# Pamiętaj o bezpieczeństwie w bankowości internetowej!

BGK
BANK GOSPODARSTWA KRAJOWEGO

W związku z rosnącą liczbą zagrożeń wpływających na bezpieczeństwo aplikacji internetowych, pragniemy zwrócić Państwa szczególną uwagę na tematykę bezpieczeństwa systemu bankowości internetowej.

## Z jakimi zagrożeniami mamy do czynienia?

### ZAŁĄCZNIK DO WIADOMOŚCI ZE ZŁOŚLIWYM OPROGRAMOWANIEM CLIPBANKER

Ostrzegamy przed nowym rodzajem ataku, na klientów korzystających z bankowości internetowej. Atak jest przeprowadzany z wykorzystaniem rozsyłanych wiadomości o tytule „gdzie realizacja zamówienia!?!" i polega na przesłaniu załącznika w formie pliku np. „przelew.exe", którego ikona może sugerować, że jest to dokument PDF. Próba otwarcia załącznika powoduje uruchomienie złośliwego programu, który podmieni 26 cyfrowy numer rachunków.

Zalecenie:

- **nie otwieraj przesyłek poczty elektronicznej niewiadomego pochodzenia oraz załączonych do nich plików lub linków, szczególnie w przypadkach gdyby wskazywały na okoliczności zdarzeń, które nie miały miejsca z Państwa udziałem,**
- **sugerujemy, by przed autoryzacją i przed wysłaniem przelewu, zawsze sprawdzić czy numer rachunku odbiorcy przelewu jest prawidłowy porównując go z dokumentem źródłowym.**

### UKRYTE ZŁOŚLIWE OPROGRAMOWANIE

Przestrzegamy przed pochopnym otwieraniem wiadomości pochodzących z niewiadomego źródła oraz załączonych do e-maili plików lub linków, które mogą zawierać ukryte złośliwe oprogramowanie. Dodatkowo, zalecamy ostrożność, gdyż świeżo spreparowany przez cyberprzestępców kod złośliwy może **nie być zidentyfikowany** przez program antywirusowy, ponieważ informacja o nim może nie znajdować się jeszcze w bazie systemu. Przestępcy wykorzystują socjotechnikę, której celem jest wywołanie u odbiorcy wiadomości zainteresowania lub nawet niepokoju, który sprawi, że odbiorca otworzy wiadomość i przesłane wraz z nią załączniki lub linki. Dołączone do takiego maila pliki z reguły zawierają złośliwe oprogramowanie, a ich opis oraz umieszczona w nich ikona dokumentu sugeruje inne przeznaczenie.

Ostrzegamy przed fałszywymi wiadomościami e-mail, w których hakerzy podszywają się pod różne firmy lub bank (np. T-Mobile, Poczta Polska, Orange, Play itp.) i informują o rzekomej płatności lub ważnej informacji, którą należy uregulować z tytułu rzekomej faktury za telefon lub z tytułu oczekującej przesyłki kurierskiej albo zalogować się do systemu bankowego.

Opierając się na zaufaniu klienta do znanej firmy pod którą się podszywają, a dodatkowo na niepokoju związanym z rzekomą płatnością do uregulowania, przestępcy nakłaniają klienta do otwarcia załącznika do e-maila rzekomo zawierającego szczegóły zaległej płatności.
W rzeczywistości jednak, otwarcie załącznika nie prezentuje żadnych dodatkowych informacji, a jedynie infekuje komputer na którym załącznik jest otwierany złośliwym oprogramowaniem mogącym skutkować kradzieżą danych poufnych klienta, a przede wszystkim pojawianiem się oszukańczych komunikatów podczas logowania do bankowości elektronicznej z zainfekowanego komputera, autoryzując nieświadomie przestępczy przelew z własnego rachunku.

Zalecenie:

- **nie otwieraj przesyłek poczty elektronicznej niewiadomego pochodzenia oraz załączonych do nich plików lub linków, szczególnie w przypadkach gdyby wskazywały na okoliczności zdarzeń, które nie miały miejsca z Twoim udziałem,**
- **dokonuj regularnej – okresowej, archiwizacji własnych zasobów danych na innych (zewnętrznych) nośnikach informacji.**

## ATAK PHISHINGOWY

Ostrzegamy przed nową formą ataku phishingowego, w którym przestępcy wysyłają wiadomości za pośrednictwem poczty elektronicznej o „zidentyfikowaniu szeregu błędów w informacjach zapisanych na koncie". Przestępcy w celu uwiarygodnienia tej tezy podają szereg okoliczności, które mogą być tego przyczyną. Odwołując się do możliwości wadliwego funkcjonowania serwisu bankowości internetowej proszą o podanie innych danych poufnych związanych z funkcjonowaniem systemu.

W związku z powyższym informujemy, że **bank nigdy nie wysyła wiadomości z prośbą o przekazanie informacji poufnych** związanych z korzystaniem z jakiegokolwiek instrumentu płatniczego (bankowości internetowej, kart płatniczych, bankowości telefonicznej itp.).

**Zalecenie:**

- **w przypadku otrzymania tego typu wiadomości bezzwłocznie skontaktuj się z bankiem oraz nie otwieraj załączonych do wiadomości plików lub linków, gdyż może to grozić zainfekowaniem komputera złośliwym oprogramowaniem.**

## PODMIANA NUMERU RACHUNKU

Ostrzegamy przed nowym rodzajem ataku, przeprowadzanym z wykorzystaniem **trojana Banatrix**. Atak polega na przeszukiwaniu przez trojan pamięci procesów przeglądarek internetowych: Chrome, Internet Explorer, Firefox oraz Opera w celu znalezienia **ciągu liczb, który odpowiada numerowi rachunku bankowego, a następnie zamianie go na inny numer rachunku podstawiony przez przestępców.**

W efekcie, na stronach internetowych banków zostają zamienione wszystkie numery polskich rachunków bankowych. Osoba, która nie zauważy tej zmiany może przelać środki na inny rachunek bankowy wykorzystywany przez hakerów. Szczegóły działania trojana Banatrix opisane zostało na stronie: http://www.cert.pl/news/8999.

Podmiana właściwego numeru rachunku może również nastąpić w wyniku kradzieży identyfikatora i hasła dostępu do bankowości internetowej. Dzięki temu złodziej może modyfikować w dowolnym momencie numery rachunków docelowych w zdefiniowanych wcześniej przelewach i zdefiniowanych kontrahentach. Także w przypadku korzystania przez Klienta z metody kopiuj / wklej, w momencie kopiowania (zapamiętywania) numeru rachunku np. z faktury otrzymanej drogą elektroniczną, a następnie wklejania tegoż w formatkę przelewu, może nastąpić podmiana numeru NRB na inny.

**Zalecenie:**

- **przed autoryzacją i przed wysłaniem przelewu, zawsze sprawdź czy numer rachunku odbiorcy przelewu jest prawidłowy porównując go z dokumentem źródłowym.**

## Jak się bronić?

Stale pracujemy nad rozwiązaniami mającymi chronić finanse naszych Klientów i staramy się, aby były one zgodne z najnowszymi standardami bezpieczeństwa. **Pamiętaj jednak, że to od Ciebie zależy, czy będziesz z nich korzystał we właściwy sposób.**

### Zasady bezpiecznego korzystania z bankowości internetowej:

- sprawdzaj przed autoryzacją i przed wysłaniem przelewu, czy numer rachunku odbiorcy przelewu jest prawidłowy porównując go z dokumentem źródłowym;
- sprawdzaj czy strona do logowania posiada odpowiedni adres: https://www.bgk24biznes.pl/pl oraz czy połączenie z Systemem jest szyfrowane (adres URL witryny powinien rozpoczynać się od https:// i wyświetla się ikona kłódki);
- nie podawaj poufnych informacji na stronach np. przypominających swoim wyglądem strony banku;
- zawsze kończ pracę korzystać z polecenia „Wyloguj";
- nie otwieraj podejrzanych i niespodziewanych załączników z poczty e-mail od nieznanych nadawców;
- nie używaj do logowania adresu lub linku podesłanego w wiadomości e-mail;

- nie korzystaj z „obcych" komputerów oraz z „obcych" sieci udostępniających internet, np. sieć WiFi;
- zainstaluj na komputerze oprogramowanie antywirusowego uznanej firmy i dbaj o aktualizację programu antywirusowego, oprogramowania przeglądarki oraz systemu operacyjnego.

**Jeżeli zauważysz nietypowe działanie serwisu bankowości internetowej prosimy o kontakt z bankiem (BGK Linia: 801 66 76 55, (22) 596 59 00).**

**Dodatkowe źródła informacji:**

1. BGK opublikował „Zasady bezpiecznego korzystania z bankowości elektronicznej" na stronie www.bgk.pl
http://www.bgk.pl/bgk24-biznes-1/zasady-bezpiecznego-korzystania-z-systemow-bgk
http://www.bgk.pl/aktualnosci/28-01-2015-zasady-bezpiecznego-korzystania-z-bankowosci-elektronicznej-1
2. KNF - „Poradnik klienta usług finansowych - bezpieczeństwo finansowe w bankowości elektronicznej"
http://www.knf.gov.pl/Images/Bezp_finansowe_tcm75-39005.pdf
3. ZBP
http://www.zbp.pl/bezpieczny_bank
http://zbp.pl/dla-konsumentow/bezpieczny-bank/bankowosc-internetowa