

Uwaga na oszukańcze ogłoszenia związane z epidemią koronawirusa (COVID-19)

Komunikat Komendy Głównej Policji i FinCERT.pl – Bankowego Centrum Cyberbezpieczeństwa ZBP z dnia 15 marca 2020 r.

Wstęp – na główną stronę Instytucji publikującej

Wersja krótsza:

Komenda Główna Policji oraz FinCERT.pl – Bankowe Centrum Cyberbezpieczeństwa ZBP ostrzegają przed oszukańczymi ogłoszeniami związanymi np. potrzebą zapłaty za szczepionkę przeciwko koronawirusowi COVID-19, czy przejęciem przez NBP środków klientów zdeponowanych w bankach jako tzw. „rezerw krajowych NBP”.

Wersja dłuższa:

Komenda Główna Policji oraz FinCERT.pl – BCC ZBP ostrzegają przed oszukańczymi ogłoszeniami związanymi np. potrzebą zapłaty za szczepionkę przeciwko koronawirusowi COVID-19, czy przejęciem przez NBP środków klientów zdeponowanych w bankach jako tzw. rezerw krajowych NBP.

Ostrzegamy przed fałszywymi informacjami dotyczącymi epidemii koronawirusa (COVID-19) nakłaniającymi klientów banków do dokonywania transakcji finansowych. Niniejsze ostrzeżenie jest adresowane do klientów wszystkich polskich banków.

Jeśli podejrzewasz, że jesteś ofiarą internetowego oszustwa, zgłoś to jak najszybciej do swojego banku, najbliższej jednostce Policji a następnie zespołowi reagowania na incydenty CERT.PL (pod adresem <https://incydent.cert.pl/>). Wskazane powyżej instytucje przekażą Ci informacje na temat kolejnych kroków/działań.

Pamiętaj: w tym szczególnym okresie najskuteczniejszą metodą kontaktu z bankiem może okazać się przesłanie wiadomości e-mail. Ze względu na obostrzenia epidemiologiczne, które dotyczą także banków i ich pracowników czas połączenia telefonicznego z konsultantem może się wydłużyć. Staraj się zrozumieć tą sytuację. Twoje zgłoszenie mailowe będzie przeanalizowane i będą podjęte stosowne działania.

[Pełna wersja komunikatu – na dedykowanej podstronie Instytucji publikującej](#)

Uwaga na oszukańcze ogłoszenia związane z epidemią koronawirusa (COVID-19)

Komunikat
Komendy Głównej Policji i FinCERT.pl – Bankowego Centrum
Cyberbezpieczeństwa ZBP
z dnia 15 marca 2020 r.

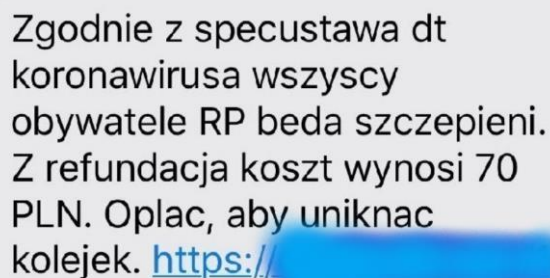
Komenda Główna Policji oraz FinCERT.pl – Bankowe Centrum Cyberbezpieczeństwa ZBP ostrzegają przed oszukańczymi ogłoszeniami związanymi np. potrzebą zapłaty za szczepionkę przeciwko koronawirusowi COVID-19, czy przejęciem przez NBP środków klientów zdeponowanych w bankach jako tzw. „rezerw krajowych NBP”.

Ostrzegamy przed fałszywymi informacjami dotyczącymi epidemii koronawirusa (COVID-19) nakłaniającymi klientów banków do dokonywania transakcji finansowych. Niniejsze ostrzeżenie jest adresowane do **klientów wszystkich polskich banków**.

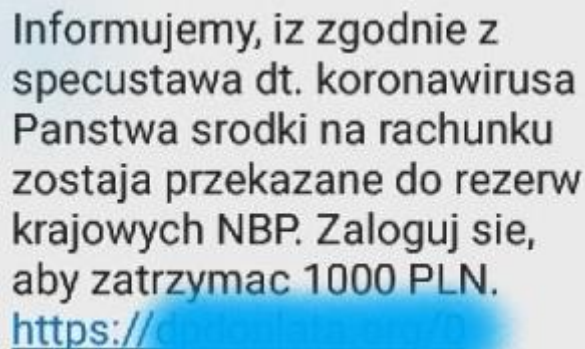
Przestępcy używają jako tła swojej działalności komunikaty i fałszywe informacje związane z epidemią koronawirusa (COVID-19). Podszywają się pod instytucje zaufania publicznego takie jak banki, urzędy państwowe, centralne oraz lokalne.

W przesyłanych wiadomościach zawarte są linki prowadzące do stron przestępców, których **jedynym zadaniem jest wyłudzenie loginów i haseł** do bankowości internetowej a także kodów autoryzacyjnych dających możliwość zatwierdzenia przelewów na rachunek przestępców. W niektórych przypadkach linki mogą prowadzić do stron **zawierających złośliwy kod powodujący przejęcie urządzenia klienta, na którym otrzymał wiadomość**.

Przykład fałszywej wiadomości sms:



Zgodnie z specustawa dt koronawirusa wszyscy obywatele RP beda szczepieni. Z refundacja koszt wynosi 70 PLN. Oplac, aby uniknac kolejek. [https://\[redacted\]](https://[redacted])



Informujemy, iz zgodnie z specustawa dt. koronawirusa Panstwa srodki na rachunku zostaja przekazane do rezerw krajowych NBP. Zaloguj sie, aby zatrzymac 1000 PLN. [https://\[redacted\]](https://[redacted])

Przykład fałszywej strony internetowej:

The screenshot shows the website of the Ministry of Health (mzg.gov.net). The header includes the Polish coat of arms, the text 'Ministerstwo Zdrowia', and 'Serwis Rzeczypospolitej Polskiej'. Below the header are buttons for 'Login' and 'Profil Zaufany'. The main content area is titled 'Wsparcie żywieniowe - Koronawirus'. It contains a paragraph stating that according to the Ministry's decision, every citizen is entitled to nutritional support in connection with the COVID-19 epidemic. Below this, it lists the support provided per person: 20 l of water, 3.5 kg of cereals, bread, potatoes, pasta, and rice; 2.5 kg of fruits in cans or jars and nuts; 4 kg of dried legumes and vegetables in cans or jars; 2.6 kg of milk and dairy products; and 1.5 kg of meat, fish, and eggs, or alternatively eggs in a package (fresh eggs last for a few days, frozen for a few months).

Źródło: zaufanatrzeciastrona.pl

Ofiary ataków, które nie zachowują ostrożności, mogą stracić swoje oszczędności. Ponadto, nieświadomi konsumenci ujawniając swoją tożsamość przestępcom mogą doprowadzić do wykorzystania jej do zawarcia w ich imieniu umów i w konsekwencji np. zaciągnięcia zobowiązań finansowych.

Rekomendacje:

- przypominamy, że jedynymi i prawdziwymi źródłami informacji są komunikaty przekazywane przez służby lub/i zamieszczane na oficjalnych stronach internetowych. W związku z koniecznością ograniczenia rozprzestrzeniania się choroby zakaźnej COVID-19, wywoływanej przez koronawirusa, na bieżąco komunikaty przekazują również przedstawiciele najwyższych władz Państwa w mediach masowych;
- sprawdź w pasku przeglądarki, czy jej adres internetowy zgadza się z adresem strony Twojego banku. Jeśli adres jest inny niż zwykle, nie loguj się na tej stronie - nie podawaj tam swoich danych oraz powiadom o tym swój bank;
- zawsze czytaj bardzo uważnie treść każdego SMSa z kodem autoryzacyjnym lub treść komunikatu autoryzacyjnego przesłanego za pośrednictwem bankowej aplikacji mobilnej. Jeśli twój bank to umożliwi zamień SMSy na autoryzację za pośrednictwem aplikacji mobilnej.

Jeśli podejrzewasz, że jesteś ofiarą internetowego oszustwa, zgłoś to jak najszybciej do swojego banku, najbliższej jednostce Policji a następnie zespołowi reagowania na incydenty CERT.PL (pod adresem <https://incydent.cert.pl/>). Wskazane powyżej instytucje przekażą Ci informacje na temat kolejnych kroków/działań.

Pamiętaj!!!

W tym szczególnym okresie najskuteczniejszą metodą kontaktu z bankiem może okazać się przesłanie wiadomości e-mail. Ze względu na obostrzenia epidemiologiczne, które dotyczą także banków i ich pracowników czas połączenia telefonicznego z konsultantem może się wydłużyć. Staraj się zrozumieć tą sytuację. Twoje zgłoszenie mailowe będzie przeanalizowane i będą podjęte stosowne działania.

Aby uzyskać więcej informacji, odwiedź stronę Komendy Głównej Policji – <http://www.policja.pl/pol/aktualnosci/186430,Uwaga-na-oszukancze-ogloszenia-zwiazane-z-epidemia-koronawirusa-COVID-19.html>

*FinCERT.pl – Bankowe Centrum Cyberbezpieczeństwa ZBP
Komenda Główna Policji*

Więcej porad znajdziesz:

<https://www.zbp.pl/dla-klientow/bezpieczne-bankowanie/bezpieczne-zakupy-przez-internet>

<https://www.zbp.pl/dla-klientow/bezpieczne-bankowanie/bankowosc-internetowa>

<https://www.zbp.pl/dla-klientow/bezpieczne-bankowanie/Aktualnosci>