edukacja medialna

Jak wzmocnić swoją prywatność?

WIEDZA W PIGUŁCE

Współczesne media społecznościowe nieustannie zachęcają użytkowników do porzucenia własnej prywatności na rzecz dzielenia się wszystkim z innymi. Nowe pokolenie celebrytów, robiące karierę za pośrednictwem Snapchata i Instagrama, udostępnia zapisy niemal każdej chwili swojego życia. Co ryzykujemy, rezygnując z dbania o prywatność?

Anonimowość jest jedną ze strategii ochrony naszej wolności i swobody. Im więcej podajemy o sobie informacji, tym większe prawdopodobieństwo, że ktoś wykorzysta je przeciwko nam. Nasze dane mogą się stać przedmiotem handlu i zostać wykorzystane w celach marketingowych. Nieraz konsekwencje niedbania o prywatność bywają bardzo niebezpieczne – takie działania prowokują cyberprzestępstwa, np. podszywanie się czy stalking.

Materiał raz udostępniony w sieci, nigdy w niej do końca nie ginie. Filmik dokumentujący zabawę ze znajomymi może być dla ciebie teraz świetną pamiątką, ale za kilka lat może zniechęcić potencjalnego pracodawcę do zatrudnienia cię. Udostępnione przez nas informacje mogą również łatwo trafić w niepowołane ręce – nie da się mieć pełnej kontroli nad tym, kto się na nie natknie i jak ich użyje.

Prywatność jest ważną wartością, jednak trudno ją chronić. Zwłaszcza że komunikacja w internecie zawsze narażona jest na nadzór – żadna metoda kontaktu za pomocą mediów nie daje nam stuprocentowej gwarancji prywatności. Warto jednak wyrobić sobie przyzwyczajenia, które pomogą ci na co dzień o nią dbać.

Przede wszystkim staraj się nie dzielić większą ilością informacji, niż jest to potrzebne. Nie wyrażaj zgody na przesyłanie ofert marketingowych czy newsletterów, na które nie masz ochoty. Zachowuj dystans w stosunku do proponowanych ci usług, zwłaszcza jeśli korzystanie z nich wiąże się z koniecznością udostępnienia twoich danych. Miej zwyczaj wylogowywania się z serwisów, które wymagają logowania, oraz korzystaj z bezpiecznych haseł.

Zadbaj również o to, aby stałe ustawienia twojego sprzętu gwarantowały ci maksymalną prywatność w sposób automatyczny. Aktualizuj swoje oprogramowanie i posiadaj sprawdzony program antywirusowy. Zachowaj umiar w korzystaniu z programów opartych na geolokalizacji i zawsze ją wyłączaj, jeśli jej rzeczywiście nie potrzebujesz. Zapewnia ona ciągły przesył danych o tym, gdzie się znajdujesz, przez co przekazujesz internetowym gigantom całą historię twojego przemieszczania się.

Wreszcie, jeśli potrzebujesz przekazać komuś poufne informacje o sobie, korzystaj ze sposobu komunikacji o dużym stopniu prywatności. Najlepiej zrób to osobiście lub telefonicznie, przebywając poza przestrzenią publiczną. Możesz również skorzystać z szyfrowanego maila lub innego sposobu szyfrowanej komunikacji. Należy w tym celu posiadać dodatkowe oprogramowanie, a także udostępnić odbiorcy metodę na odkodowanie twojej wiadomości. Klasyczny mail czy komunikacja przez Skype'a nie zapewniają wystarczającej prywatności – ich treści są automatycznie skanowane. Najmniej bezpieczne są czaty na portalach społecznościowych (również w formie osobnych aplikacji, takich jak Messenger Facebooka) i otwarte fora internetowe.

Nie rezygnuj ze swojej prywatności z lenistwa lub tylko dlatego, że panuje taka moda. Nigdy nie wiesz, w jaki sposób może się to obrócić przeciwko tobie.

SŁOWNICZEK

- **geolokalizacja**: określenie fizycznego położenia geograficznego osoby i urządzenia telekomunikacyjnego za pomocą systemu GPS lub adresu IP.
- **szyfrowanie poczty elektronicznej**: metody szyfrowania treści komunikacji e-mail tak, by odczytać ją mogli tylko nadawca i adresaci.

Tekst: Urszula Dobrowolska, scenariusz: Monika Prus-Głaszczka, konsultacja merytoryczna: Wojciech Klicki. Materiał pochodzi z serwisu edukacjamedialna.edu.pl prowadzonego przez Fundację Nowoczesna Polska.

Źródło: http://edukacjamedialna.edu.pl/lekcje/jak-wzmocnic-swoja-prywatnosc/.

Publikacja zrealizowana w ramach projektu "Cybernauci - kompleksowy projekt kształtowania bezpiecznych zachowań w sieci", finansowanego ze środków Ministra Edukacji Narodowej.

Podstawa programowa:

Wiedza o społeczeństwie, III poziom edukacyjny
Treści nauczania
Życie społeczne
Życie społeczne

Nowa podstawa programowa:

Etyka, IV-VIII klasa
Treści nauczania
Uczeń podaje przykłady właściwego i niewłaściwego wykorzystywania nowoczesnych technologii informacyjnych.

Wychowanie do życia w rodzinie, liceum i technikum
Treści nauczania
rozumie, na czym polega prawo człowieka do intymności i ochrona tego prawa.

Informatyka, liceum i technikum
Treści nauczania
stosuje dobre praktyki w zakresie ochrony informacji wrażliwych (np. hasła, pin), danych i bezpieczeństwa systemu operacyjnego, objaśnia rolę szyfrowania informacji.