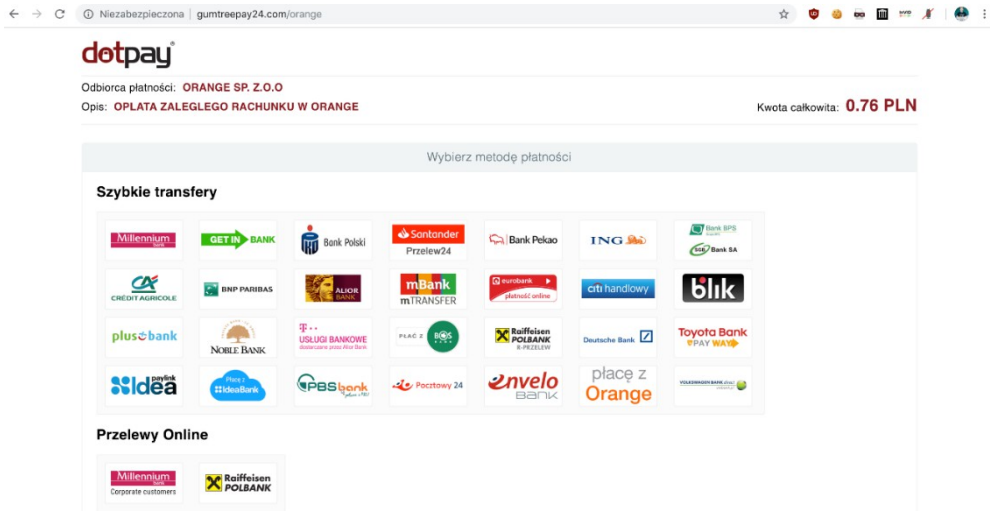
Uwaga na fałszywe strony udające pośredników szybkich płatności

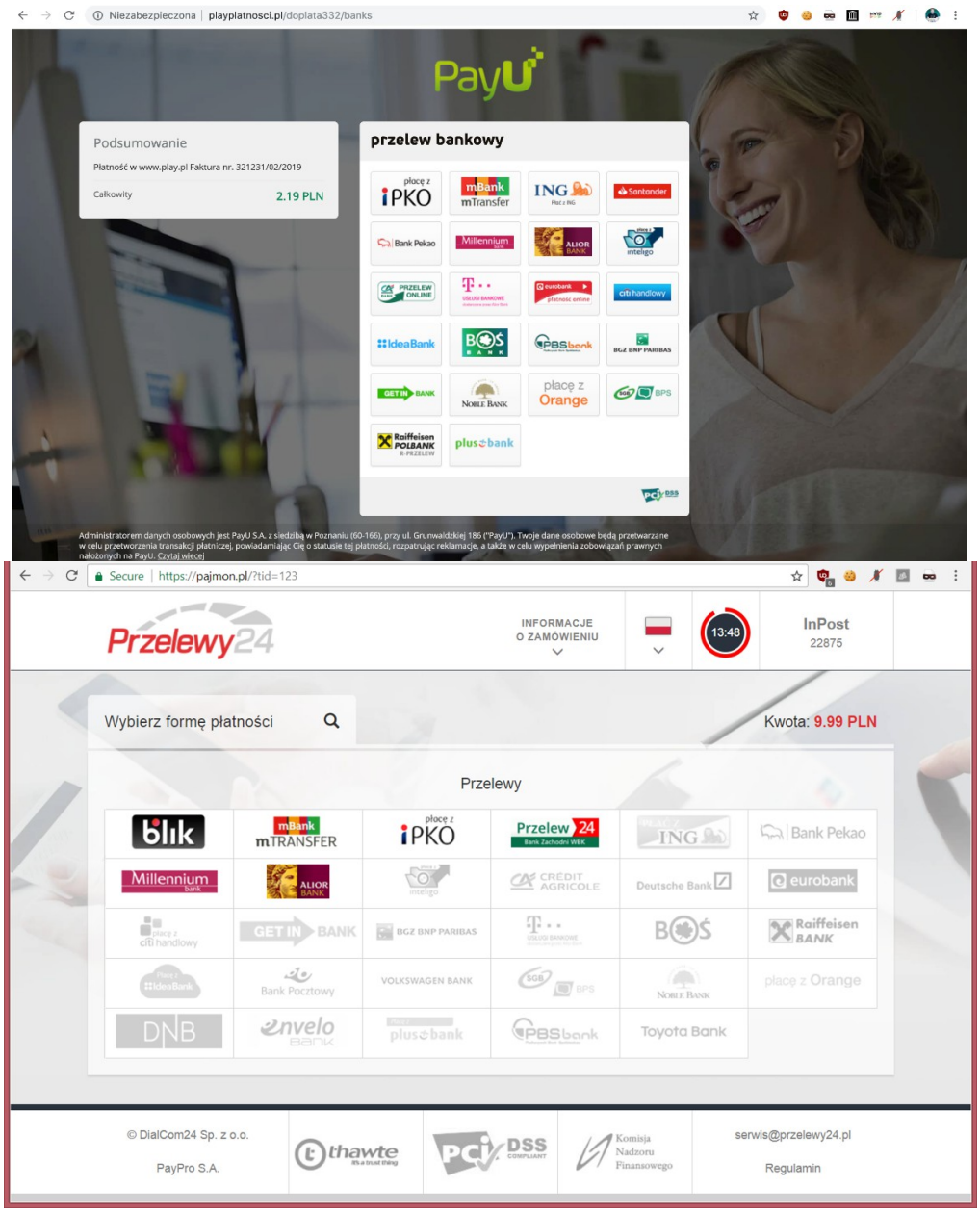
Komunikat
Prokuratury Krajowej
Komendy Głównej Policji
Urzędu Ochrony Konkurencji i Konsumentów
Europejskiego Centrum Konsumenckiego
FinCERT.pl – Bankowego Centrum Cyberbezpieczeństwa ZBP
z dnia 15 maja 2019 r.

Ostrzegamy przed fałszywymi stronami udającymi pośredników szybkich płatności. Na atak narażeni są użytkownicy bankowości internetowej i mobilnej robiący zakupy przez internet.

Przestępcy podszywają się pod serwisy oferujące szybkie przelewy (np. Dotpay, PayU, czy Przelewy24). Podstawione strony przestępców wyłudzają loginy i hasła do bankowości internetowej oraz kody autoryzacyjne zatwierdzające przelewy.

Przykłady fałszywych stron internetowych przygotowanych przez przestępców.
Źródło: zaufanatrzeciastrona.pl



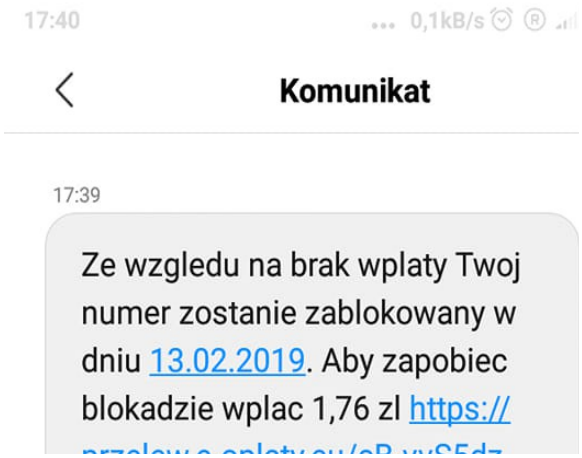


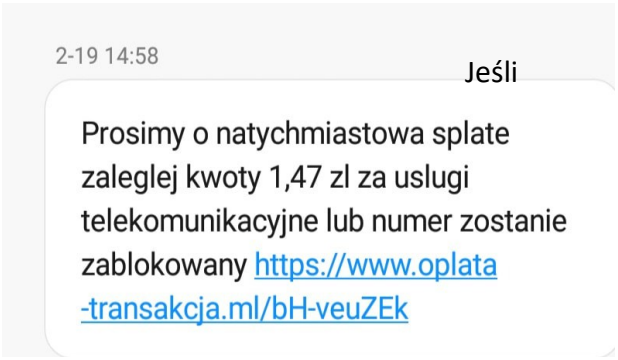
Ofiary ataków, które nie zachowają ostrożności, mogą stracić swoje oszczędności. Problem jest poważny - tylko w marcu odnotowano ponad 100 różnych stron udających pośredników płatności, używanych przez przestępców. Nieświadomi konsumenci ujawniając swoją tożsamość przestępcom mogą doprowadzić do wykorzystania jej do zawarcia w ich imieniu umów i w konsekwencji np. zaciągnięcia zobowiązań finansowych.

Przestępcy używają różnych sposobów, by ściągnąć ofiary na fałszywe strony. Użytkownicy mogą być do nich kierowani przez linki w SMSach, komunikatorach internetowych lub poprzez fałszywe sklepy internetowe. Aby nie zostać ofiarą przestępców należy zwrócić uwagę na kilka ważnych elementów:

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

Przykład wiadomości SMS rozsyłanych przez przestępców.
Źródło: zaufanatrzeciastrona.pl





- Jeśli strona prosi o login i hasło do bankowości internetowej, 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 uważnie treść każdego SMSa z kodem autoryzacyjnym od swojego banku. Jeśli twój bank to umożliwia zamień SMSy na autoryzację za pośrednictwem aplikacji mobilnej.

Jeśli podejrzewasz, że jesteś ofiarą internetowego oszustwa, zgłoś to jak najszybciej do swojego banku, a następnie zespołowi reagowania na incydenty CERT.PL (pod adresem https://incydent.cert.pl/) oraz najbliższej jednostce Policji. Wskazane powyżej instytucje przekażą Ci informacje na temat kolejnych działań. Masz też prawo złożyć reklamację do swojego banku.

Prokuratura Krajowa
Komenda Główna Policji
Urząd Ochrony Konkurencji i Konsumentów
Europejskie Centrum Konsumenckie
FinCERT.pl – Bankowe Centrum Cyberbezpieczeństwa ZBP