Grunt to dobre nawyki – lista rozszerzona

Poniżej zamieszczam rozszerzony zbiór reguł, które opracowałem, dotyczących bezpiecznego korzystania z komputera podczas dokonywania transakcji online:

- nie zezwalaj przeglądarce na zapisywanie haseł i nazw użytkownika,
- korzystaj z oddzielnych, przeznaczonych do tego menedżerów haseł typu KeePass (z włączoną opcją TCATO) lub RoboForm,
- nie przechowuj nazw użytkownika, hasła lub listy haseł jednocześnie w jednym i tym samym miejscu – nie zapisuj nigdzie PIN-u oraz nie udostępniaj swoich danych innym osobom,
- nie przechowuj bazy danych z hasłami i swoich poufnych danych na zewnętrznych serwerach online (np. na serwerze pocztowym czy serwerze FTP),
- stosuj silne hasła,
- stosuj różne hasła (nie używaj tylko jednego hasła, kiedy logujesz się na różnych stronach w myśl zasady: 1 hasło = 1 strona WWW),
- korzystaj z konta z ograniczonym dostępem na systemach Windows – konto "Gość" (*LUA*) zamiast konta z uprawnieniami administratora – włącz UAC (*Vista/7*),
- pamiętaj o tym aby mieć zainstalowane i zaktualizowane oprogramowanie zabezpieczające,
- używaj firewall-a (najlepiej takiego który będzie informował o każdym nowym połączeniu wychodzącym z Twojego komputera),
- ze wzmożoną czujnością korzystaj z komputerów, do których dostęp mają również inne osoby lub komputerów w miejscach publicznych np. w kafejkach internetowych (unikaj logowania z tego typu komputerów – jeśli w 100% nie jesteś pewien jakie oprogramowanie jest na nich zainstalowane),
- jeśli możesz lub masz taką możliwość upewnij się do czego tak naprawdę jest podłączona klawiatura z której masz zamiar skorzystać, sprawdź czy przypadkiem nie jest ona **podłączona** do hardware'owego keyloggera,
- jeśli koniecznie musisz zalogować się na stronie bankowej np. z kafejki internetowej – staraj się korzystać z zaimplementowanej przez bank klawiatury ekranowej (o ile jest ona dostępna) – unikaj korzystania z klawiatury ekranowej wbudowanej w systemy Windows,
- upewnij się, że strona Twojego banku jest faktycznie stroną Twojego banku, a nie specjalnie spreparowaną (wyglądającą podobnie) fałszywą stroną – sprawdź dwa razy czy adres URL jest poprawnie wpisany,

- sprawdź, czy połączenie z bankiem jest szyfrowane – adres strony powinien rozpoczynać się od https://, a nie http://, dodatkowo obok paska adresu lub w prawym dolnym rogu okna przeglądarki powinien pojawić się symbol kłódki,
- przed podaniem jakichkolwiek danych sprawdź dane certyfikatu bezpieczeństwa serwisu – dane te dostępne są po kliknięciu na ikonę kłódki w przeglądarce internetowej,
- nie ignoruj zaobserwowanych różnic w wyglądzie strony lub w wymaganych przez system danych. Pamiętaj, że do logowania służy wyłącznie Identyfikator i PIN, bank nigdy nie wymaga żadnych innych danych przy logowaniu,
- zawsze kończąc pracę korzystaj z opcji wylogowania, jeśli to możliwe usuwając również wszystkie pliki *cookie* oraz pamięć *cache* (pliki tymczasowe), które podczas Twojego surfowania po Internecie zostały zapisane przez przeglądarkę,
- staraj się nie korzystać w miejscach publicznych z niezabezpieczonych sieci Wi-Fi (tzw. *hotspot'ów*),
- nie pobieraj na dysk i nie uruchamiaj w systemie programów typu *crack*, *keygen*, etc.,
- nigdy nie otwieraj linków, które otrzymujesz poprzez komunikator lub Email – taki link może wyglądać normalnie i mieć konstrukcję np. microsoft.com, ale jego odwołanie (*href*) może przekierować Cię na zupełnie inna, specjalnie spreparowaną lub/i zainfekowaną stronę,
- ignoruj wiadomości Email, których nadawca prosi o podanie (np. w celach weryfikacyjnych) Twoich poufnych danych,
- korzystaj tylko z oryginalnego systemu operacyjnego, pochodzącego z legalnych źródeł (nie z przeróbek typu np. MX w przypadku Windows lub kopii ściągniętych z torrentów) – dodatkowo, jeśli jest to system Windows, dbaj również o to aby zainstalowane były wszystkie poprawki firmy Microsoft,
- staraj się, aby programy z których korzystasz zawsze były zaktualizowane do najnowszej dostępnej publicznie stabilnej wersji,
- w trakcie wprowadzania bankomatowego kodu PIN staraj się zasłaniać wybierane przez Ciebie klawisze, tak aby w sytuacji gdyby była tam zainstalowana kamera – nie zarejestrowała wybieranych przez Ciebie cyfer,
- upewnij się, że w trakcie Twojego logowania, nikt nie zerka Ci przez ramię.

Myślę, że warto sobie tę listę wydrukować i mieć ją pod ręką tak aby zawsze, gdy to konieczne być pewnym, że nie pominęło się żadnego istotnego elementu składającego się na nasze bezpieczeństwo przy dokonywaniu transakcji online.

Piotr Pawelec (Creer),
ITSecurityEnthusiast.wordpress.com