

Kupując w Internecie...

- zawsze sprawdzaj u kogo kupujesz - na stronach sklepu internetowego muszą się znajdować wszelkie informacje o sprzedawcy - adres, telefon/fax, NIP itp. Jeżeli takich danych nie ma to można uznać, że nie jest to poważny sprzedawca i lepiej u niego nie kupować.
- poważny sklep ma poważny adres - jeżeli więc, spotkasz się ze sklepami z adresami wskazującymi na darmowe serwery WWW, musisz być przygotowany na to, iż jest to 'prywatny sklep' jakiegoś internauty.
- wielkie obniżki choć przyciągają, powinny wzbudzić podejrzenie.- zawsze czytaj wszelkie dodatkowe informacje zawarte na łamach stron WWW poszczególnych sklepów - zwłaszcza regulaminy.
- pamiętaj, że oprócz strony WWW, zawsze możesz zadzwonić do danego sklepu - każdy sklep z prawdziwego zdarzenia ma telefon stacjonarny.
- cena towaru musi być jednoznaczna czy jest to netto/brutto - nie może być też ukrytych kosztów np. dowozu.

Jeżeli chcesz zapłacić kartą...

Sklepy, które obsługują płatności kartami kredytowymi są do tego odpowiednio przystosowane informatycznie, oznacza to że można tam płacić bezpiecznie. Jeżeli więc na witrynie któregoś sklepu chcesz zapłacić kartą kredytową sprawdź czy korzysta on z pośredników takich jak eCard lub Polcard oraz czy połączenie pomiędzy Tobą a serwerem jest szyfrowane. Zawsze jednak zapisuj wszelkie dokonane transakcje przy użyciu karty i porównuj je z otrzymanym wyciągiem bankowym. Jest też wiele sklepów, które pozwalają płacić klientom kartami, ale odbywa się to w sposób taki, że klient podaje dane swojej karty, a sklep telefonicznie potwierdza wypłacalność klienta w centrum autoryzacyjnym. Nie jest to jednak metoda najbezpieczniejsza, bo obsługa sklepu poznaje nasze dane. Dlatego przed zawarciem transakcji dowiedzmy się, czy sklep obsługuje bezpieczny model transakcji kartami.

Odwoływanie zamówień

Może się zdarzyć, że zamiast nas zakupów dokona np. nasza pociecha - i co wtedy? Bez paniki, wszystko da się załatwić.

- Po pierwsze zapoznajmy się z kilkoma metodami stosowanymi przez sklepy on-line:- zamówienie potwierdzone e-mail - kiedy dokonamy zakupu w sklepie, nasze zamówienie jest potwierdzone listem elektronicznym, znajduje się tam wyszczególnienie co zamówiliśmy, kiedy itp. Jeżeli dziecko poda nasz adres e-mail, to po otrzymaniu takiej przesyłki powinniśmy podjąć następujące kroki jak - telefoniczne poinformowanie obsługi sklepu, że niczego takiego nie zamawialiśmy, i że chcemy odwołać to zamówienie. Możemy też odwołać nasze wirtualne zakupy nawet w momencie, kiedy to właśnie my mieliśmy na coś ochotę i kupiliśmy to - przynajmniej teoretycznie. Obsługa sklepu odpowiada na każdy e-mail i robi to na bieżąco. Im wcześniej poinformujemy obsługę, że nie chcemy już jakiegoś produktu - tym lepiej. Dla pewności możemy również zadzwonić - adres i telefon firmy zajmującej się sklepem znajdziemy na jej stronie internetowej - adres łatwo jest ustalić - wystarczy spojrzeć z jakiego konta pochodzi wiadomość e-mail - jeżeli będzie to np. sklep@empik.com to adres sklepu analogicznie brzmi www.empik.com - zresztą w stopce listu najczęściej znajduje się właściwy adres sklepu.
- konieczność potwierdzenia zamówienia poprzez e-mail - metodę taką stosuje np. supersam.yoyo.pl - kiedy dokonamy zakupu - sklep wyśle do nas list e-mail ze wszystkimi szczegółami transakcji - jeżeli to my składaliśmy zamówienie musimy odpowiedzieć na ten e-mail - jest to więc pewnego rodzaju potwierdzenie. Jeżeli na przysłany nam list nie odpowiemy w okresie do 7 dni, zamówienie nie zostanie zrealizowane. Warto, więc zabezpieczyć program pocztowy przed dostępem innych osób do naszych kont pocztowych.
- potwierdzenie poprzez telefon - ta metoda jest najpopularniejsza, czyli obsługa sklepu zadzwoni na podany w formularzu zamówienia numer telefonu w celu potwierdzenia złożonego zamówienia.

A co gdy paczka przyjdzie do nas do domu?

Istnieje taka powszechna zasada, że żadna z paczek adresowanych do nas nie musi być przez nas odebrana - kiedy więc listonosz lub kurier zapuka do naszych drzwi z jakąś paczką, za którą przyjdzie nam zapłacić - po prostu odmówmy jej przyjęcia - paczka zostanie wtedy odesłana do miejsca nadania. Paczki zawsze otwieraj w obecności listonosza, kuriera, wtedy łatwiej będzie reklamować np.: pękniętą obudowę sprzętu czy samą zawartość. Jeśli zawartość się nie zgadza należy sporządzić od razu protokół reklamacyjny w obecności dostawcy.

Uczulmy też rodzinę, żeby nie odbierała żadnych paczek adresowanych na nas. Gdybyśmy jednak przyjęli paczkę można zastosować się do przepisu umieszczanego najczęściej na dokumentach dołączonych do przesyłki. Przepis ten brzmi przykładowo: "Zakupione artykuły możesz zwrócić w ciągu 10 dni od daty otrzymania przesyłki. Artykuły zwrócone w późniejszym terminie nie będą przyjmowane. Prawo do zwrotu dotyczy tylko artykułów fabrycznie zafoliowanych lub posiadających wadę. Zwroty nadesłane pocztą kurierską na koszt odbiorcy nie będą przyjmowane.

"Według prawa (Ustawa z dnia 2 marca 2000 r. "O ochronie niektórych praw konsumentów") klientowi przysługuje 10 dniowy okres zwrotu zakupionego na odległość towaru bez podania przyczyny, ale:- w przypadku kaset audio/wideo, płyt audio, gier, programów itp. nie może zostać zerwane fabryczne opakowanie - bo w takim przypadku zwrotów się nie uznaje. Pamiętajmy więc aby niczego nie rozpakowywać dogłębnie po odebraniu, jeżeli mamy to zamiar zwrócić. Warto też zwrócić uwagę, że termin 10 dni liczony jest od momentu, kiedy towar zostanie nam wydany, czyli np. kiedy go odbierzemy na poczcie, lub kiedy przywiezie nam go kurier. Za zwrócony towar sprzedawca musi wypłacić klientowi tę samą kwotę, którą klient zapłacił. Nie może przy tym pobierać od klienta żadnych dodatkowych pieniędzy np. z popularnego tytułu 'kosztów manipulacyjnych'.

Phishing - jak nie dać się złowić oszustom?

Oszuści internetowi są tylko tak sprytni, jak my jesteśmy naiwni. Ale przestępców można przechytryć.

Nie ma nic bardziej upokarzającego niż dać się okraść we własnym domu. I to na dodatek samemu otworzyć drzwi złodziejowi. W zeszłym roku spotkało to prawie 100 mln osób na całym świecie. Wielu z nich dało się nabrać na proste e-maile, których autorzy, podszywając się pod uznane instytucje finansowe, starali się wydobyć od internautów informacje na temat ich rachunków bankowych.

Zjawisko to zwane phishingiem przybiera na sile. Cybernetyczni przestępcy wyjątkowo często w tym roku pukają do naszych skrzynek pocztowych. W lipcu organizacja Anti-Phishing Working Group wykryła ponad 1,9 tys. tego typu ataków. Dla porównania w grudniu 2003 r. było ich zaledwie 116. Jeden atak oznacza w praktyce od tysięcy do milionów rozesłanych e-maili. Tylko w zeszłym roku 78 mln Amerykanów ujawniło oszustom swoje dane osobowe - wynika z danych firmy badawczej Gartner. Straty szacuje się na 1,3 mld dol.

Podaj mi swoje hasło do banku

Jak działa mechanizm wyłudzenia danych? Do internautów trafiają e-maile przypominające graficznie strony internetowe np. banków. W liście bank informuje nas o tym, że musimy zweryfikować swoje dane lub zweryfikować ostatnią transakcję, jakiej dokonaliśmy. Po kliknięciu na link jesteśmy przekierowywani na stronę do złudzenia podobną do strony banku. Jest ona oczywiście fałszywa, a my, podając nasze dane, odsłaniamy się na atak oszustów. Przestępcy najczęściej zainteresowani są hasłami i kodami do rachunków bankowych. W Polsce podobne e-maile imitowały m.in. strony mBanku i Citibanku. Okazuje się, że 5 proc. odbiorców oszukańczych e-maili na nie odpowiada.

Phishing może przybierać także inne formy. Jeden z najsłynniejszych ataków przeprowadził w styczniu rosyjski złodziej ukrywający się pod pseudonimem Robotector. Wysłał on e-mail o treści "Wciąż Cię kocham" do 3 mln osób. Po otwarciu wiadomości uruchamiał się program, który przez następne kilkanaście dni śledził, czy użytkownik nie wchodzi na jedną z 30 stron bankowych na

świecie. Kiedy internauta chciał dokonać przelewu, program przechwytywał treść wpisywaną z klawiatury (czyli hasło i PIN) i wysyłał dane do Robotectora. Przed takimi próbami można się zabezpieczyć tak jak przed wirusami (patrz poprzednia część cyklu). Trzeba także unikać otwierania wiadomości i załączników od nieznanych osób.

Coraz rzadziej stosowane, ale wciąż popularne są e-maile oferujące udział w intratnym przedsięwzięciu, na którym można zarobić dużo pieniędzy. Niby wszystko jest w porządku, ale czemu ktoś, kogo nie znasz, miałby Ci oferować pieniądze? Tego typu e-maile zyskały już nawet nazwę "nigeryjskiego przekrętu", bowiem większość ofert pochodziła właśnie z tego kraju.

Jeśli tyłu oszustów kontaktuje się z nami za pomocą e-maila, samo nasuwa się pytanie: skąd mają nasz adres? Cyberprzestępcy podobnie jak twórcy wirusów wykorzystują do tego specjalne programy, które badają strony internetowe i wyłapują z nich adresy e-mailowe. Jeśli chcemy uniknąć niechcianych e-maili (tzw. spamu) i ofert oszustów, wystarczy, że nie będziemy publikowali na forach internetowych naszego adresu.

Na aukcjach też oszukują

Oszuści upodobali sobie także aukcje internetowe. Tutaj mogą czuć się anonimowo. W największym polskim serwisie aukcyjnym Allegro niejednokrotnie zdarzały się już przypadki oszustw. Najgłośniejsze z nich dotyczyły najczęściej wyjątkowo atrakcyjnych ofert, w których sprzedający np. monitory ciekłokrystaliczne wymagali wpłaty pieniędzy na rachunek bankowy przed wysłaniem towaru. Oszuści zwykle od miesiący przygotowywali się do dużego "skoku na kasę". Przez kilka lub kilkanaście tygodni sprzedawali na aukcjach drobne przedmioty. Każda sprzedaż zwiększała im renomę w serwisie aukcyjnym. Kiedy byli już wystarczająco wiarygodni - przedstawiali ofertę nie do odrzucenia. Osoby, które chwyciły okazję, wpadały w pułapkę.

Najbardziej spektakularne przypadki miały miejsce stosunkowo niedawno. Policja aresztowała rodzinę z Lęborka, której udało się wyłudzić w ten sposób 25 tys. zł. Trzy osoby - 69 letnia babcia, jej 18-letni wnuczek i matka dziecka - sprzedawały m.in. telefony komórkowe. Było to ich główne źródło utrzymania. Ich ofiarą padło w sumie 13 osób. Niedawno oszust o nicku komputery00, który sprzedawał na aukcji dyski twarde i pamięci do komputerów, nabrał co najmniej 46 osób na kwotę ok. 60 tys. zł. Poszkodowani stworzyli forum internetowe.

Przed phishingiem i nieuczciwymi sprzedawcami można się w prosty sposób obronić. Ich skuteczność to przede wszystkim efekt nierozwagi użytkowników.

Jak nie paść ofiarą cybernetycznych przestępców?

- Nigdy nie klikaj na link zawarty w e-mailu od instytucji finansowej bez wcześniejszego sprawdzenia właściwej strony. Gdy przyjdzie do Ciebie zaskakujący e-mail z banku, otwórz przeglądarkę i wpisz oficjalny adres WWW banku. Strona podana w linku różni się zwykle od oficjalnej. Na tej ostatniej można nawet znaleźć ostrzeżenia przed oszustami.
- Wpisując hasło i kod do rachunku internetowego, korzystaj zawsze z oficjalnej strony banku.
- Nigdy nie podawaj w e-mailu poufnych informacji: kodów, haseł, numerów PIN lub numerów kont bankowych.
- Nie odpowiadaj na e-maile pochodzące od nieznanych osób, które oferują Ci możliwość łatwego zarobienia pieniędzy.
- Jeśli masz jakieś wątpliwości co do pochodzenia informacji z instytucji finansowej, rozwiń je, dzwoniąc na infolinię.
- Zainstaluj oprogramowanie antywirusowe i zaporę internetową (firewall). Dzięki temu zmniejszasz prawdopodobieństwo dostania się na twój dysk twardy złośliwych programów, które mogą przechwytywać wpisy z klawiatury.
- Jeśli nadal nie czujesz się bezpiecznie, możesz ściągnąć z internetu programy filtrujące przychodzącą pocztę, które odrzucają większość e-maili o charakterze phishingowym. Jak nie dać się oszukać na aukcji?

- **Unikaj zawierania transakcji z osobami, które wysyłają towar tylko po uprzednim przelaniu pieniędzy na podany rachunek. Nawet jeśli mają dużo pozytywnych komentarzy od innych internautów, nie masz żadnej gwarancji, że nie chcą cię oszukać.**
- **Jeśli sprzedawca chce mieć pewność, że przelejesz mu pieniądze, a nie akceptuje przesyłek za pobraniem, zaproponuj rachunek Escrow. W tej formie płatności przelewasz pieniądze na specjalny rachunek serwisu aukcyjnego. Po tym jak towar do ciebie trafi, potwierdzasz dostawę i dopiero wtedy serwis przelewa pieniądze do sprzedawcy. Taka forma zabezpiecza obie strony transakcji.**
- **Jeśli sprzedawca jest z twojej miejscowości lub okolic, staraj się umawiać na osobisty odbiór, a nie na przesyłkę pocztą.**
- **Przejrzyj opinie o pozostałych transakcjach sprzedawcy lub nabywcy (o ile są dostępne). Wszystkie opinie, które pojawiają się dzień lub dwa po zakończeniu transakcji, są wątpliwej wiarygodności. Przesyłka towaru trwa zwykle więcej niż 1-2 dni. Chyba że strony transakcji pochodzą z tej samej miejscowości, co może oznaczać, że umówiły się na odbiór osobisty.**
- **Nie ufaj sprzedawcom, którzy zobowiązują się opłacić koszt przesyłki. Sprzedawca nie ma żadnego interesu, żeby dopłacać do transakcji. W obrocie aukcyjnym przyjęło się, że za przesyłkę płaci kupujący.**