcy często budują poczucie zagrożenia, nie dają właścicielowi konta czasu na zastanowienie, szczegółową analizę sytuacji.

Przypuszczasz, że wyłudzono twoje dane, pieniądze? Koniecznie:

- **skontaktuj się z bankiem, używając zweryfikowanego kanału kontaktu,**
- **zgłoś sprawę Policji.**

2. **Aplikacje do odbioru przesyłek, poczty głosowej, MMS-ów**

Cyberprzestępcy przesyłają SMS-y wzywające do działania, np. dopłaty do paczki, aby móc ją odebrać. Wiadomość SMS może również informować o otrzymaniu MMS-a albo wiadomości głosowej. Treść jest tak skonstruowana, aby przekonać odbiorcę, że musi niezwłocznie

kliknąć w link, by załatwić sprawę. Kliknięcie powoduje przeniesienie na fałszywą stronę. W celu wykonania rzekomej operacji użytkownik jest zachęcany do pobrania i zainstalowania aplikacji, która okazuje się być złośliwym oprogramowaniem.

Po pobraniu i zainstalowaniu takiej aplikacji przejmuje ona kontrolę nad urządzeniem. Jej odinstalowanie nie jest proste, a od momentu instalacji może wykradać dane z telefonu. Istnieje duże ryzyko kradzieży środków z konta w banku.

Otrzymałeś wiadomość SMS i zastanawiasz się czy twój telefon jest bezpieczny? Koniecznie sprawdź:

- **prześlij SMS do CERT Polska – numer 799 448 084,**
- **odczytałeś SMS-a, ale nie kliknąłeś w link – bądź ostrożny i nie klikaj w link,**
- **wszedłeś na stronę, ale nie pobrałeś aplikacji – bądź ostrożny, natychmiast zamknij stronę,**
- **pobrałeś aplikację, ale jej nie zainstalowałeś – nie instaluj, lecz usuń pobrany plik,**
- **zainstalowałeś aplikację - powinieneś niezwłocznie:**
  - włączyć tryb samolotowy w telefonie – złośliwe oprogramowanie nie będzie w stanie wysyłać SMS-ów i nawiązywać kontaktu z serwerami oszustów,
  - sprawdzić stan konta bankowego, czy nie doszło na nim do nieuprawnionych operacji - nie loguj się z zainfekowanego urządzenia, skorzystaj z innego. Jeżeli stwierdzisz kradzież środków, skontaktuj się z bankiem oraz zgłoś sprawę policji,
  - sprawdzić stan konta bankowego, czy nie doszło na nim do nieuprawnionych operacji. Nie sprawdzaj tego przez swój zainfekowany telefon. Jeżeli stwierdzisz kradzieży środków, skontaktuj się z bankiem oraz zgłoś sprawę policji,
  - zrobić kopię danych z telefonu - takich jak zdjęcia, czy pobrane dokumenty - korzystając np. z kabla USB,
  - przywrócić ustawienia fabryczne w telefonie. Prowadzi to do wykasowania wszystkich danych z telefonu, więc ważne jest wykonanie najpierw ich zapasowej kopii,
  - zmienić hasła do wszystkich kont, które były obsługiwane na telefonie.

Złośliwe oprogramowanie może wykradać kontakty w celu dalszych infekcji. Warto poinformować znajomych o ryzyku otrzymania SMS-ów ze szkodliwym oprogramowaniem.

3. **Płatność za gaz, prąd, telewizję**

Przestępcy wysyłają wiadomości SMS, zawierające informacje o rzekomej zaległej płatności za gaz, prąd, media. Grożą, że brak zapłaty spowoduje odłączenie energii elektrycznej, czy telewizji. Nalegają, aby uregulować należność wchodząc w link z SMS-a. Kliknięcie w niego może spowodować przekierowanie na fałszywą bramkę płatności, która wygląda jak prawdziwa usługa. Podane na tej stronie dane nie trafiają do banku, tylko do oszustów. W ten sposób zyskują dostęp do danych logowania do konta bankowego konsumenta, a następnie wykonują operacje w jego imieniu. To z kolei powoduje wysłanie SMS-ów z banku z kodami potwierdzającymi.

Zakłady energetyczne, gazowe wysyłają wiadomości SMS, w których przypominają o uregulowaniu zobowiązań. Proszą jednak o kontakt telefoniczny z Biurem Obsługi Klienta lub odwiedzenie e-BOK, gdzie klient ma swoje konto. Po zalogowaniu się konsument może sprawdzić stan konta i zdecydować w jaki sposób chce wnieść opłatę, np. zaległą płatność za prąd.

Podejrzewasz, że doszło do wyłudzenia twoich danych, pieniędzy? Niezwłocznie:

- **skontaktuj się ze swoim bankiem, używając zweryfikowanego kanału kontaktu,**
- **następnie zmień hasło do bankowości internetowej,**
- **prześlij SMS do CERT Polska – numer 799 448 084.**

Jeżeli doszło do wyłudzenia środków finansowych, należy to zgłosić policji.

- Stosowanie przez oszustów chwytów psychologicznych jest elementem przestępczej strategii. Kontaktują się i informują o rzekomym zagrożeniu zdrowia lub życia bliskiej osoby, próbie kradzieży środków z konta bankowego, czy pilnej potrzebie pomocy policji. Osoba zostaje osaczona przez przestępców, żeby nie mogła skontaktować się z rodziną, bankiem, policją. Ofiara oszustów nie ma czasu na zastanowienie, zweryfikowanie informacji. Racjonalne myślenie schodzi na dalszy plan. Dlatego tak ważne jest nieustanne piętnowanie tych praktyk i ostrzeganie. Trzeba wciąż przypominać, że pracownik banku nie poprosi klienta o podanie loginu i hasła do konta. Warto zachowywać ostrożność, nie działać pod wpływem impulsu, zweryfikować informacje w kilku źródłach, a w razie potrzeby

zadzwonić pod numer 112 lub powiadomić najbliższą jednostkę organizacyjną Policji – mówi młodszy inspektor Wanda Mende, Naczelnik Wydziału Profilaktyki Społecznej Biura Prewencji Komendy Głównej Policji.

Prezes UOKiK zaprasza kolejne media, organizacje społeczne i instytucje do włączania się w kampanię „Stracisz dane, stracisz pieniądze!". Komplet materiałów można znaleźć na stronie Stracisz dane, stracisz pieniądze!

Pomoc dla konsumentów:

Tel. 801 440 220 lub 222 66 76 76 – infolinia konsumencka
E-mail: porady@dlakonsumentow.pl
Rzecznicy konsumentów – w twoim mieście lub powiecie
Rzecznik Finansowy – po odrzuceniu reklamacji przez instytucję finansową

Dodatkowe informacje dla mediów:

Biuro Prasowe UOKiK
pl. Powstańców Warszawy 1, 00-950 Warszawa
Tel.: 22 55 60 246
E-mail: biuroprasowe@uokik.gov.pl
Twitter: @UOKiKgovPL
Znajdziesz nas również na Instagramie: @uokikgovpl