Bezpieczeństwo w sieci

Anna Radziejowska

WSTĘP

Ilość spraw, jakie przeciętny użytkownik może załatwić przez Internet, rośnie w szybkim tempie. Dzięki Internetowi możemy komunikować się ze znajomymi, znaleźć dane niezbędne do nauki lub codziennej pracy, zagrać, przeczytać prasę lub ściągnąć film, zapłacić ratę za mieszkanie, wypowiedzieć poglądy, kupić samochód lub zarejestrować firmę w ZUSie. Internet ułatwia życie, szczególnie jeśli mieszkamy z dala od dużych skupisk miejskich.

Niestety, Internet to nie tylko źródło zabawy i możliwość załatwienia od ręki wielu spraw. Podobnie jak w życiu realnym, tak i w Internecie, możemy natknąć się na oszustów i dowcipnisi, czyhających na naszą naiwność. Internet jest siecią otwartą, co sprzyja kontaktom międzyludzkim, ale tez wystawia nas na zagrożenia, na jakie w normalnym życiu, zachowując rozsądek, sami byśmy się nie narazili.

W omawianym materiale skupimy się na zagrożeniach, które dotyczą indywidualnego użytkownika Internetu, korzystającego z niego w domu lub miejscu publicznym (np. biblioteka, kafejka). Nie będziemy opisywać problemów dużych firm, instytucji finansowych i agencji publicznych.

DWA RODZAJE ZAGROŻEŃ

Przeciętny użytkownik Internetu, siadając przed monitorem, może zetknąć się z dwoma typami niebezpieczeństw.

Kradzież danych osobowych – czyli informacji, które mogą nas zidentyfikować np. imię, nazwisko, data urodzenia, adres zamieszkania, numer telefonu, PESEL, numer konta bankowego, karty kredytowej. itp. Oszust, mając takie dane, może się łatwo pod Ciebie podszyć i np. ukraść numery kart kredytowych i przejąć pieniądze, podszywać się pod tożsamość na ulubionym forum lub ściągnąć zdjęcia z bloga i używać ich do własnych, często przestępczych, celów.

Niebezpieczeństwa technologiczne lub **techniczne** to szkodliwe programy komputerowe. Głownie – wirusy, robaki, trojany, które mogą służyć do kradzieży naszych danych, ale są też niebezpieczne z racji na możliwość zablokowania systemu operacyjnego Twojego komputera lub utraty danych potrzebnych Ci do nauki lub pracy.

Lista zagrożeń obu typów jest tak długa, że w zasadzie nie powinieneś korzystać z Internetu, aby nie narazić się na niemiłe lub wręcz kosztowne sytuacje. Niemniej, stosując odpowiednie zabezpieczenia technologiczne oraz fizyczną ostrożność, możesz zmniejszyć niebezpieczeństwo. Z bezpieczeństwem w Internecie jest tak samo, jak z bezpieczeństwa w życiu fizycznym. Gdy wychodzisz z domu zamykasz drzwi na klucz – jeden lub więcej. Jeśli trzymasz w domu coś kosztownego, zdecydujesz się pewnie na zamontowanie solidnych, antywłamaniowych drzwi, a możliwe też, że dodatkowo ubezpieczysz mieszkanie. Podobnie z korzystaniem z Internetu – instalacja odpowiedniego oprogramowania oraz zwykła czujność mogą Cię uchronić przed wieloma zagrożeniami.

Pamiętaj! Za programem komputerowym zawsze stoi **człowiek**. Szkodliwe programy są pisane i rozsyłane przez złodziei i oszustów, którzy chcą uzyskać dostęp do twojego konta lub danych.

KRÓTKI PRZEGLĄD ZAGROŻEŃ TECHNICZNYCH

Najstarsze i najpowszechniejsze zagrożenie to wirusy. **Wirus komputerowy** to program, który działa poprzez dołączenie się do innego pliku (tak samo, jak wirusy biologiczne). Nie jest samodzielny –

dostaje się do Twojego komputera wraz z innymi plikami, które otrzymujesz poprzez email lub ściągasz z sieci, a także instalujesz samodzielnie, wkładając do komputera inne nośniki (płyty CD, DVD, pamięci masowe itp.). Wirusy dołączane są najczęściej do plików graficznych, dźwiękowych, animacji. Efekty zarażenia mogą być różne – wirus może sprawiać, że komputer będzie w nieskończoność odgrywał jakąś melodyjkę, ale może również zablokować właściwe funkcjonowanie programów pocztowych, graficznych czy edytora tekstów.

Są też bardziej złośliwe rodzaje wirusów, które, usuwając dane z dysku, niszczą je, blokują system operacyjny (nagle „coś" się zawiesza) a nawet unieruchamiają programy antywirusowe.

Najgroźniejszymi typami wirusów są dziś **robaki** i **trojany** (nazwa pochodzi od konia trojańskiego). **Robaki** są samodzielne, przedostają się do komputera głównie przez pocztę elektroniczną i mogą dalej działać w systemie, niszcząc pliki lub rozsyłając z naszej skrzynki spam. Znacznie groźniejsze **trojany** pozwalają na wykradanie danych z Twojego komputera lub nawet przejęcie nad nim kontroli. Takie przejęcie jest szczególnie groźne, gdy jesteś akurat zalogowany do stron transakcyjnych (bankowych lub aukcyjnych) i wykonujesz w tym czasie płatności. Ktoś, kto włamuje się do Twojego komputera za pomocą trojana, może bowiem przekierować pieniądze znajdujące się na Twoim koncie na inne konto, czyli po prostu Cię okraść.

Odpowiednie programy zabezpieczające
Najprostszym sposobem ochrony przed wirusami, robakami i trojanami jest **instalacja odpowiedniego oprogramowania,** które pomogą ochronić Twój komputer i dane.

Podłączając komputer do Internetu, **zainstaluj zaporę sieciowa tzw. firewall.** Firewall jest jednym ze sposobów zabezpieczania sieci i systemów przed intruzami. Termin firewall może odnosić się zarówno do sprzętu komputerowego wraz ze specjalnym oprogramowaniem, jak i do samego oprogramowania blokującego niepowołany dostęp do komputera, na którego straży stoi. Zapory sieciowe są zwykle stawiane na styku dwóch sieci komputerowych, np. Internetu i sieci lokalnej (LAN) oraz na ważnych serwerach. Zaporę możesz kupić jednocześnie z systemem operacyjnym lub, jeśli jeszcze jej nie masz, kupić w sklepie lub Internecie i zainstalować ją samemu. Większość programów ma tak wyraźne instrukcje, że powinieneś zainstalować je samodzielnie. Jeśli nie masz takiej pewności, poproś kogoś zaufanego. Popularne zapory programowe to Sygate Personal Firewall, Agnitum Outpost Firewall Pro.

W tej samej kolejności zainstaluj na komputerze **aktualny program antywirusowy**. Przeszukuje on wszystkie pliki i programy zainstalowane na komputerze i te ściagane z Internetu i sprawdza, czy nie ma w nich wirusów i innych szkodliwych aplikacji. Programy antywirusowe skanują wszystkie informacje, które instalujesz na swoim komputerze, również te, które sam wprowadzasz do komputera mechanicznie, nie korzystając z Internetu - przez płyty CD, DVD, pamięci masowe, pen drive'y.

Pamiętaj również, aby zainstalować firewall i oprogramowanie antywirusowe przed podłączeniem komputera do Internetu!

Programy antywirusowe istnieją w wersjach bezpłatnych w Internecie – są to zazwyczaj wersje próbne (wersja testowa, trial), których czas funkcjonowania wynosi zazwyczaj 30 dni. W przypadku, gdy decydujesz się ściągnąć wersję bezpłatną, pamiętaj, aby po zakończeniu okresu próbnego natychmiast zainstalować kolejną wersję programu antywirusowego. Można też zakupić takie oprogramowanie (w racjonalnej cenie ok. 100 zł za rok). Popularne programy to AVG, avasti!, este NOD.

Poczta mailowa jest najbardziej rozpowszechnioną usługą internetową. Z poczty korzysta prawie każdy użytkownik Internetu. Zazwyczaj korzystamy z poczty na dwa sposoby – przez program pocztowy (najpopularniejszym jest Microsoft Outlook – sprzężony z systemem Windows) lub przez przeglądarkę internetową (np. logujemy się do poczty bezpośrednio z serwisu np. onet.pl, wp.pl lub gmail.com). Program pocztowy najczęściej mamy zainstalowany na stale na komputerze osobistym

(stacjonarnym domowym lub na laptopie). Dostępu do poczty z poziomu przeglądarki internetowej używamy poza domem.

W obu przypadkach – poczta to jedno z najbardziej wrażliwych miejsc, przez które mogą przedostać się wirusy. Programy pocztowe wyposażone są w standardowe zabezpieczenia, które filtrują naszą pocztę ze spamu oraz usuwają podejrzane pliki, zawierające wirusy lub szkodliwe aplikacje. Producenci tych programów stale pracują nad ich udoskonalaniem, dlatego warto na bieżąco aktualizować program pocztowy i inne ustawienia systemowe. Jeśli masz system Windows i używasz przeglądarki Internet Explorer, zrób to w następujący sposób. Kliknij przycisk start i wejdź do panelu sterowania, tam znajdź ikonkę Aktualizowanie automatyczne i ustaw aktualizację programów np. co 24 godziny. Następnie kliknij ikonkę system i dalej, również w tym aplecie włącz opcję Aktualizowanie automatyczne co 24 godziny.

Aktualizacja. Nawet najlepsze oprogramowanie antywirusowe nie pomoże, jeżeli nie będziemy go aktualizować. Wirusy, robaki i trojany stale się zmieniają, podobnie jak i oprogramowanie antywirusowe, dlatego korzystaj z zasobów sieci i instaluj je za darmo, jak najczęściej! Podobnie rzecz ma się z oprogramowaniem - systemem operacyjnym (Windows, Linux), programami pocztowymi – one też są stale ulepszane na wypadek ataku wirusowego, dlatego pobieraj aktualizacje jak najczęściej.

Kopie zapasowe danych oraz systemu. Poza regularną aktualizacją, raz na jakiś czas pamiętaj o robieniu kopii swoich danych oraz systemu, na którym pracujesz. Najlepiej kupić w tym celu drugi twardy dysk o odpowiedniej pojemności i np. co miesiąc podłączać go do komputera i kopiować dane. Racjonalnie jest kopiowanie tych folderów, na których stale pracujemy lub w których coś zmienialiśmy. Na dodatkową pamięć warto skopiować również sam system (Windows lub inny) na wypadek, gdyby wirusy zainfekowały pliki systemowe i trzeba było przywracać do działania cały system operacyjny.

BEZPIECZNE SERFOWANIE W INTERNECIE

Bezpieczne korzystanie z Internetu nie opiera się wyłącznie na zabezpieczeniach technologicznych, czyli różnego rodzaju narzędziach wykrywających i usuwających szkodliwe programy z Twojego komputera. Równie ważne jest Twoje rozsądne działanie. Poniżej przegląd kilku najbardziej oczywistych sytuacji, w których, świadomie lub nie, narażamy się na najpowszechniejsze niebezpieczeństwo Internetowe – kradzież danych osobowych. Przypomnijmy: dane osobowe to wszelkie informacje umożliwiające identyfikację osoby – jej tożsamość adres, numer NIP, numer telefonu, data urodzenia, ale też cechy fizyczne – wygląd, wzrost, wykształcenie itp. Do kradzieży danych osobowych należy również kradzież naszych zdjęć ze stron, na których je zamieszczamy.

Hasło

Serfując po Internecie, przeglądasz tysiące stron i często logujesz się na nich, żeby pogadać, ściągnąć filmy, zagrać lub za coś zapłacić.
Sprawa podstawowa - zadbaj o hasło. Niezależnie od tego, czy korzystasz z Internetu w domu czy poza nim, bądź szczególnie wrażliwy na to, jak układasz swoje **hasła**. Hasło musi być mocne – najlepiej, żeby składało się z kombinacji cyfr i liter – małych i dużych np. **AjuK1o22**. Stosuj mocne hasła do wszystkich stron, na jakich się logujesz – nie tylko do banku.

Używaj różnych haseł do **różnych usług**. To bardzo ważne. Używanie tego samego hasła do różnych witryn jest wygodne, ale bardzo niebezpieczne. Można to porównać do posiadania dziesięciu domów, w różnych częściach kraju, do których pasuje jeden klucz. Jeśli zgubisz ten klucz i trafi on w niepowołane ręce, stracisz majątek nie z jednej, lecz z 10 nieruchomości.

Rejestrując się na jakiejś stronie (banku, na forum), mamy wrażenie, że podane przez nas hasło jest szyfrowane i nawet administratorzy nie mają do nich dostępu. Nigdy nie ma jednak takiej pewności, po pierwsze, czy hasło zostało zaszyfrowane, po drugie, czy administrator systemu nie okaże się nieuczciwy. Dlatego należy zdecydowanie unikać powtarzania haseł. Raz ukradzione hasło sprawia

bowiem, że złodziej uzyska dostęp do pozostałych usług, z których korzystamy – a co najgroźniejsze – do naszych kont.

Korzystając z innego komputera niż własny, nigdy **nie „zapamiętuj" haseł w menedżerach**. W zasadzie zalecenie to powinno dotyczyć również komputera w domu (lub osobistego laptopa) – przecież i z niego może skorzystać ktoś niepowołany. Nawet w domu powinniśmy nauczyć się wpisywać hasło z klawiatury. To trudne, ale wykonaj ten wysiłek kilka razy, tak aby wszedł Ci w nawyk. Jeżeli przypadkiem zapamiętasz na cudzym komputerze swoje hasło i login – niepowołana osoba będzie mogła zapoznać się z Twoim danymi. Bądź na to szczególnie wrażliwy korzystając z poczty w miejscu publicznym – kafejce lub bibliotece.

Często lekceważymy tę kwestię mówiąc – w miejscach publicznych Internetu używam tylko do sprawdzenia poczty, nie płacę rachunków, nie podaję numeru karty kredytowej. Nawet dostęp do Twojej poczty może być jednak dla oszusta atrakcyjny. Mając dostęp do Twojego konta e-mail, może przejąć kontrolę nad Twoim kontem Allegro (zespół Allegro przesłał Ci przecież na Twoją pocztę hasło i login użytkownika, prawda?), czy numerem GG (często przesyłamy ten numer znajomym przez pocztę mailową). Ktoś może podszyć się pod Ciebie na GG i narobić wiele zamieszania wśród znajomych lub upublicznić Twoją korespondencję ze szczegółami, które chciałbyś zachować dla siebie.

Prywatność i anonimowość
Wielu z nas jest przekonanych, że korzystanie z sieci zapewnia jej anonimowość. Nick na forum, numer GG pozwalają ukryć imię i nazwisko, a wręcz wymyślić nową osobę.

Pamiętaj: nigdy nie jesteś anonimowy w Internecie. Stosunkowo łatwo można dotrzeć do Twoich danych. Udzielając się na forach, logując się do poczty lub innego serwisu internetowego, zostawiasz po sobie ślad, jakim jest adres IP komputera. Adres IP to zbiór cyfr, który ma każdy komputer podłączony do sieci. Dostawcy Internetu posiadają dokładne rejestry zapisujące dane osoby łączącej się spod określonego adresu. Pozwala to lokalizować konkretną osobę, jej dane i adres, na jaki wykupiła usługę dostarczania Internetu. Po adresie IP można dotrzeć do Twojego miejsca zamieszkania – osoby uprawnione np. policja często korzystają z takiej możliwości.

Nie trzeba być jednak policjantem, żeby odkryć Twoje dane osobowe. Mimo że do adresu IP zazwyczaj nie są przyporządkowane kompletne dane – najczęściej jest to tylko adres pocztowy, a nie imię i nazwisko użytkownika, to pozostałe elementy nietrudno jest uzyskać. Skąd? Np. z serwisów społecznościowych – typu nasza-klasa, grono lub komunikatorów np. Gadu-Gadu. Duża cześć użytkowników, rejestrując się na takich serwisach, zostawia tam prywatne dane – numer telefonu, adres mail, numer GG do publicznego wglądu. **Pamiętaj – nie podawaj zbyt hojnie swoich danych na jakichkolwiek serwisach.** Informacje, które mogą naprowadzić oszustów na nasz trop, należy **ukrywać** lub podawać bezpośrednio na mail osobom, które znamy. W przypadku, w którym nie jesteś pewien z kim rozmawiasz na czacie, forum czy gg – nigdy nie podawaj swojego nazwiska, a tym bardziej adresu zamieszkania.

Podobnie rzecz ma się z komunikatorami – często szukając informacji w sieci (szukając produktów, znajomych na forach itp.), podajemy swoje imię i nazwisko wraz z numerem GG! Odszukanie nas w takim przypadku jest dziecinnie łatwe – wystarczy wpisać nasz numer GG w wyszukiwarkę – i jeżeli gdziekolwiek podaliśmy numer połączony z nazwiskiem – wystarczy cierpliwie przeszukać strony wyświetlone przez wyszukiwarkę. Potem połączony numer GG z nazwiskiem ponownie wstukać w wyszukiwarkę, i jeżeli taka kombinację podaliśmy w serwisie społecznościowym typu nasza-klasa, osoba sprawdzająca nas będzie miała komplet danych łącznie z adresem, datą urodzenia i innymi danymi, które hojnie umieszczamy np. na naszej-klasie. **Pamiętaj – bycie anonimowym w Internecie jest prawie niemożliwe.**

Blogi

Duża cześć młodych użytkowników Internetu zakłada swoje blogi, czyli internetowe pamiętniki, aby publikować na nich swoje historie, często z pełna dokumentacją fotograficzną. Najczęstszym atakiem, jaki dotyka bloga, **jest kradzież fotografii.** Ta sama uwaga dotyczy zamieszczania zdjęć na serwisach społecznościowych. Niestety, jak pokazuje statystyka, złodzieje bardzo często wykorzystują te zdjęcia do montażu zdjęć pornograficznych. Jak się przed tym ustrzec? Przede wszystkim zamknij swój blog na otwarty dostęp z sieci, tak, żeby był niewidoczny po ręcznym wpisaniu adresu. Każdy narzędzie do pisania bloga ma taką funkcję. Adres zamkniętego bloga wraz z kodem dostępu do niego prześlij tylko tym znajomym, których uważasz za bliskich. Na serwisach społecznościowych nie zamieszczaj zbyt śmiałych zdjęć, tym bardziej zdjęć dzieci. **Pamiętaj – nigdy nie wiesz co może spotkać Twój wizerunek (zdjęcie), jeśli wrzucisz je do otwartej sieci.**

Czaty i gry sieciowe
Problem anonimowości dotyczy również w dużej mierze gier sieciowych i czatów. Tam również podajemy sporo informacji o sobie. Pamiętaj – nigdy nie podawaj swoich danych osobowych – imienia, nazwiska lub adresu innym użytkownikom gry lub czatu, gdyż mogą je wykorzystać do celów, których się nie spodziewasz.

PIENIĄDZE
Najbardziej boleśnie kradzież danych odczuwamy wtedy, gdy tracimy pieniądze. Wchodząc do normalnego sklepu w mieście, widzimy osobiście sprzedawcę lub właściciela przedmiotu, który chcemy kupić. Korzystając z analogicznych usług w Internecie – nie wiemy w istocie, kto jest twórcą serwisu, z którego korzystamy, a w przypadku aukcji internetowych – jaka jest reputacja tego, kto wystawia na sprzedaż swój przedmiot. Dlatego zawsze warto sprawdzić reputację sklepu, dane teleadresowe firmy zawarte na stronie lub po prostu zadzwonić pod wskazany numer telefonu.

Na poważne oszustwa jesteśmy narażeni przede wszystkim korzystając ze stron sieciowych usługodawców: banków, sklepów, linii lotniczych. Wszędzie tam gdzie przelewamy pieniądze – czy bezpośrednio z konta, czy też z karty kredytowej, musimy zwrócić szczególną uwagę na to, jakich zabezpieczeń technicznych używają się do ochrony wpisywanych przez nas danych. Standardową metodą powinno być szyfrowanie danych wpisywanych przez klienta.

Szyfrowanie danych
Okazuje się, że duża cześć oszustów czerpie informacje o przyszłych ofiarach z Internetu. Nie dzieje się to jednak wyłącznie przez odkrycie danych osobowych, które zbyt lekkomyślnie pozostawiamy do otwartego wglądu na forach lub serwisach społecznościowych. Nie chodzi również o włamanie się do poczty i pobranie z niej prywatnej korespondencji lub haseł i loginów do serwisów aukcyjnych.

Statystycznie, najbardziej bolesne kradzieże – te finansowe, dokonują się niejako za naszymi plecami. Jak to się dzieje? Rejestrując dane (hasła i kody) w Internecie, nie przesyłamy ich bezpośrednio na serwer usługodawcy. Zanim do niego dotrą, „podróżują" przez kilka serwerów przenoszone przez specjalne aplikacje. Teoretycznie, usługodawcy powinni dbać o maksymalne bezpieczeństwo przesyłu danych, dlatego je szyfrują. W praktyce jednak nadal jest to ryzykowne, gdyż aplikacje przenoszące dane są w istocie aplikacjami otwartymi.

Przede wszystkim **sprawdź, czy transakcja jest szyfrowana**. Gdy korzystasz ze stron transakcyjnych, czyli dokonujesz płatności, najczęściej w prawym dolnym rogu przeglądarki powinna pojawić się niewielka ikonka przedstawiająca żółta kłódkę. Jeżeli ten obrazek się pojawi – możesz mieć pewność, że transakcja zostanie zaszyfrowana. Po kliknięciu na kłódkę można otrzymać informację nt. sposobu szyfrowania. Sposoby te są różne, najczęściej wykorzystywanym i bardzo bezpiecznym sposobem jest wykorzystanie protokołu Secure Sockets Layer (SSL). Informacje przechodzące przez ten protokół są automatycznie szyfrowane przy użyciu klucza szyfrującego o długości 128 bitów (jest to najwyższy poziom szyfrowania dostępny komercyjnie). Większość sprawdzonych usługodawców używa protokołu SSL.

Zakupy i płatności

Jeżeli płacisz należności z banku lub używasz karty kredytowej do tego, żeby zapłacić za coś w Internecie, **cały czas musisz znajdować się w trybie szyfrowanym.** Jeżeli mimo to boisz się podać numer karty, można skorzystać z innego sposobu. Część witryn umożliwia przesłanie go faksem lub podanie przez telefon. Pamiętaj! To ty musisz zadzwonić do sklepu. W żadnym wypadku nie należy podawać numeru karty osobie, która zadzwoniła do nas i o to poprosi. Trzeba zainicjować połączenie dzwoniąc wyłącznie na numer podany na stronie internetowej! Podobnie, nigdy nie wysyłaj informacji o karcie pocztą elektroniczną! Każdy krok (rejestracja, zamówienie, podanie nowego numeru karty) jest potwierdzany emailem przesyłanym na podane wcześniej konto pocztowe.

Niestety, bezpieczeństwo transakcji nie kończy się na szyfrowaniu. Ważne jest też to, jak bank lub sklep, w którym coś kupiliśmy za pomocą karty przez Internet, przechowuje nasze dane. Przechowuje je na serwerach, które powinny znajdować się pod bardzo ścisłą ochroną, zarówno pod względem fizycznym, jak i elektronicznym. Serwery te nie powinny być na stałe podłączone do sieci Internet, a dostęp do nich powinny mieć tylko osoby uwierzytelnione.

O ile jednak pewność, że duże instytucje np. banki, przechowują nasze dane w taki sposób, ta pewność jest znacznie ograniczona jeśli chodzi o internetowe sklepy. W praktyce, trudno wyobrazić sobie, żeby wszystkie dysponowały własnymi, odrębnymi serwerami do gromadzenia danych, nie podłączanymi zbyt często do sieci. Utrzymanie takich „nieaktywnych" serwerów jest przecież bardzo kosztowne.

Dlatego rób **zakupy w dużych, znanych i renomowanych sklepach internetowych**. Takie firmy inwestują znaczne pieniądze w zapewnienie bezpieczeństwa transakcji i gromadzonych danych. Zapewniają także profesjonalną obsługę. O mniejszych, mało znanych sklepach warto dowiedzieć się czegoś więcej – zorientować się, czy rzeczywiście są to sklepy, a nie przedsięwzięcia mające na celu wyłudzenie Twoich pieniędzy. **Zanim dokonasz kupna, sprawdź,** jakie są koszty przesyłki oraz akceptowane sposoby płatności. Wybieraj sklepy, które akceptują przelewy lub płatności przy odbiorze – unikasz wtedy podawania własnych danych transakcyjnych usługodawcy.

Ponadto polecam klasyczne formy potwierdzenia wiarygodności kontrahenta – sprawdzenie, czy właściciel opublikował na stronie sklepu dane umożliwiające kontakt, czy można zweryfikować dane firmy. Jeśli cokolwiek budzi Twoje wątpliwości – **zadzwoń pod podany numer kontaktowy**.

Aukcje

Bardzo chętnie kupujemy towary na aukcjach internetowych. Najczęstszym oszustwem jest oczywiście sprzedaż rzeczy używanych jako nowe lub podróbek jako markowe. Warto wtedy odesłać towar, zawiadomić obsługę Allegro i w przypadku problemów z odzyskaniem pieniędzy – wystawić kontrahentowi negatywny komentarz. Większym niebezpieczeństwem są jednak fikcyjne transakcje, gdzie płacisz, a towar nie zostaje dostarczony, a konto kontrahenta znika.
Oszuści aukcyjni działają często w grupach, tworząc konta i wystawiając sobie wzajemnie pozytywne komentarze. Dlatego, sprawdzając komentarze, patrz, z jakiego pochodzą okresu (oszuści nie budują reputacji długo – ich komentarze często wystawione są w krótkim okresie czasu) i czy nicki komentujących powtarzają się. Ponadto, duże serwisy aukcyjne (Allegro i ebay) ubezpieczają transakcje. Np. na Allegro w ramach „Programu ochrony kupujących" można uzyskać rekompensatę finansową nawet do 10 000 – warunkiem jest złożenie zawiadomienia o przestępstwie w rejonowej Komendzie Policji.

Banki, czyli tam, gdzie trzymamy najwięcej

Przejdźmy do transakcji bankowych. Najbardziej rozpowszechnioną formą okradania klientów banków przez Internet był do tej pory tzw. **phishing,** czyli wyłudzenie haseł do kont poprzez podszywanie się pod bank i np. rozsyłanie korespondencji udającej bankową. Sytuacja wygląda następująco. Masz konto w banku z dostępem elektronicznym. Na Twoje konto mailowe przychodzi list. List zawiera link do strony Twojego banku. Po kliknięciu na link wskazany w mailu, użytkownik zostaje przekierowany na podrobioną stronę banku – często o bardzo podobnym adresie do oryginalnego (np. bzg.pl zamiast bgz.pl – przykład teoretyczny). Jeśli ktoś nie spojrzy dokładnie na

pasek adresu i próbuje zalogować się na takiej stronie, nieświadomie przekazuje oszustowi login i hasło do konta. Banki uprzedzają swoich klientów, żeby przed zalogowaniem się nigdy nie wpisywali na stronie startowej ani haseł jednorazowych, służących wyłącznie do potwierdzania poleceń na stronach transakcyjnych, ani numeru rachunku. **Zawsze sprawdzaj żółtą kłódkę,** tylko wtedy transmisja odbywa się w bezpiecznym połączeniu (protokół SSL). Po zakończeniu czynności związanych z obsługą konta, wyloguj się ze strony, wybierając odpowiednią opcję – najczęściej „Log out", „Wyloguj" lub „Wyjście".
Patrz na adres! Formę oszustwa związaną z przekierowaniem na podrobione strony łatwo jednak wytropić, patrząc uważnie na adres, jaki wyświetla nam się na pasku, przed zalogowaniem. Zamiast www.mbank.com.pl może pojawić się np. www.mbakn.com.pl. Strona może wyglądać tak samo, a jednak być zarządzana przez złodziei. Chroni przed tym ręczne wpisywanie adresu strony w przeglądarce!

Oszuści wymyślają więc coraz bardziej skomplikowane formy kradzieży. W Polsce pojawiły się już trojany, które bez wiedzy użytkownika przekierowują go na fałszywą stronę, nawet gdy wpisze on w przeglądarce adres banku. Robią to za pomocą wirusów nakładanych na przeglądarki internetowe. Bądź czujny cały czas i cały czas sprawdzaj, na jakiej jesteś stronie.

FIZYCZNA CZUJNOŚĆ

Poza zabezpieczeniami technologicznymi przed wirusami, trojanami i pozostałymi szkodliwymi większość zabezpieczeń wymaga Twojej fizycznej czujności.

Pamiętaj:
- nie dopuszczaj nieuprawnionych użytkowników do własnego komputera,
- gdy robisz zakupy lub płacisz przelewy - sprawdzaj, czy połączenie jest szyfrowane, a adres banku – właściwy,
- zawsze wyloguj się z sesji transakcyjnych,
- nie udostępniaj danych osobowych na forach, czatach, serwisach społecznościowych,
- twórz mocne hasła,
- nie zapamiętuj haseł w menadżerach haseł,
- używaj różnych haseł do różnych usług.

Te proste czynności, nie wymagające wielkich nakładów z Twojej strony, ani finansowych, ani technologicznych, a pozwolą znacznie zmniejszyć niebezpieczeństwo związane z kradzieżą danych lub pieniędzy.

GDY JUŻ SIĘ STANIE

Jak postępować w momencie, gdy padniemy już ofiarą oszustwa? Pierwszym krokiem jest zawiadomienie o przestępstwie. Nie bagatelizuj tego – coraz więcej komend policji zatrudnia specjalistów od tropienia przestępstw internetowych. Jeżeli złodziej, który podszył się pod Ciebie na aukcji i przejął Twoją należność używa stałego adresu IP, jego namierzenie jest dla policji bardzo prostą kwestią. Przestępstwo takie należy zgłosić we właściwej miejscu zamieszkania Komendzie Policji. Jest ono ścigane z artykułu 286 §1 Kodeksu karnego, który stwierdza, że odpowiedzialności karnej podlega osoba, która w celu osiągnięcia korzyści majątkowej doprowadza inną osobę do niekorzystnego rozporządzenia własnym lub cudzym mienie za pomocą wprowadzenia jej w błąd lub niezdolności do należytego pojmowania przedsiębranego działania. Warto pamiętać, że kodeks nie określa w przypadku oszustwa minimalnej kwoty przesądzającej o uznaniu go za przestępstwo.

Podsumowując kwestię kradzieży i wyłudzeń – ważna rada. Płacąc za cokolwiek przez Internet, należy korzystać wyłącznie ze sprawdzonych i pewnych komputerów. W żadnym wypadku z ogólnodostępnych stanowisk internetowych (np. w kawiarenkach internetowych, bibliotekach publicznych, szkolnych laboratoriach, itd.). Należy być również czujnym podłączając się do sieci otwartych LAN za pomocą własnego komputera lub korzystając z hot-spotów i połączeń GSM. Złodzieje, stosując odpowiednie oprogramowanie, „podsłuchują" ruch w sieci (**sniffing)** i w ten

sposób mogą odczytać nasze hasła. Nie ma niestety dobrego zabezpieczenia przed sniffingiem – szczególnie, jeśli administrator sieci LAN jest temu niechętny. Dlatego po raz kolejny zachęcam do niewchodzenia na strony transakcyjne w publicznych miejscach, a w przypadku wyjazdów, w trakcie których na dłuższy czas rozstajemy się z zabezpieczonym dostępem do sieci, pozostawienia na kontach dyspozycji zapłacenia rachunków, tak abyśmy nie musieli tego dokonywać w przypadkowych warunkach.

UZALEŻNIENIE I INNE NIEBEZPIECZEŃSTWA

Poza opisywanymi zagrożeniami istnieje jeszcze cały szereg niebezpieczeństw, na które możesz natknąć się w Internecie. Są to m.in niebezpieczne treści – przemoc, pornografia, hazard, handel używkami. Stron poświęconych przemocy i pornografii jest statystycznie najwięcej. Natykasz się na nie, czy tego chcesz, czy nie.

Łamanie prawa. Sieć jest pełna stron, z których możesz bezpłatnie ściągnąć filmy, muzykę, prace magisterskie i wypracowania – pamiętaj, że w większości przypadków – łamiesz prawa autorskie. Internet jest też źródłem informacji dla terrorystów – ilość informacji, która w nim krąży, daje podstawę do opracowania dokładnych planów miejsc ataku, daje możliwość nieograniczonej komunikacji przestępcom. Poza wymienionymi, siłą rzeczy pobieżnie, niebezpieczeństwami Internet niesie również szereg zagrożeń psychospołecznych. Długotrwałe korzystanie z Internetu utrudnia nawiązanie relacji w prawdziwym życiu i prowadzi do uzależnienia.

Uzależnienie od Internetu (*online addiction*, *Internet addiction*) staje się dziś takim samym problemem społecznym jak alkoholizm czy zażywanie narkotyków. Jest to zjawisko coraz częściej opisywane choć trudno się je bada. Nie dość, że trudno zdefiniować grupę reprezentatywną dla użytkowników, to ciężko jest precyzyjnie ustalić, co konkretnie jest uzależnieniem. Czy czas spędzony przy komputerze? Czy korzystanie z poczty? Przeglądanie serwisów informacyjnych?

Jeśli istnieje coś takiego jak uzależnienie od Internetu, to jest to niemożność oderwania się od jakiejś jego funkcji – a w przypadku odłączenia się od sieci – częstotliwość myślenia o podłączeniu się do niego. Ponieważ jest to mechanizm bardzo skomplikowany, przyjmij, używając zdrowego rozsądku, że jeżeli zaczynasz spędzać w Internecie tyle czasu, że zaczyna Ci go brakować na realne kontakty z innymi ludźmi – jesteś uzależniony. Gdy wchodzisz do domu i zaraz po zdjęciu butów a przed umyciem rąk włączasz komputer bez wyraźnego powodu – można to uznać za symptom uzależnienia.

Jak się przed tym bronić? Zachować zdrowy rozsądek – ograniczać czas spędzany przed monitorem, nie zostawiać włączonego komputera przez cały czas, nie sprawdzać poczty co 5 minut, nie przeglądać informacji bez widocznego celu, a przede wszystkim pamiętać o tym ,że kontakt z maszyną nie zastąpi kontaktu z innymi ludźmi.

Jeśli zaczynasz podejrzewać uzależnienie od Internetu w przypadku Twojego dziecka – nie panikuj. Poobserwuj dziecko i jego zwyczaje przez kilka dni i jeśli zauważysz, że spędza przed monitorem więcej czasu niż poza nim – porozmawiaj spokojnie z dzieckiem. Nie groź, nie strasz. Powiedz, że czujesz się zaniepokojony; wyznaczcie wspólnie ramy czasowe poruszania się w Internecie oraz określcie podstawowe funkcje, które ma on dla dziecka spełniać. Jeśli dziecko zbyt dużo gra – zaproponuj, żeby grało tylko co drugi dzień, jeśli zbyt dużo czatuje – zaproponuj, żeby zaprosiło kolegów do domu. Jeśli podejrzewasz, że problem jest głębszy – skontaktuj się z organizacjami, które zajmują się uzależnieniami wśród młodzieży i poproś o konsultacje. Pomoc znajdziesz na stronach: www.kidprotect.pl, www.sieciaki.pl, www.dzieckowsieci.pl.