

Ostrzegamy przed fałszywymi informacjami dotyczącymi epidemii koronawirusa (COVID-19) nakłaniającymi klientów banków do dokonywania transakcji finansowych.

Przestępcy używają jako tło 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.**

Przykłady oszukańczych wiadomości opublikowane są na stornach Policji w sekcji Aktualności dotyczą między innymi nieprawdziwej informacji o konieczności poniesienia kosztów szczepień, reglamentacji wypłat środków czy innych towarów.

#### **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. Zalecamy zamianę SMSy na autoryzację za pośrednictwem aplikacji mobilnej (CitiMobile Token).

Jeśli podejrzewasz, że jesteś ofiarą internetowego oszustwa, zgłoś to jak najszybciej do 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.