



Notesik do zapisywania hasel

W ostatnim okresie dostawałem całą serię emaili od znajomych, wszystkich z kontami w yahoo. Emaily wyglądały dość podobnie - "hej, zobacz co ciekawego znalazłem" i link do strony internetowej. Jeśli tekst jest po angielsku, a Twój korespondent używa polskiego, łatwo jest od razu być podejrzliwym, ale nie zawsze tak jest. Link prowadzić może do strony, która zainfekuje Twój komputer, może nawet próbować ukraść hasła, które używasz. To zjawisko ma już swoją nazwę (Spear Phishing - łowienie z ostrym narzędziem?).

Mam też znajomych którzy popadają w drugie ekstremum i unikają jakiegokolwiek obecności w sieci - nie zapisują się do społeczności, nie odpowiadają na emaily (albo nawet nie używają komputera, co jest już ekstremizmem konserwatywności). Ludzie Ci wylewają dziecko z kąpielą, gdyż obecność w sieci ma swoje autentyczne zalety, co jest widoczne szczególnie mocno wtedy kiedy jak my jesteśmy daleko od bliskich sobie ludzi (lub na odwrót, to bliscy czy rodzina wyjechali daleko).

Zdarza mi się też od czasu do czasu zajmować się czymś komputerem lub laptopem całkowicie opanowanym przez wirusy. Zwykle wygląda to tak, że komputer chodzi bardzo wolno, a jakkolwiek próba połączenia ze stroną internetową powoduje przekierowanie na inną stronę (prawdopodobnie jeszcze bardziej zainfekowaną). W takim przypadku najlepszym rozwiązaniem jest skopiowanie cennych materiałów (a następnie przepuszczenie plików przez dobry program antywirusowy) i kompletne sformatowanie twardego dysku.

Zdarza się też dość często, że poczta jest odrzucona przez serwer odbiorcy (ze słabą wymówką). Ten problem jest o tyle skomplikowany, że widzi go tylko nadawca (odbiorca zwykle odpowiada "przecież do mnie poczta zawsze dochodzi"...), a naprawić go może tylko odbiorca.

Jak z tym wszystkim sobie poradzić? Nie ma w tym żadnej wielkiej magii, wystarczy zdrowy rozsądek. Poniżej kilka uwag z własnego doświadczenia:

Hasła

Jakkolwiek używanie hasła ma swoje wady, nie ma dziś nic lepszego, co by hasła zastąpiło. Przy liczbie serwisów, sklepów, banków mamy wiele loginów i wiele haseł. Hasło nie może być zbyt proste, bo takie można złamać bez większego wysiłku. Są strony Internetowe z długimi listami złamanych haseł. Atak słownikowy rozłamuje hasła składające się z jednego słowa (dziś używa się słowników w wielu językach). Alternatywą jest danie hakerowi dostępu do listy znajomych i do całego swojego zbioru listów (w tym tych prywatnych)

Aby utrudnić złamanie, można złożyć hasło z dwóch niezwiązanych słów, przyozdobić liczbą i znakami przestankowymi. Wstawienie dużej litery też pomaga.

- Nigdy nie używać tego samego hasła w dwóch miejscach. To jest kuszące - i może spowodować całkowite przejęcie przez hakera Twoich danych w różnych serwisach.
- Nie zapisywać haseł nigdy w postaci komputerowej - nie na dysku, nie 'online'. Włamywacz dostawszy się do jednego miejsca ma natychmiast dostęp do wszystkich. Polecane jest użycie techniki 'out-of-band' czyli zapisanie haseł w notesiku na papierze. Haseł jest dużo, pamięć zawodna, a papier jest cierpliwy.

Email

Jeśli ktoś włamał się do Twojego konta, i rozsyła wirusy do znajomych, należy: a) Natychmiast

zmienić hasło i b) Zamknąć konto. Ten drugi etap może być bolesny - przyzwyczailiśmy się do adresu emailowego, trzeba wszystkich zawiadomić, co za kłopot ;-). Niektórzy robią to dopiero po drugim włamaniu. Ale włamywacz miał dostęp do wszystkiego - listy kontaktów, całej poczty, przesyłanych otwartym tekstem haseł. I może dalej dokonywać szkody podszywając się pod Ciebie i wysyłając dalsze listy.

Podobnie jest w przypadku serwisu który blokuje przychodzące do ciebie emaile. Zgłoszenie zażalenia czasem pomaga, ale wiele serwisów to zupełnie ignoruje. Tutaj zawsze sugeruję założenie alternatywnego adresu emailowego, szczególnie jeśli ten główny jest służbowy. Gmail jest dobrym kandydatem, gdyż ma bardzo dobre (i ciągle ulepszane) zabezpieczenia. Lokalny dostawca usług może być też dobrą opcją dla alternatywnego emailu. Można wtedy przekierować pocztę (do tego serwisu który jest łatwiejszy w obsłudze), i przyzwyczajać swoich korespondentów do drugiego adresu. Jeśli jeden padnie, jest zainfekowany lub blokuje pocztę, zawsze wtedy jest ten drugi, już gotowy.

Antywirus

Choć to wydaje się oczywiste, powtórzę na wszelki wypadek. Należy mieć zawsze aktualny program antywirusowy! Jest sporo darmowych, jedne reklamują się takimi lub innymi funkcjami. Ale nawet tani lub darmowy program jest duuużo lepszy od nieaktywnego lub żadnego. Wirus, który zainfekuje Twój komputer potrafi ukraść Twoje wszystkie hasła (dlatego polecam zapisywanie ich na papierze); zamienić go w 'zombie' który na zdalne polecenie z Chin lub Rosji zacznie wysyłać masowo pakiety blokujące jakiś bank albo komputer rządowy w Estonii; spowolnić Twój komputer do zupełnej nieużyteczności; wymazać lub zaszyfrować twardy dysk i dokonać wiele innych szkód.

Prywatność i okruszki

Musimy się pogodzić z tym, że aby działać w sieci, musimy się pożegnać z pełną anonimowością. Zresztą, kto tak naprawdę chciałby być anonimowy. Wszystkie serwisy, sklepy, banki, portale zbierają o nas informacje. Szczególnie przodują w tym portale społecznościowe, takie jak Facebook czy Nasza Klasa. Google również zbiera informacje o Tobie. Bardzo często zresztą ułatwia to życie - Google wie, gdzie jestem, i nie próbuje serwować mi informacji z drugiego kontynentu (ale łatwo mogę mu wytłumaczyć, że ta ulica Podrzeczna jest w Łodzi). Przy każdym użyciu Internetu zostawiamy po sobie okruszki (bread crumbs). Ale ilość i jakość informacji z jaką się rozstajemy można łatwo kontrolować. Jeśli denerwuje Cię, że reklamy są zbyt trafne (mnie bardziej weseli, kiedy są zupełnie nietrafione) czytaj dalej:

- Można używać więcej niż jednej przeglądarki. Niektóre operacje dokonywać w jednej a inne w drugiej. To bardzo mocno rozkłada algorytmy zbierania informacji.

- Używać trybu prywatnego w przeglądarce (przykładowo w Firefox: File/New Private Window; w Chrome: Ctrl+Shift+N New Incognito Window). Szczególnie jeśli oglądasz rzeczy których nie powinienes :-))
- Od czasu do czasu szukać rzeczy zupełnie z księżyca. To też gubi algorytmy podające Ci reklamy.
- W portalach społecznościowych publikować podstawowe informacje o sobie. Imię, nazwisko, miasto, uczelnię. Przydaje się też zdjęcie. To pomaga innym rozpoznać Cię, odróżnić od innych, znaleźć w tłumie, skontaktować się. Inne informacje można podawać już w prywatnych, zamkniętych kręgach. Ale są portale, takie jak LinkedIn, gdzie wskazane jest podać informacje o swojej karierze zawodowej - pomaga to i w szukaniu pracy i innym w znalezieniu odpowiedniego kontaktu.

Szyfrowanie

Jakkolwiek nie używane na co dzień, jest bezcenne przy przesyłaniu poufnej informacji - haseł, informacji finansowych, tajemnic firmowych. Prowadząc z USA firmę w Polsce używałem szyfrowania bardzo często. Świetny program PGP (Pretty Good Privacy) stworzony przez Phila Zimmermana jest jednym z najczęściej używanych metod kryptograficznych dla emaili. Wersja w systemie Otwartego Programowania o nazwie GPG jest powszechnie dostępna. Szyfrowanie takie jest praktycznie nie do złamania i nie wymaga transferu prywatnego klucza (ogłasza się tylko klucz publiczny, którym można zakodować ale nie odkodować wiadomość). Podobnych technik używa się także dla zapewnienia autentykacji nadawcy. Nie polecam tego na co dzień, ale jeśli ktoś obawia się podsłuchu, ma powody podejrzewać kogoś o czytanie prywatnej poczty itp., jest to gotowe rozwiązanie którego instalacja zajmuje 10 minut.

Komputer i herbata

Komputer trzeba utrzymywać w porządku, nie instalować zbyt wiele programów, usuwać wszystkie obce paski narzędzi z przeglądarek (zawsze się tam dostają, jeśli nie uważa się przy instalacji innych programów), aktualizować zainstalowane programy. Ale i tak komputer często się zatrzymuje, nie może się połączyć z siecią, nie robi tego, co chcemy. W takich przypadkach sugeruję w miarę uniwersalny przepis z użyciem herbaty. Procedura jest następująca. 1) Wyłączamy komputer, używając klawisza "start" w PC z Windows do wersji 7, albo przyciskając guzik zasilania przez 8 lub więcej sekund, jeśli pierwsze rozwiązanie nie daje efektu. 2) Zaparzamy sobie herbatę. 3) Włączamy komputer ponownie - i wszystko działa. Procedura ta jest skuteczna zwykle w 90% przypadków. Użycie kawy jest opcjonalne.

Marek Zieliński

Wpisany przez Marek Zieliński

poniedziałek, 18 stycznia 2016 00:00 - Poprawiony piątek, 11 grudnia 2015 21:02

Artykuł ukazał się 14 lipca 2013 w *Blogu archiwistów i bibliotekarzy Instytutu Piłsudskiego*

Może Cię też zainteresować:

- [Pamięć masowa dla archiwów cyfrowych](#)
- [Archiwa i Wikipedia](#)
- [Co jest na odwrocie zdjęcia cyfrowego](#)