Jak zadbać o bezpieczeństwo IT pracując w domu?

Leszek Rycharski, zdalniej.pl

Wydanie: 1
Data: 20.06.2011
ISBN: Darmowy

Zarówno autor jak i wydawnictwo zdalniej.pl dołożyli wszelkich starań, by poradnik zawierał treści rzetelne i wartościowe. Jednak nie biorą żadnej odpowiedzialności za interpretację oraz wykorzystanie publikacji przez Czytelnika.

Ebook jest udostępniany na zasadach Creative Commons CC-BY-NC-ND.

W szczególności publikacja może być kopiowana, dystrybuowana, wyświetlana i użytkowana:

- pod warunkiem umieszczenia informacji o autorze jakim jest „Leszek Rycharski, zdalniej.pl"
- tylko w celach niekomercyjnych
- ale bez możliwości wprowadzania zmian i dystrybucji utworów zależnych.

Spis treści

Wstęp

Ten poradnik przeznaczony jest dla mniej zaawansowanych technicznie użytkowników, którzy chcieliby się dowiedzieć, **jak uchronić się przed wirusami komputerowymi oraz utratą cennych danych**. Znajdziesz w nim szereg wskazówek i porad, które możesz wykonać samodzielnie. Pracując w domu rzadko możemy liczyć na wsparcie ze strony działu IT firmym więc odpowiedzialność za bezpieczeństwo informatyczne spada na nasze barki.

Największe zagrożenia IT podczas pracy w domu

Pracując w siedzibie większej firmy masz zazwyczaj do dyspozycji zatrudnionych tam informatyków, którzy dbają o bezpieczeństwo IT całej firmy. Ponadto Ty sam się bardziej pilnujesz, bo ktoś akurat może zajrzeć Ci przez ramię i donieść, że w godzinach pracy korzystasz z serwisów społecznościowych. Kiedy pracujesz w domu i korzystasz z jednego komputera do pracy i do rozrywki drastycznie wzrasta ryzyko, że **surfując po Sieci złapiesz złośliwe oprogramowanie** albo omyłkowo ktoś z Twoich domowników lub nawet **Ty skasujesz ważne dane**, by zrobić miejsce na film lub grę. **Tym bardziej musisz zadbać o bezpieczeństwo IT samodzielnie**.

Musisz jednak wiedzieć, że **NIE ISTNIEJE 100% pewny sposób, by uchronić się przed zagrożeniami IT**. Jeśli przestępca będzie chciał wykraść Twoje dane i hasła lub zainfekować komputer, to zawsze znajdzie jakiś sposób. Jedyne co możesz zrobić, to zminimalizować ryzyko ataku, którego nie jesteś bezpośrednim celem. Pamiętaj, że przestępca może uzyskać Twoje dane nie tylko z Twojego komputera, lecz również z baz danych firm, którym kiedyś podawałeś swoje dane (w 2011 głośna była sprawa wykradzenia danych z kont 75 milionów osób zarejestrowanych z Sony Playstation Network. Jeśli Sony nie mogło się ochronić przed bezpośrednim atakiem, to pomyśl jakie Ty miałbyś szanse przed atakiem skierowanym bezpośrednio w Ciebie?). Nie ma co jednak wpadać w paranoję. Jeśli zdarza Ci się jeździć samochodem (nieważne czy jako kierowca czy pasażer), to również masz świadomość, że w każdej chwili może zdarzyć się śmiertelny wypadek, przed którym się nie uchronisz. Jeśli uderzy w Ciebie impetem ciężarówką pijany pirat drogowy, to wszystkie Twoje zabezpieczenia nie mają już znaczenia. Jednak zapinanie pasów, nieprzekraczanie dozwolonej prędkości, zasada ograniczonego zaufania, niewsiadanie za kółkiem pod wpływem alkoholu, na pewno znacznie zwiększają Twoje

szanse, że nie przydarzy Ci się nic nieprzyjemnego na drodze. Niestety pewności nigdy nie masz.

Co zyskasz, dzięki temu poradnikowi?

Przede wszystkim wprowadzisz działania prewencyjne, dzięki którym:

- zaoszczędzisz pieniądze na kosztowne odzyskiwanie danych lub usuwanie wirusów z Twojego komputera.
- zaoszczędzisz czas, bo kopie zapasowe uchronią Cię przed robieniem drugi raz tego samego.
- zwiększysz komfort swojej pracy.

Kopie zapasowe

Czy wiesz, że PCworld donosi, że ⅓ firm nie tworzy backupu cennych danych, a **połowa przedsiębiorstw, które utraciły ważne informacje bankrutuje w ciągu dwóch następnych lat**?

Czemu tracimy dane i jak się przed tym uchronić?

Najczęstsze powody utraty danych to:

1. Usterka sprzętu
2. Złośliwe oprogramowanie
3. Człowiek
4. Siła wyższa
5. Inne

Jak zminimalizować ryzyko utraty danych?
Ad. 1 Usterka sprzętu. Zabrzmi to jak truizm (którym w zasadzie jest), ale używaj komputera zgodnie z jego przeznaczeniem i po prostu o niego dbaj (głównie o czystość). Nie jest najlepszym pomyłem branie laptopa, na którym pracujesz, na imprezę, by puszczać z niego muzykę. Nawet jeśli nikt nic na niego nie wyleje (patrz "człowiek" dalej), to okruszki i kurz mogą się dostać się do środka i przyśpieszyć jego niszczenie. Każdy sprzęt się jednak amortyzuje, więc KWESTIĄ CZASU jest, kiedy się popsuje. Pamiętaj, że gwarancja na sprzęt nie uwzględnia odzyskiwania danych.

Ad. 2 Złośliwe oprogramowanie. Kieruję do osobnego podrozdziału nt. ochrony przed złośliwym oprogramowaniem.

Ad. 3 Człowiek. To zdecydowanie najsłabsze ogniwo, które odpowiada za największą liczbę przypadków utraty danych. Człowiek regularnie popełnia błędy i to jest nasza ludzka natura. Zacznę od najbardziej prozaicznych, które mogą doprowadzić do fizycznych zniszczeń, a skończę na tych, które choć niezauważalne mogą przynieść straty w postaci wyczyszczonego konta bankowego:
Jedzenie i picie przy komputerze. Może się Tobie wydawać, że zaoszczędzisz więcej czasu,

kiedy jesz i pijesz przy komputerze, ale co jeśli coś wylejesz na komputer? Ja osobiście wylałem kiedyś piwo na laptopa służbowego. Na szczęście komputer i dane udało się odratować, ale straciłem czas i pieniądze (laptop poszedł do naprawy) i o mało nie dostałem zawału serca, bo byłem w trakcie pewnego projektu, który zajął mi do momentu "awarii" 80 godzin. To przypadek ekstremalny, ale nawet okruszki sypiące się na klawiaturę laptopa prowadzą do jego szybszej amortyzacji.
Formatowanie dysku. Jeśli system operacyjny spowolnił wyraźnie swoje działanie, może to być właściwy czas na format. Pamiętaj jednak, by najpierw zrobić kopię zapasową najważniejszych danych, bo format polega właśnie na tym, że usuwa wcześniej zapisane dane. Znam przypadki pracowników, którzy zlecili działowi IT format dysku, a potem się dziwili (ba! byli oburzeni), że nie mogą znaleźć swoich wcześniejszych projektów.
Za dużo osób ma dostęp do danych. Do ważnych informacji dostęp powinny mieć wyłącznie osoby upoważnione. Jeśli umożliwiasz domownikom korzystanie z Twojego komputera służbowego (bo np. macie tylko jeden komputer w domu), to utwórz dla nich dodatkowy profil użytkownika np. dom i np. zablokuj im dostęp do wybranych dysków. Daj im hasło tylko do tego profilu. To ograniczy przypadki, kiedy ktoś usunął efekty Twojej pracy, bo nie było miejsca na film...
Twoje hasło to TWOJE hasło. Czasem zdarza się nam podawać z różnych powodów nasze hasła znajomym, czy rodzinie. Jeśli podasz swojej partnerce/partnerowi hasło do Twojego konta na DropBox to nie zdziw się, że po rozstaniu straciłeś pewne dane, bo zostały nadpisane przez ciąg bezsensownych znaków.
Nie surfuj po podejrzanych stronach WWW. Złośliwe oprogramowanie tylko na to czeka.
Nie ściągaj podejrzanych plików. Niektóre torrenty celowo zawierają złośliwe oprogramowanie. Pewien raper z premedytacją umieścił na torrentach swoją "najnowszą płytę", lecz zamiast niej de facto ściągało się nieprzyjemnego wirusa.
Nie instaluj podejrzanych programów. Idealnym przykładem jest program do kontroli innych użytkowników, który działa na zasadzie zczytywania wpisywanych znaków z klawiatury. Twórcy "reklamują" ten produkt mówiąc, że "będziesz wiedzieć z kim czatuje Twoja niewierna żona". W praktyce program ten jest wykorzystywany do wykradania haseł.

Ad.4. Siła wyższa. Np. kataklizm, który fizycznie zniszczy wszystkie urządzenia, na których przechowywujesz ważne dane. Jedyne co możesz zrobić, oprócz przechowywania fizycznych nośników w domu, to zapisywanie danych także w Internecie (czy wrzucając przez FTP, czy za pomocą specjalnych webaplikacji). Pamiętaj jednak, by serwery

znajdowały się w innej fizycznej lokalizacji - lokalny patriotyzm w tym przypadku może Ci zaszkodzić. Jeśli prawdopodobieństwo, że żywioł zniszczy urządzenia z danym w Twoim domu wynosi 0,0001 %, a prawdopodobieństwo, że żywioł zniszczy serwery z Twoimi danymi wynosi 0,000001%, to prawdopobieństwo, że utracisz swoje dane w obu źródłach jest równe 0,000000001% .

Programy do kopii zapasowych

Aplikacje do tworzenia backupów możemy podzielić na dwie kategorie:

1. te, które zapisują dane na internetowym dysku oraz
2. te, które zapisują dane na komputerze lub nośniku zewnętrznym.

Ad.1 Programy działające na zasadzie zapisu danych na internetowym dysku synchronizują wskazany folder na Twoim komputerze, a następnie automatycznie i w czasie rzeczywistym (lub bardzo często) tworzą kopię zapasową każdego pliku znajdującego się w danym folderze.

Zaletą jest uniezależnienie od fizycznych nośników w Twoim domu (nawet gdyby Twój komputer się spalił to możesz odzyskać wszystkie dane), automatyzacja (nie musisz o niczym pamiętać) oraz zapis w czasie rzeczywistym.

Wadą jest brak wcześniejszych wersji, która wynika z zapisu w czasie rzeczywistym. Jeśli omyłkowo usuniemy plik, to również w kopii zapasowej plik zniknie. Oczywiście możemy plik jeszcze odzyskać z kosza.

Oto lista przykładowych programów tego typu:

- DropBox - wersja bezpłatna do 2GB
- SpiderOak - wersja bezpłatna do 2GB
- Wuala - wersja bezpłatna do 1GB
- Auto-Backup - polska aplikacja, wersja bezpłatna do 1GB

Ad. 2 Programy, które zapisują dane na komputerze lub nośniku zewnętrznym tworzą

kopię zapasową w wybranej przez Ciebie ścieżce dla wskazanych folderów i plików.

Kopie zapasowe są tworzone automatycznie i mogą być przygotowywane również bardzo często, a ich dodatkową zaletą jest fakt, że zapisują także kopie historyczne z danego okresu (jest on ograniczony z powodu redundancji danych). Dzięki temu, jeśli dziś zauważysz, że dany plik został wczoraj usunięty, a nie ma go w koszu, to możesz go odtworzyć z kopii historycznej.

Największy sens tworzenia takiej kopii zapasowej występuje wtedy, kiedy masz dysk zewnętrzny, wówczas w razie awarii komputera dane postaną na tym nośniku.
Tworzenie kopii zapasowej na tym samym komputerze ma sens jedynie, jeśli zależy nam na kopiach historycznych, w przeciwnym wypadku wyłącznie stracimy miejsce na dysku kilkakrotnie zapisując te same dane.

Oto lista przykładowych programów tego typu:
Back2zip Legacy - chodzi o starszą wersję programu (obecna wersja 2.0 tworzy backup w chmurze i opiera się na płatnym Amazon S3). Jest darmowa, a dane są zapisywane w archiwum .zip w celu ograniczenia miejsca.
BackUp Maker - tworzy kopię zapasową do wskazanej ścieżki lub nawet na zewnętrzny serwer po FTP. Kopia jest zipowana. Narzędzie jest darmowe.
AceBackup - kolejny darmowy program o podobnych funkcjach.

Dłuższą listę programów do tworzenia kopii zapasowych znajdziecie na:
http://www.blitz-art.com/blog/category/kopie-zapasowe-backup-danych/

System tworzenia kopii zapasowych

Często stoisz przed pewnym ograniczenia, jeśli chodzi o backup np. wielkość plików. Jeśli jesteś pisarzem, to możesz sobie pozwolić na backupowanie wszystkich danych, ponieważ teksty ważą niewiele. Kiedy jednak jesteś architektem, to Twoje projekty mogą tyle ważyć, że system tworzenia kopii zapasowych będzie składał się z kilku poziomów.

Twój własny system tworzenia kopii zapasowych, powinien spełniać następujące wytyczne:

- **Twórz backup jedynie dla najważniejszych danych**. To co nie jest ważne nie powinno być archiwizowane, by nie marnować miejsca. Nie twórz więc kopii zapasowych np. dla filmów, które obejrzałeś albo gier, w które od dawna nie grasz.
- **Zautomatyzuj proces backupu**. Backupowanie ręczne dla każdego pliku byłoby zbyt czasochłonne oraz zawodne, ponieważ łatwo o tym zapomnieć, a później trudno sobie przypomnieć, które pliki się przeoczyło. Z tego powodu warto korzystać z programów do kopii zapasowych, które backup wykonują automatycznie.
- **Sprawdź czy backup działa**. Warto dodatkowo ręcznie sprawdzać, czy kopia zapasową można odczytać oraz czy wszystko się zapisuje jak należy.
- **To Twój system**. Dobierz programy i nośniki, które najlepiej będą spełniać Twoje wymagania.

Przykładowe systemy tworzenia kopii zapasowych

Przykład #1: Dziennikarz online od newsów

Opis sytuacji: Dużo podróżuje. Teksty mają krótką datę ważności.

Rozwiązanie: Dzięki temu, że teksty publikowane są na stronie portalu, dziennikarz nie musi ich archiwizować na własną rękę, bo zawsze można do nich wrócić online. Krótki data ważności newsów zmniejsza potrzebę tworzenia backupu danych. Najlepszym rozwiązaniem byłoby więc korzystanie z Google Docs (dokumenty Google dostępne wraz z Gmail), które są z mniejszym prawdopodobieństwem ulegną awarii niż komputer dziennikarz, a dodatkowo umożliwiają mu pracę na różnych komputerach, dzięki cloud computing (stacjonarny w domu, netbook w pociągu, laptop na konferencjach). Raz na tydzień może dodatkowo zrzucić dane z Google Docs na dysk twardy ręcznie za pomocą darmowego GDocBackup lub regularnie i automatycznie, dzięki np. Google Apps Backup Utility za 30 dolarów rocznie.

Koszt: od 0 do 90 zł rocznie.

Przykład #2: Pisarz

Opis sytuacji: Sławny pisarz. Dużo plików tekstowych. Obawia się korzystania z zewnętrznych aplikacji, by nikt nie przeczytał tego, co do tej pory napisał.

Rozwiązanie: W tym wypadku odpadają zewnętrzne systemy do backupu na zasadzie internetowego dysku. Czy ktoś z nich wykradnie zarys książki? Wątpie, ale po co się dodatkowo stresować. Jednak brak automatycznego backupu online jest zbyt ryzykowne, tym bardziej, że proces pisania książki może trwać latami. Proponuję skorzystać z AceBackup i oprócz zapisywania wszystkiego na dysku zewnętrznym (starczy nam w pełni 320 GB za 120 zł) wysyłać dane na zewnętrzny serwer dedykowany (od 79 zł miesięcznie).

Koszt: 120 zł jednorazowo + 79 zł miesięcznie.

Przykład #3: Architekt / Projektant CAD

Opis sytuacji: Dużo plików, które dużo ważą.

Rozwiązanie: Back2zip Legacy tworzący backup 2x dziennie do dysku zewnętrznego o pojemności 2TB (można kupić już za 270 zł). Dodatkowo (na chociażby najważniejsze projekty) pojemność 250GB w Wuala za 350 dolarów rocznie będzie przydatna (każde kolejne 100GB za kolejne 150 dolarów). Na pewno nie uda się nam

Koszt: 270 zł jednorazowo + 1050 zł rocznie.

A co jak już utraciliśmy dane?

Pozostaje nam w takiej sytuacji tylko zwrócić się do profesjonalistów świadczących profesjonalną usługę odzyskiwania danych, która by Cię kosztowała od kilkuset do kilku tysięcy złotych, przy czym nie masz pewności, że wszystkie dane odzyskasz.

Dane osobowe i hasła

Już w podrozdziale o tworzeniu kopii zapasowych mogłeś zapoznać się z dwiema cennymi wskazówkami:

- Nie dziel się z nikim Twoimi hasłami
- Nie instaluj oprogramowania do kontroli innych użytkowników, które działa na zasadzie sczytywania klawiatury.

W tym rozdziale rozwinę temat ochrony danych osobowych.

Źródła zagrożeń

Rejestracja w podejrzanych serwisach. Udostępniając swój pierwszy adres e-mail (służbowy, czy też prywatny) w szemranych serwisach lub w komentarzach musisz się liczyć z otrzymywaniem SPAMu. Na szczęście obecne filtry antyspamowe działają dość dobrze i ten problem może być prawie niezauważalny. Pamiętaj jednak, by najlepiej od razu wyrzucać SPAM, gdyż może on rozprzestrzeniać złośliwe oprogramowanie.
Jedno hasło. Wiadomo, że jest to wygodne, bo wystarczy pamiętać tylko jedno hasło, ale dla złodzieja jest to również komfortowa sytuacja, bo za jednym zamachem może ukraść wszystko.
Dzielenie się hasłem. Nawet jeśli ufasz osobom, z którymi dzielisz się hasłem, to mniej na uwadze, że nie wiesz jak one Twoim hasłem zarządzają. Być może zapisały to sobie w pliku “hasła” w notatniku na pulpicie?
Sieci bezprzewodowe niewiadomego pochodzenia lub publiczne / Kafejki internetowe. Nie jest najlepszym pomysłem logowanie się do swojej pierwszej poczty, serwisów społecznościowych, a w szczególności banków i stron związanych z pracą (np. Google Apps). Nigdy nie wiesz, kto odpowiada za bezpieczeństwo takiej sieci lub w kafejce.
Strony www bez SSL. SSL to certyfikat bezpieczeństwa przydzielany danej witrynie przez niezależnego wystawcę. Sprawia on dwie rzeczy: zamiast http w pasku adresu widzimy https oraz jesteśmy chronieni przed tzw. atakiem man in the middle, które polega na wykradaniu pakietów danych (w tym haseł) przez pośredni serwer. NIGDY nie podawaj numeru Twojej karty płatniczej na stronach bez SSL, nawet jeśli z pozoru ten przykładowy sklep internetowy wygląda wiarygodnie.

Podejrzane programy do kontroli innych użytkowników. Pisałem o tym wcześniej. Instalacja oprogramowania, które "monitoruje" użytkowników danego komputera, a de facto zczytuje z klawiatury między numery kont oraz hasła.
Człowiek. Sami jesteśmy największym źródłem wycieku danych osobowych na nasz temat. Pomyśl jak często zamieszczasz śmieszne zdjęcia z Tobą w roli głównej w serwisach społecznościowych. Czy masz świadomość, że takie zdjęcie będzie mogło być wykorzystane przeciwko Tobie, a Ty nic z tym nie będziesz mógł zrobić? Przypominam spot ze słynnej kampanii społeczecznej "Think before you post".

Jak się przed tym zabezpieczyć?

Unikalne i skomplikowane hasła. W każdym serwisie powinieneś posiadać osobne, unikalne, trudne (czyli małe i duże litery, znaki i liczby) hasło. W praktyce ciężko jest spamiętać wszystkie takie hasła. Masz kilka możliwości:

- Korzystaj z managera haseł. Jest to specjalny program, który gromadzi wszystkie Twoje hasła w zakodowanej formie. Pytanie brzmi tylko jak bardzo możesz ufać takiemu programowi.
- System tworzenia haseł. Możesz posiadać hasło główne i dodawać do niego ciąg znaków wg Twojego własnego algorytmu. Dzięki temu wszystkie hasła są unikalne, a Ty nie musisz ich pamiętać. Np. Twoje hasło główne to "zeN0n" następnie dodajesz rok rejestracji, a następnie odwróconą nazwę programu lub serwisu, z którego korzystasz. Jeśli w 2010 rejestrowałeś się w nk.pl, wówczas otrzymujesz hasło "zeN0n2010kn", a Twoje hasło do mBank wygląda analogicznie "zeN0n2009knabm". Pomocna może okazać się Fabryka Haseł.
- Przypomnienie hasła. Możesz ograniczyć pamiętanie haseł do kilku najważniejszych, a w przypadku reszty serwisów za każdym razem przypominać sobie hasło, a następnie je zmieniać na jakieś karkołomne.
- Priorytety. Koncentruj się na unikalnych hasłach jedynie w usługach i na witrynach, które są ważne tj. posiadają o Tobie więcej informacji niż tylko e-mail i/lub przechwycenie Twoich kont w tych serwisach mogłoby być dla Ciebie szkodliwe. W reszcie serwisów stosuj jedno hasło i podaj Twój śmieciowy mail.

Zmieniaj hasła. Kiedy byłeś zmuszony korzystać z Internetu, co do którego nie masz szczególnego zaufania (uczelnia, daleki znajomy, kafejka internetowa) zmieniaj hasło.

Śmieciowy mail. Jest to specjalny adres e-mail do podawania w razie rejestracji na witrynach, które tego wymagają, a niekoniecznie im ufasz. Pamiętaj jednak, by do śmieciowego maila mieć unikalne hasło, które pamiętasz.

Nie podawaj danych, jeśli nie masz pewności co się z nimi stanie. Nie kupuj w sklepach bez SSL.

Korzystaj z Internetu tylko pochodzącego z zaufanego źródła. W przeciwnym wypadku ogranicz swoją aktywność do przeglądania treści stron.

Uważaj, co i gdzie zamieszczasz. Dane osobowe to nie tylko tekst, lecz również zdjęcia.

Złośliwe oprogramowanie

Złośliwe oprogramowanie to nie tylko wirusy, lecz również:

- robaki
- trojany
- programy szpiegujące
- dialery
- i niestety wiele innych (przeczytasz o nich na http://pl.wikipedia.org/wiki/Z%C5%82o%C5%9Bliwe_oprogramowanie)

W tym rozdziale skoncentruję się na wskazówkach, jak się przed nimi uchronić:
Zacznij od wyboru programu antywirusowego. Powołam się na testy darmowych programów antywirusowych przeprowadzonych pod koniec 2010 przez redakcję dobreprogramy.pl. Oto wyniki:

1. avast! (wersja FREE)
2. Comodo
3. AVG (wersja FREE)

Pragnę jednak podkreślić, że programy te są darmowe jedynie do użytku NIEKOMERCYJNEGO. Wyjątkiem jest Comodo, które również do użytku komercyjnego jest za darmo i dlatego polecam ten program. Również w 2010 redakcja PCworld dokonała zestawienia komercyjnych programów antywirusowych. Pierwsza dziesiątka wygląda następująco:

1. BitDefender
2. AVG (wersja PRO)
3. Panda
4. Norton
5. avast (wersja PRO)
6. http://www.kaspersky.pl/
7. Outpost
8. McAfee
9. ESET NOD32
10. Avira

Badanie nie uwzględniało wcześniej rekomendowanego darmowego Comodo.

Włącz firewall (zaporę sieciową). Jeśli korzystasz z Windows wewnętrzna zapora sieciowa powinna starczyć, ale możesz ją "uszczelnić" dodatkowo instalując bezpłatną zaporę zewnętrzną. Listę takich firewalli znajdziesz na: http://www.zwodnik.pl/index.php?id=5

Aktualizuj oprogramowanie. Po co? Bo w aktualizacja autorzy załatali m.in. błędy bezpieczeństwa, którymi nie chwali się wszem i wobec.

Uważaj, co otwierasz. Nie otwieraj załączników niewiadomego pochodzenia. Słyszeliście o kazusie wirusa "I Love You"? Wirus rozprzestrzeniał się za pomocą poczty e-mail. Po otwarciu załącznika sam się kopiował i wysyłał na wszystkie maile w książce adresowej. Nie winię nikogo, że otworzył wiadomość e-mail od klienta zatytułowaną "ILOVEYOU", ale otwarcie załącznika było już nieodpowiedzialne, tym bardziej, że wirus nadpisywał ważne pliki.

Wyłączanie makr w plikach MS Office. Makra wykonalne są tworzone w VBS, w którym stworzone słynnego wirusa "I Love You".

Nie instaluj podejrzanych aplikacji.

Skorzystaj z programów prewencyjnych. Programy prewencyjne (intrusion Prevention System) są komplementarne z antywirusami i pomagają uchronić Cię przed m.in. bezpośrednimi atakami (czyli kierowanymi celowo w Ciebie) oraz keyloggerami (programami zczytującymi dane z klawiatury). Polecam darmowy GeSWall.

Może inny system operacyjny? To mit, że nie ma wirusów na Maca czy Linuksa. Oczywiście, że istnieją, ale w znacznie mniejszej ilości. Jeśli jesteś Twoja praca nie wymaga specjalistycznego oprogramowania działającego jedynie w środowisku Windows, pomyśl o darmowym Linuksie zaopatrzonym w OpenOffice (umożliwia zapisywanie i odczytywanie plików MS Office, dzięki czemu klient może nawet nie zauważyć zmiany). Będzie za darmo i będzie legalnie. Linux zaopatrzony w środowisko graficzne Gnome lub KDE zarówno z wyglądu, jak i z interfejsu przypomina Windows. Portal hack.pl dla poczatkujących poleca

Mandrivę, Ubuntu lub OpenSUSE.

Regularnie skanuj komputer.

Uważaj na nośniki pamięci, które miały styczność z komputerem używanym przez wiele osób (np. w punkcie ksero albo kawiarni internetowej). Najlepiej wyłącz autouruchamianie z pamięci USB, CD/DVD, dzięki czemu zawsze będziesz mieć czas dokonać skanu. Jeśli korzystasz z Windows XP przyda Ci się instrukcja opisana tu: http://x86.pl/wylaczenie-autouruchamiania-cd-dvd-usb-pendrive/