

UWAGA NA FAŁSZYWE STRONY BANKÓW!

Data publikacji 11.09.2022

Blisko 30 tysięcy złotych stracił 52-latek z pow. łęczyńskiego, po tym jak poprosił brata aby ten zalogował się na jego konto bankowe. Po wpisaniu w wyszukiwarkę internetową nazwy banku mężczyzna kliknął w wyświetlony pierwszy link. Następnie został przekierowany na stronę banku. Po nieudanej próbie logowania wpisywał w wyskakujące okienka kody aktywacyjne, które otrzymał za pośrednictwem wiadomości sms. Po chwili okazało się, z konta szybkimi przelewami zostały wypłacone pieniądze. Apelujemy o ostrożność i zwracanie uwagi na poprawność adresu strony banku widniejącej w przeglądarce.



Do łęczyńskich policjantów zgłosił się 52-letni mieszkaniec gminy Puchaczów. Mężczyzna oświadczył, że poprosił swojego brata aby zalogował się do jego konta bankowego. Na komputerze w wyszukiwarkę internetową mężczyzna wpisał nazwę banku. Następnie kliknął w link, który wyświetlił się jako pierwszy. Po czym został przekierowany na stronę banku. Tam wpisał login i hasło. Logowanie nie powiodło się dlatego jeszcze kilkakrotnie podejmował próby logowania. W między czasie na telefon otrzymywał smsy z kodami aktywacyjnymi, które wpisywał w pojawiające się okienka na tej stronie. Dopiero kolejny sms dotyczący zmiany numery telefonu do kodów dał mu do myślenia, że coś dzieje się niepokojącego. Wówczas skontaktował się pracownikiem banku gdzie uzyskał informację, że z konta zostały wypłacone pieniądze w kwocie 29500 złotych. Wyjaśniamy okoliczności zdarzenia i apelujemy o ostrożność!

Korzystanie z bankowości elektronicznej wymaga ciągłej czujności i ostrożności. Oszuści nie próżnują i ciągle wymyślają metody aby uzyskać dostęp do naszych kont i ukraść z nich pieniądze między innymi tworząc fałszywe strony banków

Pamiętaj! Logując się na stronę banku nie korzystaj z linków do zalogowania, które pojawiają się w formie reklamy, zazwyczaj wyświetlają się jako pierwsze. Sprawdź poprawność adresu strony widniejącej w przeglądarce. Najlepiej wprowadź adres ręcznie. Sprawdź czy połączenie jest szyfrowane-symbol zamkniętej kłódki. Bardzo ważne jest uważne czytanie otrzymanych wiadomości sms do autoryzacji. Jeśli treść wiadomości budzi wątpliwości nie wpisuj hasła do autoryzacji. W przypadku pojawienia się jakichkolwiek nieprawidłowości natychmiast skontaktuj się z pracownikiem banku

starszy aspirant Magdalena Krasna