BEZPIECZNY INTERNET KROK PO KROKU

PORADNIK NIE TYLKO DLA SENIORA

Wojciech Wrzos

SPIS TREŚCI

WSTĘP

Internet: Spacer po polu minowym?

– To widzimy się na Skypie?
– Wrzuć to na Youtube'a!
– Daj mi znać na fejsie.
Zapewne nie raz, nie dwa – przysłuchując się rozmowom młodych ludzi, choćby naszych dzieci lub wnuków – słyszeliśmy podobne zdania. I niejeden raz zadawaliśmy sobie w duchu pytanie: W jakim świecie oni żyją? Czy to inna rzeczywistość niż ta, w której żyję ja? Odpowiedź na to pytanie nie jest wbrew pozorom skomplikowana. Młodzież porusza się dzisiaj równie sprawnie w świecie rzeczywistym, jak i w wirtualnej przestrzeni internetu. Często my, ludzie dojrzali, chcielibyśmy także funkcjonować w globalnej sieci, ale powstrzymuje nas obawa przed nieznanym gruntem, który wydaje nam się bardzo grząski. Nie warto jednak tak myśleć – internet jest środowiskiem, które może znacząco poprawić jakość naszego życia w wielu jego dziedzinach: ułatwić kontakty z bliskimi, zdobyć nowych znajomych, uzyskać ciekawe informacje, przeczytać interesującą książkę, szybko załatwić przelew w banku albo niejedną urzędową sprawę, wreszcie zapewnić fajną rozrywkę przy zabawie w gry czy oglądaniu filmów.
Niektórzy powtarzają jak mantrę, że internet jest niebezpieczny. Że może nam wyrządzić krzywdę, a różnej maści zagrożenia tylko czekają na to, by nas

zaatakować, zniszczyć nasz komputer, oszukać nas samych, wykraść poufne dane i ograbić nasze konto bankowe. Czy mają rację? Byłoby kłamstwem powiedzieć, że absolutnie się mylą, a globalna sieć jest miejscem idealnie bezpiecznym. Nie jest. Ale też nie jest bardziej groźna niż otaczający nas realny świat, który świetnie znamy i w którym potrafimy się poruszać. W jaki sposób udało nam się dożyć w tym świecie wieku, w którym skroń przyprószyła już siwizna? Po prostu jesteśmy świadomi istniejących w nim zagrożeń, a zdrowy rozsądek i inteligencja pozwalają nam unikać tych pułapek.

Tak samo jest w wirtualnej rzeczywistości internetu. Wystarczy wiedzieć, gdzie czekają na nas zdradliwe mielizny, by żeglować po tych wodach bezpiecznie i cieszyć się taką podróżą.

ROZDZIAŁ I

Poznaj swojego wroga

ROZDZIAŁ I
Poznaj swojego wroga

O tym, że zombie to nie tylko wymysł filmowców, że nie każdy policjant jest prawdziwy, a wędkowanie to nic przyjemnego, jeśli my jesteśmy rybą.

Znajomość zagrożeń, które możemy napotkać podczas korzystania z internetu, to pierwszy krok do tego, by sprawnie ich unikać. Przez kilkadziesiąt lat funkcjonowania globalna sieć dorobiła się pokaźnej kolekcji rozmaitych pułapek i narzędzi, którymi posługują się cyberprzestępcy po to, aby w wirtualnej przestrzeni zaszkodzić nam w sposób jak najbardziej realny. Oto szybkie spojrzenie na najważniejsze z nich.

Wirusy, trojany, rootkity i inne...

Jeżeli nasz system operacyjny jest słabo zabezpieczony lub gdy my sami niefrasobliwie zachowujemy się w sieci, to do naszego komputera mogą przedostać się szkodliwe kody różnej maści.

Komputerowy wirus przypomina w zachowaniu swojego imiennika ze świata biologii. Jego najważniejszą cechą jest zdolność do samodzielnego powielania. Wirus do zarażenia komputera potrzebuje nosiciela, podczepia się więc do określonego rodzaju pliku i w ten sposób jest przekazywany w internecie. Taki szkodnik może mieć wbudowane różne destrukcyjne funkcje, takie jak kasowanie danych czy uszkadzanie systemu operacyjnego.
Nazwę **„trojan”** słusznie skojarzymy ze znanym z historii starożytnej koniem trojańskim. Kryją się pod nią podstępne kody, które podszywają się pod niewinne z pozoru oprogramowanie, a po przedostaniu do komputera instalują szkodliwe funkcje i procedury.

Jeszcze bardziej perfidna jest natura **rootkita**. Pełni on rolę ochroniarza innych groźnych programów, na przykład wspomnianych trojanów, i sprawia, że stają się one niewidoczne dla aplikacji antywirusowej zainstalowanej w komputerze.

Robak internetowy jest bliskim krewnym wirusa, ale nie jego bratem bliźniakiem. Różnica polega na tym, że robak do działania nie potrzebuje pliku – nosiciela. Aby przedostać się do systemu, wykorzystuje luki w zabezpieczeniach systemu operacyjnego lub innych zainstalowanych aplikacji. Robak może realizować funkcje destrukcyjne lub szpiegowskie – ich dobór zależy wyłącznie od twórcy takiego szkodliwego kodu.

Keylogger to program, który bardzo dokładnie będzie patrzył nam na ręce, a dokładniej na to, co tymi rękami wpisujemy do komputera za pośrednictwem klawiatury. Keylogger zbiera te wszystkie znaki wystukane na klawiaturze po to, by przekazać na zewnątrz poufne dane, na przykład loginy i hasła do kont bankowych.

Spyware to po prostu dobrze wyszkolony szpieg. Tego typu oprogramowanie zbiera wszelkie informacje o wykonywanych przez nas w sieci czynnościach. Są wśród nich adresy odwiedzanych stron internetowych, numery kart kredytowych, loginy i hasła do serwisów.

Phishing – nie daj się złapać na haczyk

Z angielska *phishing* oznacza wędkowanie. Ale w dziedzinie internetowych zagrożeń nie ma on nic wspólnego z przyjemnym siedzeniem nad brzegiem rzeki i przysłowiowym moczeniem kija. To my bowiem występujemy w roli ryby, na

Prosimy o natychmiastowa odpowiedz

Drogi Kliencie,

Twoj kod dostepu wraz z hasłem do ING Bank wygasnie 26 lutego 2012, jako ze nastapi zmiana starego systemu bankowego na ulepszony system HLOB 2012.

Prosze KLIKNAC TUTAJ aby zagwarantowac ciagnac Twojego konta online, aby nie zostalo ono zaklocone lub deaktywowane.

Dziekujemy za ciagle wsparcie.

© ING Bank .

Tak może wyglądać próba wyłudzenia danych dostępowych do konta bankowego

którą polują cyberprzestępcy. Wysyłają oni do nas e-maile udające korespondencję od zaufanych instytucji (na przykład banków) i wyłudzają w ten sposób dane dostępowe do naszych kont (zob. ilustrację na s. 7). Phishing może też polegać na tworzeniu fałszywych witryn internetowych z oknem logowania, w które ofiary wpisują poufne informacje (zob. ilustrację na s. 9). To zaś już prosta droga do tego, by złodzieje otworzyli sobie drzwi do naszego rachunku bankowego.

Botnet – o rany, jestem zombie!

Działający obecnie w sieci przestępcy to nie tylko zwykli detaliści, starający się okraść pojedynczych internautów z ich poufnych danych albo z pieniędzy. W internecie, podobnie jak w realnym świecie, działają duże, dobrze zorganizowane grupy przestępcze, które przeprowadzają ataki na komputery największych firm czy też rozsyłają w świat miliony spamu (niechcianych, szkodliwych e-maili – będzie o nich mowa w rozdziale III). Do wykonania takich operacji konieczne jest wspólne działanie tysięcy pojedynczych komputerów podłączonych do internetu. Skąd przestępcy biorą je w takiej liczbie? Po prostu przejmują je od nas. W praktyce oznacza to, że komputery prywatnych użytkowników są bez ich wiedzy zamieniane w składniki armii zwanej botnetem (w żargonie takie maszyny nazywane są zombie) i wykonują wspólnie pożądane działania – wysyłają masowo spam lub uczestniczą w zmasowanym ataku na wskazane serwery. Kiedy nasz komputer zostanie wpięty do botnetu, nie będziemy nawet wiedzieli o tym, że bierzemy udział (wraz z tysiącami innych internautów) w przestępstwie.
Kiedy nasz pecet może stać się maszyną zombie? Wtedy, gdy przez niedostateczną ochronę lub nieuwagę pozwolimy na zainstalowanie w nim odpowiedniego szkodliwego oprogramowania.

Ransomware – przebrani za policjantów

To wyjątkowo wredny sposób wyciągania od internautów pieniędzy. Ransomware jest rodzajem złośliwego oprogramowania, które nie dość, że chce okraść ofiarę, to w dodatku potrafi ją mocno wystraszyć. Po przedostaniu się do komputera szkodnik blokuje całkowicie jego działanie, a na ekranie wyświetla ostrzeżenie. Jest w nim mowa o tym, że rzekomo popełniliśmy internetowe przestępstwo (na przykład używaliśmy pirackich programów) i w związku z tym zablokowano nam możliwość korzystania z peceta. Pod wiadomością podpisują się ludzie podający się najczęściej za policjantów. Są oni skłonni podać nam kod do odblokowania komputera, ale pod

warunkiem że wniesiemy odpowiednią (i dosyć wysoką) opłatę na wskazane konto bankowe. Ransomware jest niestety trudny do usunięcia dla większości zwykłych użytkowników – w wypadku zainfekowania komputera takim złośliwym kodem będziemy musieli poszukać pomocy specjalisty.

Kolejny przykład phishingu

Benecol

Specjalista w obniżaniu cholesterolu

Benecol **skutecznie obniża cholesterol** dzięki zawartości naturalnych stanoli roślinnych

JEDNO Z 10 NAJWIĘKSZYCH OSIĄGNIĘĆ W ŻYWIENIU ZAWIERA STANOLE ROŚLINNE

Stanole roślinne **blokują wchłanianie** spożytego cholesterolu oraz **zwiększają wydalanie** go z organizmu

CHOLESTEROL

Dzięki margarynie Benecol **kontrolujesz cholesterol i przywracasz jego prawidłowy poziom**

REKOMENDOWANY PRZEZ FUNDACJĘ ROZWOJU KARDIOCHIRURGII W ZABRZU

Benecol gwarantuje obniżenie cholesterolu o 7-10% po 2-3 tygodniach stosowania

Udowodniono, że estry stanoli roślinnych obniżają stężenie cholesterolu we krwi. Wysokie stężenie cholesterolu jest czynnikiem ryzyka rozwoju choroby wieńcowej serca. Korzystny efekt występuje w przypadku dziennego spożycia 1,5-2,4 g stanoli roślinnych.

www.benecol.pl

ROZDZIAŁ II

E-mail: Listonosz godny zaufania

ROZDZIAŁ II
E-mail: Listonosz godny zaufania

O tym, że dobre hasło przydaje się nie tylko podczas nocnej warty, jaki jest sposób na kłopoty z pamięcią i o tym, że Google to nie tylko wyszukiwarka.

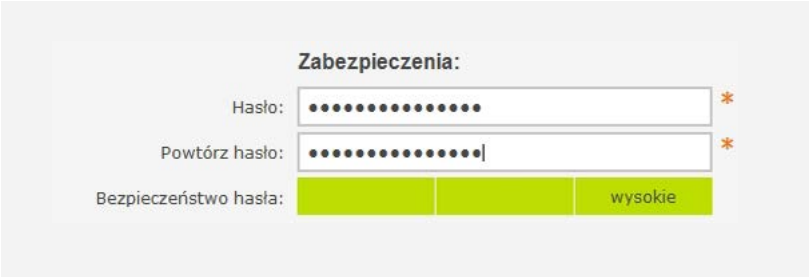
Wysyłanie i odbieranie wiadomości elektronicznych (e-maili) jest jedną z podstawowych aktywności użytkowników internetu. Chociaż pierwszy e-mail wysłano już ponad 40 lat temu, to internauci i dzisiaj nadal chętnie korzystają z tej formy korespondencji. Wystarczy powiedzieć, że tylko w ciągu jednej minuty na całym świecie zostaje wysłanych ponad 200 milionów elektronicznych wiadomości.
Z bezpieczeństwem poczty e-mail jest trochę tak jak z bezpieczeństwem naszej tradycyjnej, papierowej korespondencji. Złodziej może się niestety włamać do naszej skrzynki pocztowej, możemy też dostać w kopercie bombę zamiast oczekiwanego listu. Podobnie wygląda sprawa z e-mailami. Dlatego ważne jest odpowiednie zabezpieczenie naszego elektronicznego konta pocztowego i rozpoznanie potencjalnie groźnych przesyłek.

Hasło: Bezpieczny klucz, nie tylko do skrzynki

To może zabrzmieć banalnie, ale odpowiednie hasło do konta e-mail stanowi jedno z najważniejszych i najbardziej pewnych zabezpieczeń naszej elektronicznej korespondencji. Zwykle wybierając hasło do rozmaitych usług czy serwisów internetowych, padamy ofiarą własnej wygody i lenistwa. Ustalamy ciąg znaków (zwykle dosyć krótki), który będzie nam łatwo zapamiętać, a w dodatku lubimy stosować to samo hasło do logowania w kilku różnych usługach

(na przykład do poczty, profilu na Facebooku, Skype'a i internetowego konta bankowego).
Skutki takiego postępowania mogą być bardzo poważne. Wystarczy bowiem, by przestępcy złamali tylko jedno z naszych haseł, a będą mieli otwarte drzwi do wszystkich pozostałych, używanych przez nas usług. Mamy więc wiele do stracenia.
Na bezpieczeństwo konkretnego hasła ma wpływ kilka czynników. Pierwszy to jego długość – im dłuższe hasło, tym trudniej je odkryć. Za w miarę bezpieczny klucz można uznać taki, który składa się przynajmniej z ośmiu znaków, oczywiście lepsze efekty uzyskamy, stosując hasła zawierające 10, a nawet 14 znaków.
Dlaczego piszemy o znakach, a nie po prostu o literach lub cyfrach? Tutaj kłania się druga, obok długości, cecha dobrego, trudnego do złamania klucza. Możemy bowiem ustalić ciąg składający się, powiedzmy, z ośmiu symboli, który jednak pod względem zabezpieczeń nie będzie nic warty. Chodzi o takie hasła, jak na przykład **abcdefgh** czy też **12345678**. Są one do złamania niemal natychmiast przez specjalne, ale powszechnie dostępne w sieci programy przeznaczone do łamania kluczy. Podobnie przestawia się sprawa z rozmaitymi słowami, które wydają nam się proste i wygodne do zapamiętania, jednak ich wartość jako kluczy bezpieczeństwa jest wątpliwa. Mowa o takich hasłach jak **basia60** lub **barcelona**.
Idea dobrego hasła kryje się, obok jego długości, w stopniu skomplikowania i losowości. Dlatego najlepiej, aby klucz był wystarczająco długi, składał się z dużych i małych liter, a także znaków specjalnych, które widzimy na klawiaturze. Oczywiście idąc tym tropem, możemy dosyć łatwo utworzyć następujące hasło: **Mn1R@#5*jcbD*&^%**. Pozostaje jednak dosyć istotne pytanie: Kto z nas zapamięta takie monstrum? No właśnie... Dlatego spróbujmy utworzyć odpowiedni klucz nieco inną metodą.
Zacznijmy od popularnej piosenki, którą wielu z nas śpiewało w młodości na harcerskich obozach: **Płonie ognisko w lesie, wiatr smętną piosnkę niesie, przy ogniu zaś drużyna gawędę rozpoczyna**. Teraz stwórzmy szkielet hasła, używając pierwszych liter słów składających się na tę zwrotkę. Będzie to wyglądało tak: powlwspnpozdgr. Za mało. Dlatego co druga litera będzie duża: **PoWlWsPnPoZdGr**. Teraz wstawmy w miejsce niektórych liter podobne do nich cyfry, na przykład zamieńmy **o na 0, a l na 1**. Uzyskamy teraz taki klucz: **P0W1WsPnP0ZdGr**. Jesteśmy już bliscy celu, jednak możemy jeszcze dodatkowo utrudnić złamanie hasła, dodając znaki interpunkcyjne oraz specjalne symbole na początku i na końcu. Ostateczna

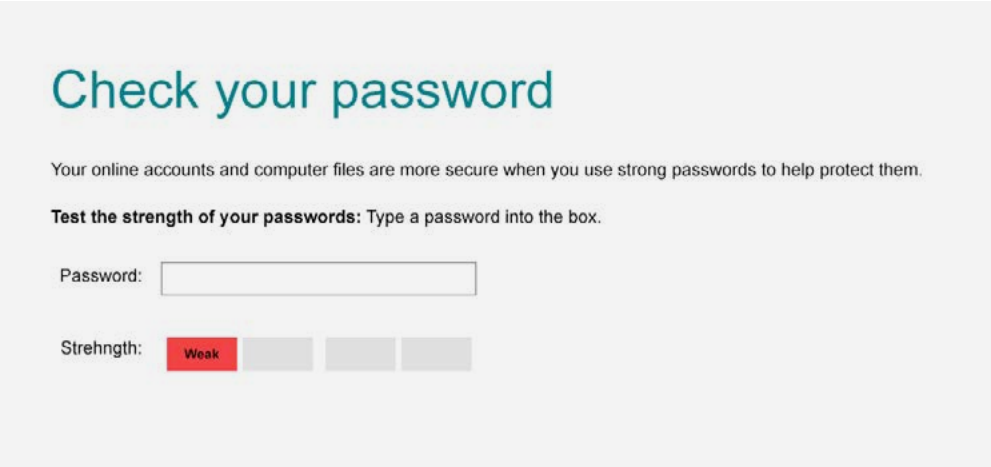
forma naszego klucza będzie wyglądała tak: **!P0W1,WsPn,P0Zd,Gr”**.
Takie hasło możemy uznać za odpowiednie, zawiera bowiem wszystkie elementy istotne z punktu widzenia wymogów co do jego skomplikowania i losowości. Zapamiętanie tego klucza ułatwi nam na pewno to, że pochodzi od dobrze znanej nam piosenki. Dodatkowo powinniśmy na próbę kilka, a najlepiej kilkanaście razy wpisać je na klawiaturze po to, by zapamiętać układ i kolejność używanych klawiszy.



Jak mocne jest nasze hasło?

Podczas zakładania konta pocztowego w wielu tego typu usługach (na przykład Onet Poczta, Gmail) przy ustalaniu hasła zobaczymy specjalny pasek, który pokaże nam stopień jego bezpieczeństwa. To jedna ze wskazówek pomagających przekonać się, czy utworzony przez nas klucz jest wystarczająco silny.

Innym sposobem ustalenia, czy hasło jest wystarczająco mocne, jest sprawdzenie go na jednej ze specjalistycznych stron internetowych. Muszą być one jednak godne zaufania. Jedna z takich witryn to www.microsoft.com/security/pc-security/password-checker.aspx. Wpiszmy na niej jedno ze wspomnianych wcześniej słabych haseł, na przykład **basia60**. Od razu zobaczymy, że nie jest ono bezpieczne.

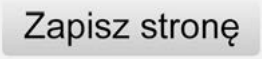


Teraz w tym samym oknie umieśćmy nasze wygenerowane w pocie czoła, skomplikowane hasło !P0W1,WsPn,P0Zd,Gr". Wynik nie wymaga komentarza:

Jak to wszystko zapamiętać?

Na początku tego rozdziału wspomnieliśmy o tym, że jednym z największych grzechów internautów jest stosowanie tego samego hasła w kilku różnych serwisach i usługach dostępnych w sieci. No tak, ale tworzenie oddzielnego klucza dla każdego logowania nastręcza dużych problemów z ich zapamiętaniem i wygodnym stosowaniem. Co zrobić? Na szczęście są sposoby, by w tym względzie ułatwić sobie życie.
Możemy skorzystać ze specjalnych programów, takich jak na przykład LastPass. Jest to aplikacja, która w zaszyfrowanej formie przechowuje nasze hasła do serwisów i pozwala logować się do nich bez konieczności każdorazowego zapamiętywania i wpisywania klucza. Program LastPass jest darmowy, ściągniemy go ze strony Lastpass.com. Aplikację instalujemy jako dodatek do używanej przez nas przeglądarki internetowej. Po dokonaniu tej czynności w nowym oknie przeglądarki klikamy na przycisk, który się tam pojawił:

Następnie rejestrujemy nowe konto w LastPass.
To wystarczy. Teraz po wejściu na konkretną stronę podajemy nasz login i hasło. Pojawi się pasek programu LastPass z propozycją zapisania naszych danych. Wybieramy przycisk:



Od tego momentu po każdorazowej wizycie na tej stronie nie będziemy już musieli wpisywać hasła. Zostanie ono automatycznie uzupełnione.

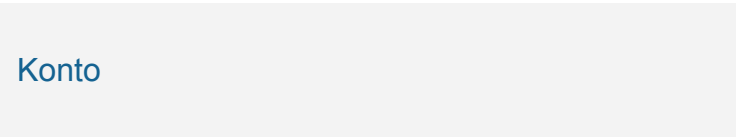
Gmail: Bezpieczeństwo w chmurze

Dzisiaj darmowe konto e-mail to codzienność. Dostęp do usług pocztowych zapewniają zarówno największe polskie

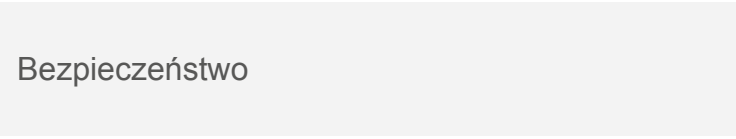
portale (Onet, Wirtualna Polska czy Interia), jak i dedykowane specjalne platformy (Gmail lub Outlook.com). Założenie konta pocztowego i korzystanie z niego online ma sporo zalet. Pozwala na przykład na obsługę naszej elektronicznej korespondencji bez konieczności korzystania z programów pocztowych, takich jak Outlook Express czy Thunderbird. Wystarczy, że zalogujemy się do usługi w konkretnym serwisie i mamy dostęp do całej naszej poczty niezależnie od miejsca, w którym akurat przebywamy i urządzenia, z jakiego korzystamy – może to być komputer biurkowy, notebook lub modny ostatnio tablet.
Jeśli chodzi o kwestie bezpieczeństwa, to wspomniane platformy zrobiły i robią wiele, by zasłużyć sobie na miano godnych zaufania. Jednak zawsze mogą zdarzyć się sytuacje, gdy ktoś z zewnątrz przejmie nasze konto pocztowe (na przykład za pomocą wspomnianego w poprzednim rozdziale oprogramowania spyware lub keyloggera). Dlatego warto poznać podstawowe zasady kontrolowania, czy wszystkie ustawienia konta e-mail są prawidłowe i czy w naszej skrzynce nie pojawili się nieproszeni goście.
Zobaczmy, jak to zrobić na przykładzie **Gmaila** – jednej z najbardziej popularnych obecnie usług pocztowych.

W głównym oknie naszego konta klikamy na ikonę awatara – jeśli nie umieściliśmy tam swojej fotografii, klikamy na pustą ikonę,

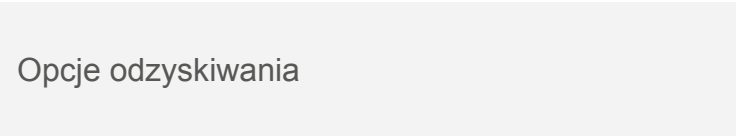
a następnie na przycisk:



Pojawi się nowa strona, na której wybieramy opcję:



Pierwszą rzeczą, która powinna nas zainteresować ze względów bezpieczeństwa, jest sekcja:



Po kliknięciu opcji Edytuj możemy wprowadzić alternatywny adres e-mail (inny niż ten, na który się obecnie zalogowaliśmy) lub numer telefonu. To pozwoli nam na odzyskanie dostępu do konta Gmail po jego przejęciu przez inną osobę lub przypomnienie nam hasła w wypadku jego utraty.

Przejdźmy teraz do działu:

Najnowsza aktywność

Jest on istotny, bo pozwoli nam na ustalenie, czy na naszym koncie nie zanotowano podejrzanych wydarzeń. Chodzi na przykład o to, czy na koncie nie doszło do logowania z poziomu innej przeglądarki internetowej niż ta, z której korzystamy. Przypadek takiego logowania można zobaczyć na ilustracji poniżej. Powiedzmy, że na co dzień do obsługi Gmaila używamy przeglądarki Opera. Tymczasem w widocznym zapisie znajdziemy logowania z Firefoksa i Chrome'a. To może być ważny sygnał, że ktoś niepowołany dostał się do naszej poczty. W takim wypadku najbezpieczniej będzie skorzystać z opcji proponowanej przez administratorów Gmaila, czyli:

– i zmienić dotychczasowe hasło do skrzynki.

Kilka szczegółów podwyższających bezpieczeństwo naszej poczty zmienimy w Ustawieniach konta. W głównym oknie wybieramy ikonę zębatego koła

i klikamy na:

Ustawienia

W zakładce Ogólne zaznaczamy opcję:

Używaj zawsze bezpiecznego protokołu HTTPS

natomiast w zakładce POP/IMAP opcję:

Wyłącz POP

jeżeli na co dzień nie używamy programu pocztowego do odbioru wiadomości z Gmaila. W ten sposób ograniczymy możliwość przesyłania dalej naszych wiadomości w przypadku ewentualnego włamania na konto.
Na koniec pozostaje jeszcze rodzaj pocztowego testamentu. Chodzi bowiem o decyzję, co ma się stać z naszym kontem e-mail w wypadku jego długiej bezczynności. Klikamy ponownie na Konto i wybieramy opcję:

Określ, co ma się stać z Twoim kontem, gdy przestaniesz korzystać z Google.
Dowiedz się więcej i przejdź do konfiguracji.

Pojawi się nowe okno, w którym możemy ustalić, po jakim okresie braku aktywności na koncie ma ono ulec likwidacji, w jaki sposób i kogo Gmail ma powiadomić o wygaśnięciu konta, a także od razu usunąć nasze konto pocztowe z usługi Gmail.

ROZDZIAŁ III

Spam: W powodzi e-mailingu

O tym, co łączy pocztę elektroniczną z puszką mielonki, jak odsiać ziarno od plew i co złego może nam zrobić jeden e-mail.

W znakomitym filmie „Dzień świra" Marka Koterskiego jest pewna scena. Grany przez Marka Kondrata Adam Miauczyński wraca do swojego mieszkania w bloku na osiedlu. Na klatce schodowej otwiera skrzynkę pocztową. Jednak zamiast oczekiwanych listów wysypują się na niego same ulotki i niechciane ogłoszenia.
Pomimo tego, że „Dzień świra" powstał ponad 10 lat temu, w kwestii poczty niewiele się zmieniło i dzisiaj podobne zjawisko przeniosło się na stałe do jej elektronicznego odpowiednika. Każdego dnia, otwierając skrzynkę odbiorczą, napotykamy na kilkanaście lub kilkadziesiąt nowych e-maili, których wcale nie oczekiwaliśmy. Zdarzają się wśród nich obietnice wakacyjnych wojaży pod palmy, wyjątkowo kuszące zniżki w sklepach, zachęty do wzięcia pożyczek czy zaproszenia do odwiedzin na konkretnych stronach WWW. Całą tę korespondencję w internetowym żargonie określa się jedną wspólną nazwą: **Spam**.

Spam jest w gruncie rzeczy niewinnym słowem – nazwą pewnej popularnej w USA konserwy zawierającej, znaną także u nas, wieprzową mielonkę. Nie wiadomo do końca, kto pierwszy niechciane wiadomości elektroniczne określił mianem spamu – historycy internetu są zdania, że jej zastosowanie ma wiele wspólnego z jednym ze skeczy grupy Monty Pythona.

Bomba w kopercie

Choć – jak wspomnieliśmy – samo słowo „spam" ma niewinny rodowód, to jego dzisiejsze powszechne zastosowanie odnosi się do jednej z największych plag internetu. Każdego dnia na świecie wysyłanych jest kilka miliardów niechcianych wiadomości, które zapychają skrzynki odbiorcze internautów – ale nie tylko. Te e-maile mogą być także groźne, ponieważ wiele z nich służy za nośniki szkodliwych plików lub narzędzia do wyłudzania danych (phishingu, o którym wspominaliśmy w rozdziale I).
Chociaż spam znany jest właściwie od początku istnienia globalnej sieci, to jego natura w ciągu dziesięcioleci uległa ewolucji. W ostatnich latach liczba niechcianych e-maili powoli spada, jednak jednocześnie spam staje się groźniejszy niż kiedyś.
Według danych firmy Kaspersky Lab, jednego z największych producentów oprogramowania antywirusowego, w trzecim kwartale 2013 roku spam stanowił 68% wszystkich wysłanych na świecie wiadomości elektronicznych. Dobra wiadomość jest taka, że to o 2,5% mniej niż w drugim kwartale tego samego roku. Ale są też o wiele gorsze wieści – w tym samym okresie dwukrotnie wzrósł odsetek spamu zawierającego groźne pliki, a trzykrotnie zwiększyła się liczba e-maili służących do phishingu.

Na szczycie rankingu najpopularniejszego szkodliwego oprogramowania rozsyłanego za pośrednictwem spamu znalazł się Trojan-Spy.HTML.Fraud.gen. Szkodnik ten podszywa się pod stronę HTML, która służy jako formularz rejestracyjny dla serwisów bankowości online, i jest wykorzystywany przez phisherów do kradzieży informacji finansowych.

Te wycinkowe dane pochodzące zaledwie z krótkiego okresu mogą nas przekonać o tym, że spam to nie tylko nachalna reklama, ale bardzo realne zagrożenie pukające do skrzynek naszej elektronicznej poczty.

Złodziej o niewinnych oczach

Na pierwszy rzut oka spam nie sprawia groźnego wrażenia i wydaje się łatwy do zdemaskowania – przecież każdy z nas potrafi w mgnieniu oka zorientować się, że ma do czynienia z uciążliwą reklamą. Problem polega jednak na tym, że autorzy szkodliwego spamu są często równie inteligentni jak my. Mają swoje sposoby na to, by przebrać wilka w skórę owcy i przyciągnąć naszą uwagę. Stąd po spektakularnych katastrofach czy klęskach żywiołowych widzimy w naszych skrzynkach maile zachęcające do obejrzenia ponoć autentycznych zdjęć z miejsca tych wydarzeń, przy okazji medialnego szumu wokół tej czy innej gwiazdy

oferuje się nam dostęp do pikantnych filmów z jej udziałem, a co pewien czas jesteśmy proszeni o rzekome wsparcie dla chorej lub ubogiej osoby. Wszystkie te maile mogą nas zaprowadzić prosto w pułapkę, jeśli tylko klikniemy na zawarty w nich link lub otworzymy dołączony do listu załącznik.
Niebezpieczny spam może mieć także inną formę, nastawioną na złapanie w sidła określonej grupy odbiorców. Najlepszym przykładem jest jedna z akcji spamowych przeprowadzonych w 2013 roku. W sieci pojawiły się wówczas maile pochodzące ponoć od producentów znanych programów antywirusowych – Microsoft Security Essentials, Windows Defender, AVG Internet Security i Kaspersky Anti-Virus. Niezależnie od wersji oprogramowania tytuł korespondencji był zawsze taki sam: **Ważna aktualizacja systemu – wymagane natychmiastowe działanie.** W treści maila można zaś było przeczytać taki tekst: *Ważna aktualizacja systemu – wymagane natychmiastowe działanie. Zainstalowanie tej aktualizacji bezpieczeństwa jest bardzo istotne ze względu na najnowsze złośliwe oprogramowanie, które pojawiło się w sieci. Aby dokończyć operację, należy dwukrotnie kliknąć na łatkę KB923029 w załączniku. Instalacja zostanie uruchomiona w trybie cichym. Prosimy zachować szczególną ostrożność oraz poinformować nas w razie jakichkolwiek problemów.*

Prawda, że brzmi wiarygodnie i przekonująco? Oczywiście. Nic więc dziwnego, że tysiące użytkowników uruchomiły wspomnianą w wiadomości łatkę i… straciły dostęp do komputera. Okazało się bowiem, że tak naprawdę załącznik zawierał program typu ransomware i dalszy ciąg był dokładnie taki, o jakim wspominaliśmy wcześniej w rozdziale I. Trojan blokował dostęp do komputera i szyfrował zgromadzone w nim pliki. Aby odzyskać do nich dostęp, należało zapłacić przestępcom okup.
Ten przykład pokazuje jasno, jak bardzo niebezpieczny, a jednocześnie podstępny potrafi być spam. A tak na marginesie – trzeba pamiętać, że **żaden** producent oprogramowania antywirusowego nie wysyła swoim klientom aktualizacji w formie załączników do e-maili. Są one przeprowadzane automatycznie z poziomu zainstalowanej w komputerze aplikacji. Warto o tym pamiętać!

Siatka na muchy

Spam narodził się wraz z internetem i na razie nic nie wskazuje na to, by szybko miał zniknąć. Czy zatem jesteśmy skazani na używanie poczty elektronicznej z ciągłą obawą, że w każdej chwili może się w niej pojawić e-mail, który wysadzi w powietrze nasz komputer albo pozbawi nas poufnych danych? Na szczęście nie. Naszymi sprzymierzeńcami są

dostawcy usług e-mail oraz producenci odpowiednich programów do zwalczania spamu.
Jeżeli używamy poczty elektronicznej wyłącznie w wersji online (na przykład Gmaila), to znaczną część procesu filtrowania spamu bierze na siebie dostawca tej usługi. Po zalogowaniu się do serwisu w głównym oknie po lewej stronie zobaczymy pozycję o nazwie:

Spam

Po kliknięciu na nią pojawi się okno, w którym znajdziemy wszystkie wiadomości zakwalifikowane przez Gmail do tej kategorii:

CITEAM.PL - Podróże	syd.warschauer@gmail.com	Klimat nadmorski czy górolski? Wybierz sobie Ferie!	8 sty
CITEAM.PL - Cała Polska	syd.warschauer@gmail.com	Odbitki * Opiekacz grillowy Kalorik * Magnetyczne hula-hoop * Ławeczka do ćwiczeń * Odz...	8 sty
Sklep internetowy Agito..	syd.warschauer@gmail.com	Sprawdź nowości i promocje stycznia!	8 sty
MandM Direct	syd.warschauer@gmail.com	Up to 75% off the biggest fitness brands – new year, new you	7 sty
CITEAM.PL - Podróże	syd.warschauer@gmail.com	Podróżowe destynacje dla wymagających turystów → sprawdź	7 sty
Behance Team		Top Tips, Insights & Tricks For Better Productivity	7 sty
Endo	syd.warschauer@gmail.com	Ceny spadły z hukiem! Zobacz wyprzedaż aż do -60%!	7 sty

Dlaczego? Ano dlatego, że wbudowane w usługi pocztowe filtry antyspamowe, choć działają coraz lepiej, to nie zawsze są doskonałe. Zdarza im się więc czasami umieścić w folderze z niechcianymi wiadomościami także te zupełnie niewinne i być może istotne. Krótki rzut oka na ten folder pozwoli nam od razu zorientować się w sytuacji. Jeżeli odnajdziemy tam ważny dla nas mail, możemy szybko przenieść go do zwykłej skrzynki odbiorczej. Wystarczy, że otworzymy tę wiadomość i w górnej części okna klikniemy na przycisk:

To nie jest spam

Do folderu ze spamem powinniśmy zaglądać od czasu do czasu, a także w tych przypadkach, gdy spodziewamy się otrzymania jakiegoś maila, a mimo to nie widzimy go w skrzynce odbiorczej.

W wypadku wyjątkowo podejrzanych egzemplarzy spamu, gdy jesteśmy przekonani o tym, że stanowią one próbę kradzieży lub wyłudzenia informacji, możemy poinformować o tym firmę

Google, operatora serwisu Gmail. Takie zgłoszenie pomoże zespołowi specjalistów z Google'a dodatkowo usprawnić działanie filtrów antyspamowych. Po otwarciu podejrzanej wiadomości w górnej części okna wybieramy przycisk:

i klikamy na opcję:

Zgłoś próbę wyłudzenia informacji

Pojawi się nowe okno, w którym wybieramy przycisk:

Zgłoś wiadomość od niewiarygodnego nadawcy

Zgłoszenie zostanie wysłane.
Co dzieje się z wiadomościami – śmieciami umieszczonymi w folderze Spam? Po miesiącu zostaną one automatycznie usunięte przez mechanizm Gmaila. Możemy jednak pozbyć się ich wcześniej. W tym celu w głównym oknie ze spamem wybierzmy opcję:

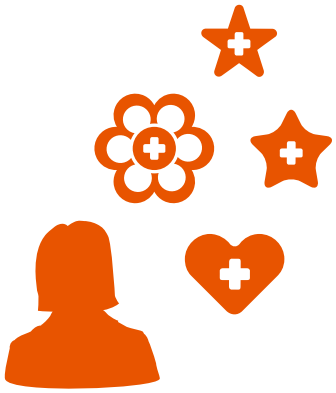
Usuń teraz cały spam

Po chwili okno z wiadomościami – śmieciami będzie zupełnie puste.

Nieco gorzej od użytkowników serwisów pocztowych obsługiwanych online mają osoby używające elektronicznej korespondencji w sposób tradycyjny, to znaczy za pomocą zainstalowanych w komputerze programów, takich jak Outlook Express. Chodzi bowiem o to, że tego typu aplikacje nieco słabiej radzą sobie z oddzielaniem ziarna od plew, czyli rozpoznawaniem i filtrowaniem spamu. Można temu jednak zaradzić, instalując w komputerze aplikacje wyspecjalizowane w wyławianiu niechcianych wiadomości z naszej poczty. Jednym z godnych polecenia darmowych programów tego typu jest Spamihilator. Ściągniemy go ze strony www.spamihilator.com. Po instalacji aplikacja działa w tle i umieszcza maile zakwalifikowane jako spam w oddzielnym folderze. Od czasu do czasu należy jednak do tego folderu zajrzeć, by skontrolować, czy nie ma tam ważnych wiadomości, które nie stanowią spamu.

ROZDZIAŁ IV

Przeglądarki internetowe: Jak je uzbroić?



O tym, że aktualność jest dobra nie tylko w gazecie, a właściwe dodatki przydają się nie tylko w kuchni i przy doborze wieczorowej kreacji.

Przeglądarka stron WWW dla każdego internauty jest oknem na świat, podstawowym narzędziem służącym do kontaktu z globalną siecią. Problem polega jednak na tym, że wiemy o tym nie tylko my sami – wiedzą o tym także inni, na przykład firmy zajmujące się internetową reklamą czy cyberprzestępcy. Dlatego ważne jest to, byśmy we własnym dobrze pojętym interesie zadbali o bezpieczeństwo i prywatność podczas korzystania z naszej przeglądarki.

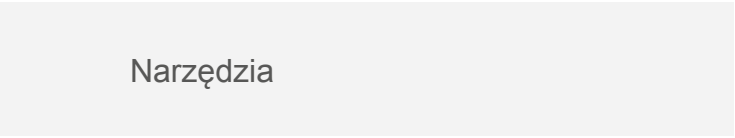
Ustawienia programu

Pierwszą rzeczą, jaką możemy zrobić od ręki, to odpowiednie skonfigurowanie w przeglądarce opcji dotyczących bezpieczeństwa. Zobaczmy to na przykładzie programu Firefox, który obecnie jest w naszym kraju najbardziej popularną przeglądarką internetową.

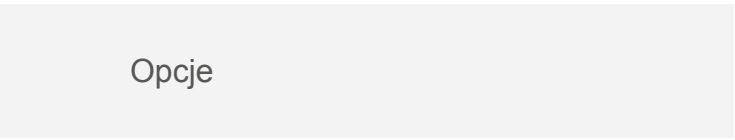
Uwaga!

Zarówno w Firefoksie, jak i w innych przeglądarkach, podstawowy krok w kierunku zapewnienia im (a więc i nam samym) bezpieczeństwa to instalacja wszystkich aktualizacji opublikowanych przez producenta programu. Aktualizacje zawierają nie tylko usprawnienia dotyczące funkcjonowania aplikacji, ale także niezbędne łatki blokujące nowe zagrożenia pojawiające się w sieci.
W przeglądarce Firefox domyślnie zaznaczona jest opcja automatycznych aktualizacji, które są instalowane bez

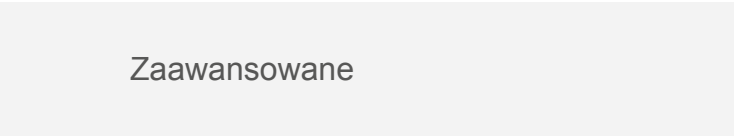
udziału użytkownika. Warto jednak sprawdzić, czy ta opcja nie została przypadkowo wyłączona. W głównym oknie programu na górnym pasku wybieramy przycisk:



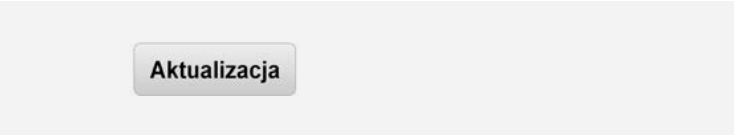
a następnie:



Przechodzimy do zakładki:



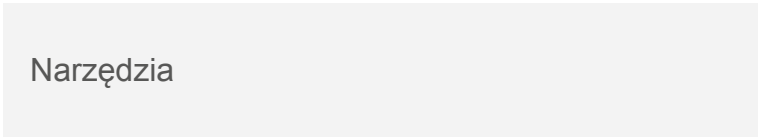
i opcji:



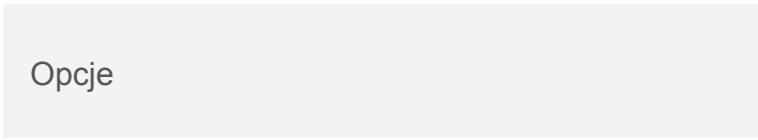
W nowym oknie sprawdzamy, czy zaznaczona jest funkcja:

Jeżeli nie, to zaznaczamy ją ręcznie.

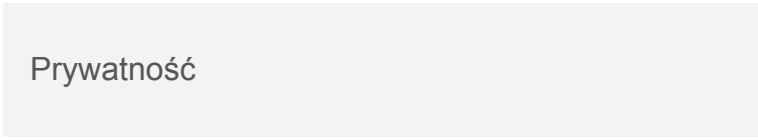
Teraz możemy skonfigurować pozostałe elementy przeglądarki związane z bezpieczeństwem. Znowu klikamy na:



i



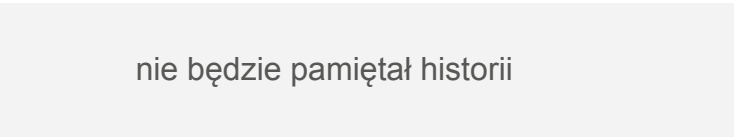
Wybieramy zakładkę:



Pojawi się nowe okno. Możemy w nim zaznaczyć opcję:

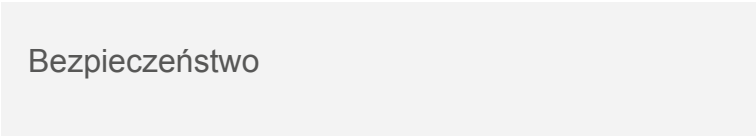
ale nie spodziewajmy się po niej zbyt wiele, choć nazwa brzmi obiecująco. Co prawda każda z odwiedzanych przez nas stron WWW otrzyma informację o tym, że nie chcemy być śledzeni, jednak często twórcy witryn nie przejmują się podobnymi żądaniami. Następna opcja dotyczy historii przeglądanych przez nas stron interenetowych i łączy się z dosyć kontrowersyjną sprawą tak zwanych ciasteczek (*cookies*). Są to niewielkie informacje tekstowe wysy-

łane do komputera użytkownika przez odwiedzaną przez niego witrynę. Swego czasu w sieci zrobiło się głośno o szkodliwości ciasteczek i przylepiono im łatkę złowrogich szpiegów. Tymczasem nie do końca tak jest. Co prawda ciasteczka zawierają pewne informacje o użytkowniku i jego zachowaniu na konkretnej stronie, jednak nie są to dane bardziej niebezpieczne niż inne ślady, które pozostawiamy po sobie w sieci. Z drugiej strony ciasteczka znacznie ułatwiają nam nawigowanie po często odwiedzanych witrynach – pozwalają między innymi na zapamiętanie naszych loginów (nie musimy logować się na każdej osobnej podstronie wymagającej weryfikacji użytkownika) czy też preferencji ustalonych na konkretnych stronach. Jeżeli uważamy, że ciasteczka zbyt głęboko penetrują naszą prywatność, to we wspomnianej wcześniej części dotyczącej historii przeglądania wybierzmy opcję:

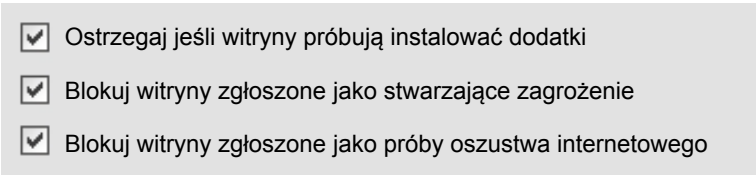


Jeśli zaś sądzimy, że ciasteczka nie są wyłącznie złem wcielonym i jednak ułatwiają nam żywot, to pozostańmy przy domyślnie włączonej opcji:

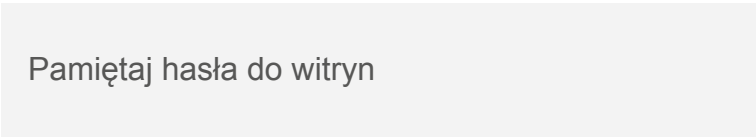
Teraz klikamy na przycisk:



W tym oknie praktycznie wszystkie opcje powinny być zaznaczone.



W części o nazwie Hasła w zasadzie możemy usunąć zaznaczenie przy opcji:



Dlaczego? Ano dlatego, że jeśli korzystamy z programu LastPass opisanego w rozdziale II, to Firefox nie musi już nas wyręczać w pamiętaniu loginów i haseł do poszczególnych serwisów i usług.

Dodatki do przeglądarek

Dostępne dzisiaj najpopularniejsze przeglądarki stron WWW mają dużą zaletę: każda z nich oferuje spory zestaw dodatków rozszerzających funkcjonalność tych programów. Są wśród nich także takie, które pozwalają na zwiększenie stopnia naszego bezpieczeństwa i prywatności. Instaluje się je z poziomu sa-

mej przeglądarki. W Firefoksie dostęp do dodatków uzyskamy, klikając na przycisk:

Narzędzia i Dodatki

Otworzy się nowa strona WWW, na której wybieramy opcję:

Pobierz dodatki

a na kolejnej witrynie

Prywatność i bezpieczeństwo

Oto kilka dodatków do Firefoksa dotyczących bezpieczeństwa i prywatności użytkownika:
AdBlock – Dodatek, którego zadaniem jest blokowanie na odwiedzanych stronach reklam i innych uciążliwych elementów.
NoScript – Blokuje kod JavaSript na przeglądanych witrynach. Dzięki temu zwiększa nasze bezpieczeństwo, gdyż luki w oprogramowaniu Java są jedną z dróg najczęściej wykorzystywanych przez cyberprzestępców do przeprowadzania ataków.
Web Of Trust (WOT) – Dodatek informujący nas, czy odwiedzana strona WWW jest uznawana za bezpieczną. WOT oznacza witryny według własnej skali bezpieczeństwa, posługując się bazą danych zawierających ponad 20 milionów stron.
Ghostery – Program, który informuje użytkownika o tym, czy konkretna strona WWW stara się nas namierzyć. Jeśli tak, to mamy szansę opuszczenia tej witryny bez pozostawiania na niej swoich śladów.
Close'n'Forget – Dodatek, który usuwa z komputera wszystkie ciasteczka po opuszczeniu konkretnej witryny internetowej.
Foxy Proxy – Program, dzięki któremu łączymy się ze stronami WWW za pośrednictwem serwerów proxy, co zapewnia nam spory poziom anonimowości w sieci (na przykład ukrycie naszego numeru IP).
Oczywiście w innych przeglądarkach internetowych znajdziemy także zestaw dodatków spełniających podobną rolę co te wymienione wcześniej i przeznaczone do Firefoksa. Warto z nich skorzystać, bowiem dzięki takim niewielkim aplikacjom nasza przeglądarka może zostać przyzwoicie uzbrojona i stać się twierdzą o wiele trudniejszą do zdobycia niż „goły", pozbawiony dodatków program przeznaczony do surfowania w internecie.

CafeSenior

Jesteś 60+? Zajrzyj do nas!

POLECAMY W CAFESENIOR.PL

JAK ZMIENIĆ SWÓJ STYL

NOTEBOOK – TAK. ALE JAKI?

CO ZROBIĆ, ŻEBY DŁUGO ŻYĆ?

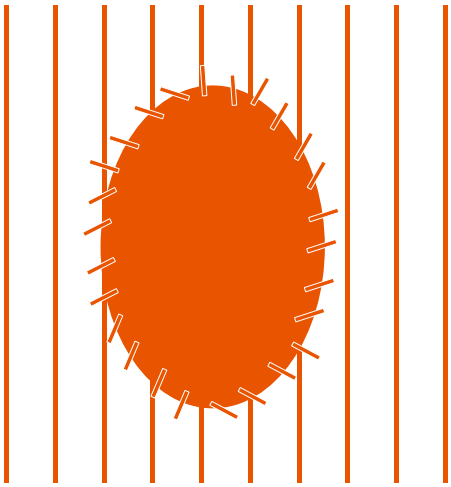
WEJDŹ DO SERWISU CAFESENIOR

- Uczymy, jak coraz lepiej korzystać z Internetu
- Piszemy o ważnych dla seniorów sprawach prawnych i finansowych
- Krok po kroku prowadzimy po meandrach współczesnych technologii
- Podpowiadamy, jak dbać o zdrowie, dobrze się odżywiać i jaki sport jest odpowiedni dla osób 60+
- Dzielimy się pasjami i wrażeniami z lektur, filmów i podróży, a także popularyzujemy akcje i inicjatywy skierowane do seniorów

www.cafesenior.pl

ROZDZIAŁ V

Bezpieczne WiFi: Nie daj się sąsiadom



O tym, że dziurawa sieć szkodzi nie tylko rybakom, a uszczelnianie okna na świat przydaje się nie tylko zimą.

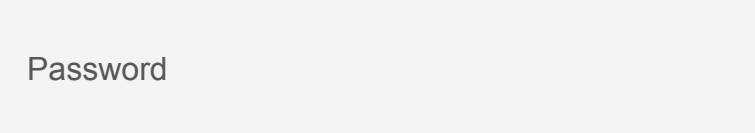
Wielu z nas w domu korzysta z bezprzewodowego połączenia z internetem w standardzie WiFi. To oczywiście bardzo wygodne rozwiązanie. Dzięki niemu możemy łączyć się z siecią z dowolnego pokoju i za pomocą różnych urządzeń. Nic jednak za darmo. Co prawda WiFi daje nam wolność, która jest mocno ograniczona w wypadku połączenia przewodowego, jednak z drugiej strony źle zabezpieczona bezprzewodowa łączność jest podatna na włamania. Zaś jego konsekwencje mogą być różne – od uciążliwych, ale mało groźnych, aż po bardzo poważne.
W wypadku słabych zabezpieczeń lub wręcz ich braku można wyobrazić sobie sytuację, w której niezbyt miły i uczciwy sąsiad podłącza się pod naszą sieć WiFi i korzysta z darmowego dostępu do internetu, za który to my przecież płacimy naszemu dostawcy. W wypadku takiego włamania możemy dostrzec (szczególnie przy wykupionym niskim transferze danych) wolniejsze niż zwykle połączenie z siecią – strony WWW w przeglądarce będą otwierały się ospale, a ściągnięcie z internetu jednego pliku będzie trwało dłużej niż jeszcze kilka dni temu.
To niestety nie wszystko. Błędy w zabezpieczeniach WiFi mogą spowodować, że złodzieje po włamaniu się do sieci uzyskają dostęp do naszych ważnych danych, które przekazujemy podczas połączeń z internetem – na przykład loginów i haseł do kont bankowych. Czym to grozi – nie trzeba nikomu tłumaczyć... Istnieje także zagrożenie innego ro-

dzaju. Otóż obca osoba włamująca się do naszej sieci może ją wykorzystać do popełnienia rozmaitych nadużyć, a nawet przestępstw w internecie – na przykład okradać internetowe rachunki w bankach. Podczas dochodzenia policja szybko ustali na podstawie numeru IP, z jakiej sieci dokonano kradzieży. I wówczas okaże się, że winny jest... nasz router (urządzenie, które rozsyła sygnał WiFi w naszej sieci). I będziemy mieli spore kłopoty. Zanim uda nam się wszystko wyjaśnić, może minąć sporo czasu, nie wspominając już o stresie, przez jaki będziemy musieli przejść przy okazji takiej przygody.
Widać więc, że kwestia zabezpieczenia domowego WiFi nie jest kwestią błahą i warto poświęcić jej nieco uwagi we własnym, dobrze pojętym interesie.

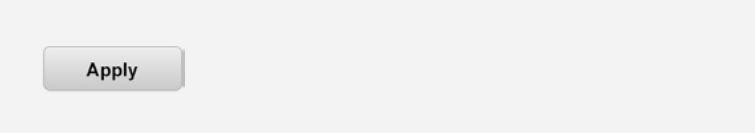
Nie wierzmy dostawcy

Powyższy tytuł nie zawiera wcale ukrytej sugestii, że firma zapewniająca nam dostęp do internetu nie jest godna zaufania. Najprawdopodobniej jest. Chodzi raczej o to, że każdy dostawca usług internetowych, zapewniając nam w domu bezprzewodową sieć WiFi, musi zamontować u nas router lub modem. Takie urządzenie posiada już zdefiniowane wcześniej hasło administratora. Aby odpowiednio zabezpieczyć sieć, należy je zmienić.

Jak to zrobić? Logujemy się do naszego routera lub modemu. W okno przeglądarki wpisujemy adres posiadanego urządzenia (znajdziemy go w załączonej dokumentacji lub instrukcji, możemy też zwrócić się o ten adres do dostawcy usług). Po zalogowaniu odnajdujemy pozycję dotyczącą hasła, na przykład:



Teraz zmieniamy domyślne hasło – zasady tworzenia dobrego, trudnego do złamania klucza opisano wcześniej w rozdziale II. Nasz wybór zatwierdzamy odpowiednim przyciskiem, który zależy od modelu routera, może to być na przykład:



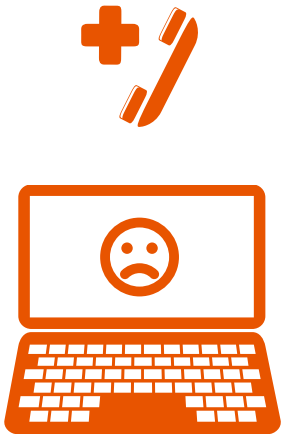
Podobnie musimy postąpić w sytuacji, gdy korzystamy tylko z połączenia przewodowego i sami kupujemy router do założenia sieci WiFi. Domyślne hasło ustalone przez producenta urządzenia jest bowiem bardzo łatwe do odnalezienia w sieci. Po zalogowaniu do tego routera zmieniamy hasło, powinniśmy także upewnić się, że ustawione jest szyfrowanie sieci w standardzie WPA2. Inne standardy – WPA i WEP – są o wiele bardziej podatne na włamania niż WPA2.

Przy konfiguracji zabezpieczeń ważne jest nie tylko hasło dostępu, ale także nazwa sieci bezprzewodowej, czyli w skrócie SSID. Nazwa sieci nie powinna mieć związku ani z położeniem fizycznym routera (nie powinna zawierać na przykład adresu), ani też z nazwą producenta routera. Dlaczego? Ano dlatego, że każda wskazówka, umieszczona nawet w nazwie sieci bezprzewodowej, jest cenna dla potencjalnego intruza. Nie powinniśmy ułatwiać mu zadania.

W internecie można spotkać sporo porad dotyczących zabezpieczenia sieci WiFi, których wartość jest co najmniej dyskusyjna. Często powtarza się na przykład wskazówka, by ukryć SSID. Oczywiście możemy użyć tej opcji, ale trzeba pamiętać, że jest ona złudna. W rzeczywistości bowiem nie ukrywamy nazwy sieci, a sprawiamy jedynie, że nie jest ona nadawana dalej. Tymczasem potencjalnemu włamywaczowi ustalenie SSID zajmie najwyżej kilkanaście sekund, ponieważ pojawia się ona „czarno na białym" za każdym razem, gdy jakikolwiek komputer łączy się z punktem dostępowym, a więc naszym routerem. Większego sensu nie ma też porada, by filtrować adresy MAC (sprzętowe adresy urządzeń sieciowych). Chodzi o ustalanie białej listy adresów MAC i zezwalanie na połączenie z siecią tylko dla nich. Niestety każdy, kto szpieguje daną sieć, będzie w stanie zobaczyć adresy MAC, którym zezwolono na połączenia, i w ciągu kilku sekund przekonfigurować swój interfejs sieciowy tak, by odpowiadał dopuszczonemu adresowi z listy adresów MAC właściciela sieci. Takie „zabezpieczenie" służy więc bardziej naszemu dobremu samopoczuciu niż rzeczywistej i skutecznej ochronie domowej sieci WiFi.

ROZDZIAŁ VI

Antywirus: Wynajmij ochroniarza



O tym, że nie musimy płacić za dobrego goryla, jak można go oswoić i jak rozpoznać, że komputer jest chory.

Wiemy już, jak odpowiednio zabezpieczyć dostęp do naszej skrzynki mailowej, jak rozpoznać i odsiać atakujący ją spam, znamy też sposoby na podniesienie stopnia ochrony przeglądarki internetowej. Pozostaje jednak kwestia wszystkich krążących w sieci zagrożeń, które wymieniliśmy w rozdziale I.
Jak sobie poradzić z tymi wszystkimi wirusami, trojanami i rootkitami? Jak się przed nimi bronić? Odpowiedź sprowadza się do jednego: odpowiedniego pakietu bezpieczeństwa, zwanego popularnie (choć nie do końca prawdziwie) antywirusem.
Pierwsze oprogramowanie antywirusowe powstało pod koniec lat 80. ubiegłego wieku i przez ponad 20 lat swojego istnienia przeszło długą drogę. Dzisiaj antywirus to skomplikowana aplikacja, która musi radzić sobie każdego dnia z nowymi rodzajami szkodliwych kodów.
Obecnie program antywirusowy zawiera zwykle dwa moduły. Pierwszy z nich to skaner, który sprawdza komputer w poszukiwaniu wirusów oraz podobnych kodów i w razie konieczności zajmuje się ich neutralizacją. Drugim elementem jest monitor, który na bieżąco chroni system przed dostępem rozmaitych zagrożeń.
Dlaczego napisałem wcześniej, że nazwa „antywirus" nie do końca odpowiada oprogramowaniu, które chroni obecnie nasze komputery? Chodzi o to, że sama aplikacja antywirusowa jest zwykle tylko jednym z elementów większego kompletu narzędzi służących do zwalczania

zagrożeń. Oprócz niej w pakietach spotkamy także firewall (zaporę chroniącą przed atakami i włamaniami z sieci), moduł ochrony rodzicielskiej czy elementy chroniące nas podczas dokonywania operacji bankowych lub zakupów w internecie.
Jeszcze kilka lat temu wszyscy fachowcy podkreślali, że oprogramowanie antywirusowe (pozostańmy przy tej nazwie dla większej wygody) to główna podstawa zapewnienia bezpieczeństwa komputera podłączonego do sieci. Ostatnio jednak coraz więcej specjalistów od spraw ochrony informatycznej przyznaje, że oni sami zrezygnowali z używania tego typu aplikacji. Tłumaczą to w taki sposób: *Przestępcy do dokonywania skutecznych, najgroźniejszych ataków wykorzystują zawsze najnowsze metody, których i tak nie dostrzegą programy antywirusowe. Używanie antywirusów nie ma zatem większego sensu.* Czy mają rację? Chyba nie do końca. Trzeba pamiętać, że przeważająca część zagrożeń czyhających w sieci to wcale nie są stworzone od podstaw nowe narzędzia, ale modyfikacje istniejących już od dawna szkodników. Takie kody są z powodzeniem wyłapywane i neutralizowane przez oprogramowanie antywirusowe. Dlatego podobne aplikacje wciąż mają rację bytu w naszych komputerach i nie należy z nich rezygnować. Dowód? Wystarczy choćby taki przykład:

Kilka lat temu przeprowadzałem wywiad z przedstawicielem jednej z firm produkujących pakiety antywirusowe. Podłączyliśmy wówczas do internetu zupełnie nowy komputer ze świeżo zainstalowanym systemem operacyjnym, pozbawiony jednak antywirusa. Wystarczyło kilka minut surfowania w sieci i używania poczty elektronicznej, by maszyna została zainfekowana kilkoma odmianami doskonale znanych specjalistom wirusów i trojanów. Oczywiście można przypuszczać, że gdyby wspomniany komputer działał w internecie jeszcze przez kilka godzin, stopień infekcji byłby o wiele poważniejszy.

Płacić czy nie?

Według firmy analitycznej Gartner w 2012 roku użytkownicy na całym świecie kupili oprogramowanie do ochrony komputerów za łączną sumę ponad 5 miliardów dolarów. To oczywiście świetna wiadomość dla producentów tych aplikacji, którzy na każdym kroku podkreślają, że tylko komercyjne, płatne wersje programów antywirusowych zapewniają właściwe zabezpieczenie przed zagrożeniami.
Trzeba pamiętać, że kupno antywirusa będzie kosztowało ponad sto złotych, a to dla wielu z nas poważna suma.
I na tym wydatki się nie kończą. Zwykle bowiem oprogramowanie antywirusowe

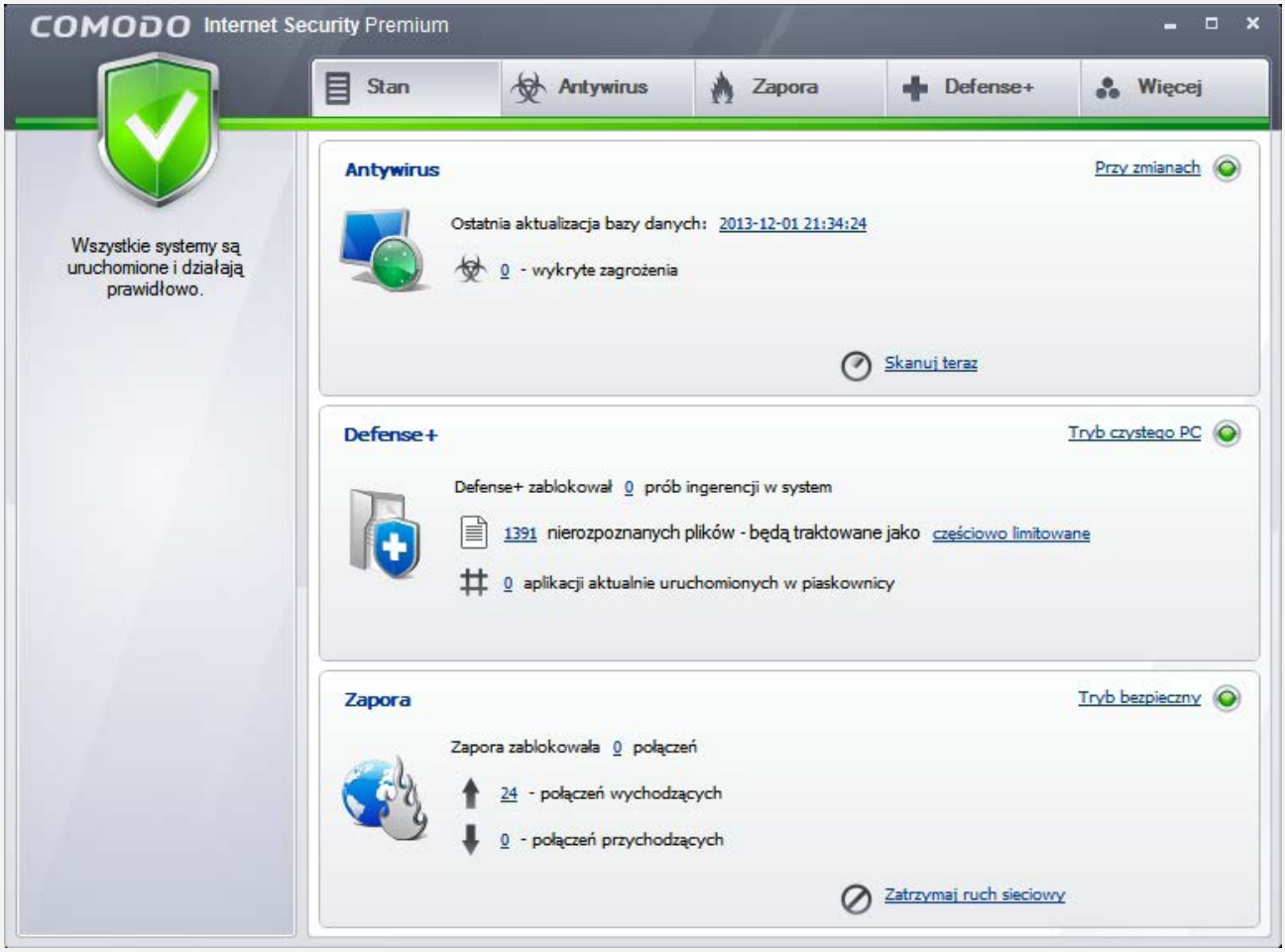
ma roczną licencję na aktualizację bazy sygnatur nowych zagrożeń. Jej odnowienie oznacza dodatkową opłatę. Inaczej nasz antywirus nie będzie aktualizowany i stanie się praktycznie bezużyteczny.
Czy zatem, chcąc zapewnić sobie ochronę domowego komputera, zawsze musimy płacić? Na szczęście nie. Na rynku funkcjonuje przynajmniej kilka dobrych programów antywirusowych, których można legalnie używać zupełnie za darmo. Czy są one gorsze od rozwiązań komercyjnych? W zasadzie nie. Najlepsze z darmowych aplikacji wykazują rozpoznawanie zagrożeń na podobnym poziomie co programy płatne, nie obciążają też bardziej komputera w trakcie swojego działania.

Wśród najbardziej cenionych darmowych antywirusów wymienia się Ashampoo Anti-Malware, avast! Free Antivirus, AVG Anti-Virus Free Edition, Avira Free Antivirus czy Comodo Internet Security. Warto zainteresować się tą ostatnią propozycją. Comodo Internet Security (CIS) jest bowiem jedynym pośród wymienionych aplikacji kompletnym pakietem ochronnym, który oferuje nam nie tylko program antywirusowy i ochronę komputera w czasie rzeczywistym, ale także chwaloną za skuteczność zaporę sieciową o nazwie Comodo Personal Firewall. Na przykładzie CIS zobaczymy, jak odpowiednio skonfigurować oprogramowanie ochronne, tak aby dobrze spełniało powierzone mu zadania.

Antywirus w akcji

Pakiet CIS ściągniemy za darmo ze strony internetowej www.comodo.com. Podczas instalacji aplikacja powiadomi nas o potrzebie przeskanowania całego komputera w poszukiwaniu zagrożeń jeszcze przed pełną instalacją. Najlepiej się na to zgodzić. Następnie kończymy instalowanie pakietu. Wyłączamy i ponownie uruchamiamy nasz komputer. Comodo uruchomi się automatycznie wraz ze startem Windows, a na dole ekranu po prawej, w tak zwanym zasobniku systemowym, zobaczymy niewielką ikonę programu:

Na początku nie powinien dziwić fakt, że nasz nowy antywirus będzie się na dość długo łączył z internetem. Musi to zrobić po to, by ściągnąć ze swojej bazy na serwerach Comodo wszystkie aktualne bazy danych. Później – przy codziennych aktualizacjach – nie będzie to już uciążliwe, ponieważ program pobierze tylko najnowsze sygnatury wykrytych zagrożeń obecnych w sieci.
W zasadzie przy domyślnych ustawieniach nasz pakiet jest bezobsługowy



Comodo Internet Security jest kompletnym pakietem bezpieczeństwa, którego obsługa nie sprawi nam kłopotu

– pracuje dyskretnie w tle i będzie nas niepokoił tylko w przypadku wykrycia i usunięcia niebezpiecznych obiektów. Możemy się spotkać na przykład z sytuacją, gdy podczas instalacji jakiegoś programu w komputerze pojawi się komunikat o zablokowaniu przez Comodo pliku związanego z tym programem. Wówczas, aby kontynuować proces instalacji, klikamy na przycisk **Zezwól** lub **Dodaj do zaufanych** – zależnie od wersji wyświetlonego okna z wiadomością. W ustawieniach programu znajdziemy szerokie możliwości konfiguracji zabezpieczeń. Aby się do nich dostać, klikamy dwukrotnie na ikonę programu w zasobniku systemowym. Otworzy się główne okno Comodo Internet Security.

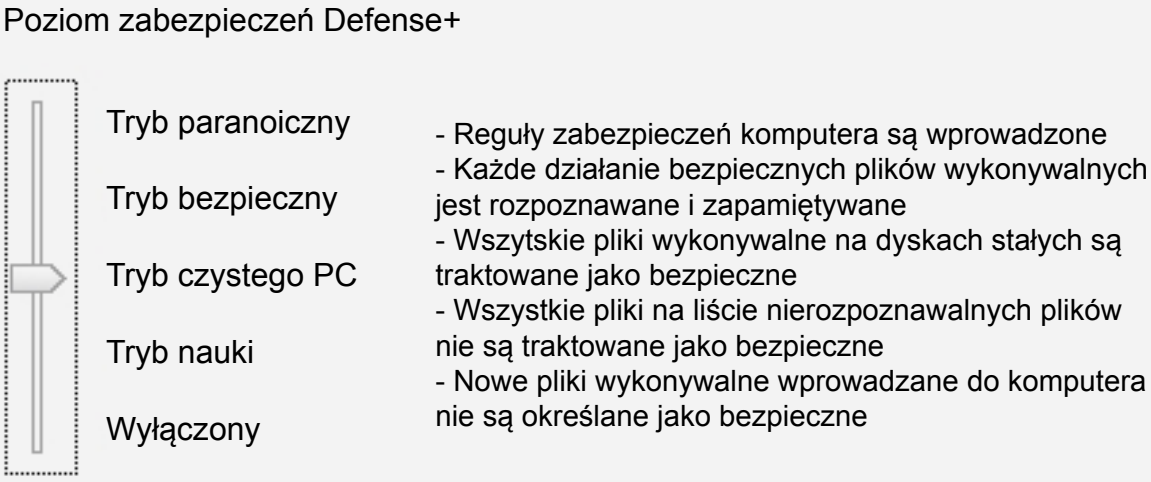
Wybieramy przycisk:

a następnie:

Ustawienia Defense+

Pojawi się okno ze specjalnym suwakiem:

Jeżeli zdecydujemy się na wyższe pozycje, to program będzie reagował nerwowo na wiele błahych w gruncie rzeczy zdarzeń i o każdym z nich alarmował specjalnym komunikatem. To może być uciążliwe podczas codziennego korzystania z komputera. Z kolei przesunięcie suwaka na najniższe pozycje nie zapewni nam dostatecznej ochrony ze strony Comodo Internet Security. Podobny wachlarz możliwości zmian stopnia



Przy każdym z ustawień suwaka znajdziemy opis zachowania się programu po jego zastosowaniu. Optymalnym rozwiązaniem będzie ustawienie:

Tryb czystego PC

ochrony znajdziemy w ustawieniach zapory sieciowej, które uruchomimy pod przyciskiem:

Skanery online: za darmo i skutecznie

Była już mowa o tym, że dobry, nawet darmowy antywirus zainstalowany w komputerze powinien zapewnić nam skuteczną, stałą ochronę przed zagrożeniami płynącymi z internetu. Jednak do dyspozycji mamy jeszcze inne przydatne narzędzie: skanery online.
Chodzi o mechanizmy antywirusowe dostępne wyłącznie w internecie. Mogą się one przydać co najmniej w dwóch przypadkach. Pierwszy to ten, gdy chcemy sprawdzić, czy używany przez nas na co dzień antywirus rzeczywiście jest tak dobry, jak twierdzi jego producent i skutecznie wyławia wszystkie szkodliwe kody. Jeżeli według jego wskazań wszystko jest w porządku, a mimo tego skaner wykryje jednak pominięte zagrożenia, to należy się zastanowić nad zmianą oprogramowania antywirusowego.
Skaner online może się przydać także wówczas, gdy chcemy na szybko sprawdzić stan bezpieczeństwa naszego komputera.
W sieci funkcjonuje kilka niezłych skanerów online. Na uwagę zasługują między innymi: ESET Online Scanner, F-Secure Online Scanner czy Bitdefender QuickScan.

Skaner online pozwoli nam szybko zorientować się, czy nasz komputer nie jest opanowany przez wirusy, trojany i inne szkodliwe oprogramowanie

Uwaga!

Niezależnie od oprogramowania antywirusowego zainstalowanego w naszym komputerze powinniśmy pamiętać o jednej, podstawowej zasadzie bezpieczeństwa: zawsze instalujmy poprawki bezpieczeństwa w systemie Windows publikowane przez producenta – koncern Microsoft. Luki w systemie operacyjnym to bowiem otwarta brama dla wszelkich ataków i włamań, i nawet najlepszy antywirus nie uchroni przed szkodnikami niezałatanego Windowsa.
Dla użytkowników nieco starszego systemu Windows XP mamy niestety złą wiadomość. Otóż według zapowiedzi Microsoftu w połowie 2014 roku przestaną być publikowane poprawki dotyczące tego systemu. To oznacza, że

osoby korzystające z Windows XP już teraz powinny pomyśleć o przesiadce na Windows 7 lub Windows 8. W przeciwnym razie mogą bowiem zostać pozbawione jednego z filarów zabezpieczeń komputera.

Na koniec: Objawy choroby

Jeżeli nasze oprogramowanie antywirusowe i wszelkie inne środki bezpieczeństwa zawiodą i komputer zostanie zainfekowany szkodliwym oprogramowaniem, jak rozpoznamy objawy takiego zakażenia? Jest kilka symptomów, które mogą wskazywać na obecność w systemie wirusów lub trojanów. Oto niektóre z nich:

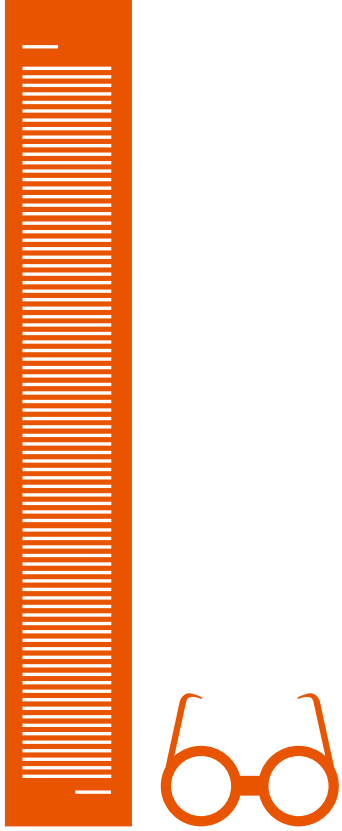
- Pojawianie się na ekranie nieoczekiwanych komunikatów lub nieznanych obrazów, dziwne sygnały dźwiękowe dobiegające z komputera.
- Niespodziewane, samoczynne uruchamianie się napędu CD lub DVD.
- Nagłe uruchamianie się programów, których sami nie włączaliśmy.
- Powiadomienia o próbach samoczynnego nawiązywania połączenia internetowego przez niektóre aplikacje.
- Nasi znajomi wspominają, że otrzymali od nas wiadomości, których nigdy nie wysyłaliśmy.
- Skrzynka pocztowa zawiera wiele wiadomości bez adresów nadawcy lub nagłówka.
- Komputer często zawiesza się lub występują problemy w jego działaniu.
- Podczas uruchamiania programów wydajność komputera znacznie się zmniejsza.
- Nie można uruchomić systemu operacyjnego.
- Pliki i foldery są nagle usuwane lub ich zawartość zmienia się samoczynnie.
- Dostęp do dysku twardego jest uzyskiwany zbyt często (dioda dysku na obudowie komputera szybko pulsuje).
- Przeglądarka internetowa zawiesza się lub działa nieprawidłowo (na przykład nie jest możliwe zamknięcie jej głównego okna).

ROZDZIAŁ VII

Surfowanie w sieci: Unikajmy mielizn

ROZDZIAŁ VII
Surfowanie w sieci: Unikajmy mielizn

O tym, jak nie zostać w internecie frajerem, że czytanie bywa przydatne, a za ściąganie z sieci filmów nie pójdziemy siedzieć.



We wstępie do tego e-booka była mowa o tym, że inernet może być miejscem niezbyt bezpiecznym, ale wystarczy wiedzieć, gdzie czają się zagrożenia, by sprawnie ich unikać i jednocześnie korzystać ze wszystkich zalet globalnej sieci. Dowiedzieliśmy się już sporo na temat zabezpieczenia podstawowych narzędzi służących do obsługi internetu – poczty elektronicznej i przeglądarek internetowych. Specjaliści od bezpieczeństwa w sieci, na przykład były znany haker Kevin Mitnick, podkreślają jednak, że najsłabszym ogniwem w ochronie przed zagrożeniami internetowymi jest... użytkownik komputera. Bowiem w ostatecznym rozrachunku nierozważne i często wynikające z niewiedzy postępowanie internautów doprowadza do największej liczby infekcji, przypadków kradzieży danych lub tożsamości czy wręcz utraty pieniędzy z powodu internetowych oszustw. Rzućmy więc okiem na niektóre mielizny, na które możemy wpłynąć, surfując w sieci.

W sidłach regulaminu

Dla większości z nas przeglądanie internetu oznacza otwieranie kolejnych stron WWW w poszukiwaniu rozmaitych treści – wiadomości z wielu dziedzin życia, porad czy rozrywki. Z pewnością nie musimy się obawiać odwiedzin na dobrze znanych witrynach, które są po prostu bezpieczne. Oczywiście z rozmaitych względów trzeba zachować ostrożność przy otwieraniu stron internetowych

cieszących się z definicji złą sławą – na przykład witryn pornograficznych. I to nie z powodu prezentowanych na nich treści. Chodzi raczej o to, że niektóre kategorie stron częściej niż inne są nośnikami szkodliwych kodów. Przed większością z nich powinny nas uchronić mechanizmy, które już zastosowaliśmy w naszym komputerze – wspomniane wcześniej wtyczki bezpieczeństwa w przeglądarce czy też pracujący w tle program antywirusowy. Lepiej jednak zachować ostrożność i na przykład nie klikać na kuszące, barwne banery umieszczone tłumnie na wielu podejrzanych witrynach.

Prawdziwą czujność powinniśmy jednak wykazać w przypadku, gdy odwiedzana przez nas platforma wymaga bardziej zaawansowanej interakcji niż zwykłe kliknięcie w obrazek lub odnośnik. Chodzi o witryny, na których do dalszego działania niezbędna jest **rejestracja użytkownika**.

Załóżmy, że chcemy wykonać niewinną czynność: ściągnąć ze strony WWW interesujący nas darmowy program komputerowy. Wchodzimy więc na niebudzącą podejrzeń stronę, na której oferowane jest oprogramowanie z różnych kategorii. Klikamy na wybraną aplikację, oczekując, że rozpocznie się pobieranie pliku instalacyjnego. Tymczasem pokazuje się okno informujące o tym, że przed ściągnięciem programu konieczna jest rejestracja w serwisie. Nie podejrzewając niczego, wpisujemy w rubryki nasze dane, takie jak imię, nazwisko, adres i e-mail. Odruchowo zaznaczamy też ptaszkiem opcję: „Oświadczam, że zapoznałem się z regulaminem i akceptuję jego warunki". Kto by czytał regulamin? Przecież we wszystkich napisane jest mniej więcej to samo.

Po zarejestrowaniu kończymy pobieranie programu i instalujemy go w komputerze. Wszystko jest fajnie do czasu, gdy w naszej skrzynce pojawia się niepokojący e-mail wysłany przez właściciela serwisu, który odwiedziliśmy. Wynika z niego, że rejestrując się na stronie, zaakceptowaliśmy regulamin, według którego wykupiliśmy płatną usługę dostępu do konkretnej platformy.

I teraz musimy zapłacić na przykład 100 złotych za roczny abonament. Jeśli tego nie zrobimy, to właściciel serwisu będzie do nas wysyłał ponaglenia, w końcu zaś może zacząć grozić nam sprawą sądową i komornikiem.

To oczywiście bardzo uproszczony scenariusz, jeden z wielu możliwych – sposób wyłudzania pieniędzy od nieostrożnych internautów wygląda za każdym razem nieco inaczej, zależnie od charakteru wyłudzającego serwisu. Czasami operator takiej platformy kusi nas krótkim (na przykład 14-dniowym) okresem próbnym, w którym możemy w pełni korzystać z oferowanych usług.

Później wysyła do nas potwierdzenie zawarcia umowy. Jeżeli nie zareagujemy wtedy na czas i nie wyślemy wiadomości o odrzuceniu umowy, to według sprytnie spreparowanego regulaminu powinniśmy wnieść stosowną opłatę. Tego typu próby wyłudzenia pieniędzy pojawiają się w sieci regularnie co kilka miesięcy, a ich przykładem mogą być takie witryny, jak Dobre-programy.pl, Plikostrada.pl, Taniezakupy.pl czy słynny i nie działający już Pobieraczek.pl, któremu do skóry dobrał się Urząd Ochrony Konkurencji i Konsumentów, nakładając na serwis prawie ćwierć miliona złotych kary za stosowanie niedozwolonych praktyk i oszukiwanie internautów. UOKiK prowadzi zresztą postępowania także wobec kilku innych podobnych platform, co oznacza, że wyłudzanie pieniędzy od internautów jest coraz skuteczniej tępione przez odpowiednie instytucje państwowe. Nie zwalnia nas to jednak z obowiązku zachowania ostrożności.

Symbolem polskich serwisów próbujących wyłudzać pieniądze od internautów jest Pobieraczek.pl, przykładnie ukarany przez Urząd Ochrony Konkurencji i Konsumentów

Oczywiście nakreślony wcześniej scenariusz wyłudzania pieniędzy nie oznacza, że należy skreślać z góry każdy serwis internetowy, który będzie od nas wymagał rejestracji. Taki krok trzeba jednak za każdym razem uważnie przemyśleć. Na przykład przyjrzeć się dokładnie, jakich danych osobowych żąda właściciel strony – jeśli są one zbyt szczegółowe i naszym zdaniem niekonieczne do świadczenia konkretnej usługi, powinniśmy poszukać innej podobnej, ale mniej wścibskiej witryny.

Druga kwestia niektórym wyda się trywialna, ale pomimo tego zaznaczmy ją wyraźnie i wielkimi literami: **ZAWSZE CZYTAJMY UWAŻNIE REGULAMIN SERWISU PRZED JEGO AKCEPTACJĄ!**

Taki krzykliwy komunikat może wyglądać na grubą przesadę. Dla mnie jednak nią nie jest – przepracowałem kilka lat między innymi jako dziennikarz zajmujący się pomocą osobom, które dały się nabrać rozmaitym internetowym oszustom. I z zebranych – nie tylko przeze mnie – doświadczeń wynika niestety, że nie czytamy regulaminów – najczęściej ze zwykłego lenistwa, ale czasem także z zupełnie innego powodu. Otóż właściciele wielu serwisów specjalnie przygotowują takie teksty regulaminów, które trudno zrozumieć bez dyplomu prawnika i tytułu biegłego sądowego w kieszeni. Tak więc generalna zasada bezpieczeństwa jest taka: jeżeli nie rozumiemy regulaminu danej usługi, a nie mamy pod ręką specjalisty, który może rozwiać nasze wątpliwości i przetłumaczyć pseudoprawniczy bełkot na język polski – zrezygnujmy z rejestracji w takim serwisie. Przy dzisiejszej konkurencji na internetowym rynku szybko znajdziemy inną ofertę podobnej usługi, której warunki będą dla nas bardziej zrozumiałe.

Przy okazji serwisów, które chcą „naciągnąć nas na kasę", warto zwrócić uwagę na jeszcze jeden szczegół – siedzibę firmy, która jest właścicielem takiej strony. Bardzo często bowiem podmioty, które mają nieczyste intencje, najchętniej rejestrują się w rozmaitych egzotycznych regionach świata – na przykład w Zjednoczonych Emiratach Arabskich czy Katarze. Takie rozwiązanie pozwala tym firmom uniknąć polskiej jurysdykcji w wypadku dochodzenia roszczeń lub innych problemów prawnych.

Ponieważ jako przykłady podstępnych serwisów wyłudzających pieniądze przytoczyłem akurat platformy w większości oferujące dostęp do rozmaitych programów komputerowych, to wspomnę jeszcze o jednym. Otóż instalowanie w komputerze aplikacji z podejrzanych źródeł niesie ze sobą dodatkowe niebezpieczeństwo w postaci zainfekowania systemu. Dlatego jeżeli chcemy wyposażyć nasz komputer w jakiś interesujący, darmowy program, nie powinniśmy ślepo wierzyć przy wyborze źródła

„dobremu wujkowi Google'owi". Chodzi bowiem o to, że po wpisaniu w oknie tej wyszukiwarki nazwy konkretnej aplikacji na pierwszych miejscach wyników mogą pojawić się strony, z których akurat nie powinniśmy korzystać, choćby ze względów wymienionych wcześniej. Najlepiej zrobimy, pobierając takie aplikacje bezpośrednio ze stron ich producentów albo ze sprawdzonych polskich serwisów – na przykład Dobreprogramy.pl czy też działy Download należące do internetowych stron znanych pism komputerowych.

To ty jesteś towarem!

W trakcie naszej aktywności w internecie powinniśmy zdawać sobie sprawę z tego, że funkcjonują w nim nie tylko serwisy, których celem jest bezprawne wyciągnięcie pieniędzy z naszych kieszeni. Może to zabrzmieć niezbyt miło, ale niestety, buszując w globalnej sieci, sami stajemy się towarem. A ściślej rzecz biorąc – towarem stają się wszystkie informacje na nasz temat. Wydaje nam się, że na przykład popularna wyszukiwarka Google oferuje nam możliwość szybkiego dotarcia do różnych źródeł informacji za darmo? Jeśli tak, to jesteśmy w dużym błędzie. Fortuna koncernu Google nie wzięła się bowiem z powietrza – została zbudowana dzięki sprzedaży ogromnych ilości danych na temat zachowań internautów innym podmiotom, na przykład firmom reklamowym. Dzięki informacjom na temat konkretnego użytkownika sieci można do niego skierować spersonalizowany przekaz reklamowy, a więc w konsekwencji zarobić pieniądze.
Co możemy z tym zrobić? Nic. Musimy pogodzić się z tą swoistą wymianą albo... zrezygnować z internetu. Oczywiście istnieją sposoby na to, by ograniczyć liczbę informacji, które sieć gromadzi na nasz temat. Możemy na przykład nie włączać w konkretnych serwisach opcji geolokalizacyjnych czy też przy rejestracji w wielu serwisach podawać fikcyjne dane. Na dłuższą metę takie metody mogą się jednak okazać męczące.
Czy taka swoista inwigilacja ze strony internetu jest dla nas niebezpieczna? Nie dajmy się zwariować. Globalna sieć jest dzisiaj po prostu częścią współczesnej rzeczywistości, która nas otacza. Pamiętajmy, że mnóstwo informacji na nasz temat znajduje się także w innych miejscach – mają je na przykład operatorzy komórkowi czy nadawcy telewizyjni. Czy świadomość tego każe nam zrezygnować z używania telefonu lub oglądania telewizji? Raczej nie. A idąc dalej podobnym tropem, zaczynamy zbliżać się do granic absurdu. Bowiem ważne informacje na nasz temat są zebrane choćby w osiedlowym sklepie – przecież to na podstawie danych, które mimochodem pozostawiliśmy wcześniej w tym miejscu

pani Basia za ladą zaproponuje nam z uśmiechem nowy gatunek twarożku podobny do tego kupowanego przez nas zazwyczaj.

W zgodzie z paragrafami

Globalna sieć może być nie tylko źródłem informacji, ale także magazynem treści o charakterze rozrywkowym. W powszechnej świadomości funkcjonuje potoczna opinia o tym, że ściąganie z internetu filmów, nagrań muzycznych czy gier jest nielegalne, a my, korzystając z podobnych treści, stajemy się piratami łamiącymi przepisy prawa autorskiego. Okazuje się jednak, że tylko w pewnej części ta opinia jest prawdziwa. Zróbmy więc szybki przegląd tego, co wolno, a czego nie należy robić w sieci w świetle ochrony praw własności intelektualnej.

Ściąganie filmów

Jest możliwe w ramach tak zwanego dozwolonego użytku osobistego. W artykule 23. ustawy o prawie autorskim czytamy bowiem, że *wolno nieodpłatnie korzystać z już rozpowszechnionego utworu*. W dodatku według polskich przepisów użytkownik nie ma obowiązku nakazanego prawem sprawdzenia legalności. To oznacza, że możemy pobierać z sieci filmy bez konieczności uzyskania odrębnej zgody uprawnionego lub zapłaty wynagrodzenia.

Uwaga!

Istnieje tu pewna prawna pułapka. We wspomnianej ustawie o prawie autorskim jest mowa o utworach już rozpowszechnionych. W praktyce chodzi o to, że możemy bez wchodzenia w konflikt z prawem ściągnąć film, który został wcześniej wyemitowany w telewizji lub wyświetlony w kinie. Natomiast ryzykowne jest pobieranie pirackiej kopii utworu, który na przykład „wyciekł" do sieci jeszcze przed swoją oficjalną premierą.

Ściąganie muzyki

Jest dozwolone na takiej samej zasadzie jak w przypadku kopiowania filmów. Należy jednak pamiętać, że przepisy nie zezwalają na korzystanie z utworu w taki sposób, by osiągać z tego tytułu korzyści majątkowe. Innymi słowy, możemy na przykład ściągnąć z internetu kilkadziesiąt piosenek ulubionego wykonawcy, skompilować je razem i wypalić na płycie CD. Taką płytę zgodnie z prawem możemy na przykład podarować znajomym. Ale nie wolno nam wypalić, powiedzmy, stu kopii takiej płyty i je sprzedawać.

Ściąganie książek w formie elektronicznej (e-booków)

Jest dozwolone. Tutaj także mają zastosowanie przepisy o dozwolonym użytku osobistym. Nie wolno nam jednak roz-

powszechniać dalej skopiowanych z sieci e-booków.

Ściąganie filmów, muzyki i innych utworów z sieci p2p

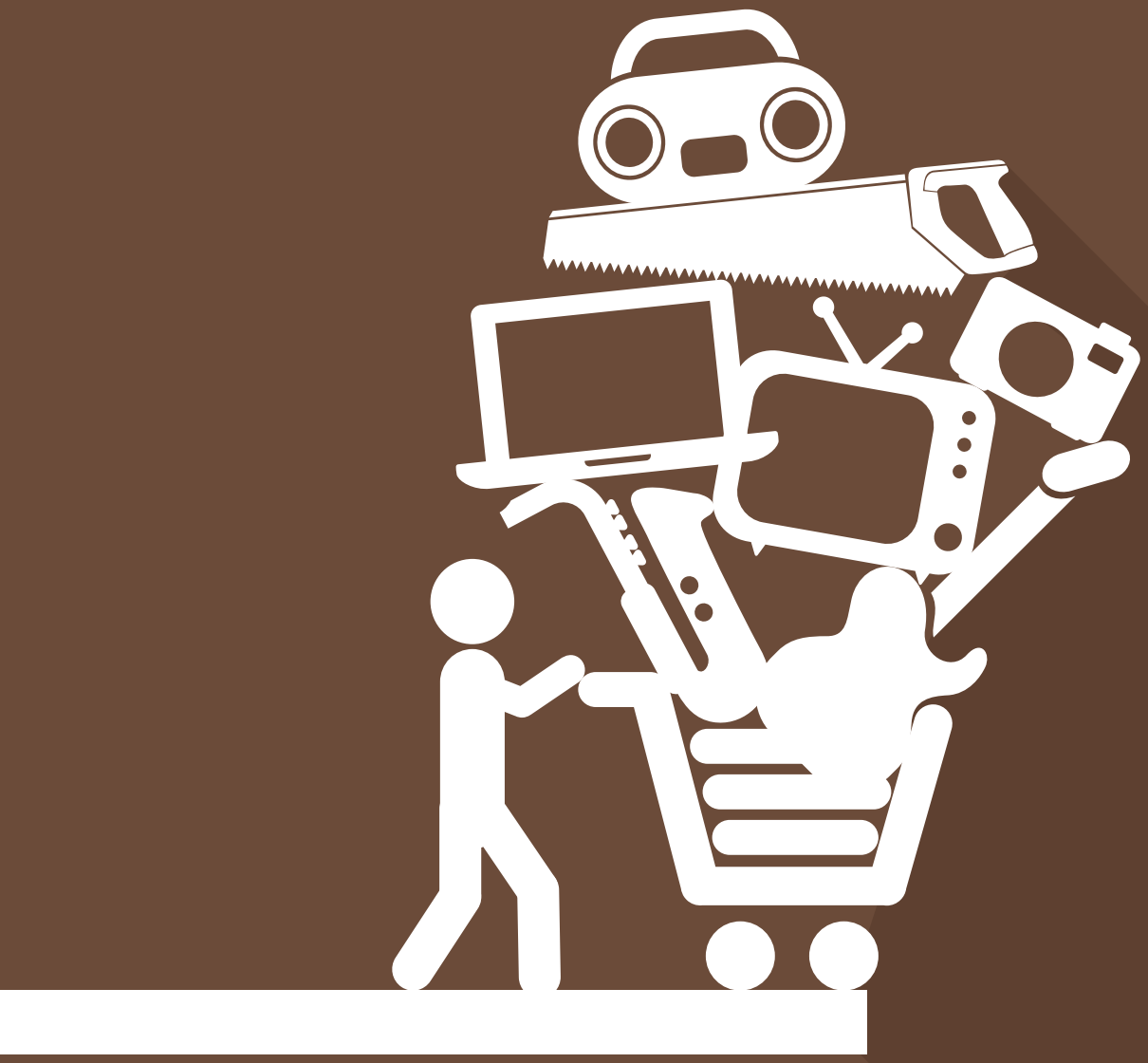
Jest dozwolone, ale ryzykowne. Pułapka kryje się w samej zasadzie funkcjonowania sieci wymiany plików p2p (od ang. *peer-to-peer*, czyli równy z równym): to sieć, w której użytkownicy wymieniają się plikami między sobą – a nie ściągają je z serwera (służą do tego takie programy, jak Ares, eMule, BitComet, BitTorrent i inne – odradzamy ich stosowanie). Grozi za to kara ograniczenia lub pozbawienia wolności do dwóch lat, a także odpowiedzialność na gruncie prawa cywilnego, co w praktyce oznacza konieczność zapłaty odszkodowania właścicielowi praw autorskich do danego utworu. Na podobnej zasadzie nie wolno nam publikować w sieci ściągniętych wcześniej utworów za pomocą takich kanałów, jak własna strona WWW, serwis społecznościowy czy też forum internetowe.

Ściąganie gier i komercyjnych wersji programów komputerowych jest nielegalne!

W świetle polskiego prawa nie wolno nam kopiować z internetu do komputera gier i aplikacji, które do używania wymagają odpowiedniej licencji. A taki unikalny dokument (w formie papierowej lub elektronicznej) możemy uzyskać wyłącznie przy zakupie gry albo programu. Oczywiście nie dotyczy to aplikacji rozpowszechnianych na zasadach freeware, a także próbnych (ograniczonych czasowo lub funkcjonalnie) wersji programów i gier komercyjnych. Za używanie nielegalnych kopii aplikacji można trafić do więzienia nawet na pięć lat. Warto o tym pamiętać!

ROZDZIAŁ VIII

Kupujmy z głową!



O tym, że kupowanie w sieci nie gryzie, kiedy regulamin to pułapka i co ma wspólnego Nigeria z naszym portfelem.

Wspomniałem już na stronach tego e-booka, że internet ułatwia życie. Poważną częścią naszego życia są zakupy, a możliwość dokonywania ich w sieci może być prawdziwym błogosławieństwem. Szczególnie dla tej części czytelników, którzy z racji wieku mają problemy z chodzeniem po sklepach w poszukiwaniu potrzebnych towarów. Trzeba też pamiętać, że kupowanie online może przynieść ulgę dla portfela – oferty internetowe są często znacznie tańsze niż te spotykane w tak zwanym realu.
Niestety, zakupy w internecie mają swoją mroczną stronę. Możemy się bowiem natknąć na nieuczciwego sprzedawcę, który na przykład nie dostarczy na czas – albo w ogóle nie wyśle – zakupionych artykułów lub będzie nam sprawiał kłopoty przy reklamacji wadliwego towaru. Dlatego wybierając się do e-sklepów, trzeba pamiętać o kilku zasadach, które pozwolą nam uniknąć rozczarowań.

Podejrzane okazje

Podstawowy problem to: jak wyszukać w sieci interesujący nas towar w korzystnej cenie i jak znaleźć uczciwy sklep, który szybko i sprawnie zrealizuje nasze zamówienie.
W internecie funkcjonują platformy zwane porównywarkami cen, które pozwolą nam łatwo zorientować się, jakie są koszty zakupu konkretnego towaru w sieci – mowa o takich serwisach, jak jak Ceneo.pl, Skapiec.pl, Nokaut.pl czy też porównywarka cen leków na stronie Medme.pl.

Porównywarki cen są także dobrym pośrednikiem w dotarciu do konkretnego sklepu, bowiem stosują swój własny system weryfikacji ofert i z reguły odsiewają na swoich stronach podejrzane podmioty. Jeśli więc znajdziemy przedmiot w atrakcyjnej cenie, możemy od razu kliknąć na link do oferującego go e-sklepu bez wielkich obaw, że trafimy na oszustów.

Dobrym źródłem wiedzy na temat konkretnego sprzedawcy są także serwisy grupujące opnie o sklepach, na przykład Opineo.pl. Warto też pamiętać, że wspomniane wcześniej porównywarki także zamieszczają opinie klientów na temat tego lub innego sprzedawcy. Na pewno warto się z nimi zapoznać przed rozpoczęciem zakupów.

Porównywarki cen to dobre miejsce, od którego możemy zacząć poszukiwanie w internetowych ofertach interesujących nas towarów

Cena może być także pierwszym sygnałem, że mamy do czynienia z podejrzaną ofertą. Jeżeli w jednym sklepie koszty zakupu konkretnego artykułu są znacznie niższe w porównaniu ze średnią obowiązującą w sieci, to bardzo możliwe, że mamy do czynienia z nieuczciwym sprzedawcą. Może się na przykład okazać, że zakupiony towar w ogóle do nas nie dotrze, koszty wysyłki mogą być szczególnie wysokie, często bywa też tak, że wyjątkowo taniego artykułu nie ma w sklepie, a niska cena miała tylko przyciągnąć naszą uwagę do konkretnego sklepu.
Cena nie jest oczywiście jedynym kryterium, które pomoże nam w ocenie uczciwości sprzedawcy. Dobry sklep internetowy, który poważnie traktuje klientów, zamieszcza na swojej stronie wszystkie informacje niezbędne do szybkiego i łatwego z nim kontaktu. Powinien tam być adres siedziby firmy prowadzącej sklep, numer telefonu i adres e-mail. Jeżeli dane sklepu są podejrzanie skromne, to lepiej zrobimy, szukając takiego samego towaru u innego dostawcy. Tak będzie bezpieczniej.
Bardzo ważnym elementem, podobnie jak w przypadku serwisów internetowych oferujących rozmaite usługi (patrz rozdział VII), jest **regulamin sklepu**. Powinniśmy szczególnie zwrócić uwagę na to, czy w regulaminie nie umieszczono zapisów znajdujących się na liście klauzul niedozwolonych – pełny spis takich klauzul znajdziemy na stronach Urzędu Ochrony Konkurencji i Konsumentów (http://uokik.gov.pl/niedozwolone_klauzule.php). Do najczęściej spotykanych zabronionych zapisów w regulaminach można zaliczyć:

- Narzucanie lokalizacji sądu, który będzie rozstrzygał ewentualne spory.
- Wskazywanie firmy trzeciej, do której należy odsyłać zwracany towar.
- Odliczenie kosztów wysyłki towaru od zwracanej kwoty w wypadku rozwiązania umowy.
- Nieponoszenie przez sprzedawcę odpowiedzialności za błędy w opisie produktu na stronie z ofertą.
- Uchylanie się sprzedawcy od odpowiedzialności za uszkodzenie przesyłki i opóźnienia w dostawie.
- Żądanie spisania protokołu uszkodzenia w obecności kuriera lub dostawcy przesyłki.

Pamiętajmy, że witryny służące do logowania czy rejestracji w konkretnym sklepie powinny się rozpoczynać nie od liter http:, jak na zwykłej stronie WWW, ale od **https**:, co oznacza stronę odpowiednio zabezpieczoną. Jest to ważne między innymi ze względu na ochronę naszych danych.
Musimy też mieć świadomość tego, że w odróżnieniu od cen w tradycyjnych

sklepach te obowiązujące w internecie składają się zwykle z dwóch elementów: kosztów samego towaru oraz jego wysyłki do klienta. Nie wszędzie podawana cena uwzględnia od razu opłatę za kuriera czy paczkę pocztową. Dlatego warto upewnić się na stronie sklepu, ile życzy on sobie za dostarczenie zakupionego towaru. Czasem bywa tak, że początkowa cenowa okazja jest zwykłym oszustwem, bo po doliczeniu ceny wysyłki wychodzi nam suma wyższa od cen w wielu innych e-sklepach czy u sprzedawców stacjonarnych.

Jakie mamy prawa?

Trzeba przyznać, że klienci sklepów internetowych są w lepszej sytuacji, niż osoby kupujące towary w realu. Chodzi chociażby o to, że kupując w sieci, mamy prawo do rezygnacji z zakupu bez podania konkretnej przyczyny i odesłania sprzedawcy towaru. Zrezygnować możemy w ciągu 10 dni od momentu otrzymania przedmiotu i nie musi on być wadliwy lub uszkodzony – wystarczy po prostu, że nam się nie spodoba. Niestety są też wyjątki od tej reguły, o których warto pamiętać. Przepisy nie dotyczą na przykład rozpakowanych już płyt z nagraniami muzycznymi czy programów komputerowych (a więc i gier). Taki towar możemy odesłać, ale pod warunkiem, że nadal znajduje się w oryginalnym opakowaniu, a folia nie została naruszona.
Poza tym mamy oczywiście wszystkie inne prawa przysługujące konsumentom w świetle polskich przepisów. W ciągu dwóch lat od momentu zakupu towaru możemy go reklamować, powołując się na niezgodność przedmiotu z umową, lub skorzystać z warunków reklamacji oferowanej przez producenta.

Allegro: Kupujemy

Obecnie jednym z największych sklepów funkcjonujących w polskiej sieci jest serwis Allegro. Nie, to nie jest pomyłka. Platforma, która przed ponad dekadą startowała jako strona aukcyjna, liczy dzisiaj ponad 12 milionów użytkowników, ale o prawdziwych aukcjach rzadko kto już dzisiaj na niej pamięta. Obecnie gros transakcji na Allegro jest dokonywanych w opcji Kup teraz, czyli jak w każdym innym sklepie internetowym. Trzeba przy tym pamiętać, że na Allegro swoje towary sprzedaje coraz więcej firm, które traktują ten serwis jako dodatkowy kanał dystrybucji. Nic więc dziwnego, że ta platforma przypomina dzisiaj wielki internetowy pchli targ – można na nim kupić dosłownie wszystko, i to zarówno w stanie fabrycznie nowym, jak i używanym.
Jako kupujący mamy na Allegro pewien kłopot – chodzi o weryfikację sprzedaw-

cy pod względem jego czystych intencji. Co kilka tygodni w internecie pojawiają się doniesienia o tym, że oto kolejni oszuści nabrali setki allegrowiczów, przyjmując od nich pieniądze i wysyłając w zamian, zamiast obiecanego towaru, przysłowiową cegłę opakowaną w kartonik.

Jak się przed tym ustrzec? Najłatwiej będzie nam zweryfikować rzetelność sprzedawcy, zapoznając się z opiniami na jego temat. Oczywiście bardzo rzadko zdarzają się konta idealne, na których znajdziemy kilka tysięcy komentarzy i opinii i wszystkie z nich będą pozytywne. Zawsze znajdzie się kilka wpisów negatywnych lub neutralnych. Nie powinna nas przerażać sama sucha statystyka, choć oczywiście nieco inaczej wygląda 15 „negatywów" przy 2000 pozytywnych opinii niż dwie opinie negatywne pośród ogólnej liczby 10 wpisów. Ważniejsze jest jednak to, czego wspomniane „negatywy" dotyczą. Jeżeli są wyrazem zwykłych słownych przepychanek pomiędzy kupującym a sprzedającym, którzy oskarżają się o brak uprzejmości, albo chodzi o niewielką plamkę na używanej koszulce, to pół biedy. Naszą czujność powinny jednak wzbudzić wpisy dotyczące opóźnień sprzedawcy w dostarczaniu towaru, niezgodności oferowanego przedmiotu z opisem, zawyżonych cen wysyłki czy też w końcu braku realizacji zamówienia. Jeżeli na koncie sprzedającego znajdziemy negatywne opinie o podobnej treści, to lepiej zrezygnować z zakupu i poszukać innego sklepu lub prywatnego sprzedawcy oferującego podobny artykuł.

System komentarzy na Allegro pozwoli nam zorientować się, czy mamy do czynienia z uczciwym i rzetelnym sprzedawcą, czy też z oszustem, którego należy omijać z daleka

ROZDZIAŁ VIII
Kupujmy z głową!

Od pewnego czasu na Allegro funkcjonuje mechanizm, który w znacznym stopniu ułatwia życie kupującym. Chodzi o możliwość dokonywania zakupów bez konieczności rejestracji i aktywacji konta w serwisie. Korzystając z tej metody, dokładamy kolejne przedmioty do koszyka, następnie podajemy adres e-mail i wykorzystujemy przesłany na ten adres specjalny kod weryfikacyjny. Musimy jednak pamiętać, że czasami warto zarejestrować konto w Allegro – taka operacja nie zajmie więcej niż kilka dodatkowych minut przy komputerze. Zarejestrowane konto pozwoli nam między innymi na zadawanie pytań sprzedającemu (to ważne w wypadku, gdy mamy wątpliwości co do stanu towaru, szczegółów płatności i wysyłki), jest także niezbędne w momencie, gdy sami zechcemy coś sprzedać na tej platformie (na ten temat w kolejnym wątku).

Z punktu widzenia bezpieczeństwa zakupów na Allegro bardzo ważnym etapem zawierania transakcji jest sposób zapłaty za przedmiot i jego dostarczenie. Oczywiście najbardziej bezpieczne opcje to tak zwana wysyłka za pobraniem oraz odbiór osobisty.

W wypadku wysyłki za pobraniem za przedmiot płacimy gotówką w momencie, gdy kurier zjawi się z paczką pod naszymi drzwiami. Przesyłkę możemy spokojnie odpakować (kurierzy tego nie lubią, ale będą musieli zaczekać, nie dajmy się poganiać) i sprawdzić, czy towar jest zgodny z zamówieniem i nie został uszkodzony. Jeżeli wszystko się zgadza, to za pokwitowaniem wręczamy pieniądze doręczycielowi. Niestety wielu sprzedających na Allegro nie oferuje na swoich stronach opcji wysyłki za pobraniem. Dlaczego? Zwykle dla własnej wygody. Chodzi bowiem o to, że taka opcja dosyć znacząco wydłuża drogę gotówki od kupującego na konto sprzedawcy, bowiem pośrednikiem jest tutaj firma kurierska. Z kolei my musimy pamiętać, że zwykle przesyłka za pobraniem jest o kilka złotych droższa od tradycyjnej. Druga wada „pobraniówki" jest taka, że nie zawsze mamy w domu gotówkę. Jeśli pieniądze spoczywają na naszym koncie bankowym, musimy wybrać się do bankomatu, by je przekazać kurierowi.

Opcja odbioru osobistego towaru jest także bezpieczna, jednak umówmy się – uciążliwa. W końcu robimy zakupy w sieci po to, by nie ruszać się z domu. Jeżeli musimy wybrać się sami po odbiór zakupionego towaru, to równie dobrze możemy pójść po niego do zwykłego sklepu. No chyba, że ten w internecie jest o wiele tańszy. Odbiór osobisty nie wchodzi też często w grę z prozaicznego powodu – kupujemy towar oferowany w zupełnie innym mieście czy regionie kraju niż ten, w którym sami mieszkamy.

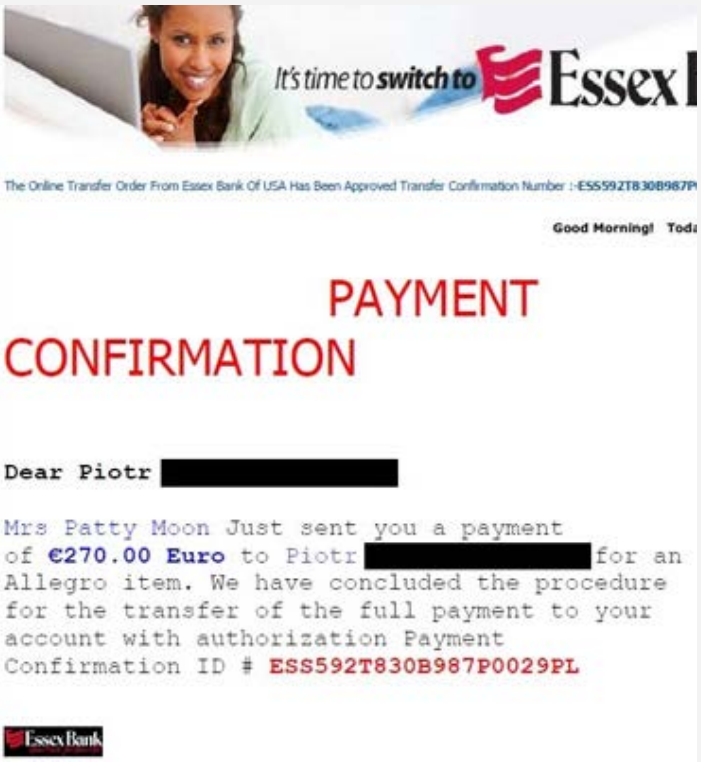
Spośród metod płatności na odległość dostępnych w Allegro najmniej ryzykow-

ne będzie skorzystanie z systemu PayU. Jest to platforma płatności elektronicznych pozwalająca na szybki przepływ pieniędzy pomiędzy kontrahentami. Opcja PayU jest domyślnie ustawiona we wszystkich ofertach wystawianych na Allegro. Pojawi się ona natychmiast w momencie, gdy dokonamy zakupu przez Kup teraz i wypełnimy na stronie formularz płatności i dostawy. Później wystarczy połączyć się z naszym internetowym kontem bankowym i zapłacić. Z naszego punktu widzenia kanał PayU jest o tyle bezpieczny, że obejmuje go Program ochrony kupujących. Oznacza to, że w wypadku braku dostarczenia przez sprzedającego towaru przysługuje nam zwrot pełnej kwoty, którą wysłaliśmy w ramach zapłaty za przedmiot. Takiej pewności nie daje już na przykład bezpośrednie przelanie pieniędzy z naszego konta na rachunek sprzedawcy. Oczywiście poświadczenie dokonania przelewu jest ewentualnym dowodem w wypadku roszczeń wobec sprzedawcy, jednak gdy padniemy ofiarą oszustwa i nie otrzymamy zamówionego towaru, to ewentualne dochodzenie z udziałem policji i sądów może trwać w najlepszym wypadku wiele miesięcy.
Podczas kupowania na Allegro powinniśmy się też wystrzegać innych pułapek. Chodzi na przykład o zakup artykułów podlegających ochronie autorskiej – programów komputerowych czy gier. Wśród milionów ofert na Allegro jest wciąż sporo pirackich kopii oprogramowania, a my kupując taki produkt, stajemy się w świetle prawa paserami. Trzeba się więc upewnić ponad wszelką wątpliwość, że mamy do czynienia na przykład z legalnym systemem operacyjnym czy programem graficznym.
Od razu możemy sobie dać spokój z ofertami, które proponują nam na przykład Windows 7 czy Photoshopa za... 30 złotych.

Allegro: Sprzedajemy

W poprzednim wątku wspomniałem o korzyściach, jakie może nam przynieść zarejestrowanie konta na Allegro. Najważniejsza z nich polega na tym, że z pozycji kupującego możemy przejść na pozycję sprzedawcy i wystawić w serwisie własną ofertę. W ten sposób można sprzedać na przykład zbędne przedmioty, które pokrywa kurz gdzieś w zakamarkach naszych szaf.
W przypadku sprzedaży jesteśmy nieco mniej narażeni na rozmaite niebezpieczeństwa niż wtedy, gdy kupujemy towary na Allegro. Oczywiście pod warunkiem, że będziemy się trzymać pewnych zasad.
Wystawiając swoją ofertę na Allegro, powinniśmy przede wszystkim sprawdzić, czy sprzedawany przez nas przedmiot nie znajduje się wśród towarów zabro-

nionych. Na takiej liście są między innymi materiały pornograficzne, alkohol, leki wydawane na receptę czy oprogramowanie naruszające prawa autorskie producenta. Pełną listę artykułów zabronionych znajdziemy na stronie: http://allegro.pl/country_pages/1/0/z2.php.
Wystawiając towar na Allegro, powinniśmy się też strzec tak zwanego przekrętu nigeryjskiego. Jest to pewien scenariusz wykorzystywany przez oszustów pochodzących najczęściej spoza granic naszego kraju.
W skrócie polega on na tym: rzekomy kupujący twierdzi, że już wysłał nam pieniądze za przedmiot, i na dowód tego przesyła nam mailem podrobione potwierdzenie przelewu, najczęściej z jakiegoś mało znanego lub nieistniejącego banku. My, nie podejrzewając niczego złego, nadajemy na podany adres paczkę z przedmiotem i czekamy, aż pieniądze pojawią się na koncie. Niestety, na próżno. Opłata nigdy nie dociera na rachunek, a my pozostajemy bez sprzedawanego towaru i bez pieniędzy. Dlatego bardzo ważna jest jedna zasada: **nie wysyłamy przedmiotu kupującemu przed pojawieniem się gotówki na koncie!**

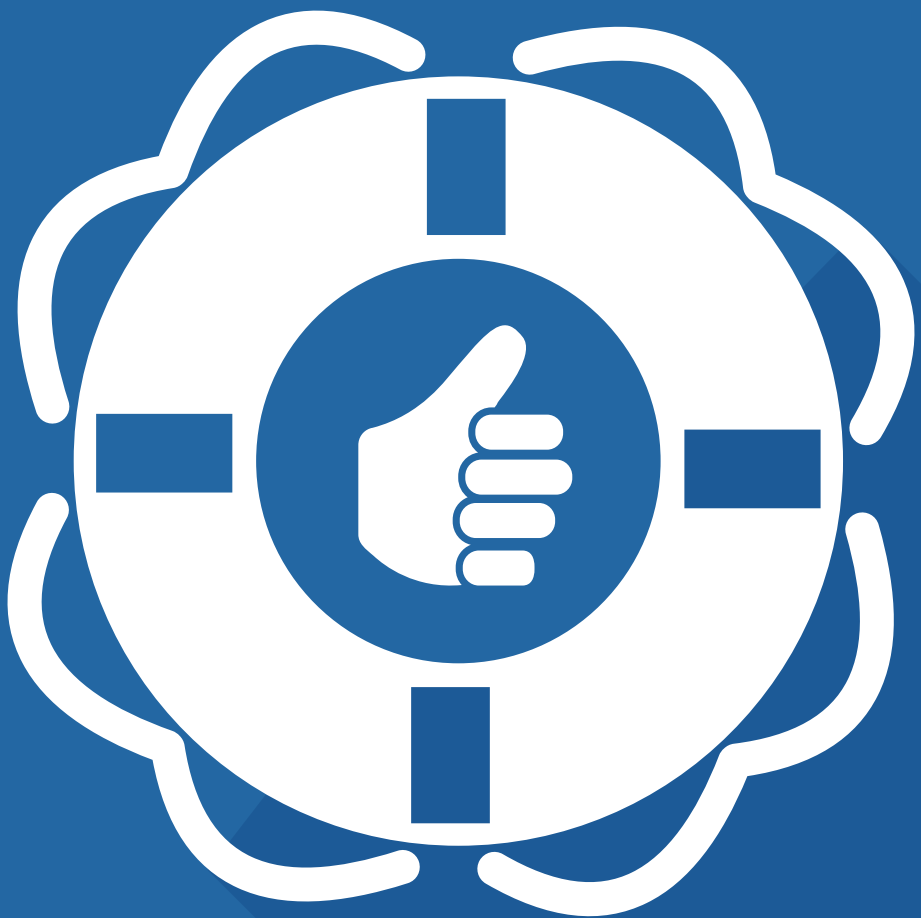


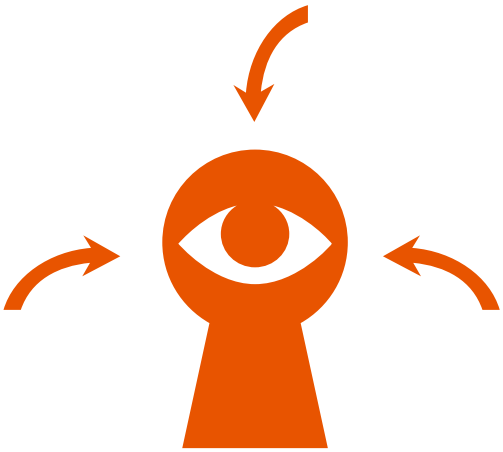
Ofiary przekrętu nigeryjskiego otrzymują fałszywe potwierdzenia przelewów z rozmaitych mało znanych lub nieistniejących banków

Jedynym wyjątkiem od tej zasady jest system PayU – kiedy otrzymamy oficjalny komunikat od tej platformy o wpłacie gotówki i potwierdzimy ten fakt na naszym koncie na Allegro, możemy bezpiecznie wysłać towar kupującemu.

ROZDZIAŁ IX

Bezpieczny Facebook





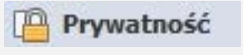
O tym, że fejs i lajki mogą się podobać, jak nie dać się podglądaczom i jak wyrzucić za drzwi nieproszonych gości.

Już od ponad dziesięciu lat w internecie funkcjonuje pojęcie Web 2.0. Oznacza ono strony internetowe, których treść jest tworzona w dużej części przez samych użytkowników. Zaliczają się do tej kategorii wszystkie tak zwane serwisy społecznościowe, cieszące się wśród internautów ogromną popularnością. Nie bez powodu. Platformy społecznościowe pozwalają nam na utrzymywanie kontaktu z rodziną i przyjaciółmi, publikowanie własnych treści i śledzenie tego, co umieszczają w sieci nasi znajomi. Jednak obecność w takich serwisach może nieść pewne zagrożenia, na przykład kradzież tożsamości i podszywanie się innych osób pod nasze konto. Warto też stworzyć na naszym profilu ograniczenia zapewniające nam pożądany stopień prywatności. Zobaczmy, jak to zrobić na przykładzie Facebooka – serwisu, który stał się dzisiaj symbolem serwisów społecznościowych i internetu epoki Web 2.0.

Prywatność

Po założeniu konta na Facebooku logujemy się na nie i w prawym górnym rogu głównej strony wybieramy przycisk:

a następnie klikamy na:



W sekcji:

Kto zobaczy Twoje przyszłe posty?

musimy zdecydować, kto będzie miał dostęp do publikowanych przez nas treści. Oczywiście najbardziej odważni z nas mogą zaznaczyć opcję:

Publiczne

Muszą się jednak liczyć z tym, że publikowane wpisy i zdjęcia będą mogli oglądać wszyscy użytkownicy Facebooka, a jest ich na świecie ponad miliard. Trzeba też pamiętać, że na nasz profil mogą trafić osoby niezbyt nam życzliwe, a w konsekwencji mogą nas spotkać nieprzyjemności. Dlatego według mnie najrozsądniejszym wyborem będzie opcja:

Znajomi

Oznacza ona, że dostęp do naszych treści będą miały tylko osoby ze statusem znajomego. A weryfikację takich użytkowników przeprowadzamy my sami, godząc się na włączenie konkretnej osoby do grona znajomych.
Przechodzimy do kolejnej sekcji, istotnej dla nas ze względów prywatności i bezpieczeństwa:

Kto może się ze mną kontaktować?

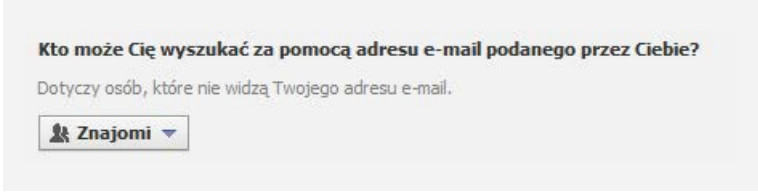
Tutaj zdecydujemy, kto może wysyłać do nas wiadomości oraz zaproszenia do grona znajomych. Jeżeli jesteśmy początkującymi użytkownikami Facebooka, to najrozsądniejszym wyborem będzie opcja:

Znajomi znajomych

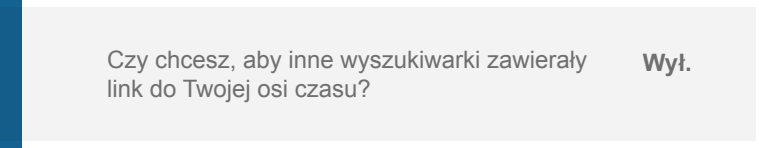
Nie mniej ważna jest kolejna sekcja o nazwie:

Kto może mnie wyszukać?

Tutaj nasze ustawienia będą decydowały o tym, czy nasze konto na Facebooku będzie widoczne w całym internecie i możliwe do odnalezienia za pomocą takich narzędzi jak wyszukiwarka Google. Jeżeli pragniemy pozostać anonimowi i w pewnej mierze ukryć się przed internetowym światem, to w pierwszej opcji wybieramy ustawienia:



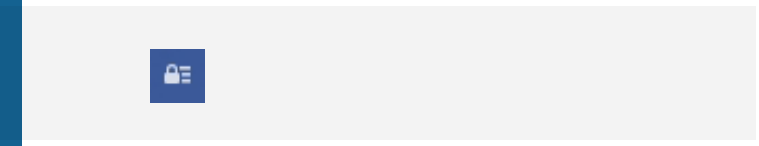
Równie ważna jest też opcja:



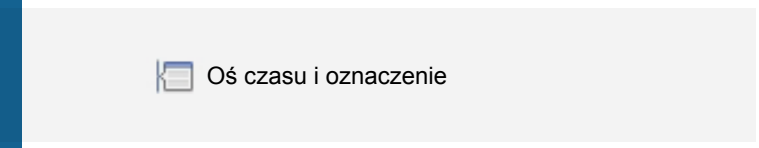
którą ustawiamy w pozycji Wyłączone.

Oś czasu

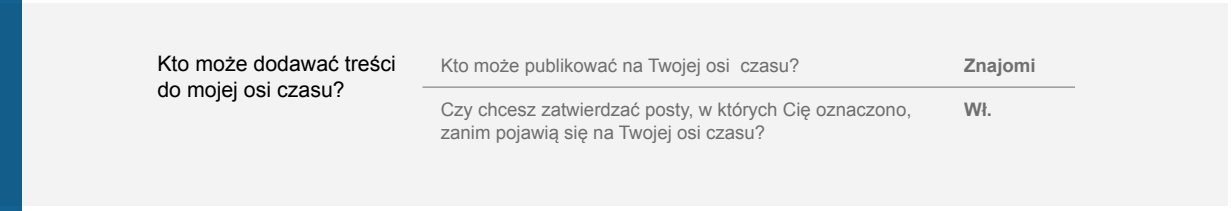
Kolejne ustawienia będą dotyczyły tak zwanej Osi czasu, czyli naszej głównej wizytówki w serwisie Facebook. Po użyciu przycisku



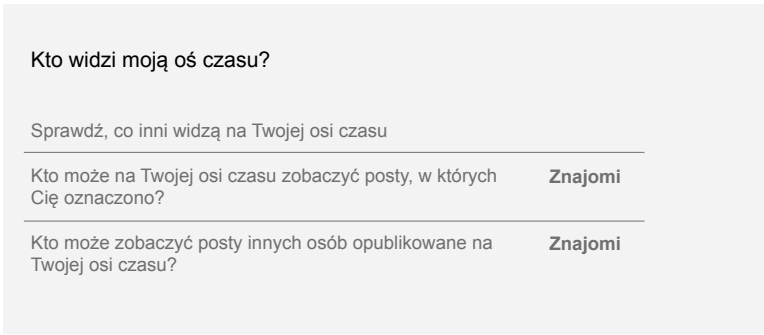
klikamy na opcję



Pierwsza sekcja jest ważna, bowiem od niej zależy, kto będzie mógł dodawać treści do naszej osi czasu. Konsekwentnie wybieramy opcję Znajomi i włączamy potwierdzenia postów, na których zostaliśmy oznaczeni przez innych:

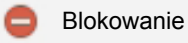


– dzięki temu będziemy mogli decydować, jakie posty naszych znajomych, w których zostaliśmy wymienieni, pojawią się na naszej Osi czasu. Oczywiście posty te będą nadal widoczne na koncie osób, które je opublikowały. W kolejnej sekcji dzięki pierwszej wymienionej w niej pozycji możemy zobaczyć, jak wygląda nasza Oś czasu z perspektywy innych użytkowników Facebooka. W pozostałych punktach wybieramy opcję Znajomi. Dzięki temu konsekwentnie ograniczymy widoczność treści na naszym profilu do osób, które już wcześniej obdarzyliśmy zaufaniem.

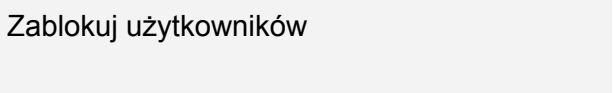


Blokady

Poniżej przycisku Oś czasu znajdziemy opcję:

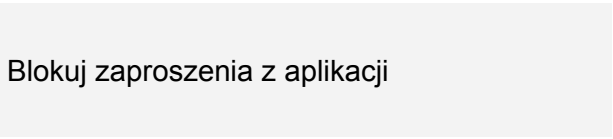


Jest ona użyteczna w wypadku, gdy zechcemy ograniczyć dostęp do naszego profilu innym użytkownikom Facebooka. W sekcji:



możemy wpisać imię i nazwisko lub nazwę konkretnego użytkownika i go zablokować.

Po przeprowadzeniu takiego zabiegu wskazana osoba zostanie usunięta z grona naszych znajomych i nie będzie mogła przeglądać publikowanych przez nas treści.
Następna sekcja:



jest istotna głównie ze względu na komfort korzystania z Facebooka. Zmorą są na nim nagminne zaproszenia do skorzystania z konkretnych aplikacji, na przykład rozmaitych gier online. Możemy jednak zablokować użytkownika, od którego non stop otrzymujemy tego typu powiadomienia.

Likwidacja i dezaktywacja konta

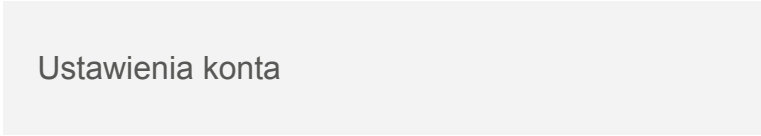
Choć Facebook jest bardzo popularną platformą, to z czasem zaczął przysparzać sobie także przeciwników. W internecie pojawiały się pretensje o to, że o ile bardzo łatwo się do Facebooka zapisać, o tyle o wiele trudniej jest wypisać się z tego serwisu.
Od tamtej pory szefostwo platformy, zresztą nie bez nacisków ze strony rozmaitych instytucji w USA, poczyniło pewne postępy związane z ułatwieniem rezygnacji z usług serwisu i likwidacji naszego profilu. Dzisiaj do dyspozycji mamy dwie drogi postępowania: całkowitą likwidację profilu połączoną ze skasowaniem wszystkich naszych danych przechowywanych na serwerach Facebooka oraz czasową dezaktywację konta, które możemy odnowić w dowolnym momencie.
Aby zlikwidować nasze konto na Facebooku, wchodzimy tu: www.facebook.com/help/delete_account.

Pojawi się strona, na której klikamy na przycisk:

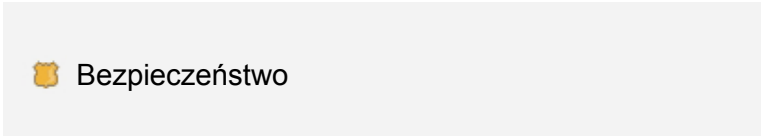
Następnie wpisujemy nasze hasło do Facebooka, przepisujemy kod zabezpieczający z obrazka i klikamy na:

Pojawi się komunikat o rozpoczęciu dwutygodniowej procedury usuwania danych.
Jeżeli zamierzamy jedynie na pewien czas dezaktywować nasze konto na Facebooku, to na głównej stronie serwisu wybieramy przycisk:

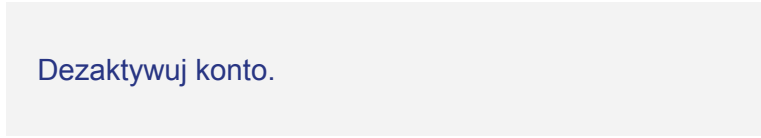
następnie klikamy na:



i:



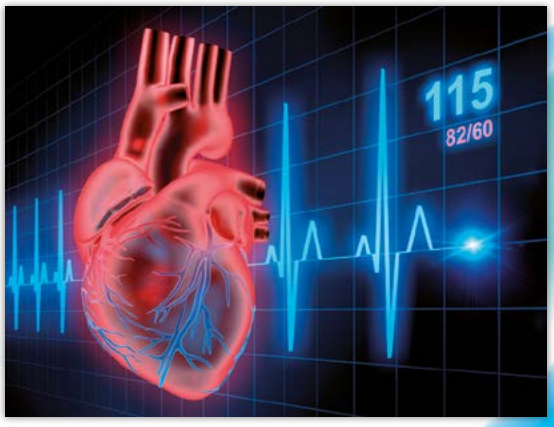
Na koniec wybieramy przycisk:



Dezaktywowane konto możemy w każdej chwili przywrócić, logując się w serwisie za pomocą naszego adresu e-mail i hasła.

medme.pl

Bądź zdrowy i żyj zdrowo



Urazy narządów ruchu

Schorzenia sercowo--naczyniowe

Serwis o zdrowym stylu życia

Reumatologia

Choroby cywilizacyjne

ROZDZIAŁ X

Bank internetowy: Oblężona twierdza

ROZDZIAŁ X
Bank internetowy: Oblężona twierdza

O tym, co zmienia w naszym banku literka „e", jak trzymać karty przy orderach i że warto dokładnie patrzeć w SMS-y.

Jeszcze jedną lub dwie dekady temu nasze pieniądze trzymaliśmy przeważnie w portfelu lub przysłowiowej skarpecie. Jeżeli już korzystaliśmy z konta bankowego, to jego obsługa bywała uciążliwa, bo każda operacja na rachunku oznaczała konieczność udania się do bankowego okienka.

Dzisiaj internet zmienił także tę dziedzinę naszego życia. Dostęp do konta bankowego jest możliwy za pośrednictwem sieci i większość działań na rachunku możemy przeprowadzić, nie ruszając się sprzed domowego komputera. To bardzo wygodne rozwiązanie, ale czy bezpieczne? W większości wypadków tak. Banki starannie dbają o informatyczne bezpieczeństwo, od niego bowiem zależy w dużej mierze liczba ich klientów. To jednak nie oznacza, że internetowi przestępcy mający chrapkę na nasze pieniądze zasypiają gruszki w popiele – co pewien czas docierają do nas informacje o atakach na internetowe konta tego czy innego dużego banku.

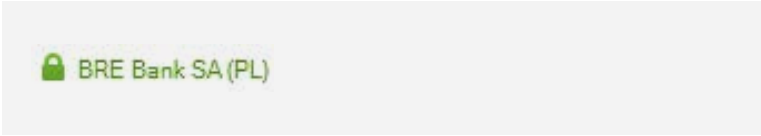
W ustawieniach posiadanego przez nas rachunku internetowego możemy zrobić niezbyt wiele, by poprawić jego bezpieczeństwo. Oczywiście, ustalając hasło do konta, powinniśmy postępować według wszystkich zasad bezpieczeństwa, które wymieniłem w rozdziale II tego e-booka. Oprócz tego jest jednak kilka innych reguł, których powinniśmy przestrzegać na co dzień po to, by nasze pieniądze w banku były zawsze bezpieczne.

Aktualność = bezpieczeństwo

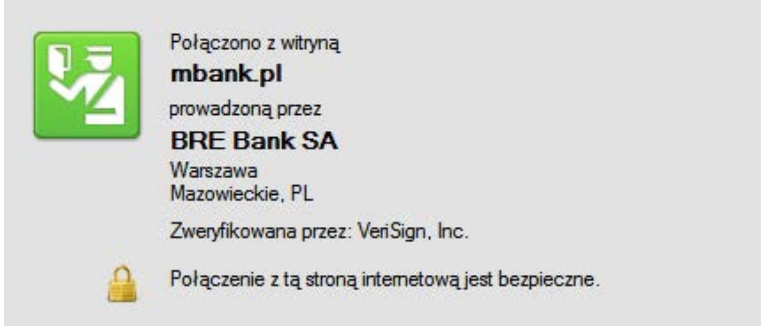
Jedna z podstawowych zasad ochrony dostępu do naszego rachunku w banku to… bezpieczeństwo naszego własnego komputera. Komputerowi włamywacze najczęściej wykorzystują luki w systemie operacyjnym oraz w zabezpieczeniach kilku popularnych programów używanych przez wielu użytkowników. Dlatego żelazna zasada, o jakiej wspominałem już w rozdziale VI, jest taka: **w naszym systemie operacyjnym powinny być zainstalowane wszystkie najnowsze aktualizacje dostarczone przez producenta**. Dodatkowo należy zadbać o zainstalowanie poprawek bezpieczeństwa w następujących aplikacjach: Adobe Reader, Adobe Flash Player, Java i Internet Explorer. Na szczęście nie musimy ręcznie sprawdzać wersji każdego z tych programów i dostępności aktualizacji. Są do tego odpowiednie narzędzia, na przykład Update Checker. Ta darmowa aplikacja dostępna jest na stronie: http://www.filehippo.com/pl/updatechecker. Sprawdza ona stan dostępnych uaktualnień i pozwala szybko je zainstalować. Aktualizacja dotyczy też w najwyższym stopniu przeglądarki internetowej, za pośrednictwem której korzystamy z naszego konta w sieci.
Kiedy nasz komputer zostanie w pełni zaktualizowany, musimy pamiętać o tym, żeby pod żadnym pozorem nie dokonywać operacji na naszym koncie za pomocą innej, przypadkowej maszyny – na przykład w kawiarence internetowej. Ważne jest także to, by nie łączyć się z bankiem za pośrednictwem niezabezpieczonych sieci bezprzewodowych – na przykład tak zwanych publicznych hot-spotów dostępnych w centrach handlowych. Do takiej sieci bowiem przestępcom bardzo łatwo się włamać i przechwycić wszystkie dane niezbędne do przejęcia kontroli nad naszym kontem.

Certyfikat – ważna rzecz

Istotna informacja na temat bezpieczeństwa strony naszego banku pojawia się jeszcze zanim zalogujemy się na konto. Po otwarciu witryny banku po lewej stronie adresu powinien pojawić się symbol zielonej kłódki



i – w zależności od wersji przeglądarki – odpowiednia informacja o certyfikacie bezpieczeństwa. Po kliknięciu na nią zobaczymy odpowiedni komunikat o autentyczności witryny:



Tylko strony z taką informacją gwarantują, że nie dostaliśmy się pod adres fałszywej witryny, która może przejąć nasze wrażliwe dane do konta bankowego.

Phishing: Jak rozpoznać wroga?

O phishingu jako metodzie wyłudzania od użytkowników wrażliwych danych, także tych związanych z kontem bankowym, wspominałem już w rozdziale I tego e-booka. W jaki sposób możemy zorientować się, że mamy do czynienia z phishingiem? Jest kilka symptomów, które powinny obudzić naszą czujność. Phishing często przybiera formę wiadomości e-mail wysłanej rzekomo przez nasz bank. W najprostszej i najbardziej prymitywnej formie nadawca listu, podając się na przykład za pracownika serwisowego, prosi nas o podanie loginu i hasła do rachunku, podobno w celu jego weryfikacji. Oczywiście nie trzeba dodawać, że **nigdy nie wolno nam odpowiadać na podobną korespondencję i w żadnym wypadku nie należy podawać wrażliwych informacji, o które prosi nadawca maila**.
Bywają też nieco bardziej wymyślne formy wyciągania poufnych danych. Mowa o wiadomościach, które także przypominają na pierwszy rzut oka mail pochodzący z banku. Z treści takiej korespondencji dowiadujemy się, że oto na nasze konto wpłynął niespodziewany przelew lub że nasz rachunek znalazł się w prawdziwym niebezpieczeństwie. Aby sprawdzić szczegóły, powinniśmy kliknąć na link zawarty w wiadomości. **Nie róbmy tego pod żadnym pozorem!** Po kliknięciu na odnośnik zostaniemy bowiem przeniesieni nie na autentyczną stronę logowania naszego banku, ale na witrynę spreparowaną przez przestępców. Czekają oni tylko na to, byśmy na takiej stronie wpisali nasz login i hasło. Będą mieli wtedy otwartą drogę do naszego konta bankowego.
Tego typu e-maile są na szczęście dość łatwe do rozpoznania po bliższych oględzinach. Często bowiem są pisane łamaną polszczyzną przy użyciu programu zwanego translatorem. Jednak nawet w przypadku, gdy język e-maila jest w miarę poprawny, pamiętajmy o kolejnej żelaznej regule ochrony internetowego rachunku: nasz bank nigdy nie wyśle do nas wiadomości e-mail z prośbą o podanie loginu i hasła do konta! Dlaczego? Ano dlatego, że procedury bezpieczeństwa w bankach wykluczają wysyłanie podobnych wiadomości w trosce o bezpieczeństwo klientów.

Kody i SMS-y: Miej otwarte oczy!

Wymienione metody phishingu to jeszcze nie wszystkie środki, którymi dysponują przestępcy, dokonując ataków na

nasze konto. W 100% nie chronią nas przed ich atakami nawet tak pozornie bezpieczne rozwiązania, jak autoryzacja operacji bankowych za pomocą unikalnych kodów lub wiadomości SMS.
Jak cyberprzestępcy mogą nam zaszkodzić, gdy przy dokonywaniu operacji bankowych online zabezpieczamy się jednorazowymi kodami, w jakie wyposaża nas bank (zwanych też zdrapkami)? Wystarczy, że w internecie trafimy na zainfekowaną stronę WWW – działające na niej szkodliwe oprogramowanie znajdzie luki w zabezpieczeniach systemu lub innych programów (wspominałem o tym przy okazji koniecznych aktualizacji) i zainstaluje się w komputerze. Później, kiedy zalogujemy się na nasze konto bankowe, zostaniemy automatycznie przeniesieni na fałszywą stronę, gdzie zostaniemy poproszeni, w celu rzekomej weryfikacji, o podanie kilku jednorazowych kodów z naszej zdrapki. Jeśli posłuchamy i spełnimy tę prośbę, możemy mieć poważne kłopoty. Przestępcy otrzymają bowiem komplet informacji potrzebnych do tego, by na przykład przelać wszystkie nasze pieniądze na swój własny rachunek bankowy. Podobnie jak bank nie wysyła nigdy maili z żądaniem podania loginu i hasła, tak samo nigdy nie wymaga od nas seryjnego wpisywania jednorazowych kodów. Warto o tym pamiętać!

Złodzieje próbują też czasami atakować systemy bezpieczeństwa oparte na autoryzacji za pomocą SMS-ów. Odbywa się to zwykle w taki sposób, że podczas logowania do banku z zainfekowanego komputera i wykonywania przelewu szkodliwe oprogramowanie przejmuje otwartą sesję w przeglądarce i wstawia zamiast podanego przez nas numeru konta odbiorcy i sumy swoje własne dane. W momencie otrzymania SMS-em kodu potwierdzającego operację i wpisaniu go na stronie pieniądze zostają przelane, ale na rachunek złodziei. Jak się przed tym ustrzec? W tym wypadku może nas uchronić jedynie brak rutyny – przed autoryzowaniem przelewu za pomocą kodów SMS-owych powinniśmy jeszcze raz uważnie sprawdzić, na jakie konto i jaka kwota ma zostać przekazana odbiorcy.

Trzymaj karty przy orderach!

Tytułowe powiedzenie pochodzi z czasów, które wielu czytelników tego e-booka może dobrze pamiętać. Kiedyś używało się tego ostrzeżenia na przykład przy brydżu i chodziło w nim o to, by nie pozwolić przeciwnikowi na zajrzenie w nasze karty. Okazuje się, że dzisiaj to powiedzonko może być także aktualne i to wcale nie przy karcianym stoliku. Zwłaszcza gdy odniesiemy je do elektronicznych kart płatniczych i kredytowych.

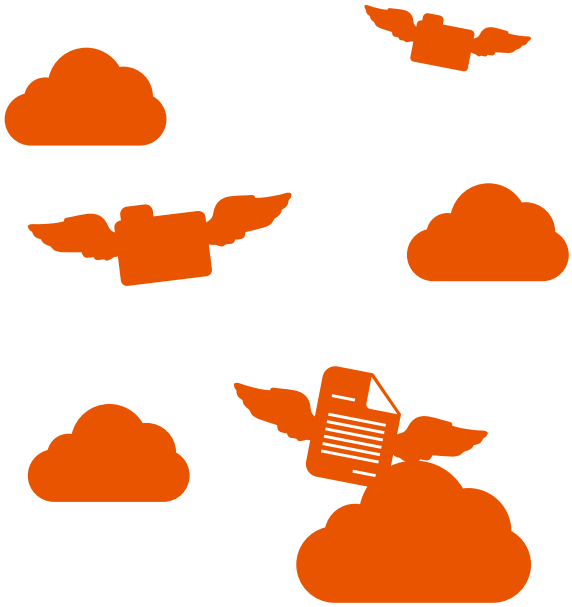
Trzeba pamiętać, że złodzieje czyhający na nasze pieniądze wcale nie muszą atakować konta bankowego. Mogą dobrać się do zgromadzonych na nim środków za pośrednictwem karty. Zapewne nie trzeba już dzisiaj nikomu przypominać, **że zapisywanie numeru PIN bezpośrednio na karcie lub noszenie go na kartce w portfelu obok karty jest złym pomysłem**, delikatnie rzecz ujmując. Niestety przestępcy mają też kilka innych sposobów na to, by dobrać się do naszego plastikowego pieniądza. Jednym z nich, dzisiaj stosowanym już coraz rzadziej, jest kopiowanie danych karty przez nieuczciwego sprzedawcę w sklepie czy kelnera w restauracji. Aby się przed tym ustrzec, nie powinniśmy po prostu spuszczać karty z oka. Drugi sposób polega na odpowiednim spreparowaniu bankomatu. Przestępcy montują w nich niewielkie skanery, które kopiują kartę, a dodatkowa nakładka na klawiaturę bankomatu przechwytuje wprowadzany PIN. Taki gotowy zestaw danych pozwala już na swobodne wypłacenie gotówki w naszym imieniu. Przed dokonaniem operacji w bankomacie powinniśmy więc najpierw nieco mu się przyjrzeć. Naszą czujność niech wzbudzi na przykład nietypowa budowa podajnika do karty, dodatkowe plastikowe banery przyczepione do obudowy czy podejrzanie wyglądająca klawiatura. Najlepiej też będzie podejmować pieniądze z bankomatów położonych przy siedzibie banku lub w ruchliwym miejscu w centrum handlowym. Dlaczego? Takie lokalizacje są często lub stale monitorowane i przestępcy mają znacznie mniejsze szanse na zamontowanie w bankomacie swoich zestawów służących do kradzieży niż w bardziej odludnych miejscach.

Istnieje też sposób na to, by nie tyle zapobiec kradzieży pieniędzy z konta za pomocą podrobionej karty, ale by zmniejszyć ewentualne straty spowodowane takim przywłaszczeniem gotówki. Na naszym koncie bankowym powinniśmy wydać dyspozycję o dziennym limicie wypłat z bankomatu. Nie pozbawi nas to możliwości płacenia plastikowym pieniądzem na przykład w sklepie, natomiast zapobiegnie wyczyszczeniu konta przez przestępców.

ROZDZIAŁ XI

Chmura: Dane pod kluczem

ROZDZIAŁ XI
Chmura: Dane pod kluczem



O tym, dlaczego warto trzymać pliki w niebie, jak załatwić sobie kilka darmowych gigabajtów pamięci i jak zamknąć chmurę na kłódkę.

Jesteśmy przyzwyczajeni do tego, że nasz dysk w komputerze gromadzi wszystkie ważne dla nas dane – dokumenty tekstowe, zdjęcia, nagrania muzyczne czy filmy. Dzięki internetowi możemy jednak skorzystać z dodatkowej przestrzeni na nasze pliki. Mowa o wirtualnych dyskach dostępnych w tak zwanej chmurze obliczeniowej. Jej idea polega na tym, że konkretna firma udostępnia nam miejsce na swoich serwerach, a my możemy przenosić tam dowolne dane. Jeszcze niedawno argumentem przeciwko wykorzystaniu takich usług była stosunkowo niewielka ilość miejsca oferowana przez wirtualne dyski – kilkaset megabajtów lub maksymalnie jeden gigabajt. Dzisiaj jednak sytuacja jest już inna. Wystarczy spojrzeć na przykłady: Dropbox udostępnia za darmo 2 GB przestrzeni, należący do Microsoftu SkyDrive 7 GB, a Dysk Google – 15 GB. Jak więc łatwo obliczyć, zupełnie za darmo możemy skorzystać z dodatkowych 24 GB przeznaczonych na nasze pliki. W porównaniu z dostępnymi dzisiaj dyskami twardymi, które mają po 250 czy 500 GB wydaje się, że to niewiele. Ale usługi w chmurze mają jedną potężną nad nimi przewagę – pozwalają nam na dostęp do danych praktycznie z każdego miejsca na świecie i przy użyciu każdego dostępnego komputera.
Niektórzy na hasło „dane w chmurze” reagują nieco nerwowo – obawiają się tego, że ich prywatne pliki znajdują się

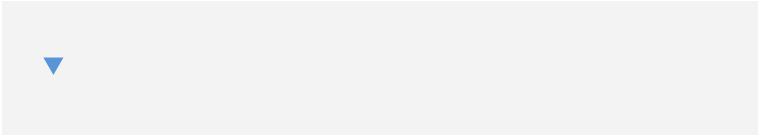
praktycznie w obcych rękach, na serwerze ustawionym gdzieś daleko na świecie. Trzeba jednak pamiętać, że dostawcy usług chmurowych bardzo dbają o bezpieczeństwo tych danych. Zależy im bowiem na rozwoju swojego biznesu i ostatnia rzecz, jakiej by chcieli, to potwierdzone opinie o tym, że pliki zgromadzone w chmurze zostały wykradzione. Trzeba jednak przyznać, że w przeszłości zdarzały się przypadki wycieku danych, na przykład z usługi Dropbox. Dlatego po tym incydencie firma wprowadziła bardziej skomplikowany i trudniejszy do złamania system dwuetapowej autoryzacji dostępu – będzie o nim mowa szerzej na kolejnych stronach.

Aby czuć się zupełnie bezpiecznie przy korzystaniu z wirtualnych dysków, powinniśmy stosować kilka zasad. Jedna z nich to nieprzechowywanie w chmurze bardzo wrażliwych danych – na przykład plików tekstowych z danymi logowania do banku czy innych ważnych dla nas serwisów. Druga polega na tym, że inne ważne pliki powinny być tylko skopiowane do chmury, a nie przenoszone tam jako jedyny istniejący egzemplarz. Po trzecie zaś, należy uważnie korzystać z opcji udostępniania danych przechowywanych w chmurze – chodzi o to, byśmy nie przekazywali dostępu do nich przypadkowym osobom.

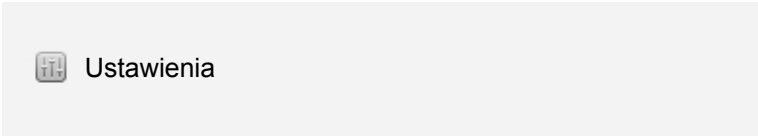
Oczywiście, tak samo jak w przypadku naszej poczty e-mail czy internetowego konta bankowego najbardziej podstawowe zabezpieczenie wirtualnego dysku to wybranie do niego odpowiednio skomplikowanego hasła dostępu (patrz rozdział II). Druga ważna czynność to ustalenie wspomnianego wcześniej dwuetapowego logowania do konta oferowanego przez niektórych operatorów usług chmurowych. Zobaczmy, jak to zrobić na przykładzie dysku Dropbox.

Dropbox – dwustopniowa autoryzacja

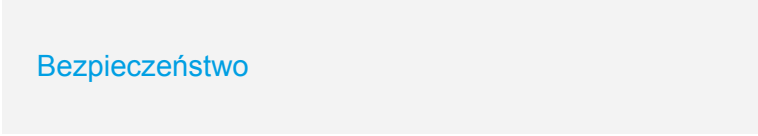
Po założeniu konta w serwisie Dropbox na stronie www.dropbox.com i zalogowaniu się do niego na głównej stronie w prawym górnym rogu klikamy na niewielki trójkącik przy nazwie konta:



Następnie wybieramy opcję:



Pojawi się nowe okno, w którym klikamy na zakładkę:



Teraz w sekcji o nazwie:

Dwustopniowe uwierzytelnianie

klikamy na przycisk Włącz.
Po wykonaniu tych czynności pojawi się kolejne okno, w którym podajemy nasze hasło do usługi Dropbox i potwierdzamy je przyciskiem:

Dalej

Teraz wybieramy sposób, w jaki będą wysyłane do nas jednorazowe kody autoryzacyjne (na przykład SMS-em):

Użyj wiadomości SMS
Kody zabezpieczajce będą wysyłane na telefon komórkowy.

Klikamy znowu na:

Dalej

Następnie wybieramy kraj, w którym działa nasz telefon komórkowy, i wpisujemy jego numer.
Po chwili otrzymamy SMS-em kod weryfikujący, który wpisujemy w kolejne okno i klikamy na:

Dalej

W następnym kroku możemy opcjonalnie podać drugi numer telefonu – okaże się przydatny w sytuacji utraty lub kradzieży naszej komórki z głównym numerem. Możemy jednak pominąć ten krok i przejść dalej.
Teraz pojawi się ważny komunikat ze specjalnym kodem, którego będziemy musieli użyć w przypadku wyłączenia dwustopniowego uwierzytelniania.
Najlepiej przepisać kod i schować w bezpiecznym miejscu:

W ostateczności możesz również użyć kodu awaryjnej kopii zapasowej w celu wyłączenia dwustopniowego uwierzytelniania i uzyskania dostepu do swojego konta.

qxud l4p8 cjx6 wsw1

Zapisz go na kartce papieru i przechowuj w bezpiecznym miejscu.

Na koniec włączamy dwustopniową autoryzację przyciskiem:

Włącz dwustopniowe uwierzytelnienie

Teraz, aby sprawdzić nowy sposób autoryzacji dostępu, wylogowujemy się z Dropboxa i ponownie logujemy w serwisie. Podczas tej operacji pojawi się dodatkowe okno. Wpisujemy w nie kod otrzymany SMS-em. Uzyskamy dostęp do naszych danych zgromadzonych na dysku Dropbox.

ROZDZIAŁ XII

Zintegrowany Informator Pacjenta: Zdrowo i bezpiecznie

ZIP

O tym, jak zamienić internet w przychodnię, na jakie pytania nie odpowiadać i o tym, że ZIP oznacza nie tylko metodę kompresji plików.

Gdzie się leczyliśmy, jakie zabiegi przeszliśmy, jakie leki wypisał nam w przeszłości lekarz – to tylko część danych składających się na historię każdego z pacjentów w Polsce. Do tej pory, aby mieć szybki dostęp do podobnych informacji, najlepiej było zbierać mozolnie do teczki wszystkie dokumenty dotyczące naszych chorób i ich leczenia. Teraz jednak może być wygodniej, dzięki specjalnej platformie elektronicznej uruchomionej przez NFZ.

Mowa o Zintegrowanym Informatorze Pacjenta (ZIP), który wystartował z początkiem lipca 2013 roku. Dzięki tej platformie pacjenci mogą za pośrednictwem internetu uzyskać dostęp do szeregu informacji. Dowiedzą się między innymi, kiedy i w których placówkach byli leczeni, jakie zabiegi na nich wykonano, jakie recepty wypisał im lekarz. Oprócz tego w ZIP Kowalski dowie się też, ile pieniędzy do tej pory wydano na jego opiekę medyczną, gdzie może się leczyć za darmo, jak wygląda kwestia jego ubezpieczenia zdrowotnego.

W nowym systemie tkwi jednak jeden, nieco uciążliwy haczyk. Chodzi o to, że wniosek o dostęp do ZIP możemy co prawda złożyć elektronicznie (na stronie https://zip.nfz.gov.pl), jednak uzyskanie danych dostępowych (loginu i hasła) będzie od nas wymagało osobistej wizyty w odpowiednim oddziale NFZ. To jednak, jak tłumaczą urzędnicy, dla naszego bezpieczeństwa – internetowe konto pa-

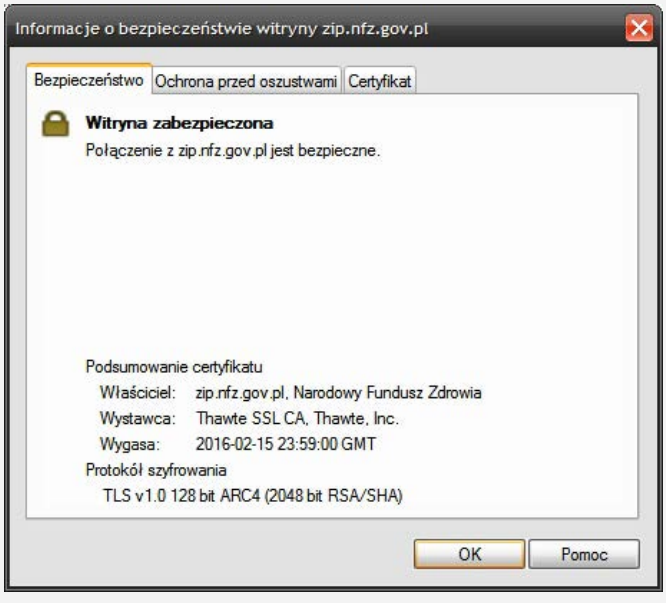
cjenta zawiera wiele wrażliwych danych, takich jak historia przebytych chorób i leczenia, a także wydatki poniesione na pacjenta. Dlatego też konieczna jest osobista weryfikacja właściciela każdego konta w ZIP.

Kiedy już uzyskamy dostęp do naszego profilu w ZIP, niewiele będziemy mogli zrobić, by zmienić w nim ustawienia dotyczące bezpieczeństwa. Wciąż będzie obowiązywała zasada, że konto powinno być chronione odpowiednio skomplikowanym hasłem. Po wejściu na stronę ZIP sprawdzamy, czy w przeglądarce jej adres rozpoczyna się od https, i klikamy na kłódkę w celu uzyskania informacji o zabezpieczeniach witryny.

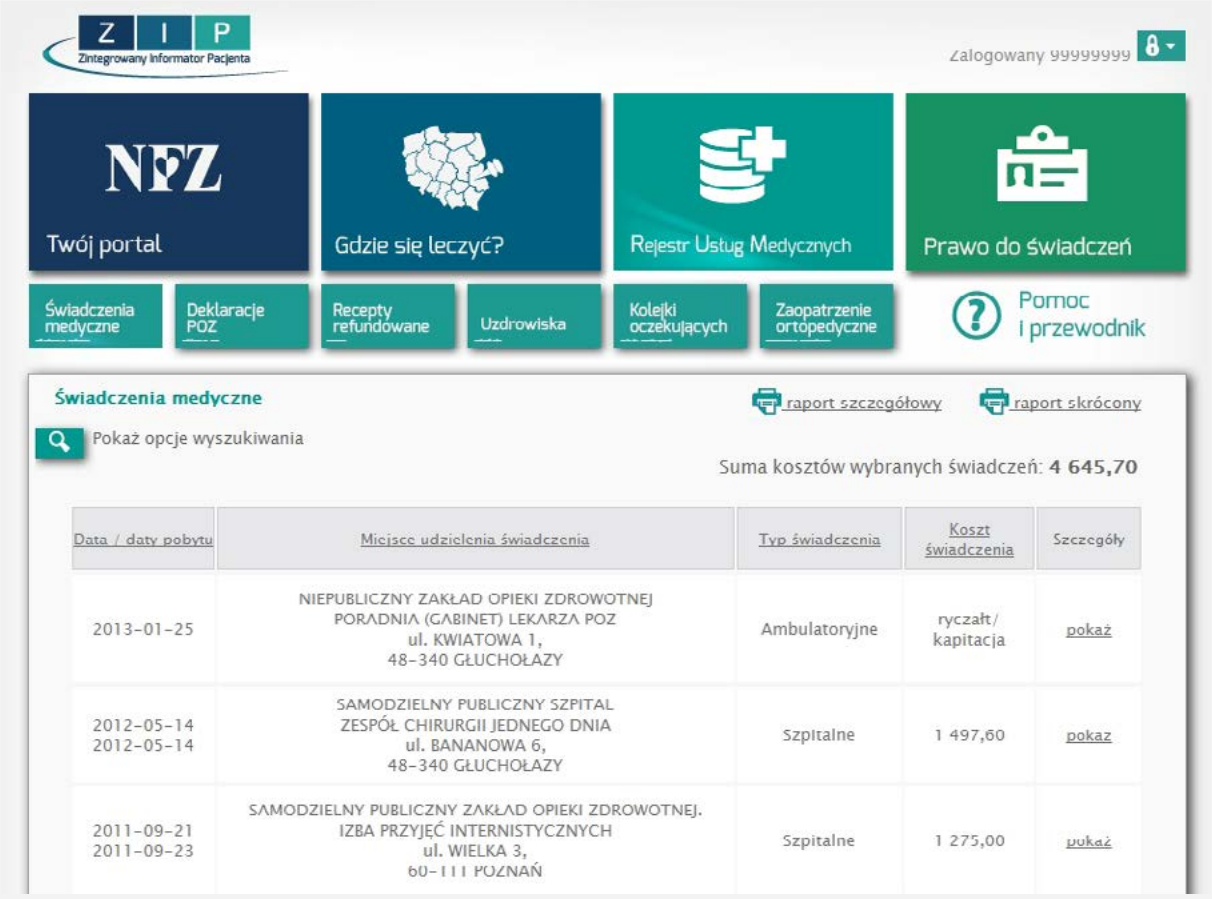
W wypadku ZIP trzeba pamiętać, że urzędnik w oddziale NFZ może poprosić nas jedynie o podanie loginu do systemu. Nie ma natomiast prawa żądać od nas hasła dostępu do naszego konta. Zignorować powinniśmy także wszelkie prośby o udostępnianie loginu i hasła przekazywane nam przez telefon lub za pośrednictwem poczty elektronicznej. Twórcy systemu ZIP zalecają, by nasze hasło było zmieniane co 30 dni. Nie jest to zwykła formalność lub nadgorliwość urzędników. Musimy pamiętać, że baza danych dotycząca stanu naszego zdrowia to prawdziwy skarb na czarnym rynku internetowym, a podobne informacje kosztują tam spore pieniądze. Dlatego przestępcy co pewien czas próbują dokonywać ataków na takie systemy i okresowa zmiana hasła powinna skutecznie utrudnić im zadanie.

Dla własnego bezpieczeństwa powinniśmy też zapisywać daty nieudanych logowań na nasze konto. Jeżeli sami nie podejmowaliśmy takich prób, to przekażmy tę informację administratorom systemu. Nieudane logowania mogą świadczyć bowiem o próbach ataku na ZIP.

Nie zapominajmy także o tym, by po zakończeniu odwiedzin na naszym koncie w ZIP za każdym razem przeprowadzić operację wylogowania. Samo zamknięcie okna przeglądarki pozostawia bowiem w sieci otwarty dostęp do konta, który może zostać wykorzystany przez przestępców.



ROZDZIAŁ XII
Zintegrowany Informator Pacjenta: Zdrowo i bezpiecznie



Zintegrowany Informator Pacjenta to wygodne narzędzie w naszych kontaktach ze służbą zdrowia. Jednak podczas korzystania z niego nie możemy zapomnieć o najważniejszych zasadach bezpieczeństwa


PŁACISZ
coraz więcej za leki?
NIE WYKUPUJESZ
leków z recepty?
NIE PRZEPŁACAJ!
Znajdź TAŃSZE
zamienniki na
www.leku.pl

Na koniec: Bądź przezorny na infostradzie

Niestety nawet w najbardziej rozbudowanej publikacji nie da się przestrzec użytkowników internetu przed wszystkimi zagrożeniami, które mogą czaić się w globalnej sieci. Tym bardziej że mamy do czynienia, co prawda z wirtualnym, ale żywym ekosystemem, w którym jedne gatunki giną, pojawiają się nowe, a niektóre po prostu ewoluują w kierunku, który dzisiaj trudno przewidzieć. Możemy oczywiście nie zgadzać się z taką koncepcją. Ale wystarczy zdać sobie sprawę z tego, że już w najbliższej przyszłości internet wejdzie na serio w erę rozszerzonej rzeczywistości, postrzeganej za pomocą okularów typu Google Glass, by zrozumieć, że globalna sieć jeszcze za naszego życia może stać się światem równie ważnym jak ten, który otacza nas od momentu narodzin. I obecność w tej rzeczywistości nie będzie już kwestią naszego wyboru, ale koniecznością, bez której nie da się funkcjonować.

Jak więc zapewnić sobie bezpieczeństwo w tym barwnym i stale zmieniającym się środowisku? Trzeba być tak elastycznym jak ono samo. Kilkakrotnie na stronach tego e-booka podkreślałem, że najlepszym sposobem jest stosowanie reguł zdrowego rozsądku. A teraz dodam jeszcze, że wbrew pozorom zasada ograniczonego zaufania obowiązuje nie tylko w przepisach o ruchu drogowym. Oprócz własnego rozumu w unikaniu internetowych pułapek może nam pomóc garść żelaznych zasad, których powinniśmy się trzymać. Oto one:

NA KONIEC:
Bądź przezorny na infostradzie

Pamiętaj, że hasło **adam123** to zdecydowanie zły wybór. O wiele lepszy to: **Qjk44_Lmn[„.**

W internecie jak w życiu: rzadko dostajesz coś za darmo. Nie odpowiadaj na maile z podejrzanymi ofertami, nie klikaj na linki w wiadomościach z nieznanego źródła.

Raz na tydzień dokonaj pełnego skanowania komputera zainstalowanym oprogramowaniem antywirusowym lub ustaw w aplikacji harmonogram tak, by skanowanie odbywało się automatycznie.

Ogranicz dostępność twojego profilu w portalach społecznościowych. Profil publiczny to dobre wyjście tylko dla odważnych i lubiących ryzyko.

Pamiętaj, że każda strona wymagająca twojego logowania powinna rozpoczynać się na pasku adresu w przeglądarce od skrótu **https**, a nie http. Sprawdzaj potwierdzenia autentyczności witryn dostępne w przeglądarkach.

NA KONIEC:
Bądź przezorny na infostradzie

Żaden bank w Polsce nie wysyła do swoich klientów maili z żądaniem podania loginu i hasła do konta. Nie wysyła też wiadomości kierujących bezpośrednio do stron logowania. Maile podobnej treści zasługują jedynie na potraktowanie przyciskiem Delete.

Przed rejestracją w jakimkolwiek serwisie internetowym **uważnie czytaj regulamin.** Wystarczająco wielu ludzi daje zarobić oszustom w sieci. Nie powiększaj tej drużyny.

Towar zakupiony w internecie możesz zwrócić sprzedawcy w ciągu 10 dni bez podawania przyczyny. Uważaj! Rozpakowane płyty z muzyką i programami nie podlegają zwrotowi!

Ściąganie z sieci filmów i muzyki jest nielegalne? To bzdura – nie daj się zastraszyć. Masz prawo ściągać wszystkie opublikowane już utwory w ramach dozwolonego użytku osobistego. **Uwaga!** Nie masz prawa udostępniać dalej ściągniętych utworów w internecie ani ściągać i używać płatnych wersji programów komputerowych.

Pamiętaj: **Najważniejszym programem do ochrony komputera w internecie jest twój rozsądek!** Bądź czujny! Wróg nie śpi! :-)

O autorze

Wojciech Wrzos jest dziennikarzem. Od 15 lat zajmuje się tematyką internetu i nowych technologii. Obecnie w serwisie www.komputerswiat.pl publikuje teksty komentujące bieżące wydarzenia w branży informatycznej i artykuły na temat wykorzystania nowoczesnych rozwiązań technologicznych w codziennym życiu.