

Bezpieczne używanie komputera osobistego

Bruce Schneier

Oryginał: <http://www.schneier.com/crypto-gram-0105.html#8>

Tłumaczenie: CERT Polska

1. Hasła. Silnego hasła nie da się w praktyce zapamiętać, więc można zrezygnować z próbowania. Lepiej wygenerować długie, losowe hasła i zapisać je, przechowując w portfelu albo specjalnym programie takim jak Password Safe. Haseł strzeż dokładnie tak samo, jak pilnujesz gotówki. Nie pozwalaj przeglądarkom na zapamiętywanie haseł, ani nie przesyłaj ich (podobnie jak kodów PIN) w formie niezaszyfrowanej e-mailem czy przez formularze WWW. Planując, uwzględniaj założenie, że każdy PIN daje się łatwo złamać.

Można skorzystać z poradnika CERT Polska - Jak skonstruować dobre hasło? http://www.cert.pl/PDF/dobre_haslo.pdf

2. Oprogramowanie antywirusowe. Używaj go. Pobieraj i instaluj aktualizacje codziennie, a także wtedy, gdy z mediów docierają doniesienia o nowym wirusie. Niektóre antywirusy pobierają aktualizacje w sposób automatyczny.

3. Osobisty firewall. Używaj go. Zazwyczaj nie ma powodu, aby akceptować przychodzące połączenia od kogokolwiek.

Można skorzystać z poradnika CERT Polska - Konfiguracja firewalla osobistego. http://www.cert.pl/PDF/konf_pers_fw.pdf

4. E-mail. Spam usuwaj bez czytania. Bez otwierania usuwaj także wiadomości z załącznikami, chyba że wiesz skąd pochodzą i czego dotyczą. Kasuj także bez otwierania wszystkie zabawne obrazki, filmy i temu podobne pliki przesyłane przez mających dobre intencje znajomych. Korzystając z poczty elektronicznej, wyłącz obsługę HTML. Nie używaj Outlooka i Outlook Expressa.

Jeżeli musisz korzystać z Microsoft Office, włącz ochronę przed wirusami makr. Używając Windows, wyłącz opcję "ukrywania rozszerzeń znanych typów plików". Pozwala ona koniom trojańskim udawać pliki innego typu. Wyłącz Windows Scripting Host jeśli nie jest Ci z jakiegoś powodu niezbędny, ostatecznie zmień przypisanie plików skryptowych do tej aplikacji, tak aby podwójne kliknięcie ich nie otwierało.

5. Strony internetowe. SSL nie jest sam w sobie gwarancją zaufania do sprzedawcy i bezpieczeństwa danych w jego bazie danych. Pomyśl zanim podejmiesz decyzję o transakcji finansowej w sieci. Ogranicz zestaw danych finansowych i osobistych, jakie wysyłane są do sprzedawcy; nie przekazuj informacji, jeśli nie jesteś przekonany o tym, że jest to korzystne. Jeśli nie chcesz przekazywać danych osobistych przy

rejestracji konta, podawaj dane zmyślone. Wypisz się z biuletynów marketingowych. Jeśli w serwisie dostępna jest opcja nie przechowywania danych osobistych – skorzystaj z niej.

6. Korzystanie z przeglądarki. Ogranicz korzystanie z cookies i apletów tylko do tych serwisów, które tego wymagają. Regularnie usuwaj cookies i foldery tymczasowe (skorzystaj z programu, który wykona to automatycznie, np.: w trakcie uruchamiania komputera). Jeżeli to możliwe, nie używaj programu Microsoft Internet Explorer.

7. Aplikacje. Ogranicz ilość oprogramowania zainstalowanego w komputerze. Jeśli nie będziesz wykorzystywał jakiegoś programu, nie instaluj go. Jeśli któryś jest już niepotrzebny, odinstaluj go. Jeśli stale korzystasz z jakiegoś programu, regularnie sprawdzaj czy zostały wydane uaktualnienia i instalować je w razie potrzeby.

8. Kopie zapasowe. Regularnie twórz kopie zapasowe. Nagrywaj je na dysk, taśmę lub CD-ROM. Co najmniej jeden zestaw kopii zapasowych przechowuj poza fizyczną lokalizacją systemu (sejf jest dobrym miejscem) i co najmniej jeden zestaw w niej. Pamiętaj o niszczeniu starych kopii zapasowych; fizycznie niszczy dyski CD-R.

9. Bezpieczeństwo laptopów. Poza domem, laptop trzymaj cały czas przy sobie; myśl o nim jak o portmonetce lub portfelu. Regularnie usuwaj z laptopa zbędne pliki. Te same uwagi dotyczą PDA; dane osobiste, takie jak hasła i Piny trzymane są na nich nawet częściej niż na laptopach.

10. Szyfrowanie. Zainstaluj program szyfrujący dane i e-maile (taki jak PGP). Szyfrowanie całej korespondencji jest nierealne, ale niektóre maile są zbyt ważne by wysyłać je w czystej postaci. Podobnie niektóre dane są zbyt ważne by je przechowywać na dysku niezaszyfrowane.

11. Ogólne. Wyłączaj komputer gdy z niego nie korzystasz, zwłaszcza jeśli posiadasz stałe łącze. Jeśli to możliwe, nie używaj Microsoft Windows.