UWAGA NA OSZUSTÓW

WYKORZYSTUJĄCYCH TZW. SPOOFING/PHISHING

BĄDŹ CZUJNY, A BĘDZIESZ BEZPIECZNY !

„NIE DAJ SIĘ ZŁOWIĆ CYBERATAKOM „

Dzwoni do ciebie pracownik Banku, ZUS, BIK czy Policja ? Uważaj na oszustwa spoofingu telefonicznego - podrabiania połączeń telefonicznych polegające na podszyciu się pod czyjś numer telefonu (Abonent A) i wykonaniu połączenia telefonicznego do innej osoby (Abonent B). Zapamiętaj jedno! **Nie ufaj temu co pojawi się na ekranie Twojego smartfona**, kiedy ktoś do ciebie dzwoni lub pisze SMS. Zachowaj ostrożność zwłaszcza wtedy kiedy dzwoni do Ciebie jakaś instytucja np. (Bank, Policja). Jeśli nie jesteś pewien czy rozmawiasz z autentycznym pracownikiem instytucji, natychmiast rozłącz połączenie telefoniczne. Rozłączenie połączenia uchroni cię przed próbą oszustwa.

Komenda Miejska Policji w Tarnowie

WIĘCEJ INFORMACJI NA

fb.com/tarnowska.policja | tarnow.policja.gov.pl

PODEJRZANY SMS LUB MAIL

ZGŁOŚ INCYDENT

Oszuści codziennie wysyłają SMS-y o różnej treści np.:

- „wymagana dopłata do paczki",
- „odbiór środków od kupującego",
- „BLIK. Ktoś wyslal ci przelew na telefon 450 zł, skorzystaj z poniższego linku do odbioru środków (link)".

Zespół CERT Polska apeluje, gdy otrzymasz podejrzaną wiadomość SMS przed kliknięciem w link lub przesłaniem pieniędzy, wstrzymaj się daj sobie kilka minut na zastanowienie i przekazanie podejrzanej wiadomości SMS.

Zachowaj szczególną ostrożność w przypadku podejrzanych linków wysyłanych przez e-mail, SMS lub wiadomości z popularnych komunikatorów internetowych i mediów społecznościowych. Jeśli nie masz pewności, że nadawca wiadomości jest prawdziwy, nie klikaj w żadne linki oraz nie pobieraj załącznika, zgłoś incydent do CERT Polska.

PRZEŚLIJ PODEJRZANY SMS DO CERT na numer

+48 799 448 084

NASK CERT.PL

wszystkie podejrzane incydenty można zgłaszać za pomocą formularza na stronie incydent.cert.pl lub mailowo cert@cert.pl

NASK CERT.PL

Należy pamiętać, że w każdej wojewódzkiej komendzie Policji działa Wydział do Walki z Cyberprzestępczością.

– Policja – Biuro do Walki z Cyberprzestępczością: cyber-kgp@policja.gov.pl

ZADBAJ O CYBERBEZPIECZEŃSTWO SWOICH BLISKICH.

NASK CERT.PL | NEBEZPIECZNIK.PL | POLICJA | Aplikacja mobilna „Moja Komenda" Kontakt z policją i z dzielnicowymi na wyciągnięcie ręki | Komenda Miejska Policji w Tarnowie

Apelujemy o ostrożność i dokładne czytanie wiadomości od rzekomych operatorów, firm kurierskich czy banków. Poświęć kilka sekund na zweryfikowanie, jaką transakcję masz zaakceptować. Zdrowy rozsadek może uratować ciebie przed utratą pieniędzy. Liczba oszustw internetowych i ataków telefonicznych stale utrzymuje się na wysokim poziomie. Na chwilę obecną jesteś najlepszą bronią w ich wykrywaniu i zatrzymywaniu. Nie bądź obojętny, chroń siebie i swoich bliskich!

ZAPAMIĘTAJ ZALECENIA I OSTRZEŻENIA:

1. Zachowaj ostrożność w kontaktach telefonicznych z nieznajomymi, oszust może podszywać się za pracownika banku czy policjanta- zweryfikuj jego tożsamość dzwoniąc na infolinię, jeśli masz obawę natychmiast rozłącz się!. Nigdy nie ufaj wyświetlanemu identyfikatorowi osoby dzwoniącej. Cyberoszuści często fałszują wyświetlany numer tak, by wyglądał na pochodzący od prawdziwej organizacji i nie wzbudzał Twoich podejrzeń.
2. Chroń swoje dane oraz kontakty. Podczas logowania do aplikacji czy portali społecznościowych używaj unikatowych haseł (niepowtarzalnych i silnych), korzystaj z weryfikacji dwuetapowej to podwójne sprawdzenie tożsamości (uwierzytelniania).Polecamy korzystanie z menagera haseł.
3. Nigdy nie loguj się do bankowości internetowej z linku, który przyszedł do Ciebie mailem lub SMS-em, ani poprzez link z wyszukiwarki. Wpisuj adres strony logowania ręcznie lub korzystaj z przycisku logowania na oficjalnej stronie banku.
4. Nigdy nie przekazuj nikomu swoich danych do logowania (login i hasło)w internetowym systemie bankowości elektronicznej, nawet jeśli rozmawiasz z pracowaniem banku czy policjantem. Pamiętaj, że pracownik banku podczas rozmowy telefonicznej nigdy nie poprosi Cię o podanie haseł dostępu, kodów PIN/SMS lub innych danych pozwalających na dokonanie transakcji.
5. Nigdy nie instaluj dodatkowej aplikacji czy oprogramowania na urządzeniach, z których logujesz się do bankowości elektronicznej. Powinieneś pamiętać, że podczas rozmowy telefonicznej pracownik bank nigdy nie wymaga od nas instalowania jakiegokolwiek oprogramowania. Jeśli osoba podająca się za pracownika banku wymaga od nas zainstalowania oprogramowania (np. AnyDesk, TeamViewer), które umożliwia zdalny pulpit na obsługiwanym urządzeniu, zawsze w takiej sytuacji rozłącz się i najlepiej z innego aparatu telefonicznego zadzwoń do biura obsługi klienta banku, zgłoś taki incydent !
6. Nigdy nie potwierdzaj (autoryzuj) transakcji , których sam nie wykonujesz. Nie podawaj nikomu żadnych kodów autoryzacyjnych (np. BLIK) w przypadku kiedy ktoś do Ciebie dzwoni.

7. Sprawdzaj adresy stron www, na których się logujesz, oraz ważność ich certyfikatów. Adres strony logowania powinien zaczynać się od https (oznacza to bezpieczne połączenie internetowe).
8. Nigdy nie loguj się przez publiczną, niezabezpieczoną sieć WI-FI lub hotspot do bankowości internetowej czy aplikacji mobilnej oraz nie loguj się do bankowości na urządzeniach publicznie dostępnych, np. w hotelach, kafejkach itp.
9. Zapamiętaj aby regularnie aktualizować oprogramowanie na twoim komputerze i smartfonie (system, aplikacje, przeglądarki, antywirusy).
10. Sprawdź wyciek danych. Chcesz się dowiedzieć czy twój adres mailowy bądź nr telefonu został wykradziony?
    Skorzystaj ze strony https://haveibeenpwned.com/ na której darmowo można sprawdzić czy nasz adres mailowy i hasło nie zostały wykradzione. Jeśli twoje dane wyciekły niezwłocznie, dokonaj zmiany haseł do aplikacji czy portali społecznościowych.
11. Zawsze zachowaj zdrowy rozsądek!. Najprostszym sposobem obrony przed atakami socjotechnicznymi cyberprzestępców jest po prostu zdrowy rozsądek. Jeśli coś wydaje się podejrzane albo ma się co do tego złe przeczucia, to może być atak. Częste oznaki ataku socjotechnicznego to:

- wywoływanie wrażenia, że sprawa jest niezwykle pilna. Nacisk, aby podjąć bardzo szybką decyzję (np. informacje, że włamano się na twoje konto bankowe, bądź usiłowano dokonać wypłaty z twojego konta),pamiętaj - odrzuć pośpiech!
- prośba o informację, do której ta osoba nie powinna mieć dostępu (np. rzekomy pracownik banku prosi cię o podanie login i hasła do twojej bankowości elektronicznej), pamiętaj również aby nie podawać swojego nr PESEL, nazwiska panieńskiego matki, numeru karty bankomatowej, daty jej ważności oraz kodu weryfikacyjnego umieszczonego na odwrocie blankietu Kod CVC/CVV.
- żądania ominięcia bądź zignorowania zasad lub procedur bezpieczeństwa (np. rzekomy pracownik banku namawia cię do zainstalowani aplikacji AnyDesk)
- coś jest zbyt piękne, by było prawdziwe. Typowy przykład stanowi informacja o wygranej na loterii (pomimo braku udziału), (np. Jeśli otrzymałeś SMS, np. o treści: BLIK. Ktos wyslal ci przelew na telefon 450zł, skorzystaj z poniższego linku do odbioru środków [LINK]), pamiętaj nigdy nie klikaj w link.
- częste ataki socjotechniczne wykonywane są przez osoby posługujące się łamaną polszczyzną, (np. rzekomy pracownik banku dzwoni do ciebie i łamaną polszczyzną pytała, czy potwierdzasz transakcję wykonywaną kilak sekund temu, której ogóle nie wykonywałeś).

„NIE DAJ SIĘ ZŁOWIĆ CYBERATAKOM„

SPOOFING

tak naprawdę, fachowa nazwa tego ataku to CallerID Spoofing. Polega on na podszyciu się pod czyjś numer telefonu (Abonent A) i wykonaniu połączenia telefonicznego do innej osoby (Abonent B).

PHISHING

to metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji (np. danych logowania, danych karty kredytowej), zainfekowania komputera szkodliwym oprogramowaniem czy też nakłonienia ofiary do określonych działań.

MENAGER HASEŁ

jest to program komputerowy bądź aplikacja na smartfon, która generuje losowo unikatowe hasła oraz przechowuje je w bezpieczny , szyfrowany sposób w pamięci komputera lub telefonu. Pamiętajmy zawsze o tworzeniu niepowtarzalnego i silnego hasła dla każdego konta oraz aplikacji, z których korzystasz.

WERYFIKACJA DWUETAPOWA

zwana też uwierzytelnianiem dwuskładnikowym, to łatwe w konfiguracji i skuteczne narzędzie, które możesz wykorzystać, by chronić swoje konta w sieci. Weryfikacja dwuetapowa zapewnia dodatkową warstwę ochrony. Nawet jeśli cyberprzestępca ukradnie twoje hasło, nie uzyska dostępu do twego konta. Gdy jest to możliwe, włącz weryfikację dwuetapową na wszystkich kontach, które ją oferują. To jeden z najlepszych sposobów, by chronić siebie w sieci.

BLIK

system płatności mobilnych uruchomiony przez sieć polskich banków. Umożliwia użytkownikom smartfonów dokonywanie płatności bezgotówkowych w sklepach stacjonarnych i internetowych, wypłacanie i wpłacanie gotówki w bankomatach oraz dokonywanie przelewówi generowanie czeków z cyfrowym kodem.

Komenda Miejska Policji w Tarnowie

POLICJA

NSZZP