## KOMUNIKAT BANKU SPÓŁDZIELCZEGO W CYCOWIE

Szanowni Państwo,

mając na uwadze zdrowie i bezpieczeństwo naszych Klientów oraz Pracowników Banku, w związku z rozprzestrzenianiem się zagrożenia epidemicznego, obsługa kasowa w placówkach od dnia 20 marca br. będzie odbywać się:

**do godziny 14:00,**

**Zmiana w tym zakresie obowiązywać będzie do odwołania.**

W zastępstwie obsługi w Oddziale, a także ze względów bezpieczeństwa **uprzejmie zalecam** Państwu:

- **realizowanie płatności bez użycia gotówki np. za pomocą karty, poprzez bankowość elektroniczną oraz bankowość mobilną,**
- **wykonywanie przelewów oraz innych operacji bankowych w domu z użyciem bankowości internetowej.**

Przepraszamy za niedogodności i prosimy Państwa o wyrozumiałość, wobec tych nadzwyczajnych okoliczności.

Prezes Zarządu
Banku Spółdzielczego w Cycowie

---

## Uwaga na wyłudzenia "na koronawirusa"

Obecnie obowiązujący stan zagrożenia epidemicznego wykorzystują oszuści. To dla nich okazja do wyłudzenia loginów i haseł do bankowości za pomocą fałszywych stron płatności.

**Jak działają oszuści?**

- Używają komunikatów i fałszywych informacji związanych z epidemią koronawirusa. Podszywają się pod instytucje zaufania publicznego takie jak banki, urzędy państwowe, centralne oraz lokalne.

- Wysyłają wiadomości SMS, w których zawarte są linki prowadzące do fałszywych stron. Celem tego jest wyłudzanie 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. Powołują się na działania Rządu, Światowej Organizacji Zdrowia (WHO) lub powszechną akcję szczepień ochronnych.

- Przejmują konta np. na Facebooku, a następnie proszą naszych znajomych o przelanie pieniędzy powołując się na swoją nagłą trudną sytuację.

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

**Pamiętaj, że:**

- jedynymi i prawdziwymi źródłami informacji są komunikaty przekazywane przez służby lub/i zamieszczane na oficjalnych stronach internetowych. Na bieżąco komunikaty przekazują również przedstawiciele władz państwowych
- sprawdź w pasku przeglądarki, czy adres internetowy, na który się logujesz do bankowości internetowej, 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.

Więcej informacji o wyłudzeniach na stronie Związku Banków Polskich pod linkiem:
Więcej informacji na stronie www.zbp.pl

## 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 - 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.

Więcej informacji na stronie www.policja.pl