Poradnik bezpieczeństwa mobilnego

FUNDACJA
nowoczesna
Polska

Poradnik bezpieczeństwa mobilnego

edukacja medialna

Koordynacja: Anna Gruhn
Autorzy: Radek Czajka i Jarosław Lipszyc
na podstawie scenariuszy autorstwa Małgorzaty Bazan
Redakcja merytoryczna: Wojciech Budzisz, Łukasz Wojtasik, Michał Woźniak
Korekta językowa: Paulina Choromańska
Obraz na okładce: Werner Moser, http://pixabay.com/pl/z-265130/, CC0

Ministerstwo Administracji i Cyfryzacji

Publikacja dofinansowana ze środków Ministerstwa Administracji i Cyfryzacji
Wydawca: Fundacja Nowoczesna Polska
Warszawa 2014

Spis treści

Wstęp

Lubisz się dzielić swoimi przemyśleniami, chętnie pokazujesz innym dobre wspomnienia, chwalisz się sukcesami. Z zapałem dyskutujesz na forach lub w mediach społecznościowych. Rzadko rozstajesz się z telefonem lub tabletem, dzięki którym jesteś w stanie szybko znaleźć poszukiwane miejsce, dobrać fajny filtr do zdjęcia, wysłać wiadomość do przyjaciół. Ale czy jesteś pewien, że Twoja „słit focia" z przyjaciółką trafiła tylko do waszych koleżanek? A może Twoim najlepszym kumplem nie jest wcale Piotrek, a latarka zainstalowana w Twoim telefonie? W końcu sporo o Tobie wie. Jest nawet w stanie ustalić, gdzie się znajdujesz.

Czy wiesz, ile wiedzą o Tobie Twoje ulubione aplikacje? Czy przekazałbyś te dane równie chętnie, gdyby zapytał o nie sprzedawca w sklepie albo przechodzień na ulicy?

Zajrzyj do naszego poradnika-samouczka, a inaczej spojrzysz na swoje ulubione narzędzia. Dowiesz się, jakie informacje o Tobie gromadzi i w jaki sposób je wykorzystuje. Samouczek podzieliliśmy na dziesięć działów. Każdy z nich składa się z pigułki wiedzy – krótkiego wprowadzenia, słowniczka, który wyjaśni trudniejsze pojęcia oraz linków do interesujących artykułów. Pokaż samouczek rodzicom - zawarte tam informacje mogą przydać się również im.

Przygotowaliśmy również specjalną aplikację „Mobilne bezpieczeństwo". Ściągniesz ją ze strony edukacjamedialna.edu.pl (znajduje się na dole strony, w sekcji Narzędzia). Możesz też pobrać ją z Google Play oraz platformy F-Droid.

Pewnie żałujesz, że takich rzeczy nie uczą w szkole... Zaproponuj swojemu nauczycielowi, aby przeprowadził lekcje na podstawie scenariuszy ze strony edukacjamedialna.edu.pl. Znajdzie tam aż 10 propozycji na interesujące zajęcia o bezpieczeństwie mobilnym!

Mamy nadzieję, że wszystkie przygotowane przez nas materiały będą dla Ciebie interesujące i przydatne.

Zespół Fundacji Nowoczesna Polska

Aplikacje

WIEDZA W PIGUŁCE

Aplikacja to program komputerowy instalowany na urządzeniu mobilnym. Urządzenia mobilne, takie jak tablet czy smartfon, to dokładnie takie same komputery jak laptopy czy urządzenia stacjonarne - tylko mniejsze. Programy te mogą mieć różny status. Wśród nich warto wyróżnić:

- aplikacje systemowe, niezbędne do działania systemu operacyjnego,
- aplikacje instalowane na naszych urządzeniach przez producentów i sieci telekomunikacyjne w celach promocyjnych (przy czym zazwyczaj użytkownik nie może ich sam usunąć),
- aplikacje instalowane przez użytkownika.

Nasze urządzenia dzięki aplikacjom pełnią różnorodne funkcje: programu komunikacyjnego, gry, czytnika e-booków, mapy itd. Komputer jest uniwersalną maszyną logiczną, a więc teoretycznie może pełnić dowolną funkcję - a co konkretnie dla nas robi zależy właśnie od zainstalowanego na nim oprogramowania.

Wiele aplikacji może stanowić zagrożenie dla bezpieczeństwa naszych danych. Są takie aplikacje, które żądają dostępu do najrozmaitszych informacji (np. kalendarza, listy kontaktów, lokalizacji), choć wcale nie powinny. Są też i takie, które generują dodatkowe koszty, wysyłając bez naszej wiedzy drogie SMS-y. Jeżeli raz zezwolimy aplikacji na dostęp i wysyłanie naszych danych do internetu, nasza kontrola nad tym, co faktycznie robi dana aplikacja, jest już niewielka. Dlatego zawsze instalując aplikację, należy zastanowić się, czy jest ona potrzebna i jakich uprawnień od nas żąda. Należy sprawdzić, kto jest jej autorem i zastanowić się, czy ufamy tej osobie lub firmie. Może się okazać, że ceną za możliwość pograna w atrakcyjną grę jest inwigilacja, sprzedaż naszych danych osobowych firmom marketingowym czy dodatkowe, niechciane opłaty.

Zazwyczaj, choć nie zawsze, najbezpieczniejsze jest wolne oprogramowanie, czyli aplikacje udostępnione wraz z **kodem źródłowym** na tzw. wolnej licencji – wtedy niezależni programiści mogą sprawdzić, co dany program naprawdę robi, jakie dane uzyskuje i komu je udostępnia. Pełną kontrolę nad aplikacjami pracującymi na naszym urządzeniu uzyskamy jednak dopiero instalując wolną (tj. będącą wolnym oprogramowaniem) wersję systemu operacyjnego, co jest zadaniem stosunkowo trudnym, a czasami wręcz niemożliwym.

SŁOWNICZEK

- **aplikacja**: (in.program użytkowy) konkretny, ze względu na oferowaną użytkownikom funkcjonalność, element oprogramowania użytkowego.
- **uprawnienie (aplikacji mobilnej)**: dostęp do informacji i funkcji urządzenia mobilnego oraz możliwość wykonywania określonych czynności (np. zmiany wpisu w kalendarzu).

CZYTELNIA

- http://www.spidersweb.pl/2013/12/uprawnienia-w-androidzie.html (dostęp: 30.12.2014)
- http://www.dobreprogramy.pl/Google-Play-upraszcza-system-uprawnien-aplikacji-Androida-dla-bezpieczenstwa-to-katastrofa,News,55231.html (dostęp: 30.12.2014)

Cyberprzemoc

WIEDZA W PIGUŁCE

Cyberprzemoc to różne formy agresji polegającej na wyśmiewaniu, publikacji kompromitujących materiałów, zastraszaniu czy poniżaniu innych osób.

W internecie agresja taka bywa bardzo dotkliwa. Informacje opublikowane w sieci bardzo trudno z niej usunąć, i bywa, że będą nam towarzyszyły już przez całe życie. Banalna kłótnia z przyjacielem może więc zostać w sieci na zawsze, dostępna dla każdego.

Efektem cyberprzemocy może być poczucie prześladowania lub ośmieszenia, życie w strachu, upokorzenie. Konsekwencje mogą być groźne: zamknięcie się w sobie, depresja, a w skrajnych przypadkach próby samobójcze. Dlatego należy zawsze przeciwdziałać przemocy w sieci, a osoby prześladowane trzeba wspierać i chronić.

W przypadku poważnych spraw należy zgłosić taki przypadek policji - w Polsce uporczywe nękanie innej osoby jest przestępstwem zagrożonym karą 3 lat więzienia.

Osoby dopuszczające się cyberprzemocy nazywamy „stalkerami", od angielskiego słowa „stalking" - skradać się.

SŁOWNICZEK

- **cyberprzemoc**: (inaczej: agresja elektroniczna), stosowanie przemocy poprzez: prześladowanie, zastraszanie, nękanie, wyśmiewanie innych osób przy pomocy narzędzi typu elektronicznego, np. SMS, e-mail, witryny internetowe, fora dyskusyjne. Osobę dopuszczającą się takich czynów określa się stalkerem.

CZYTELNIA

- Cyberprzemoc w: Bezpieczeństwo dzieci online. Kompendium dla rodziców i profesjonalistów (FDN 2014) http://dzieckowsieci.fdn.pl/bezpieczenstwo-dzieci-online-kompendium-dla-rodzicow-i-profesjonalistow (dostęp: 30.12.2014)
- Jak reagować na cyberprzemoc. Poradnik dla szkół (FDN 2011) http://dzieckowsieci.fdn.pl/podrecznik-jak-reagowac-na-cyberprzemoc (dostęp: 30.12.2014)

Higiena informacyjna

WIEDZA W PIGUŁCE

W ramach higieny osobistej kąpiemy się, myjemy zęby, pierzemy ubrania, obcinamy paznokcie. Te czynności bywają nużące, ale są niezbędne, jeśli chcemy żyć czyści i zdrowi. Podobnie niezbędne są zachowania związane z higieną informacyjną, czyli rozsądnym zarządzaniem naszymi informacjami.

Podstawowe nawyki hiegieny informacyjnej to m.in.:

- bardzo restrykcyjne i oszczędne gospodarowanie naszymi danymi osobowymi w sieci, żeby nie stać się ofiarą kradzieży tożsamości. Częste używanie pseudonimów;
- ograniczenie korzystania z „usług w chmurze", czyli dostępnych przez sieć, aby utrudnić ich właścicielom kontrolowanie naszej komunikacji z innymi. Jeśli to możliwe, to należy wybierać takich dostawców usług, którzy mają dobrą politykę prywatności (np. nie czytają naszych emaili). Szczególnie dotyczy to usług takich jak email, serwisy społecznościowe, czaty, strony do publikacji zdjęć i filmów, mapy. Jeśli musimy korzystać z takich usług unikajmy logowania, bo ono zawsze nas identyfikuje. Jeżeli natomiast korzystamy z usług zalogowani - zadbajmy o odpowiednie ustawienia prywatności, żeby ograniczyć ilość informacji udostępnianych innym osobom;
- tworzenie kopii zapasowych informacji na których nam zależy (w tym zdjęć, tekstów, nagrań itp.) - żeby ich nie utracić w przypadku awarii lub zagubienia urządzenia;
- porządkowanie naszych danych w plikach i folderach, żeby łatwo znaleźć informacje gdy będą nam potrzebne;
- szyfrowanie danych na twardych dyskach, także w komórce czy tablecie, żeby uniemożliwić nieuprawnionym osobom dostęp do nich (np. w przypadku kradzieży telefonu);
- blokowanie albo regularne kasowanie „ciasteczek" w przeglądarkach internetowych (także mobilnych), żeby utrudnić szpiegowanie firmom marketingowym;
- pozostawienie telefonu w domu lub wyjęcie baterii, jeśli chcemy mieć pewność poufności;
- zaklejenie nalepkami kamer w urządzeniu, jeśli z nich nie korzystamy;
- blokowanie reklam i skryptów w czasie korzystania z sieci, by utrudnić przejęcie kontroli nad naszym urządzeniem;
- korzystanie z technologii anonimizujących (takich jak np. Tor, proxy, tryb anonimowy w przeglądarce internetu), żeby uniknąć nadmiernej inwigilacji;
- szyfrowanie emaili i wiadomości, jeśli zależy nam na zachowaniu tajemnicy, korzystanie z podpisów cyfrowych.

Nawyki higieny informacyjnej, choć trochę czasochłonne, mają przede wszystkim chronić nas przed zagrożeniami - zgodnie z zasadą: „łatwiej jest zapobiegać niż naprawiać szkodę".

SŁOWNICZEK

- **higiena informacyjna**: zasady postępowania w sytuacjach udostępniania informacji (w tym w środowisku cyfrowym). Stosuje się je w celu ochrony przed zagrożeniami np. utratą prywatności, danych, inwigilacją itp. Zgodnie z zasadami higieny informacyjnej należy np. kasować ciasteczka po wylogowaniu z serwisów społecznościowych ani nie podawać swoich danych osobowych każdemu, kto o nie prosi.

CZYTELNIA

- Wyszukiwarki [w:] Bezpieczeństwo dzieci online. Kompendium dla rodziców i profesjonalistów (FDN 2014), dostępny online: http://dzieckowsieci.fdn.pl/bezpieczenstwo-dzieci-online-kompendium-dla-rodzicow-i-profesjonalistow (dostęp: 30.12.2014)
- http://panoptykon.org/wiadomosc/internet-wie-co-robisz (dostęp: 30.12.2014)
- http://www.panoptykon.org/wiadomosc/prywatnosc-zrob-sam (dostęp: 30.12.2014)

Komu ufasz

WIEDZA W PIGUŁCE

Większość ludzi ma dobre zamiary i nie zamierza zrobić nam krzywdy, ale niestety - nie wszyscy tacy są. Dlatego, tak samo jak na drodze, w sieci należy stosować „zasadę ograniczonego zaufania".

Kiedy komunikujemy się z nieznajomą osobą nie możemy być pewni, jakie ma zamiary i intencje. Sytuację, kiedy rozmawiamy z obcymi w sieci, można porównać do rozmowy na ulicy z przypadkowym przechodniem. Nie chwalimy się wtedy, ile zarabiamy, jakimi samochodami jeździmy, kiedy opuścimy mieszkanie, nie opisujemy swoich spraw prywatnych. W szczególności trzymamy w tajemnicy nasze miejsce zamieszkania, nazwiska, informacje o numerach legitymacji i innych dokumentach.

Istnieje wiele społeczności internetowych, które opierają się na wzajemnym zaufaniu - na forach tematycznych można poznać ciekawe osoby podzielające nasze pasje i zainteresowania. Jeśli zechcemy się z nimi spotkać zachowajmy rozsądek - podzielmy się z rodziną tą informacją, poinformujmy znajomych o miejscu i czasie spotkania, zabierzmy ze sobą przyjaciółkę czy kolegę.

Zasada ograniczonego zaufania dotyczy także komunikacji z firmami. Wiele z nich będzie chciało dowiedzieć się jak się nazywamy, gdzie mieszkamy, co nas pasjonuje i co kupujemy - np. w celach reklamowych. Nie udzialajmy takich informacji, jeśli nie jest to konieczne, a firma nie budzi naszego zaufania.

CZYTELNIA

- Śliwowski K., Prujszczyk G., Bezpieczeństwo informacyjne w sieciach 2.0 [PDF] dostępny w internecie: http://www.ceo.org.pl/sites/default/files/library-files/web20.pdf (dostęp: 30.12.2014)
- Badania GIODO „Postrzeganie zagadnień związanych z ochroną danych i prywatnością przez dzieci i młodzież" - omówienie wyników, http://www.giodo.gov.pl/560/id_art/4699/j/pl/ (dostęp: 30.12.2014)
- Raport z badań GIODO "Postrzeganie zagadnień związanych z ochroną danych i prywatnością przez dzieci i młodzież, http://panoptykon.org/sites/panoptykon.org/files/raport-koncowy-z-badan.pdf (dostęp: 30.12.2014)
- Uwodzenie dzieci w internecie i inne niebezpieczne kontakty, [w:] Bezpieczeństwo dzieci online. Kompendium dla rodziców i profesjonalistów (FDN 2014), dostępny online, http://dzieckowsieci.fdn.pl/bezpieczenstwo-dzieci-online-kompendium-dla-rodzicow-i-profesjonalistow (dostęp: 30.12.2014)

Kontrola nad urządzeniem

WIEDZA W PIGUŁCE

Komputery, a więc także komórki i tablety, są posłusznymi wykonawcami poleceń. Polecenia wydawane są komputerom w formie programów komputerowych. Od zakresu naszej kontroli nad urządzeniem zależy więc czyje polecenia komputer będzie wykonywał - nasze czy może jakiejś innej osoby.

Większość urządzeń dostępnych na rynku jest w dużym stopniu kontrolowana przez podmioty trzecie - producenta, twórcę systemu operacyjnego, operatora telekomunikacyjnego. Użytkownik nie ma wówczas dużego wpływu na to, co jego urządzenie faktycznie robi. Jako substytut takiej kontroli dostaje tylko ograniczoną możliwość personalizacji – może zmienić tapetę na pulpicie albo doinstalować kolejne aplikacje z odpowiedniego sklepu.

Kluczowy dla kontroli nad urządzeniem jest system operacyjny. Jednak nie mamy tutaj dużego wyboru - poza niszowymi obecnie systemami dla urządzeń mobilnych takimi jak FirefoxOS czy Sailfish/MeeGo, większość urządzeń działa pod systemami zamkniętymi, nie poddającymi się kontroli użytkowników.

Obecnie na rynku przeważają telefony z jednym z trzech najpopularniejszych systemów: Android, iOS oraz Windows. Każdy z tych systemów pozwala jego producentowi na pełną kontrolę nad urządzeniem użytkownika, np. Google czy Apple mogą zdalnie wyłączyć jego telefon, zaktualizować oprogramowanie, wymazać dane, usunąć wybrane aplikacje, a nawet sprawić, żeby nie było możliwe dalsze korzystanie z urządzenia. Producenci często też ograniczają użytkowników do aplikacji instalowanych z jednego konkretnego sklepu albo blokują pewne sposoby korzystania z filmów czy muzyki, np. zapisywanie ich na urządzeniu.

W przypadku systemu Android i iOS użytkownik może uzyskać dostęp administracyjny do swojego urządzenia (tzw. rootowanie lub jailbrake), co pozwala na większą kontrolę nad aplikacjami. Możliwe jest również zainstalowanie zupełnie innej wersji systemu operacyjnego. Może to być nowa wersja systemu tego samego producenta, ale w przypadku Androida dostępne są także wersje modyfikowane przez społeczność, które zazwyczaj lepiej dbają o bezpieczeństwo i prywatność użytkownika urządzenia.

Osobną kwestią jest kontrola nad aplikacjami. Zależnie od systemu operacyjnego, aplikacjom przyznajemy uprawnienia „z góry", podczas instalacji programu albo później, podczas korzystania z niego. W pierwszym przypadku otrzymujemy komunikat, że np. „aplikacja X" żąda dostępu do naszej książki adresowej oraz dostępu do sieci (wysyłanie i odbieranie danych) i możemy przyznać jej te uprawnienia i zainstalować aplikację albo nie zgodzić się na to i zrezygnować z instalacji. W obu przypadkach, jeżeli zgodzimy się przyznać aplikacji takie uprawnienia, to z technicznego punktu widzenia może ona bez przeszkód wysyłać np. dane kontaktowe naszych znajomych (do których teraz ma dostęp) do swojego producenta. Może się to odbywać w dowolnej chwili i bez naszej wiedzy. Tylko dobra wola autora takiego programu powstrzymuje go przed postępowaniem w ten sposób - my, jako użytkownicy, nie mamy już nad tym kontroli.

SŁOWNICZEK

- **operator telekomunikacyjny**: podmiot gospodarczy (przedsiębiorca) uprawniony do dostarczania publicznych sieci telekomunikacyjnych lub udogodnień towarzyszących.

- **system operacyjny**: oprogramowanie zarządzające systemem komputerowym, tworzące środowisko do uruchamiania i kontroli zadań użytkownika. W celu uruchamiania i kontroli zadań użytkownika system operacyjny zajmuje się: - planowaniem oraz przydziałem czasu procesora poszczególnym zadaniom, - kontrolą i przydziałem pamięci operacyjnej dla uruchomionych zadań, - dostarcza mechanizmy do synchronizacji zadań i komunikacji pomiędzy zadaniami, - obsługuje sprzęt oraz zapewnia równolegle wykonywanym zadaniom jednolity, wolny od interferencji dostęp do sprzę-

tu. Dodatkowe przykładowe zadania, którymi może, ale nie musi, zajmować się system operacyjny to: - ustalanie połączeń sieciowych, - zarządzanie plikami.

CZYTELNIA

- http://www.dobreprogramy.pl/Google-Play-upraszcza-system-uprawnien-aplikacji-Androida-dla-bezpieczenstwa-to-katastrofa,News,55231.html (dostęp: 30.12.2014)
- http://tech.wp.pl/kat,1031195,title,Uwaga-na-ten-telefon-fabrycznie-zainstalowany-szpieg,wid,16702676,wiadomosc.
- http://www.komputerswiat.pl/jak-to-dziala/2009/11/jak-szpieguja-aplikacje-z-app-store.aspx (dostęp: 30.12.2014)

Koszty

WIEDZA W PIGUŁCE

Kupowanie towarów przez internet pozwala na lepszy ich wybór i zakup po niższej cenie, ale wiąże się także z dodatkowymi problemami bezpieczeństwa.

Podczas zakupów w internecie musimy pamiętać, że płacenie zawsze oznacza zgodę na inwigilację - płatności elektronicznej nie da się zrobić anonimowo. Dotyczy to nie tylko kupowania towarów, ale także usług. Płatny dostęp do gry, filmu czy e-booka, także w formie abonamentu, oznacza automatycznie, że ktoś może nas zidentyfikować i podglądać - sprawdzać, co czytamy, oglądamy i słuchamy.

Należy zwrócić uwagę na to, żeby niechcący nie uruchomić opcji tzw. płatności w aplikacji. Jeśli bardzo, bardzo chcemy zapłacić za jakąś usługę (niech to będzie np. lepszy czołg w grze internetowej), to wymaga to wzmożonej ostrożności - łatwo bowiem stracić kontrolę nad kosztami, a pod koniec miesiąca może nas czekać przykra niespodzianka.

W przypadku urządzeń mobilnych niektóre płatności mogą być doliczane automatycznie do rachunku za telefon - i bardzo drogie. Są to np. SMS-y premium czy połączenia ze specjalnymi numerami. Dlatego nie odpowiadajmy na wiadomości przychodzące z nietypowych numerów telefonów i nie instalujmy aplikacji, które chcą korzystać z takich funkcji.

Zakupy zwykłych towarów przez internet są bezpieczne pod warunkiem, że stosujemy się do kilku podstawowych zasad. Oto one:

1. Korzystaj tylko ze sprawdzonych, renomowanych sklepów, serwisów aukcyjnych i wyszukiwarek internetowych. Każdy sklep powinien mieć zarejestrowaną działalność gospodarczą, podany na stronie adres, numer kontaktowy itp. Zawsze możesz też sprawdzić na stronach opinie użytkowników internetu o danym sklepie lub zajrzeć pod adresy: Centralnej Ewidencji Informacji o Działalności Gospodarczej, Krajowego Rejestru Sądowego (KRS). Przeczytaj również dokładnie regulamin sklepu, zwracając uwagę, czy możesz zwrócić lub reklamować dany produkt, gdy jest wadliwy.

2. Dokładnie obejrzyj towar. Sprawdź jego parametry, stan (np. czy jest uszkodzony, rozmiary ubrań, wielkość kanapy itp.), starannie czytaj opis i teksty „drobnym druczkiem", szczególną uwagę zwróć na koszty wysyłki.

3. Zamawiając, chroń swoje dane wrażliwe – sprawdź, czy pojawia się komunikat o szyfrowaniu transmisji danych (na pasku adresu w przeglądarce powinnien pojawić się symbol kłódki, a adres zaczynać od znaków „https://").

4. Nigdy nie zgadzaj się na marketingowe wykorzystanie swoich danych kontaktowych i osobowych.

SŁOWNICZEK

- **freemium**: model biznesowy, w którym produkt lub usługa (najczęściej oprogramowanie, gra komputerowa, usługa internetowa) jest dostępna za darmo, ale korzystanie z zaawansowanych funkcji lub uzyskanie niektórych wirtualnych dóbr wymaga wykupienia wersji premium.

- **free to play**: model płatności występujący w grach komputerowych, niewymagający kupna lub płacenia abonamentu.System F2P polega na kupowaniu (poprzez tzw. mikrotransakcje lub za pomocą karty płatniczej) opcjonalnych dodatków do gier, w sytuacji gdy znaczna część świata gry, rozgrywki czy fabuły jest darmowa. Dodatkami tymi mogą być też różnorakie przedmioty czy umiejętności, pomagające w dalszej grze lub ją usprawniające. Przykładem takiego usprawnienia jest przyspieszenie zdobywania doświadczenia lub ulepszenie jakiejś umiejętności na określony czas. W grach F2P można dokonywać płatności również za przedmioty czy usługi – z punktu widzenia rozgrywki – niepotrzebne, jak np. nowy ubiór lub maskotka czy też zmiana koloru włosów awatara lub zmiana wystroju domu. W niektórych grach free-to-play

gracze płacący za dodatkowe przedmioty i funkcje zdobywają dużą przewagę nad graczami niewydającymi pieniędzy. Takie gry określa się mianem pay-to-win („płać, aby wygrać").

- **premium (usługa)**: usługa o podwyższonej płatności np. sms. Wiadomości SMS Premium to najczęściej ciąg czterech lub pięciu cyfr zaczynający się od cyfry siedem lub dziewięć. Kolejne cyfry informują o koszcie wysyłanej wiadomości SMS.

CZYTELNIA

- http://www.spidersweb.pl/2014/02/gry-freemium-free2play.html (dostęp: 30.12.2014)
- http://di.com.pl/news/51114,0,Uwaga_na_Doladujeu_Zamiast_doladowania_dostaniesz_aktywacje-Marcin_Maj.html (dostęp: 30.12.2014)

Nawigacja i lokalizacja

WIEDZA W PIGUŁCE

Słowo „nawigacja" odnosiło się jeszcze niedawno wyłącznie do sposobów prowadzenia statków lub samolotów według wyznaczonej trasy. Służyły do tego specjalne urządzenia, np. kalkulator nawigacyjny lub trójkąt nawigacyjny. Najprostszymi urządzeniami nawigacyjnymi są kompasy i busole. Dziś słowo to zmieniło trochę zakres znaczeniowy i oznacza przede wszystkim znajdowanie drogi do celu dzięki ustaleniu pozycji naszego telefonu na Ziemi. A przy okazji naszej.

Nasz telefon potrafi całkiem nieźle orientować się w przestrzeni. Położenie telefonu można sprawdzić na trzy sposoby:

- poprzez komunikację ze stacjami przekaźnikowymi telefonii komórkowej GSM,
- poprzez sprawdzenie dostępnych w danym miejscu sieci bezprzewodowych Wi-Fi,
- poprzez namierzanie satelit systemu GPS.

Tylko ostatni z tych sposobów efektywnie służy jego użytkownikowi. Informacje o logowaniu telefonu do stacji GSM to informacje, z których korzystają operatorzy telekomunikacyjnych oraz policja i inne służby. Informacje o położeniu sieci Wi-Fi zbierają dostawcy oprogramowania (np. firma Google), o ile nie wyłączymy odpowiedniej opcji. My natomiast najczęściej korzystamy z globalnego systemu pozycjonowania - zazwyczaj amerykańskiego GPS, ale istnieją także rosyjski Glonass i europejski Galileo.

Urządzenia GPS działają dzięki sieci satelitów krążących nad Ziemią i nadających cyfrowy sygnał. Nasz odbiornik zna dokładną godzinę nadawania tych sygnałów oraz położenie satelitów. Mierząc czas potrzebny na dotarcie sygnału z kilku różnych satelitów do urządzenia, możemy określić swoją własną pozycję. Oczywiście, wszystko to dzieje się automatycznie.

Niektóre aplikacje będą prosiły o dostęp do danych o naszym położeniu, bo jest to istotą ich działania: program do nawigacji samochodowej, mapa albo rejestrator treningów sportowych. Inne będą o to prosiły, bo informacja o tym gdzie jesteśmy jest bardzo cenna marketingowo. Dzięki dokładnym danym o naszym położeniu wiadomo gdzie robimy zakupy, gdzie mieszkamy, gdzie jeździmy na wakacje. A także kiedy nie ma nas w domu. Dlatego powinniśmy odmawiać podawania danych geolokalizacyjnych, jeśli nie jest to uzasadnione.

Korzystając z aplikacji lokalizacyjnych, powinniśmy szczególnie pamiętać o higienie informacyjnej. Jeśli używamy np. programu do rejestracji treningów sportowych (takiego jak Endomondo czy Strava), włączajmy GPS dopiero w rozsądnej odległości od domu - inaczej nie tylko właściciel serwisu, ale także inni jego użytkownicy będą wiedzieli, gdzie mieszkamy.

Niestety, ponieważ istotą działania większości urządzeń mobilnych jest łączenie się z siecią poprzez GSM, jedynym sposobem na zachowanie całkowitej prywatności jest... pozostawienie ich w domu. O tym, że można podsłuchać rozmowę telefoniczną oczywiście wiadomo. Nie jest także tajemnicą, że policja może sprawdzić z kim się spotykamy - wystarczy przecież zebrać dane geolokalizacyjne wszystkich urządzeń mobilnych w jednej bazie danych i będzie wiadomo, kto i gdzie razem przebywa. Mniej osób wie, że dzięki urządzeniom mobilnym można podsłuchać i podejrzeć, co dana osoba robi, zdalnie uruchamiając mikrofon i kamerę telefonu. Wiadomo także, że istnieją złośliwe aplikacje umożliwiające taką inwigilację przestępcom.

Dlatego niektórzy nazywają komórkę „indywidualnym urządzeniem śledzącym".

SŁOWNICZEK

- **geolokalizacja**: określenie fizycznego położenia geograficznego osoby i urządzenia telekomunikacyjnego za pomocą systemu GPS lub adresu IP.

- **nawigacja (satelitarna)**: określanie bieżącego położenia oraz optymalnej drogi do celu dla ludzi, statków, pojazdów lądowych i innych przemieszczających się obiektów za pomocą sygnałówradiowych wysyłanych przez sztuczne satelity Ziemi. Przykładem nawigacji satelitarnej jest GPS.

CZYTELNIA

- Usługi geolokalizacyjne, [w:] Bezpieczeństwo dzieci online. Kompendium dla rodziców i profesjonalistów (FDN 2014), dostępny online: http://dzieckowsieci.fdn.pl/bezpieczenstwo-dzieci-online-kompendium-dla-rodzicow-i-profesjonalistow (dostęp: 30.12.2014)
- Śliwowski K., Prujszczyk G., Bezpieczeństwo informacyjne w sieciach 2.0 [PDF] dostępny w internecie: http://www.ceo.org.pl/sites/default/files/library-files/web20.pdf (dostęp: 30.12.2014) (dostęp: 30.12.2014)

Phishing i spam

WIEDZA W PIGUŁCE

Phishing i spam to dwie różne metody osiągnięcia zysku naszym kosztem.

Phishing jest rzadszym, ale znacznie groźniejszym zjawiskiem, w którym atakujący usiłuje przejąć naszą tożsamość, aby uzyskać jakąś korzyść. Najczęściej skuteczny atak phishingowy oznacza, że przestępca odchodzi z pieniędzmi, a my zostajemy z długami i koniecznością udowadniania, że jesteśmy ofiarami, a nie sprawcami.

Podstawową zasadą ochrony przed phishingiem jest ochrona danych wrażliwych, do których należą wszystkie dane osobowe: imię i nazwisko, adres, itp. Szczególnie chronić należy datę i miejsce urodzenia oraz nazwisko panieńskie matki, gdyż te dane służą najczęściej do weryfikacji tożsamości w bankach przy kontaktach przez telefon.

Nigdy też nie należy podawać nikomu numeru naszego konta bankowego czy karty. Hasła i kody do kont pocztowych lub serwisów społecznościowych również powinny być ścisłą tajemnicą.

Choć zasady te brzmią prosto i rozsądnie, to atakujący różnymi metodami starają się skłonić nas do ujawnienia tych informacji. Czasami jest to telefon, w którym nieznana ci osoba prosi o podanie hasła do emaila w jakiejś nie cierpiącej zwłoki sprawie służbowej. Innym razem jest to email, w którym bank albo serwis aukcyjny prosi o podanie hasła w celu „weryfikacji tożsamości". Osoby nieobeznane z procedurami bezpieczeństwa obowiązującymi w takich firmach często padają ofiarą całkiem prostych tricków socjotechnicznych. Bywa jednak, że atakujący naszą tożsamość budują skomplikowane, rozbudowane strony internetowe łudząco podobne do autentycznych lub poświęcają na zdobycie potrzebnych im informacji dużo czasu, rozbudowując swoją opowieść i zdobywając nasze zaufanie. Jedynym rozwiązaniem jest kategoryczna wierność zasadzie ochrony danych wrażliwych.

Bardzo ważne jest też zabezpieczenie naszych urządzeń przed nieuprawnionym dostępem, ochrona dostępu hasłem, szyfrowanie pamięci urządzenia (co jest standardową opcją w najnowszych wersjach systemów operacyjnych dla urządzeń mobilnych). Atakujący mając dostęp do naszego emaila, a czasem wręcz zapisanych w plikach numerów kont i haseł, będzie miał bardzo ułatwione zadanie.

Spam, czyli niezamówione wiadomości, to zjawisko mniej niebezpieczne, ale za to znacznie bardziej uciążliwe. Spam może być zarówno legalny (wtedy, gdy pochopnie zgodziliśmy się na otrzymywanie informacji handlowych), jak i nielegalny (gdy wysyłający spam pozyskał kontakt do nas w inny sposób i wykorzystuje go w celach reklamowych bez naszej zgody).

Warto zauważyć, że spam nie zawsze musi być reklamą produktu. Spamem są też np. wysyłane nam przez znajomych „łańcuszki szczęścia" i śmieszne zdjęcia, a także np. prośby o pomoc w ratowaniu bezdomych psów lub zbieraniu nakrętek od butelek. Najważniejszym wyróżnikiem spamu jest to, że wiadomość nie jest kierowana personalnie do nas, tylko do wielu osób, a nasza korzyść z jej otrzymania jest znikoma bądź żadna.

Skutecznymi metodami ochrony przed spamem jest:

- rygorystyczne nieudzialnie zgody na wysyłanie wiadomości handlowych i przetwarzanie danych osobowych (do czego będzie nas namawiać większość przedsiębiorców podpisujących z nami jakiekolwiek umowy, włącznie z operatorami telefonii komórkowej);
- stosowanie filtru antyspamowego w poczcie elektronicznej;
- korzystanie z blokady reklam (np. AdBlock) w wyszukiwarce.

Szczególną uwagę należy zwracać na konkursy promocyjne. Szansa na wygranie odkurzacza jest dla większości osób wystarczającą obietnicą, żeby podały swój adres i zgodę na wysyłanie spamu. Starajmy się unikać takich pokus, bo adres który raz dostał się do spamerskiej bazy danych będzie wykorzystywany stale.

Nie należy także odpowiadać na spam, klikać w linki zamieszczone w podejrzanych wiadomościach ani wyłączać mechanizmów ochrony wbudowanych w klientów poczty, takich

jak blokada ładowania zewnętrznych obrazków. Wszelkie takie działania tylko niepotrzebnie przekazują spamerom dodatkowe informacje o adresacie.

SŁOWNICZEK

- **phishing**: (in. spoofing) wyłudzanie poufnych informacji osobistych (np. haseł lub szczegółów karty kredytowej) przezpodszywanie się pod godną zaufania osobę lub instytucję, której te informacje są pilnie potrzebne (np. Twój bank). Jest to rodzaj ataku opartego na inżynierii społecznej, tzn. wykorzystujący naszą nieuwagę, zaufanie do danej instytucji i często odruchowe działania.
- **spam**: niechciane, niepotrzebne, niezamówione wiadomości elektroniczne. Zwykle wysyłane za pośrednictwem e-maila i dużych serwisów społecznościowych. Spam ma najczęściej (ale nie zawsze) charakter reklamowy.

CZYTELNIA

- http://di.com.pl/news/51114,0,Uwaga_na_Doladujeu_Zamiast_doladowania_dostaniesz_aktywacje-Marcin_Maj.html
- http://www.cert.pl//news/8999/langswitch_lang/pl (dostęp: 30.12.2014)
- http://www.mbank.pl/aktualnosci/post,5928,mbank-i-zwiazek-bankow-polskich-ostrzegaja-uwaga-na-nowego-wirusa.html (dostęp: 30.12.2014)
- http://di.com.pl/news/50901,0,Dzwonia_z_propozycja_reklamy_w_sieci_Ta_rozmowa_moze_kosztowac_600-700_zl-Marcin_Maj.html (dostęp: 30.12.2014)

Uzależnienia

WIEDZA W PIGUŁCE

Uzależnienia możemy podzielić na trzy grupy:

- fizjologiczne – od nikotyny, alkoholu, środków odurzających;
- psychiczne – od internetu, gier hazardowych, kupowania, słodyczy, pracy;
- społeczne – pojawiające się pod wpływem nacisku grupy, do której uzależniony należy.

Uzależnienie od internetu, czy też szerzej od obsesyjnego korzystania z urządzeń komputerowych, jest stosunkowo nowym zjawiskiem i lekarze dopiero badają jego przyczyny, fizjologiczne podstawy oraz metody leczenia.

Oczywiście to, że często korzystamy z komórki do sprawdzania wpisów w sieciach społecznościowych albo dużo gramy w gry komputerowe, nieoznacza, że jesteśmy uzależnieni. Warto jednak wiedzieć, że istnieje takie uzależnienie, by w razie potrzeby zwrócić się o pomoc lekarską.

Lekarze opisują zespół uzależnienia od internetu jako sytuację, w której osoba uzależniona pozbawiona dostępu do urządzeń elektronicznych odczuwa niepokój, lęk, frustrację, gniew itd. Często w takich sytuacjach pojawiają się problemy w pracy i w szkole, zmiana relacji z bliskimi, porzucenie nawyków higienicznych. W efekcie spędzania długich godzin przed monitorem jesteśmy niewyspani, nie myślimy logicznie, nie potrafimy się skoncentrować. Na świecie odnotowano wręcz przypadki śmierci z powodu przemęczenia organizmu po kilku dniach bezsennego spędzania czasu z komputerem.

Osoby uzależnione od internetu, podobnie jak np. alkoholicy, bardzo często nie przyznają się do problemu albo go po prostu nie widzą. Częściej uzależnienie zauważają bliscy.

Niewątpliwie korzystanie z technologii komunikacyjnych nie pozostaje bez wpływu na nasz organizm. Korzystanie z mediów elektronicznych (w tym telewizora) wieczorem i w nocy powoduje zaburzenia cyklu dobowego i utrudnia zdrowy sen. Lekarze badający osoby grające w różnego typu gry komputerowe sprawdzili, że w trakcie i po sesjach angażujących rozgrywek zmienia się fizjologia organizmu. Pomimo braku wysiłku fizycznego tętno przyspiesza, zwiększa się ciśnienie krwi i następuje zwiększone wydzielanie adrenaliny (co może być przyczyną uzależnienia).

Twórcy gier i serwisów internetowych angażują specjalistów od projektowania takich rozwiązań, które skłonią nas do poświęcenia ich produktom jak najwięcej czasu - gdyż to przekłada się na ich zysk. Choć większości z nas daleko do uzależnienia, to warto mieć świadomość, że jest to rodzaj manipulacji. A w korzystaniu z urządzeń elektronicznych należy zachować... rozsądek.

SŁOWNICZEK

- **uzależnienie od internetu**: zespół uzależnienia od internetu (ZUI, uzależnienie od internetu; ang. Internet Addiction Disorder, IAD) – syndrom uzależnienia się użytkownika internetu od wielogodzinnego obcowania w tym środowisku. ZUI nie jest jeszcze uznaną jednostką chorobową, choć zwraca nań uwagę wielu psychiatrów.

CZYTELNIA

- Nadużywanie internetu, [w:] Bezpieczeństwo dzieci online. Kompendium dla rodziców i profesjonalistów (FDN 2014), dostępny online: http://dzieckowsieci.fdn.pl/bezpieczenstwo-dzieci-online-kompendium-dla-rodzicow-i-profesjonalistow (dostęp: 30.12.2014)

Wstęp do twojej prywatności

WIEDZA W PIGUŁCE

Gabriel Garcia Marquez, pisarz kolumbijski i laureat nagrody Nobla, powiedział:

> Każdy z nas ma trzy życia: życie publiczne, życie prywatne, i życie sekretne.

Życie publiczne prowadzimy wśród innych - w pracy i w szkole, w sklepie i na koncercie. Życie prywatne prowadzimy wśród bliskich - z rodziną, przyjaciółką, chłopakiem. Życie sekretne jest tylko nasze.

Fakt, że mamy życie sekretne, jest całkowicie naturalny. Dotyczy to zarówno spraw ważnych, jak nasze emocje czy błędy, jak i nieważnych. Bo, jak powiedział Cory Doctorow, brytyjski pisarz science-fiction:

> Nie chodzi o to, że Pan nie wie, co ja robię w ubikacji. Chodzi o to, że ja nie chcę, by Pan na to patrzył.

Każdy z nas ma prawo do życia publicznego, do życia prywatnego i do życia sekretnego.

Słownik języka polskiego definiuje słowo „prywatny" jako:

- stanowiący czyjąś osobistą własność,
- niepodlegający państwu ani żadnym instytucjom publicznym,
- dotyczący czyichś spraw osobistych i rodzinnych.

Prywatność to tyleż samo co nieformalność, kameralność, nieoficjalność, poufność, intymność.

Pierwsze nowoczesne spostrzeżenia dotyczące prawa jednostki do prywatności pojawiły się w 1890 roku w Stanach Zjednoczonych, kiedy to dwaj profesorowie prawa, Brandeis i Warren, pisali o prawie do tajemnicy, samotności, wyłączności. We współczesnym świecie często zapominamy, że prywatność jest wartością. Przypominamy sobie czasami, gdy przeczytamy o złamaniu prywatności aktorów i celebrytek, chociażby przez natrętnych fotografów. Dopiero gdy coś tracimy, zdajemy sobie sprawę z tego, jak bardzo to jest cenne.

Naszą prywatność, przynajmniej teoretycznie, chroni państwo, bo wynika to z praw przysługujących każdemu obywatelowi. Artykuł 47 Konstytucji Rzeczpospolitej Polskiej mówi wprost: „Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym". Jednak w praktyce zachowanie prywatności jest coraz trudniejsze, a jej ochrona - iluzoryczna. Kamery nagrywające nasze życie instalowane są w szkołach, firmach, sklepach, autobusach, pociągach, na ulicach. Urządzenia komunikacyjne, z których korzystamy, z jednej strony ułatwiają nam życie pozwalając na pracę, naukę i zabawę przez elektroniczne media, z drugiej zaś działają jak idealne „czarne skrzynki" rejestrujące każdą naszą życiową aktywność. Publiczną, prywatną i sekretną.

A jeśli taka informacja jest zapisana, to ktoś, kiedyś może z niej skorzystać. I nie zawsze w naszym interesie.

SŁOWNICZEK

- **wizerunek**: sposób, w jaki ktoś postrzega sam siebie lub jak widzą go inne osoby.
- **prywatność**: sfera życia człowieka, w którą nie należy wkraczać bez pozwolenia. Ma ona swój aspekt cielesny, terytorialny, informacyjny i komunikacyjny. Prywatność jest chroniona przez prawo (m.in. przez Konstytucję RP i akty prawa międzynarodowego). Ograniczenie prawa do prywatności możliwe jest tylko w określonych sytuacjach (na przykład ze względu na bezpieczeństwo publiczne czy ochronę zdrowia).

CZYTELNIA

- Seria poradników Fundacji Dzieci Niczyje na temat prywatności: http://dzieckowsieci.fdn.pl/poradniki (dostęp: 30.12.2014)
- http://www.panoptykon.org/wiadomosc/co-warto-wiedziec-o-sledzeniu-i-profilowaniu-w-sieci (dostęp: 30.12.2014)
- G. Prujszczyk, K. Śliwowski, Komunikacja, http://www.panoptykon.org/sites/panoptykon.org/files/panoptykon_poradnik_komunikacja.pdf (dostęp: 30.12.2014)
- G. Prujszczyk, K. Śliwowski, Browsing "wirtualne" zagrożenie, http://www.panoptykon.org/sites/panoptykon.org/files/panoptykon_poradnik_browsing.pdf (dostęp: 30.12.2014)