JAK NIE DAĆ SIĘ OKRAŚĆ

**Gwałtownie rośnie przestępczość elektroniczna.
Pustoszeją bankomaty, klientom banków znikają pieniądze z kont.
W sieci aż roi się od nieistniejących sklepów internetowych.
Policja apeluje o szczególną ostrożność.
Nie pozwalajmy się ograbiać „w białych rękawiczkach".**

Dziś życie toczy się bardzo szybko, w zasadzie wciąż jesteśmy w biegu. Drażnią nas uliczne korki i wszechobecne kolejki, dlatego coraz częściej korzystamy z udogodnień, jakie dają nam nowoczesne technologie. Gdy zabraknie nam gotówki, zamiast do zatłoczonego banku, idziemy do najbliższego bankomatu, albo po prostu płacimy kartą. Zakupy wolimy robić przez internet, bo w domowym zaciszu, bo szersza oferta, w dodatku przywiozą do domu. Słusznie – temu to służy. Trzeba jednak pamiętać, że wirtualny świat, podobnie jak ten realny, nie jest wolny od złodziei i oszustów.

ZŁODZIEJSKIE TRIKI

Bankomaty, odkąd tylko pojawiły się w Polsce, od razu stały się obiektami zainteresowania złodziei. Zdarzały się nawet desperackie próby kradzieży całych urządzeń, co jak wiadomo nie jest proste z racji ich gabarytów. Klientów banków początkowo przestrzegano jedynie przed noszeniem w jednym miejscu kart płatniczych i kodów PIN, bo w razie zguby czy kradzieży portfela oznaczałoby to podanie złodziejowi zawartości własnego konta na tacy. Tak czy owak – przyszłość naszych oszczędności zależała od nas. Nawet, jeśli padliśmy ofiarą kieszonkowca. Dziś sprawa jest dużo bardziej skomplikowana, gdyż przestępcy działają w bardziej wyrafinowany sposób. Nie potrzebują już bezpośredniego kontaktu z ofiarą. Nauczyli się „przerabiać" bankomaty tak, by kradły dla nich kody PIN oraz wszystkie niezbędne dane zawarte na naszych kartach płatniczych. Umożliwiają im to specjalne nakładki skanujące montowane na czytniki kart i klawiatury, czasem dodatkowo mikrokamery. Po zdobyciu poufnych informacji złodzieje („skimmerzy" – tak mówią o nich policjanci) tworzą wierne kopie kart, po czym do woli się nimi posługują. Skutki przestępczej działalności tego typu odczuli na własnej skórze w lutym tego roku mieszkańcy Wrocławia – głośno było o tym w mediach. Złodzieje przez dłuższy czas kopiowali karty użytkowników jednego z bankomatów należących do Banku Zachodniego. W jeden weekend „wyczyścili" ich konta do zera. Straty poszczególnych klientów sięgały od kilkuset złotych po naprawdę grube tysiące. Jedna z poszkodowanych klientek miała na koncie przelany kredyt na zakup mieszkania.

SPOSÓB NA SKIMMERA

Złodzieje mają nad nami tę przewagę, że wiedzą, gdzie i kiedy zainstalują urządzenia skanujące. Nie znaczy to jednak, że jesteśmy całkowicie bezbronni. Zdaniem policjantów, zachowanie przysłowiowego minimum ostrożności pozwoli uniknąć kradzieży. Oto kilka rad:

- Przed włożeniem karty do bankomatu sprawdźmy, czy nie ma nałożonej jakiejś nakładki na klawiaturę lub w miejscu, gdzie wkładamy kartę;
- Korzystając z bankomatu, stańmy tak, by zasłonić wstukiwany kod PIN i wypłacaną kwotę. Starajmy się także zakryć klawiaturę ręką lub portfelem tak, by ewentualnie zainstalowana przez przestępców kamera nie mogła dostrzec kodu PIN;
- Przy wypłacie gotówki z bankomatu nie korzystajmy z pomocy obcych osób. Jeżeli mamy jakiekolwiek wątpliwości lub potrzebujemy pomocy – skontaktujmy się z działem call-center lub poprośmy o wsparcie pracownika banku. Żadnej z tych osób kategorycznie nie podajemy numeru PIN karty;
- Jeśli to możliwe, chodźmy do bankomatu w towarzystwie drugiej, bliskiej osoby;
- Po zakończeniu transakcji pamiętajmy o odebraniu karty z bankomatu;

- Bierzmy potwierdzenie dokonywanych transakcji. Ułatwi to zgłoszenie ewentualnej reklamacji, a także przyspieszy jej rozpatrzenie;
- Płacąc kartą w sklepie czy lokalu usługowym, pamiętajmy, że karty płatniczej nie wolno nawet na chwilę spuścić z oczu. Jej skopiowanie to kwestia ułamka sekundy. Płacąc kartą, wymagajmy, byśmy osobiście mogli wczytać kartę. W razie potrzeby (jeśli nie można przynieść terminala), udajmy się z pracownikiem na zaplecze lub w inne miejsce, gdzie ów terminal jest zainstalowany;
- Jeśli terminal, zachowanie sprzedawcy, kelnera lub bankomat budzą nasze wątpliwości, natychmiast powiadommy policję;
- Na bieżąco kontrolujmy stan konta. Jeśli w historii konta zauważymy transakcje, których nie dokonaliśmy, natychmiast poinformujmy bank i zastrzeżmy swoją kartę.

TREFNE SUPEROFERTY

Innym zagrożeniem dla naszych portfeli są coraz powszechniejsze zakupy w internecie. Nie oznacza to, że powinniśmy w ogóle z nich zrezygnować. Na internetowych aukcjach znaleźć można naprawdę ciekawe i atrakcyjne oferty. Tańsze, bo bez marż i pośredników, często wprost od producenta. Wątpliwości budzić powinny aukcje oferujące towar za pół darmo. Nikt raczej nie chce dopłacać do interesu. Ktoś, kto składa taką ofertę, albo znalazł się w posiadaniu kradzionych produktów (np. telefonów komórkowych), albo w ogóle nie ma nic na sprzedaż, tylko chce naciągnąć potencjalnego nabywcę. Policja często odbiera zgłoszenia od oszukanych klientów, którzy w swej naiwności wpłacili pieniądze na konta fałszywych sprzedawców i nigdy nie doczekali się realizacji zamówienia. Parę miesięcy temu głośną sprawą stała się nieprawdziwa oferta sylwestrowa. Oszuści, podszywając się pod właściciela jednego z górskich pensjonatów, proponowali atrakcyjne cenowo noclegi w Zakopanem. Warunkiem dokonania rezerwacji było wpłacenie zaliczki – minimum 700 złotych. Nabrało się kilkadziesiąt osób, co oznacza, że przestępcy zainkasowali kilkadziesiąt tysięcy złotych. Jak uniknąć przykrej niespodzianki?

POLICJA RADZI:

- Zawsze kierujmy się ograniczonym zaufaniem do sprzedającego;
- Korzystajmy tylko ze znanych i sprawdzonych portali internetowych;
- Gdy kupujemy na aukcji internetowej, przeczytajmy komentarze o sprzedającym. Brak komentarzy pozytywnych lub ich niewielka ilość powinny wzbudzić naszą czujność;
- Przed zakupem w wirtualnym sklepie zasięgnijmy opinii o nim i sprawdźmy jego rzetelność. Można to zrobić u znajomych lub na forach internetowych. Zwracajmy też uwagę, czy sklep podaje swój adres i numer telefonu. W razie wątpliwości będziemy mogli tam zadzwonić;
- Po otrzymaniu oferty e-mailem, nie korzystajmy z linków, na stronę sklepu wejdźmy, wpisując adres w oknie przeglądarki, unikniemy w ten sposób podszywających się pod legalnie działające sklepy;
- Zamawiając sprzęt, zapytajmy, czy sprzedawca dołącza oryginalne oprogramowanie na płytach i instrukcję obsługi;
- Kupując telefon komórkowy, zapytajmy o ładowarkę i dowód zakupu, telefony kradzione sprzedawane są bez ładowarek i dokumentacji;
- Nie dokonujmy zakupów w sieci z komputera stojącego w kafejce internetowej. Tam najłatwiej utracić poufne dane. Używajmy tylko komputera domowego i zachowujmy całą korespondencję ze sprzedawcą. Jeśli nas oszuka, pozwoli to policji szybko go odnaleźć;
- Jeśli istnieje taka możliwość, zamawiajmy towar z opcją płatności przy odbiorze. Wówczas nie zapłacimy za coś, czego nie otrzymamy;
- Przy płaceniu kartą kredytową zwracajmy uwagę, czy połączenie internetowe jest bezpieczne i czy przesyłane przez nas dane nie zostaną wykorzystane przez osoby nieuprawnione. Na dole strony powinien pojawić się symbol zamkniętej kłódki, a na końcu adresu – „https”.
- I przede wszystkim – żeby nie było żadnych nieporozumień – kilkakrotnie dokładnie przeczytajmy, co pisze sprzedający. Mówi się, że czas to pieniądz. W tym wypadku spieszmy się powoli.