Jak bezpiecznie komunikować się w sieci?

3 grudnia 2014

W „pozainternetowym” życiu na ogół nie mamy wątpliwości, czy rozmawiamy z jedną osobą, czy występujemy przed szerszym audytorium. W sieci nie jest to takie oczywiste: zazwyczaj nie widzimy osoby, do której kierujemy komunikat. Ani tych osób, do których trafia on po drodze. Komunikację w Internecie można porównać do wysyłania pocztówki, z której treścią może zapoznać się nie tylko adresat, ale też każdy, przez czyje ręce ona przejdzie. Powinni sobie z tego zdawać sprawę nawet najmłodsi użytkownicy sieci.

KOMUNIKACJA – PUBLICZNA, PRYWATNA, POUFNA

Już dziecko powinno wiedzieć, że jeśli publikuje zdjęcia na blogu lub posty na forum, to trafiają one do szerszej publiczności. Można powiedzieć, że w tej sytuacji dzieli się informacją z całym światem. Inaczej jest w przypadku e-maila czy wiadomości na portalu społecznościowym, które powinny trafić tylko do konkretnych adresatów. Jednak w tym przypadku sytuacja nie jest wcale oczywista. Nawet gdy wysyłamy komunikat do ograniczonego kręgu osób, któraś z nich może go puścić dalej w świat. Wtedy tracimy nad nim kontrolę, a informacja zaczyna żyć własnym życiem. Co więcej, jeśli przesyłamy wiadomość, korzystając z jakiejś usługi (np. poczty elektronicznej, portalu społecznościowego itp.), musimy się liczyć z tym, że ma do niej dostęp również administrator.

Z treścią internetowej komunikacji mogą w wielu sytuacjach zapoznać się osoby postronne. Dlatego za jej pomocą nie powinno się przekazywać informacji, które mają poufny charakter. Chyba że zdecydujemy się na stosowanie odpowiednich środków zabezpieczających, np. szyfrowania poczty elektronicznej. Służą do tego specjalne narzędzia

kryptograficzne (PGP/GPG). To bardzo przydatne rozwiązanie, nie należy jednak do najprostszych i uniwersalnych – wymaga współpracy ze strony osób, z którymi chcemy się komunikować.

LUKI BEZPIECZEŃSTWA

Informacje, które przekazujemy w sieci, mogą trafić w niepowołane ręce różnymi drogami, choćby przy okazji korzystania z niezabezpieczonej sieci Wi-fi. Jeśli przesyłamy jakieś dane za pomocą protokołu http, mogą mieć do nich dostęp osoby trzecie. Dlatego połączenia wymagające logowania powinny być realizowane za pomocą szyfrowanego protokołu https. Zagrożeniem dla poufności informacji mogą być także wirusy i e-maile wyłudzające dane. Bardzo prozaicznym, ale niestety dość częstym problemem, jest dostęp osób niepowołanych do niezabezpieczonego sprzętu. Jeśli trafimy na życzliwego „włamywacza", może się skończyć na zabawnym wpisie na portalu społecznościowym. Jednak nie każda niefrasobliwa osoba ma tyle szczęścia.

Coraz więcej osób dba o to, by przed złośliwym oprogramowaniem i dostępem osób trzecich zabezpieczyć swój komputer. Jednak rozwój i upowszechnienie się nowych technologii rodzi nowe wyzwania. Dane zebrane przez GIODO pokazują, że z Internetu w telefonie korzysta już nie niemal co trzeci badany uczeń. Urządzenia mobilne są w sposób naturalny bardziej narażone niż domowy komputer na to, że w wpadną w niepowołane ręce. Tymczasem wiele osób nie myśli o tym, że powinny one być równie dobrze zabezpieczone.

JAK SOBIE RADZIĆ?

Trudno wyobrazić sobie bezpieczną komunikację w sieci bez elementarnej wiedzy na temat działania Internetu i potencjalnych zagrożeń. Nie każdy rodzic musi być od razu specem od IT, ale jeśli chce przygotować swoje dziecko do świadomego korzystania z nowych technologii, powinien trzymać rękę na pulsie. Od najmłodszych lat warto uczyć pociechy

podstawowych zasad bezpieczeństwa, samemu ich przestrzegać oraz wykorzystywać odpowiednie zabezpieczenia techniczne. O czym warto pamiętać?

1. Staraj się unikać przekazywania poufnych informacji (np. haseł) pocztą elektroniczną, SMS-ami. Jeśli zależy Ci na zachowaniu poufności komunikacji, używaj systemu szyfrującego komunikację e-mailową.

2. Gdy to możliwe, korzystaj z protokołu https. Przy logowaniu i przesyłaniu danych sprawdź, czy adres w przeglądarce zaczyna się od https i widnieje obok niego symbol kłódki. Zainstaluj w swojej przeglądarce wtyczkę „Https Everywhere”, dzięki której z każdą odwiedzaną stroną, która ma taką opcję, automatycznie będziesz łączyć się przez protokół https.

3. Nie przesyłaj ważnych danych, gdy korzystasz z niezabezpieczonej sieci Wi-Fi. Staraj się w takiej sytuacji unikać logowania się; jeśli masz taką możliwość, wykorzystaj do tego swoją sieć dostępną w telefonie.

4. Wymyślaj trudne do odgadnięcia hasła; używaj różnych haseł do różnych usług i regularnie je zmieniaj. Chroń swoje hasła – nie udostępniaj ich innym, nie zapisuj w widocznym miejscu.

5. Zmień ustawienia przeglądarki tak, żeby nie zapamiętywała haseł. Wyloguj się, kiedy skończysz korzystać z danej usługi.

6. Zainstaluj i regularnie aktualizuj oprogramowanie antywirusowe. Aktualizuj również inne programy, z których korzystasz i używaj najnowszych wersji przeglądarek internetowych.

7. Zabezpiecz hasłem (blokadą) dostęp do komputera, telefonu, tabletu. Szyfruj dane przechowywane na dysku.

Autorzy: Małgorzata Szumańska, Anna Obem
Źródło: Fundacja Panoptykon