Bezpieczne logowanie to nie wszystko. Jak nie wpaść w pułapkę cyberprzestępców

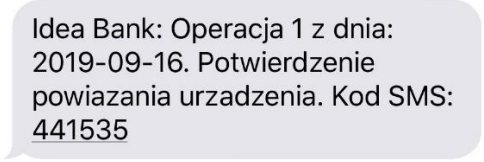
Jeśli jesteś Klientem Idea Banku, na pewno zauważyłeś już zmiany w sposobie logowania do bankowości internetowej i mobilnej. Zgodnie z zaleceniami unijnej dyrektywy PSD 2 zwiększyliśmy bezpieczeństwo logowania – więcej na ten temat przeczytasz tutaj.
Jednak dwuskładnikowe logowanie nie powinno uśpić Twojej czujności. Bo cyberprzestępcy nie śpią i mogą wykorzystywać nowe sposoby logowania do przeprowadzania zaawansowanych ataków phishingowych. Sprawdź, na co zwrócić uwagę, aby zachować bezpieczeństwo w sieci.

Nowe zagrożenia

W związku z nowym modelem logowania obowiązującym we wszystkich bankach w Polsce cyberprzestępcy mogą chcieć przekierować Klientów na strony wyglądające podobnie do strony Banku w celu wyłudzenia kodu SMS. Taki kod SMS jest wykorzystywany do kradzieży środków lub utworzenia odbiorcy zaufanego, do którego później przelewane są środki.
W celu przekierowania Klienta na fałszywą stronę przestępcy najczęściej infekują Twoje urządzenie lub korzystają z fałszywych bramek płatności (poniżej).

Jak się chronić?

Pamiętaj, by zawsze upewnić się, że przesłany kod autoryzacyjny faktycznie służy do zalogowania! Zawsze czytaj treść otrzymywanych SMS-ów. SMS potwierdzający powiązanie urządzenia będzie brzmiał następująco:



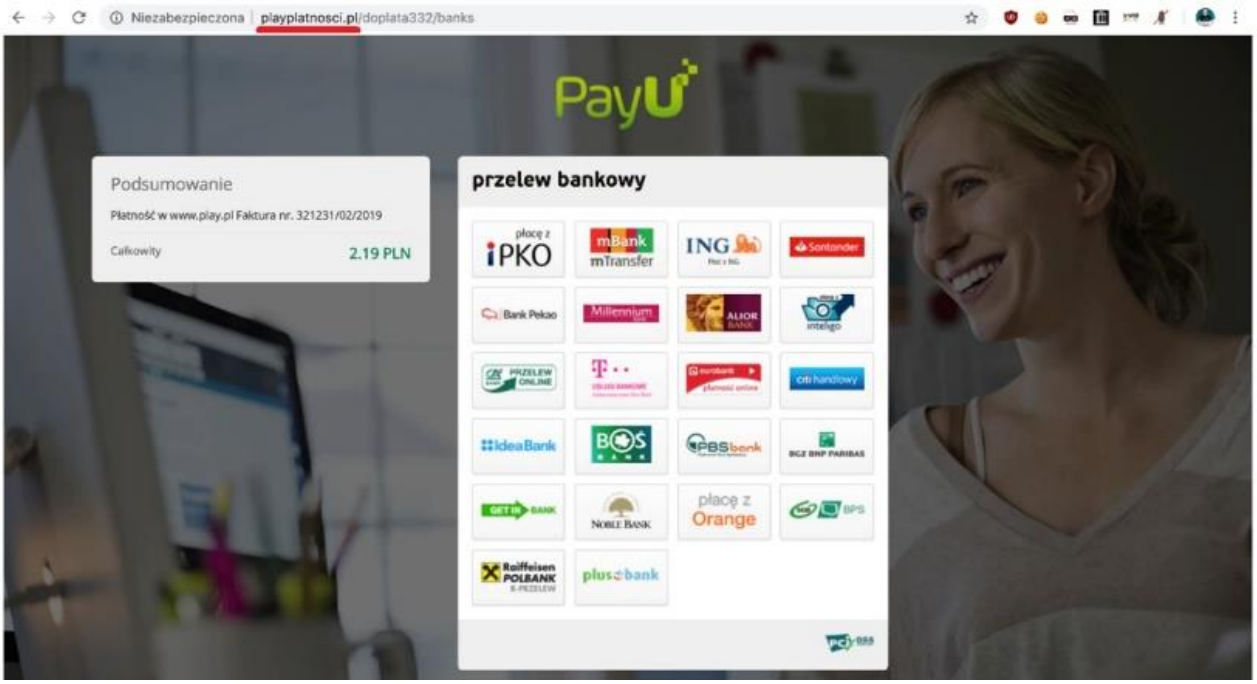
Podobnie w wypadku realizacji transakcji należy upewnić się, z jaką transakcją powiązany jest kod SMS. Zawsze weryfikuj:

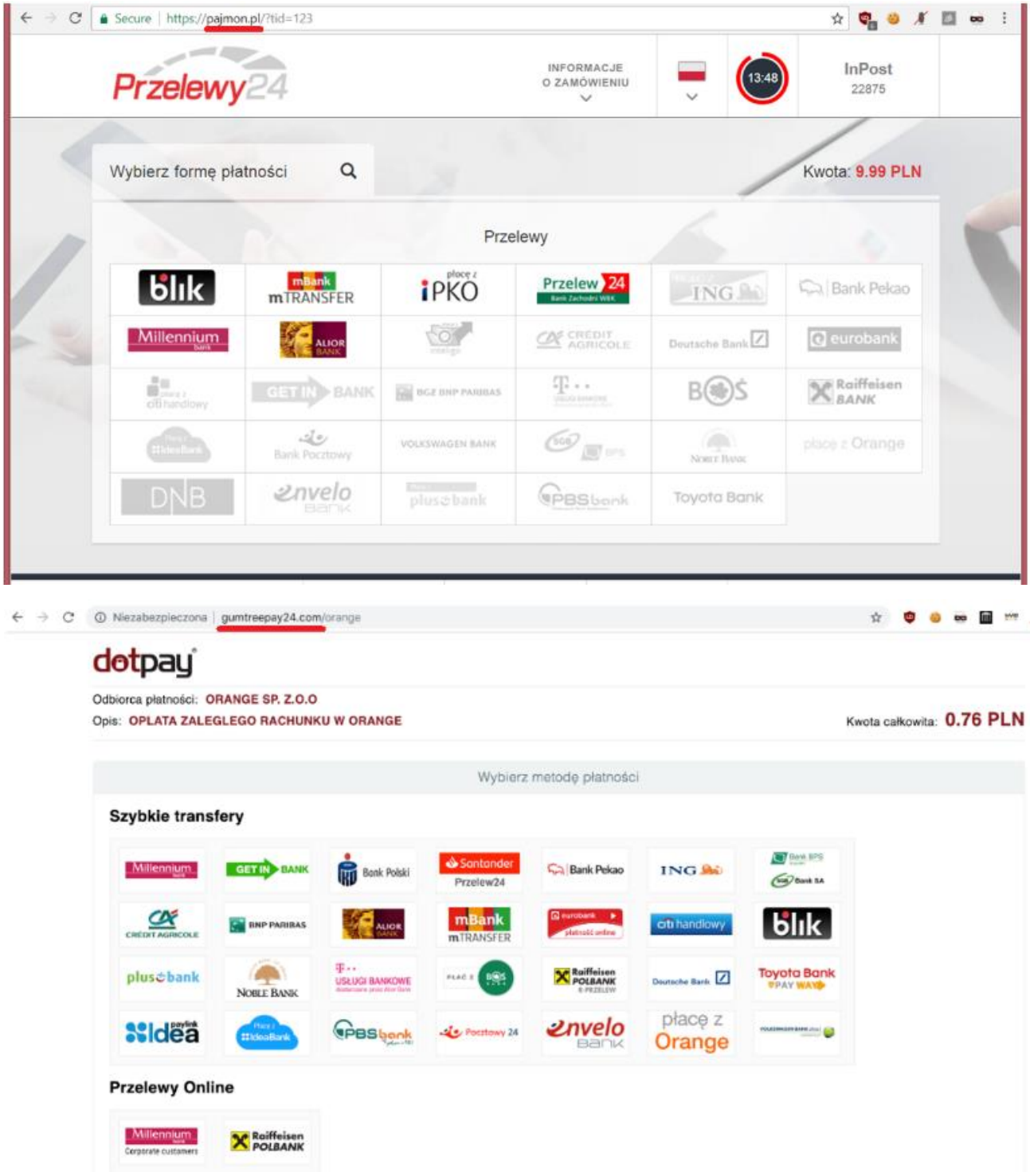
- rodzaj transakcji,
- kwotę transakcji,
- rachunek odbiorcy.

Pamiętaj – pracownicy Banku ani organy ścigania nigdy nie proszą o podanie haseł do bankowości ani haseł jednorazowych!

Fałszywe bramki płatności

Przypominamy również o tym, że przestępcy podszywają się pod serwisy oferujące szybkie przelewy (np. Dotpay, PayU czy Przelewy24). Podstawione strony wyłudzają loginy i hasła do bankowości internetowej oraz kody autoryzacyjne zatwierdzające przelewy.



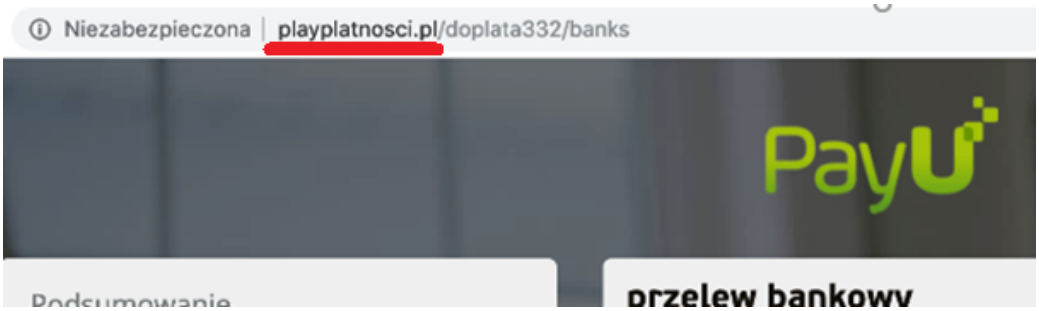


Przykłady fałszywych stron internetowych przygotowanych przez przestępców.

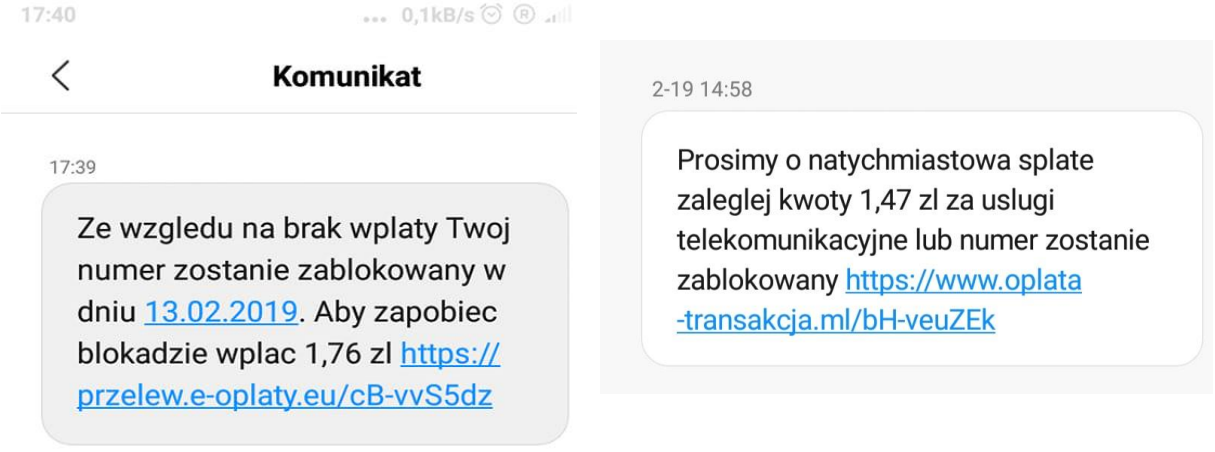
Przestępcy używają różnych sposobów, by ściągnąć użytkowników na fałszywe strony. Ofiary mogą być na nie kierowane przez linki w SMS-ach, komunikatorach internetowych lub poprzez fałszywe sklepy internetowe.

Aby nie paść ofiarą przestępców, należy zwrócić uwagę na kilka ważnych elementów:

- Zawsze sprawdzaj adres strony. Strona pośrednika płatności wygląda zazwyczaj identycznie jak oryginał, w niektórych przypadkach strona taka jest też zabezpieczona certyfikatem. Zwróć jednak uwagę, czy adres strony na pewno pokrywa się z rzeczywistym adresem pośrednika!



- Uważaj na wszystkie wiadomości o konieczności zapłaty lub dopłaty drobnych kwot (np. 0,76 PLN), zawierające link do strony udającej pośrednika płatności. Firmy praktycznie nigdy nie przesyłają takich SMS-ów! Przed wykonaniem przelewu skontaktuj się z firmą, która figuruje jako nadawca wiadomości (np. operator telekomunikacyjny, sklep czy serwis internetowy).



- Jeśli strona prosi o login i hasło do bankowości internetowej, sprawdź w pasku przeglądarki, czy jej adres internetowy zgadza się z adresem strony Idea Banku. Jeśli adres jest inny niż zwykle, nie loguj się na tej stronie oraz nie podawaj tam swoich danych.
- Nigdy nie otwieraj załączników lub odnośników z wiadomości e-mail, których się nie spodziewasz.

W wypadku jakichkolwiek wątpliwości zalecamy bezpośredni kontakt z infolinią Banku pod numerem 22 101 10 10.

Więcej informacji na temat bezpieczeństwa znajdziesz zawsze na www.ideabank.pl/bezpieczenstwo.