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 adresowym przeglądarki, czy adres internetowy, na który się logujesz do bankowości internetowej, zgadza się z adresem strony Twojego banku. Musi to być dokładnie taki adres: **https://ebank.bs.augustow.pl/** Jeśli adres jest inny niż zwykle, nie loguj się na tej stronie - nie podawaj tam swoich danych oraz powiadom o tym swój bank.
- Po wejściu na stronę logowania, jeszcze zanim podasz swój login i hasło, koniecznie zweryfikuj, czy strona jest zabezpieczona. Przede wszystkim sprawdź, czy adres zaczyna się od **https://**, a nie od **http://.** Brak literki „**s**” oznacza protokół niechroniony (od angielskiego słowa „secure” tzn. „bezpieczny”). Koniecznie też, wskaźnik myszy (strzałkę) ustaw na kłódce znajdującej się na pasku adresowym przeglądarki i sprawdź, czy strona, na której jesteś jest własnością **Banku Spółdzielczego w Augustowie**. Dopiero wtedy, gdy upewnisz się, że wszystkie informacje są zgodne z danymi wskazanymi przez Bank Spółdzielczy w Augustowie, możesz korzystać z systemów bankowości internetowej, w przeciwnym przypadku zgłoś incydent pracownikom Banku i nie korzystaj z takiej strony. Może być sfałszowana.
- zawsze czytaj bardzo uważnie treść każdego SMSa z kodem autoryzacyjnym.

Więcej informacji o wyłudzeniach na stronie Związku Banków Polskich pod linkiem:
https://zbp.pl/Aktualnosci/Wydarzenia/Uwaga-na-oszukancze-ogloszenia-zwiazane-z-epidemia-koronawirusa