KPP BRZEG

http://brzeg.policja.gov.pl/ob/akademia-bezpieczenstwa/bezpieczne-pieniadze/6020,Bezpieczne-pieniadze.html
2020-10-20, 19:29

BEZPIECZNE PIENIĄDZE

W dzisiejszych czasach coraz rzadziej posługujemy się gotówką, częściej płacimy w sklepach i punktach usługowych kartą płatniczą. Często też, wypłacając pieniądze z banku, korzystamy z bankomatów. Niejednokrotnie działamy wtedy automatycznie, zapominając o odstawowych zasadach bezpieczeństwa. Pamiętajmy jednak o zachowaniu ostrożności także w tych okolicznościach. Pozwoli nam to uniknąć strat wynikających przykładowo ze skopiowania karty przez nieuczciwego kelnera, sprzedawcę czy poprzez "nakładkę" zainstalowaną na bankomacie.

Kilka podstawowych zasad bezpieczeństwa przy korzystaniu z karty płatniczej:

1. Przed włożeniem karty do bankomatu sprawdźmy czy nie został on zmodyfikowany, czy nie ma nałożonej jakiejś nakładki na klawiaturę lub w miejscu, gdzie wkładamy kartę.
2. Korzystając z bankomatu stańmy tak, aby zasłonić wstukiwany kod PIN i wypłacaną kwotę przed innymi użytkownikami. Starajmy się także zakryć klawiaturę np. ręką tak, by ewentualnie zainstalowana przez przestępców kamera nie mogła dostrzec kodu PIN.
3. Nigdy nie zapisujmy kodu PIN na karcie płatniczej lub na kartce noszonej w portfelu razem z kartą.
4. Jeśli chcemy sprawdzić czy została wypłacona żądana kwota zróbmy to dyskretnie. Nie liczmy pieniędzy na oczach innych. Nie korzystajmy z pomocy obcych osób przy wypłacie gotówki z bankomatu. Jeżeli mamy jakiekolwiek wątpliwości, lub potrzebujemy pomocy, skontaktujmy się z pracownikiem banku. Jednakże pamiętajmy, żeby żadnej z tych osób nie podawać numeru PIN karty.
5. Bierzmy potwierdzenie dokonywanych transakcji. To ułatwi zgłoszenie ewentualnej reklamacji, a także przyspieszy jej rozpatrzenie.
6. Pamiętajmy o odebraniu karty z bankomatu po zakończeniu transakcji.
7. Jeśli to możliwe, planując wypłatę większej kwoty w bankomacie wybierzmy się do bankomatu w towarzystwie innej osoby.
8. Wypłacając pieniądze rozejrzyjmy się czy w sąsiedztwie nie stoi osoba obserwująca nas i bezpośrednie otoczenie bankomatu.
9. Kontrolujmy stan konta na bieżąco. Jeśli zauważymy w historii konta transakcje, których nie dokonaliśmy, natychmiast poinformujmy bank oraz zastrzeżmy swoją kartę,
10. Płacąc kartą w sklepie czy lokalu usługowym pamiętajmy o tym, że karty nie wolno nawet na chwilę spuścić z oczu. Skopiowanie naszej karty zajmuje ułamek sekundy! Płacąc kartą wymagajmy, żeby przyniesiono do nas terminal po to, aby osobiście móc wczytać kartę. Jeśli nie jest to możliwe, powinniśmy razem z pracownikiem zakładu usługowego udać się np. na zaplecze gdzie znajduje się terminal.
11. Jeśli terminal, zachowanie kelnera, sprzedawcy lub bankomat budzą nasz niepokój, natychmiast powiadommy o tym Policję.
12. Płacąc kartą w sklepie zwróćmy uwagę, żeby wstukiwany przez nas PIN nie był widoczny przez innych klientów.

Skimming i phishing

Upowszechnienie kart płatniczych pociągnęło za sobą rozwój nowych form przestępczości bankowej. Najczęstsze przestępstwa tego typu to "skimming" i "phishing".
"Skimming" polega na bezprawnym skopiowaniu zawartości paska magnetycznego karty płatniczej w celu utworzenia duplikatu oryginalnej karty. Taka zduplikowana karta działa jak oryginalna, a transakcje nią dokonane obciążają prawowitego właściciela.
Karty mogą być kopiowane wszędzie tam gdzie dokonujemy płatności za ich pośrednictwem. Może skopiować ją sprzedawca, który współpracuje z przestępcami lub sam jest przestępcą. Najczęściej są kopiowane karty, które nie

wymagają autoryzacji przy pomocy PIN-u (ten przestępca nie zawsze ma okazję poznać). Do kopiowania służy małe urządzenie, które później podłącza się do komputera i kopiuje zawartość odczytanych pasków magnetycznych.
Odmianą "skimmingu" jest "skimming bankomatowy". Przestępcy instalują urządzenia, służące do pozyskiwania danych paska magnetycznego kart oraz kodów PIN. Urządzenia są montowane na bankomatach lub w ich wnętrzu, w postaci kompletu nakładek (jedna część montowana jest w miejscu, gdzie wsuwa się kartę do bankomatu, druga - z zainstalowaną kamerą, jako np. dodatkowy baner świetlny podwieszony w górnej części urządzenia). Taki zestaw rejestruje dane z paska magnetycznego naszej karty i za pomocą kamery odczytuje wprowadzany PIN.
Żeby uchronić się przed skimmingiem wystarczy przestrzegać kilku wskazówek i zanim dokonamy transakcji w bankomacie sprawdzić, czy:
• czytnik kart nie wygląda podejrzanie;
• klawiatura bankomatu jest równa lub lekko obniżona w stosunku do poziomu obudowy;
• czy do bankomatu nie są przymocowane podejrzane urządzenia - odstające elementy.
Sprawdzajmy także na bieżąco saldo naszego rachunku oraz wyciągi z kart i kont.

Phishing to wykradanie numerów kart kredytowych i poufnych informacji za pomocą technik psychologicznych.
Najczęściej rozpoczyna się od rozesłania pocztą elektroniczną wiadomości, które udają oficjalną korespondencję z banku, serwisu aukcyjnego itp., zawierającą np. informację o zdezaktywowaniu konta i konieczności jego ponownego reaktywowania. Ponownej aktywacji konta można dokonać na stronie internetowej, do której zostaje podany w e-mailu link. Podana witryna, choć z wyglądu przypomina prawdziwą stronę banku, w rzeczywistości jest obsługiwana przez przestępców. Nieświadomi użytkownicy ujawniają tu swoje dane (kody pin, identyfikatory, hasła) i w ten sposób dostają się w pułapkę przestępców.

Bardzo niebezpieczniejszą dla użytkownika formą phishingu jest tzw. pharming. Zamiast wysyłania fałszywych wiadomości e-mail, przestępcy przekierowują użytkowników wpisujących prawidłowe adresy np. swojego banku na fałszywe strony internetowe.

Innym sposobem działania cyberprzestępców, jest wykorzystywanie w celu poznania poufnych danych, złośliwego oprogramowania w postaci wirusów, robaków, trojanów Takiego oprogramowanie można ściągnąć korzystając z zainfekowanych witryn internetowych.
Każdy internauta powinien mieć świadomość zagrożeń, jakie wiążą się z pobieraniem z sieci oprogramowania czy odpowiadaniem na podejrzaną pocztę elektroniczną. Pamiętajmy, że:
• serwisy nie wysyłają e-maili z prośbą o odwiedzenie i zalogowanie się na stronie;
• nie należy otwierać hiperłączy bezpośrednio z otrzymanego e-maila;
• należy regularnie uaktualniać system i oprogramowanie;
• nie wolno przesyłać mailem żadnych danych osobistych;
• banki i instytucje finansowe stosują protokół HTTPS tam, gdzie konieczne jest zalogowanie do systemu. Adres strony www rozpoczyna się wtedy od wyrażenia 'https://', a nie 'http://'. Jeśli strona z logowaniem nie zawiera w adresie nazwy protokołu HTTPS, powinno się zgłosić to osobom z banku i nie podawać na niej żadnych danych.

Każde podejrzenia odnośnie do budzących naszą niepewność witryn należy jak najszybciej przekazać policjantom lub pracownikom danego banku odpowiedzialnym za jego funkcjonowanie w sieci.