Jak chronić swoją prywatność w sieci?

10 prostych wskazówek od PARLAMENTU EUROPEJSKIEGO

1. NIE ODPOWIADAJ KIEDY PYTAJĄ

To, że Cię pytają, nie znaczy, że musisz odpowiadać. Jeżeli zakładasz tylko konto mailowe, nie musisz mieć obszernego profilu. A jeśli przyłączasz się do portalu społecznościowego, możesz ograniczyć ilość informacji o sobie do minimum. Jeżeli musisz podać swój e-mail, a nie potrzebujesz odpowiedzi, zawsze możesz podać zmyślony adres.

2. „CIASTECZKA” SĄ NAJLEPSZE, KIEDY MOŻESZ JE ZJEŚĆ.

Upewnij się, że tylko te strony internetowe, które odwiedzasz, będą mogły zbierać informacje w formie plików cookies („ciasteczek”). W tym celu ustaw swoją przeglądarkę tak, aby odrzucała pliki cookies z innych źródeł. W ten sposób zmniejszysz ryzyko kradzieży informacji przez bezwzględnych hakerów, np. za pomocą nieprawdziwych reklam umieszczanych na odwiedzanych przez Ciebie stronach.

3. HASŁO TO NIE PRZEPUSTKA.

Sprawdź, czy Twoje hasła chronią Twoje dane i czy nie są przepustką do Twoich danych osobowych. Nie używaj wszędzie tego samego hasła, nie podawaj jako hasła nazwy użytkownika stosowanej na innej stronie, hakerzy mogą to wychwycić. Używaj cyfr i liter (w tym wielkich) w kombinacjach, które nie są wyrazami słownikowymi.

4. TY ROZDAJESZ, INNI SPRZEDADZĄ.

Poszperaj trochę i przyjrzyj się profilom innych osób – to, co możesz przeczytać o nich, inni mogą przeczytać o Tobie. Zamieszczanie zdjęć też może być przyczyną kłopotów. Po wrzuceniu prywatnych zdjęć do sieci tracisz nad nimi kontrolę. Jesteś pewien, że chcesz podawać tyle informacji o sobie?

5. TRZYMAJ SWOJE DANE OSOBOWE POD KLUCZEM.

Portale społecznościowe są żyłą złota dla łowców danych, więc nie ułatwiaj im zadania i ustaw jak najwyższy poziom ochrony prywatności w swoim profilu. Podczas żywiołowej dyskusji może Ci się wymknąć więcej, niż byś chciał. Kontroluj więc, co piszesz, tak aby nie ujawniać swoich danych.

6. ZAMKNIJ JEDNE DRZWI, ZANIM OTWORZYSZ NASTĘPNE.

Pozostawanie zalogowanym na portalu społecznościowym lub na koncie bankowym to jak zostawianie otwartego samochodu: jesteś narażony na ataki hakerów. Unikaj ryzyka i wyloguj się, zanim zaczniesz buszować w sieci.

7. KTO SIĘ PODCZEPIŁ DO TWOJEJ SIECI?

Jeżeli korzystasz z sieci WiFi, upewnij się, czy nie wieziesz pasażerów na gapę. Zabezpiecz swoją sieć solidnym hasłem albo włącz kodowanie WPA, które jest pewniejsze.

8. BEZPIECZEŃSTWO DZIAŁA W OBIE STRONY.

Starasz się, żeby Twój komputer był bezpieczny, zwracasz uwagę na informacje, które zamieszczasz online, ale co z tymi, którzy przechowują Twoje dane? Mogłeś ustawić najwyższy poziom bezpieczeństwa, ale jeżeli jakaś strona nie jest w stanie bezpiecznie przechowywać Twoich danych, i tak jesteś narażony. Czy możesz ufać właścicielom stron i ich systemom bezpieczeństwa?

9. OGRANICZ SZKODY.

Zastanów się nad stosowaniem jednej metody płatności tylko do zakupów online. Ustaw niski limit kredytowy – jeżeli ktoś uzyska dostęp do Twojej karty, szkody będą mniejsze.

10. UWAGA NA DROBNY DRUK.

Tak samo w sieci, jak i gdziekolwiek indziej: sprawdzaj, co podpisujesz. Przykładowo, niektóre umowy odnawiają się automatycznie i musisz je wcześniej wypowiedzieć, jeżeli nie chcesz, żeby Twoja karta kredytowa została ponownie obciążona.

ŹRÓDŁO:

http://www.europarl.europa.eu/news/pl/

http://www.europarl.europa.eu/news/pl/top-stories/content/20130901TST18405/html/Unijna-ochrona-danych

Opracowała: Anna Siennicka

Łódzkie Centrum Doskonalenia Nauczycieli i Kształcenia Praktycznego