

**Czy zatem płatności kartą w Internecie są bezpieczne? Jak to się dzieje, że w ciągu kilku sekund po podaniu numeru naszej karty otrzymujemy wynik autoryzacji? Jakie zagrożenia mogą nas spotkać w Internecie i na co powinniśmy uważać? Na te i wiele innych pytań odpowiemy w naszym poradniku.**

**W jaki sposób dochodzi do wyłudzenia numerów kart płatniczych i kredytowych?**

Najczęściej do wyłudzenia haseł, loginów, nr kart i innych danych, których osoby trzecie znać nie powinny służą 3 metody.

**Pierwsza to phishing.** Jest to najczęściej próba oszukania użytkownika poprzez skierowanie go na fałszywą stronę. Metoda ta polega na przekonaniu osoby atakowanej do przejścia na witrynę/stronę przypominającą oryginalną. Do tego celu używa się zazwyczaj spamu, którego odbiorcą jest konkretna grupa użytkowników. Przykładowo może zostać rozesłana informacja dotycząca aktualizacji danych dotyczących konta bankowego. Aby tego dokonać użytkownik musiałby kliknąć w link i podać informacje o sobie, nr konta/karty kredytowej, pin lub nr klienta i hasło. Wszystko oczywiście odbywa się za pośrednictwem fałszywej witryny podanej w mailu, która wygląda jak autentyczna strona banku (szata graficzna, reklamy, nawet pola informacyjne, FAQ i pomoc). Oczywiście nie tylko banki są brane na cel.

**Drugi sposób to pharming.** Atak ten jest trudniejszy do przeprowadzenia, niestety idzie to w parze z wykrywalnością, ponieważ równie trudno jest poznać, że zostaliśmy zaatakowani. Tutaj istnieją dwie metody, lokalna i globalna. Lokalna jest łatwiejsza do realizacji. Zaczyna się od zainfekowania komputera ofiary koniem trojańskim, który modyfikuje plik hosts, w którym dla prawdziwej strony np. banku przypisuje się fałszywy adres. Dzięki temu zabiegowi, użytkownik wpisując w przeglądarce nazwę banku, zostaje przekierowany na fałszywą stronę (mimo wpisania dobrego adresu). Pozwala jednak na atak tylko konkretnej osoby, co może być mało zyskowne. Atakując globalnie, ma się dostęp do wiele większych zasobów. Atakowane są bowiem serwery DNS, które odpowiadają za tłumaczenie adresów stron. W ten sposób, wszystkie osoby aktualnie z niego korzystające i wchodzące na określone strony, mogą paść ofiarą wyłudzenia.

**Ostatni sposób to socjotechnika.** Jest ona obecna w dwóch pierwszych metodach (trzeba przekonać w wiarygodny sposób do kliknięcia lub podania danych). Jednak dobry socjotechnik potrafi wzbudzić w rozmówcy na tyle duże zaufanie (poprzez komunikatory, chat, mail, telefony i inne środki kontaktu), że odbiorca jest gotów podać pewne dane np. dotyczące konta. Brzmi to nieprawdopodobnie, niestety jest prawdziwe. Przekonał nas o tym m.in. Kevin Mitnick, a także kilku innych znanych socjotechników. Zazwyczaj atakujący podaje się za inną osobę - powiedzmy, pracownika banku. Może operować fachową terminologią by do siebie przekonać.

**PAMIĘTAJ: PRZY PŁATNOŚCIACH W INTERNECIE NIGDY NIE PODAWAJ SWOJEGO KODU PIN**

**PAMIĘTAJ, ZASZWSZE SPRAWDZAJ CZY NA STRONIE, NA KTÓREJ PODAJESZ NUMER KARTY KREDYTOWEJ WIDNIEJE KLÓDKA W OKNIE PRZEGLĄDARKI, A JEJ ADRES ZACZYNA SIĘ OD LITER HTTPS ZAMIAST http**

**PAMIĘTAJ: ŻADEN SKLEP NIE OTRZYMUJE NIGDY NUMERU TWOJEJ KARTY, ANI ŻADNYCH INNYCH DANYCH POZWALAJĄCYCH NA DOSTĘP DO TWOICH PIENIĘDZY**

# Zakupy przez Internet, zamówienia pocztowe i telefoniczne **PRAKTYCZNE RADY**

- Zakupów przez Internet należy dokonywać tylko za pośrednictwem zaufanego komputera, który posiada oryginalne oprogramowanie i zabezpieczenia przeciw wirusom. Należy unikać komputerów dostępnych w publicznych miejscach, ponieważ nie zapewniają one odpowiedniej prywatności i bezpieczeństwa.
- Najlepiej dokonywać zakupów u znanych nam sprzedawców internetowych, jeśli ich nie znamy - należy sprawdzić, czy zasługują na zaufanie. Komentarze lub opinie dostępne w Internecie pozwalają uniknąć niesolidnych sprzedawców.
- Przed dokonaniem zakupu należy zapoznać się z warunkami dostawy i zwrotu towaru, a także subskrypcji na korzystanie z płatnych serwisów internetowych. Pozwoli to na uniknięcie przykrych niespodzianek i dodatkowych kosztów. Bardzo popularnym trikiem stosowanym na różnych stronach jest automatyczne, comiesięczne odnawianie subskrypcji do momentu jej anulowania.
- Przed dokonaniem płatności internetowej należy się upewnić, że korzystamy z szyfrowanego połączenia: w dolnym rogu okna przeglądarki internetowej szukamy symbolu kluczyka lub kłódki, sprawdzamy też adres danej strony internetowej, który powinien zaczynać się od `https://` zamiast standardowego `http://`
- Nigdy nie ujawniamy naszego kodu PIN w Internecie. Żaden sprzedawca, tradycyjny czy internetowy, nie ma prawa tego od nas żądać.
- Nie należy również podawać PIN-u osobom podającym się za pracowników banku – pracownik banku nigdy o niego nie zapyta. Wszelkie próby wyłudzenia PIN-u należy natychmiast zgłosić na infolinii lub w oddziale banku.

Przechowujemy zapisy dotyczące dokonanych transakcji, w tym również adres sprzedawcy (internetowy i pocztowy) oraz jego numer telefonu.

- Zachowujemy e-maile z podstawowymi danymi o zakupie, jakie wiele sklepów internetowych wysyła swoim klientom. Dobrym zwyczajem jest również przechowywanie wszelkiej korespondencji prowadzonej ze sprzedawcą – może posłużyć to jako dowód w ewentualnym procesie reklamacyjnym.
- Dobrym pomysłem jest korzystanie ze specjalnych kart wirtualnych – służą one tylko do płatności zdalnych. Karta jest rodzajem elektronicznej portmonetki, a używając jej nie możemy wydać więcej niż się na niej znajduje. Istota jej działania polega na tym, że przed dokonaniem transakcji należy w tej portmonetce umieścić potrzebną kwotę. Po dokonaniu transakcji pozostałe środki należy przelać na połączone z kartą konto.
- Nigdy nie należy podawać nikomu identyfikatora i hasła służących do logowania w internetowym serwisie banku oraz telefonicznym biurze obsługi.

## **Kilka rad, które sprawią że transakcje w Internecie będą jeszcze bezpieczniejsze.**

### *Jak dbać o bezpieczeństwo?*

Dokonywana w Internecie transakcja jest bezpieczna. Problem polega na tym, aby nie pozwolić "ukraść" sobie danych kartowych, a to, jak dobrze wiemy, może mieć miejsce zarówno w sieci, jak i w sprzedaży bezpośredniej. W Internecie jest to głównie sprawa tzw. phishingu, czyli próby wyłudzenia danych poprzez "podszywanie" się pod bank (przykładem może być telefon z "banku") lub fałszywą stroną WWW (dlatego

należy zawsze sprawdzać certyfikat danej strony). Warto też słuchać znajomych i ich pozytywnych doświadczeń z konkretnymi sklepami i stronami internetowymi. Korzystajmy zatem ze sklepów, w których jasno i klarownie opisane są reguły dokonywania zakupów, a w szczególności – reguły płatności. Zwracajmy uwagę na to, kto w imieniu sklepu dokonuje autoryzacji - czy jest to znana firma, czy słyszeliśmy o niej czy zupełnie nie. Przeprowadzajmy transakcje w takich sklepach, które są obsługiwane przez znanych nam agentów rozliczeniowych, ponieważ oni dbają o nasze bezpieczeństwo. Realizując płatność pod żadnym pozorem nie podawajmy danych kartowych przez telefon, zaś jeśli płatności dokonujemy za pośrednictwem Internetu sprawdzajmy, czy strona, na którą zostaliśmy przekierowani należy faktycznie do instytucji finansowej, do której chcieliśmy się dostać. Gdy już na nią wejdziemy, zwracajmy uwagę na znak zamkniętej kłódki i certyfikat SSL. Należy także pamiętać, by nigdy nie korzystać z linków pochodzących z maili, których pochodzenia nie jesteśmy pewni, natomiast jeśli korespondujemy elektronicznie z bankiem i bank wysłał do nas link pamiętajmy, by danych kartowych takich, jak hasła czy dane karty nie podawać w korespondencji mailowej, lecz tylko i wyłącznie na stronie banku, która zawsze jest stroną bezpieczną.

Na zakończenie warto pamiętać o programach antywirusowych, których posiadanie jest już właściwie niezbędne i które należy bezwzględnie codziennie aktualizować. W celu podniesienia bezpieczeństwa naszego komputera pamiętajmy, by przynajmniej raz na 5 dni przeprowadzić jego skanowanie.

1. Zarejestruj się w programach takich jak Verified by Visa, zapewniających bezpieczeństwo transakcji dokonywanych w Internecie.
2. Chroń swoje dane osobowe; korzystając z karty, zakrywaj swój numer PIN; jeżeli to możliwe, podrzyj/zniszcz dokumenty zawierające Twoje dane osobowe (wtedy, gdy już nie będą Ci potrzebne).
3. Uważaj na phishing – nieproszoną korespondencję, rzekomo wychodzącą z banku, od detalisty lub organizacji Visa z prośbą o podanie danych osobowych. Sprawdź, jeśli masz wątpliwości.
4. Systematycznie przeglądaj wyciągi z konta karty i rachunku bankowego i informuj bank o wszelkich podejrzeniach.
5. Najlepiej jest nie powierzać nikomu karty – jeśli kelner lub sprzedawca w sklepie chce zabrać kartę, by dokonać autoryzacji, należy iść z nim.
6. Przed zatwierdzeniem transakcji podpisem lub przez wprowadzenie kodu PIN zawsze należy sprawdzić kwotę na ekranie czytnika kart lub na wydruku.
7. Po dokonaniu płatności należy upewnić się, że sprzedawca zwraca nam kartę wraz z kopią dowodu kasowego. Dobrym zwyczajem jest zachowywanie potwierdzeń płatności kartą i wydruków z bankomatu oraz porównywanie ich z wyciągami otrzymywanymi z banku.
8. Jeśli z jakiegoś powodu transakcja w sklepie jest nieudana, sprzedawca jest zobowiązany wydać nam potwierdzenie, które może być dowodem, gdyby trzeba było transakcję reklamować.
9. Dokonując płatności kartą lub wypłacając środki z bankomatu zawsze należy zakrywać klawiaturę, by nikt niepowołany nie podejrzwał PIN-u.
10. W wypadku stwierdzenia niezgodności lub natrafienia na transakcję, której nie możemy sobie przypomnieć, należy natychmiast skontaktować się z bankiem, który rozpocznie odpowiednią procedurę wyjaśniającą. Najważniejsze, by o nieprawidłowościach poinformować bank jak najszybciej.
11. Należy znać numery telefonów, pod które trzeba zadzwonić w wypadku utraty karty. Gdy zauważymy, że kartę zgubiliśmy lub została nam ona skradziona, należy ją natychmiast zastrzec.
12. Dobrym zwyczajem jest sprawdzanie, czy jesteśmy w posiadaniu wszystkich kart.
13. Numer karty i wszystkie dane widoczne na karcie należy chronić, ponieważ za ich pomocą osoba niepowołana może dokonać transakcji internetowej obciążającej nasz rachunek.
14. Należy pamiętać, by uaktualniać swoje dane teleadresowe w banku – są one niezbędne w sytuacji konieczności kontaktu z bankiem.

**Przygotowanie materiału: Kaspersky Lab Polska, First Data Polska (Polcard), Visa Europe - przedstawicielstwo w Polsce, Visa Europe – centrala w Londynie, mBank.**