Stępina, 12.01.2014 r.

Bądź bezpieczny w sieci

Korzystanie z internetu to dziś konieczność. Powszechna jego dostępność wiąże się jednak z zagrożeniami, na jakie możemy być narażeni zanurzając się w bezkres sieci.
Nie możemy przy tym popadać w przesadę (najbezpieczniejszy jest komputer zapakowany do pudełka ☺), ale również nie możemy pozwolić sobie na zupełny luz – zagrożenia jednak są realne.
Mając powyższe na względzie pamiętajmy zatem o kilku przestrogach.

Bądź dyskretny.
Nie podawaj informacji, których nie chcesz udostępniać całemu światu. Informacje raz ujawnione, są ujawnione na zawsze i dla wszystkich. Fotografie swoje czy swoich bliskich wrzucone do sieci (np. Facebook) mogą się znaleźć natychmiast na wielu innych komputerach, stąd usunięcie ich z miejsca docelowego nie daje żadnych gwarancji, że informacji w sieci już nie ma. Prezentacja bogatego wnętrza własnej willi czy wypasionej bryki wraz z dokładną ich lokalizacją oraz informacją, że czuwa jedynie samotna babcia może zachęcić potencjalnych złodziei, a informacja że byłeś na wczasach w Egipcie, gdy szef i ZUS sądzą że byłeś wówczas obłożnie chory może się źle skończyć.

Bądź anonimowy.
Całkowitej anonimowości w sieci nie ma. Zawsze można dociec skąd dana informacja została przesłana, kto łączył się z daną stroną. Ale jest to informacja o samym komputerze dostępna dla fachowca, nie zaś o jego użytkowniku. Jeśli nie musisz, nie dziel się informacjami, które pozwolą Cię (jako osobę) zlokalizować. Do takich danych zaliczamy imię i nazwisko, adresu e-mail, adres domowy czy numeru telefonu. Dane takie udostępniamy tylko na stronach, co do których jesteśmy pewni, że jest to konieczne oraz że dane te będą należycie chronione. Na co dzień korzystamy z pseudonimu i to powinno wystarczyć.

Unikaj ciemnych zakątków internetu.
Korzystając z ciemnych zaułków nieznanego miasta narażamy się na niebezpieczeństwo nie tylko utraty portfela. Podobnie jest w internecie. Strony niebezpieczne oferuj zwykle coś, co ma przyciągnąć potencjalnego użytkownika – darmowe treści (piosenki, filmy, gry), pornografia, obietnica wygranej. Kończy się to zwykle zainstalowaniem szkodliwego oprogramowania, problemami z organizacjami antypirackimi czy z własną psychiką. Zatem ograniczamy naszą aktywność do stron, co do których możemy czuć się bezpiecznie.

Nie ufaj osobom poznanym przez sieć.
Nigdy nie wiesz, kto znajduje się po drugiej stronie – przecież sami korzystamy w sieci jedynie z pseudonimów. W sieci Zosia może faktycznie być Kazikiem i na odwrót, można założyć w cudzym imieniu konto pocztowe, stronę czy profil. Zatem zaufanie ograniczone do minimum. Jeśli zaś zamierzasz spotkać się w realu z osobą poznaną przez sieć, spotykajcie się wyłącznie w bezpiecznych i publicznych miejscach, powiadom kogoś o swoich planach i zabierz na spotkanie ze sobą znajomego – tak jest bezpieczniej.
Nie otwieraj też wiadomości, których się nie spodziewałeś, od osób, których nie znasz – kto może do Ciebie pisać z Nigerii łamanym angielskim? Tylko oszust.

Nie bądź klikaczem.
Koniecznie czytaj komunikaty wyświetlane przez system i sprawdzaj adresy stron, na które masz zamiar wejść (kursor nad odnośnik i czytamy adres strony na pasku statusu). Aby wirus mógł przedostać się na nasz dysk, musimy w którymś momencie kliknąć „Tak". Zatem czytamy, by każda nasza decyzja była rozsądna pamiętając, że pytanie może być bardzo niewinne („Czy chcesz wziąć udział w …") czy też bardzo zawiłe i mało zrozumiałe.
Pamiętamy też o przeczytaniu licencji przed jej przyjęciem – gdzieś pod koniec i drobnym drukiem może być ten haczyk. Przykład z ostatnich miesięcy: Możliwość darmowego korzystania przez 3 miesiące z pewnego serwisu łączyła się z obowiązkową całoroczną płatną subskrypcją za słoną kwotę. Było to w licencji napisane, ale licencja liczyła 12 stron, więc po przeczytaniu dwóch stron znudzony kandydat wymiękał i zgadzał się na wszystko. Obecnie sprawę rozstrzygają sądy.

Zabezpiecz swój komputer.
Zainstaluj program antywirusowy, to już będzie bardzo wiele dla Twojego bezpieczeństwa. Spośród dostępnych programów wybierz odpowiedni dla Ciebie i staraj się często uaktualniać definicje wirusów. Skanuj w poszukiwaniu wirusów obce nośniki i pobrane z internetu pliki, co jakiś czas przeskanuj zawartość Twojego komputera. Takie postępowanie zmniejsza niebezpieczeństwo zawirusowania Twojego komputera. Jednakże pamiętaj, że żaden program antywirusowy nie ma stuprocentowej skuteczności. Kilka lat temu do jednego z czasopism dołączono płytę z oprogramowaniem, zawartość sprawdzono przy pomocy kilku programów antywirusowych, a mimo to na płycie znalazł się wirus.

Loguj się bezpiecznie.
Swoje hasła dobieraj zgodnie z regułami bezpieczeństwa, przechowuj je tak, by inni nie mieli do nich dostępu. Hasło powinno mieć co najmniej 8 znaków (liter, cyfr, znaków nietypowych, np. #) i nie może być oczywiste dla kogoś, kto Cię zna (imię Twojego kotka, chłopaka itp.). Nie używaj jednego hasła w wielu miejscach w sieci – niech się różnią, choćby tylko jedną literą. Pamiętaj, że jeśli się zalogowałeś, to musisz się wylogować. Zamknięcie przeglądarki bez wylogowania to dopraszanie się kłopotów.

Sieć szkolna.
W sieci szkolnej oraz na ogólnie dostępnych komputerach szkolnych mamy dostęp do wielu istotnych danych (folderów) wspólnych dla wielu użytkowników. Zatem dbaj o nie, korzystaj z folderów dla Ciebie wyznaczonych, usuwaj zawartość z rozwagą, zapisuj dokumenty tylko w miejscach do tego przeznaczonych. Jesteś tutaj gościem i gospodarzem jednocześnie i tak się zachowuj.

Zatem, korzystaj ze wskazań i zdrowego rozsądku, żegluj w sieci bezpiecznie.

W. Salamon