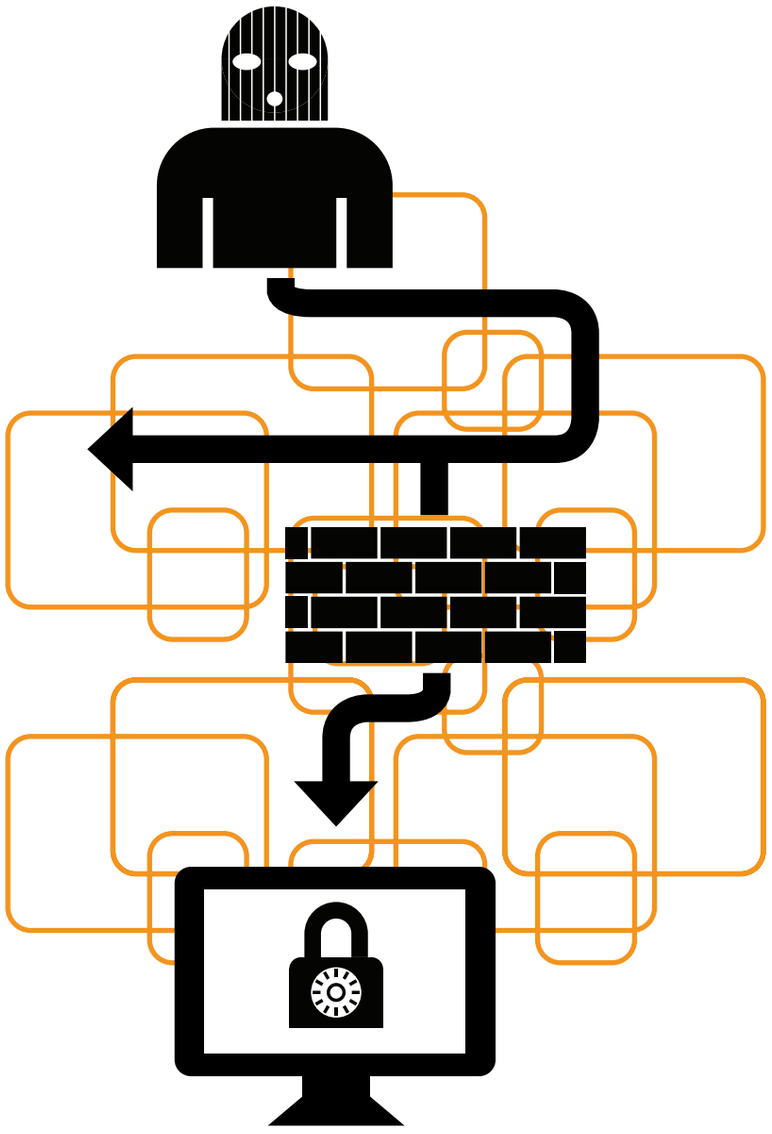


Bezpieczeństwo w sieci

3 WARSZTATY NA TEMAT BEZPIECZNEGO KORZYSTANIA Z INTERNETU
MATERIAŁ DYDAKTYCZNY

INNOWACYJNA GOSPODARKA
NARODOWA STRATEGIA SPÓJNOŚCI

MIASTA W INTERNECIE Stowarzyszenie

Ministerstwo Administracji i Cyfryzacji

UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ ROZWOJU REGIONALNEGO

Projekt współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka

POLSKA CYFROWA RÓWNYCH SZANS

Poradnik „bezpieczeństwo w sieci” opracowany został w ramach projektu POLSKA CYFROWA RÓWNYCH SZANS jako pomoc metodyczna dla Latarników Polski Cyfrowej, prowadzących zajęcia wprowadzające w cyfrowy świat osoby z pokolenia 50+.

Wydawnictwo jest wynikiem warsztatów przeprowadzonych
w Krasnobrodzie 9 kwietnia 2014r.

WYDAWCA: Stowarzyszenie „Miasta w Internecie”, 2014

AUTORZY: Dorota Gałan (Rightclick.pl), Sylwia Jakimiak (Rightclick.pl)
REDAKCJA: Magda Jackowska
PROJEKT GRAFICZNY: Jerzy Parfianowicz

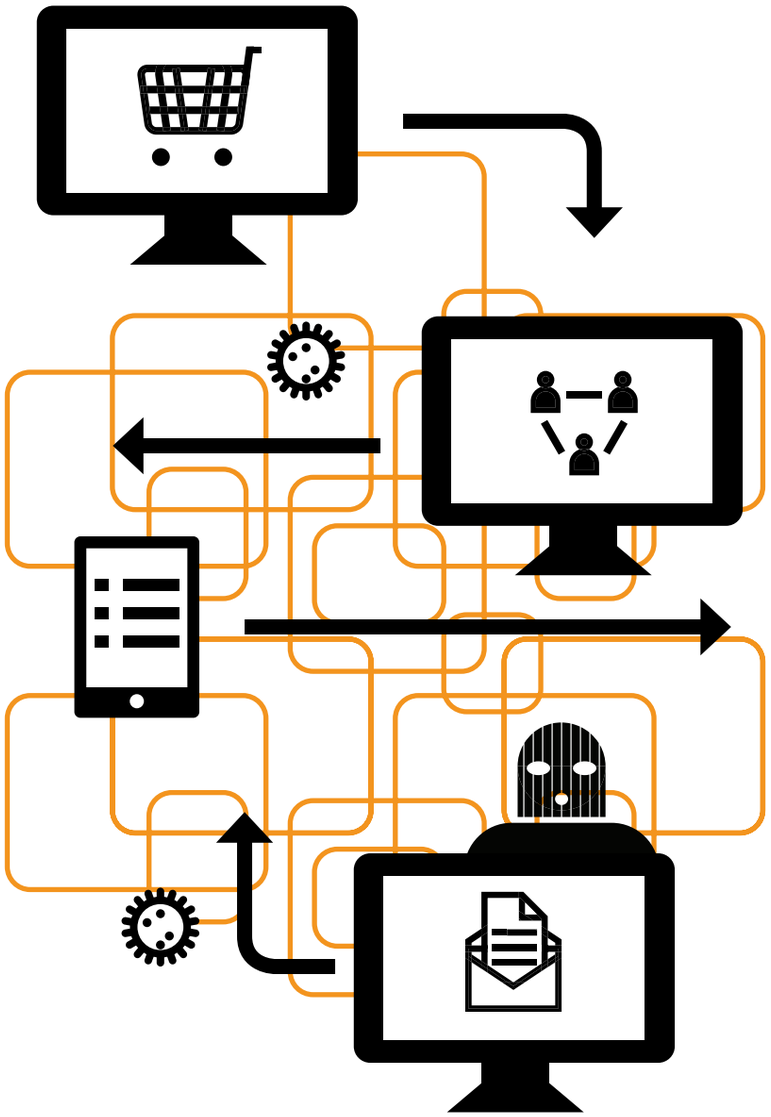
▹ Cel szkolenia

Głównym celem naszego poradnika jest uświadomienie Latarnikom Polski Cyfrowej tego, jak ważne jest bezpieczeństwo w Internecie. Przedstawimy praktyczne porady, zasady, reguły postępowania w siedmiu modułach tematycznych.

Zakładamy, że po lekturze Latarnicy będą wyposażeni w wiedzę i umiejętności pozwalające na dostateczne zabezpieczenie się w sieci Internet przed cyberzagrożeniami, a także na przekazanie zdobytych przez siebie informacji osobom w wieku 50+.

Mamy głęboką nadzieję, iż rezultaty naszych działań będą ujawniać się długo po zakończeniu projektu, a Latarnicy Polski Cyfrowej zaszczepieni zostaną gotowością autoedukacji w tematyce związanej z bezpiecznym i rozwojowym korzystaniem z Internetu.

Przełoży się to na ich bezpieczne funkcjonowanie w cyberświecie, który jest światem równoległym w stosunku do świata rzeczywistego. Umiejętności, z którymi chcemy zapoznać Latarników Polski Cyfrowej, będą niezbędne w dalszych etapach ich pracy z pokoleniem 50+.



Wstęp

Dzięki rozwojowi Internetu i stale zwiększającej się komunikacji pomiędzy połączonymi w sieć komputerami staliśmy się uczestnikami najbardziej przełomowego zdarzenia technologicznego od czasu okiełznania ognia.

John Perry Barlow, 1995 [1]

Żyjemy w otoczeniu nowych technologii: komputerów, telefonów komórkowych, smartphonów, tabletów, gier wideo, odtwarzaczy mp3 i wszystkich innych technologicznych wytworów XX i XXI wieku. Większość łączy się z Internetem, który dostarcza nam niewątpliwie wiele rozrywki, ale stanowi również źródło pewnego rodzaju zagrożeń tzw. cyberzagrożeń.

Cyfrowy świat wywołuje zmiany szybko. Jeszcze kilkanaście lat temu to potrzeby człowieka generowały nowe, unikatowe rozwiązania, dzisiaj to technologia współczesnego świata generuje w nas nieznane nam dotąd potrzeby.

Te zachodzące zmiany niezaprzeczalnie niosą za sobą wiele korzyści, ale czy jako społeczeństwo przygotowani jesteśmy na zagrożenia wynikające z tak ekspresowo zachodzącego postępu technologicznego?

Odpowiedzią na to pytanie jest niewątpliwie edukacja medialna, a takie przykłady zagrożeń jak: kradzież tożsamości internetowej, zachwiana anonimowość online, manipulacja reklamowa, problemy z e-bankowością, e-zakupami oraz bezpieczeństwem urządzeń mobilnych itp, zwracają nam uwagę jak ważna jest rola edukacji całego społeczeństwa w kierunku bezpiecznego korzystania z sieci internetowej. ▪

1 http://centrum.tl.krakow.pl/?start=artykuly

▹ Cel Poradnika

Głównym celem naszego poradnika jest uświadomienie Latarników Polski Cyfrowej o tym jak ważne jest bezpieczeństwo w Internecie. Przedstawimy praktyczne porady, zasady, reguły postępowania w siedmiu modułach tematycznych.

Zakładamy, że po lekturze Latarnicy będą wyposażeni w wiedzę i umiejętności pozwalające na dostateczne zabezpieczenie się w sieci Internet przed cyberzagrożeniami, a także na przekazanie zdobytych przez siebie informacji osobom w wieku 50+.

Mamy głęboką nadzieję, iż rezultaty naszych działań będą ujawniać się długo po zakończeniu projektu, a Latarnicy Polski Cyfrowej zaszczepią się chęcią autoedukacji w tematyce związanej z bezpiecznym i rozwojowym korzystaniem z Internetu.

Przełoży się to na ich bezpieczne funkcjonowanie w cyberświecie, który jest światem równoległym w stosunku do świata rzeczywistego. Umiejętności, z którymi chcemy zapoznać Latarników Polski Cyfrowej, będą niezbędne w dalszych etapach ich pracy z pokoleniem 50+. ▪

Anonimowość w sieci

Temat anonimowości w sieci jest dosyć trudny. Przede wszystkim należy zadać sobie pytanie, czy istnieje takie zjawisko jak anonimowość w świecie online? Wiele osób przyzna, iż sam fakt poruszania się w świecie wirtualnym zaprzecza utrzymaniu anonimowości, gdyż każdy krok zostawia tak zwany „cyfrowy ślad". Nie ważne czy jesteśmy aktywnymi użytkownikami, twórcami internetowymi czy biernymi molami sieciowymi – każda, nawet najmniejsza aktywność przyczynia się do utraty naszej anonimowości. Z góry musimy założyć, że wszystko co publikujemy w Internecie na własny temat jest PUBLICZNE. Bez odpowiednich zabezpieczeń, KAŻDY może mieć dostęp do naszych haseł, loginów czy chociażby prywatnych zdjęć.

Jak i dlaczego jesteśmy śledzeni?

Internet stał się nie tylko centrum rozrywki czy kanałem komunikacji, ale również sklepem spożywczym, bankiem czy też świetnym miejscem na reklamę. Pewnym instytucjom bardzo zależy na tym aby dobrze znać użytkowników w sieci, dlatego „kategoryzują" użytkowników i przypisują ich do pewnych grup np. osoby samotne, osoby zainteresowane modą, rodzice, fanatycy zdrowego trybu życia itp. W jaki sposób jesteśmy kategoryzowani?

Wchodzisz na stronę „x" i zostawiasz informację skąd przychodzisz.

↓

Poruszasz się po witrynie i podpowiadasz administratorowi co Cię interesuje, jakie są Twoje poglądy, preferencje itp.

↓

Strona przypisuje Ci „ciasteczko" – niewielką informację, która zapisuje się w Twojej przeglądarce.

Ciasteczko to Twój mały sieciowy ślad, które ma dobre i złe strony. Ciasteczka (z ang. cookies) pozwalają m.in:

- Zapamiętywać odwiedziny danej strony oraz nasze preferencje (ustawienia, kolory, układ itp.)
- Wskazują np. sklepom internetowym jakie produkty nas interesują
- Zapamiętują nasz „koszyk" zakupów w sklepie online
- Pomagają reklamodawcom dostosowywać reklamy do naszych upodobań
- Pomagają administratorom prowadzić statystyki witryny – kto, kiedy, dlaczego, w jakim celu korzysta z określonej strony www

Surfując w Internecie zostawiasz szereg danych o sobie, swojej rodzinie, preferencjach, upodobaniach, poglądach. Niektóre z tych danych udostępniamy nieświadomie, a niektóre świadomie, ale nierozważnie. Jakie to są dane?

Informacje udostępniane nieświadomie:

1. AUTOMATYCZNIE np. numer IP komputera, język, info o systemie operacyjnym, przeglądarce, zainstalowane czcionki, data zrobionego zdjęcia itp.

2. PÓŁAUTOMATYCZNIE np. geolokalizacja – wskazanie miejsca, w którym się aktualnie znajdujesz. Opcje geolokalizacji są często zainstalowane w telefonach typu SMARTPHONE.

Informacje udostępniane świadomie, ale często nierozważnie:

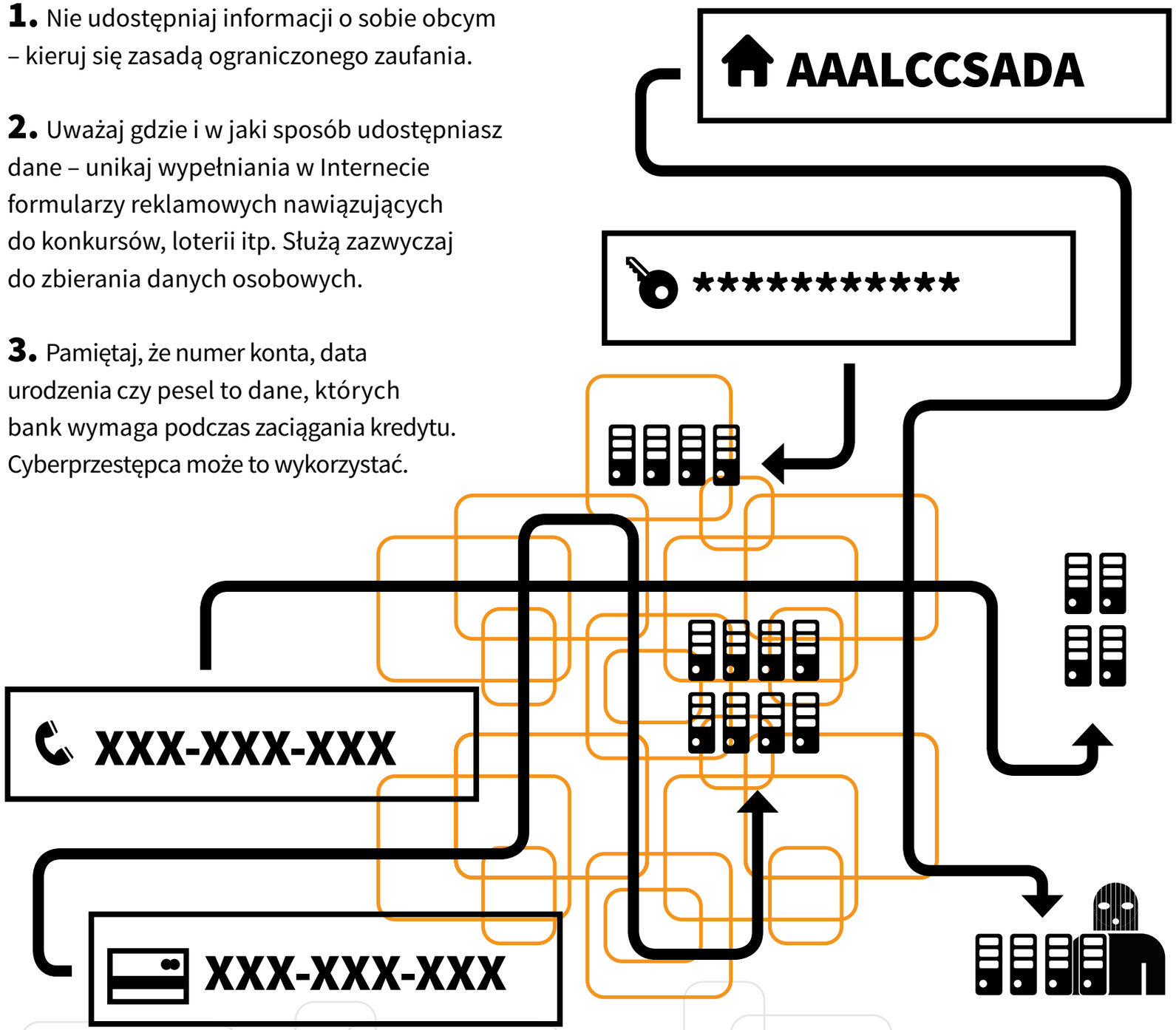
- Numer telefonu
- Adres e-mail
- Numer konta
- Pesel
- Data urodzenia

Na co należy uważać podczas udostępniania danych na swój temat:

1. Nie udostępniaj informacji o sobie obcym – kieruj się zasadą ograniczonego zaufania.

2. Uważaj gdzie i w jaki sposób udostępniasz dane – unikaj wypełniania w Internecie formularzy reklamowych nawiązujących do konkursów, loterii itp. Służą zazwyczaj do zbierania danych osobowych.

3. Pamiętaj, że numer konta, data urodzenia czy pesel to dane, których bank wymaga podczas zaciągania kredytu. Cyberprzestępca może to wykorzystać.



Prywatność na facebooku

Najbardziej popularny portal społecznościowy jakim jest Facebook stanowi jednocześnie jeden z największych agregatów danych osobowych ludzi z całego świata. Dane te służą nie tylko portalowi, ale również agencjom marketingowym czerpiącym zyski z reklam oraz przestępcom internetowym. Wiele osób ma rację twierdząc, że dzięki informacjom zdobytym o danej osobie na Facebooku, można włamać się do jej mieszkania, wziąć kredyt w banku czy ukraść samochód.

Zakładając konto na FB akceptujemy regulamin, który z każdym rokiem jest coraz dłuższy i zawiera coraz więcej punktów dotyczących danych osobowych, prywatności i bezpieczeństwa. Z jednej strony serwis zbiera informacje o swoich użytkownikach mając ku temu pewne powody, z drugiej jesteśmy narażeni na niebezpieczeństwa pochodzące ze strony innych użytkowników. Co powinniśmy wiedzieć o Facebooku i ochronie własnej prywatności?

Jakie dane zbiera o nas facebook?

- Informacje dotyczące czasu i miejsca wykonywanych zdjęć czy filmów, które udostępniamy na swoim profilu (tzw. metadane).
- Dane z systemu GPS lub inne informacje o lokalizacji „aby móc Cię poinformować, czy w pobliżu znajduje się ktoś spośród Twoich znajomych”.
- Dane, które ułatwiają obsługę reklam, rozumienie aktywności w sieci. Reklamodawca może przekazać nam informacje o Tobie (np. o Twojej reakcji na reklamę na Facebooku lub w innej witrynie), aby określić efektywność reklamy i podnieść jej jakość.

Istnieje kilka podstawowych zasad bezpieczeństwa na Facebooku. Warto zapoznać się i wcielić w życie wszystkie z nich:

- Nie publikuj swoich danych osobowych, szczególnie danych wrażliwych.
- Pamiętaj aby ustanowić mocne, trudne hasło dostępu do konta.
- Nie publikuj kompromitujących zdjęć i filmów.
- Nie udostępniaj zdjęć na których w tle pokazany jest twój dom, samochód itp.
- Regularnie sprawdzaj co nowego w zakładce ustawienia prywatności.
- Grupuj znajomych na bliższych i dalszych.
- Ignoruj podejrzane wiadomości. Często mają na celu wyłudzenie danych lub rozsyłanie złośliwego oprogramowania.
- Nie dawaj żadnej aplikacji uprawnień przed jej weryfikacją.
- Uważaj kogo dodajesz do znajomych
- Pamiętaj, aby zawsze po zakończeniu korzystania z FB wylogować się z konta. ▪

Ustawienia prywatności Google

Wielu osobom Internet kojarzy się głównie z Google – najpopularniejszą wyszukiwarką internetową. Jak się okazuje, Google to nie tylko wyszukiwarka, ale również m.in. elektroniczna poczta gmail, kalendarz, prywatny album zdjęć albo mapa. Zakładając jedno konto, mamy dostęp do wszystkich usług Google. Korzystając ze wszystkich możliwości lub chociażby z samego konta pocztowego, dostarczamy firmie (i nie tylko jej) dane dotyczące całego naszego życia. Co mogłoby się okazać gdyby ktoś uzyskał nieuprawniony dostęp do naszego konta?

Poniżej przedstawiamy kilka prostych rad, jak lepiej chronić się w Google:

1. Jeśli korzystasz z Internetu w miejscu publiczym warto włączyć „Tryb Incognito"

Jak to zrobić?

Google → Prywatność i warunki → tryb incognito

- W trybie incognito otwierane strony internetowe i pobierane pliki nie są rejestrowane w historii przeglądania ani pobierania.
- Wszystkie nowe pliki cookies są kasowane po zamknięciu wszystkich otwartych okien incognito.

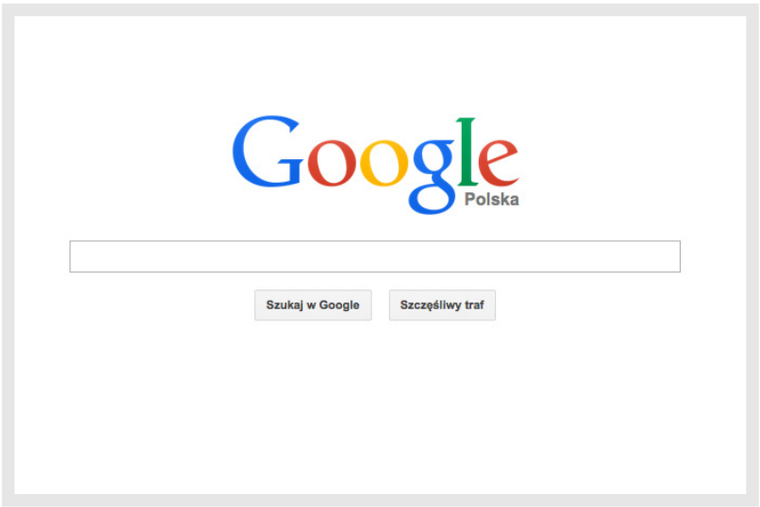
2. Włącz weryfikację dwuetapową

Dla wszystkich, którzy posiadają konto pocztowe GMAIL przydatną funkcją może być WERYFIKACJA DWUETAPOWA. Tutaj dodatkową formą zabezpieczenia przed włamaniem się na nasze konto jest numer naszego telefonu komórkowego. Aby zalogować się do konta Google, system poprosi Cię o dodatkowe zabezpieczenie w postaci kodu wysłanego na Twój telefon komórkowy. Jeśli ktoś spróbuje włamać się na Twoje konto, będzie musiał znać nie tylko login i hasło, ale również kod widniejący na wyświetlaczu komórki.

„Aby włamać się na konto z weryfikacją dwuetapową, przestępca musiałby nie tylko znać Twoją nazwę użytkownika i hasło, ale także uzyskać dostęp do telefonu".

Jak włączyć weryfikację dwuetapową?

Google → Prywatność i warunki → Weryfikacja dwuetapowa



Sceptycy tej metody uważają, iż podawanie z sieci swojego numeru telefonu jest jeszcze bardziej niebezpieczne niż brak weryfikacji dwuetapowej. Najlepszym rozwiązaniem zatem jest posiadanie dwóch numerów telefonów – jeden na potrzeby weryfikacji dwuetapowych, drugi do prywatnego użytkowania. ▪

Bezpieczne zakupy online

Coraz więcej osób robi zakupy w Internecie. Powody są różne: niższe ceny, szybka dostawa, łatwość dostępu do rzeczy unikatowych, możliwość zapoznania się z opiniami innych internautów na temat produktu, który nas interesuje, wygoda itd. Istnieje zapewne wiele plusów robienia zakupów online, ale musimy pamiętać, że transakcje dokonywane w sieci to wystawianie wielu informacji na światło dzienne. Jeśli numery naszych kart kredytowych lub kont internetowych, dane wrażliwe tj. imię, nazwisko trafią w niepowołane ręce, może mieć to dla nas przykre konsekwencje. Jak zatem zadać o to aby zakupy online były nie tylko przyjemne i wygodne, ale przede wszystkim pozbawione niebezpieczeństw?

8 Zasad Bezpiecznych Zakupów Online:

1. Sprawdź czy sklep posiada protokół SSL szyfrujący dane potrzebne do dokonania zakupu. Na początku adresu witryny powinien widnieć „https" zamiast „http". Szukaj również symbolu zamkniętej KŁÓDKI.

2. Zawsze czytaj regulamin sklepu internetowego.

3. Nie rób zakupów online korzystając z publicznych komputerów.

4. Zaktualizuj swój program antywirusowy przed dokonaniem zakupu. Zminimalizuje to ryzyko wycieku Twoich danych osobowych, numeru karty kredytowej itp.

5. Sprawdź opinie o sklepie/sprzedawcy. Zwróć uwagę na liczbę tych opinii i ich wiarygodność.

6. Sprawdź dane kontaktowe i identyfikacyjne sprzedawcy: nazwa sklepu, adres, numer telefonu czy e-mail. Gdy mamy jakiekolwiek wątpliwości co do rzetelności sklepu warto zadzwonić i zadać kilka pytań, np. o czas dostawy czy sposoby płatności.

7. Zachowaj korespondencję ze sprzedawcą do czasu zakończenia transakcji sukcesem.

8. Przy odbiorze sprawdź zakup, a później wyciąg z karty kredytowej lub stan konta

Zakupy online a prawo

Jeśli kupujesz w sieci, powinieneś znać swoje prawa. Mądre powiedzenie brzmi: przezorny zawsze ubezpieczony.

Masz prawo do:

- **Pisemnego potwierdzenia** informacji o dokonaniu zakupu. Warto **wydrukować stronę**, na której pojawia się potwierdzenie złożenia zamówienia.
- **Odstąpienia od umowy** w ciągu 7 dni roboczych (w Polsce 10 dni kalendarzowych) bez ponoszenia dodatkowych kosztów (z wyjątkiem kosztów zwrotu towaru do sprzedawcy).
- **W razie problemów ze sklepem, można zgłosić sprawę do Europejskiego Centrum Konsumenckiego. http://www.konsument.gov.pl/**

Nie masz prawa do:

- Prawa do odstąpienia **nie stosuje się** m.in. do umów o **usługi zakwaterowania, transportu, turystyczne** oraz **zakupu przez licytację.** ▪

Bezpieczne ustawienia w przeglądarkach

Nie udałoby się korzystać z Internetu gdyby nie przeglądarki internetowe takie jak np. Mozilla Firefox, Internet Explorer, Opera czy Google Chrome. Często posiadamy domyślne ustawienia przeglądarek, nie zdając sobie sprawy, że oferują nam one szereg opcji bezpieczeństwa i tylko od nas zależy co zostanie włączone a co wyłączone.

Prywatność i bezpieczeństwo w Mozilla Firefox

Jeśli korzystasz z przeglądarki Mozilla Firefox zajrzyj do górnego MENU, a następnie:

Narzędzia → Opcje → Prywatność i bezpieczeństwo

3 Zasady Główne:

1. Ustaw opcje „**Śledzenia”** w zakładce PRYWATNOŚĆ według własnych upodobań

2. W zakładce „**Bezpieczeństwo”** blokuj witryny zgłoszone jako próby oszustwa internetowego

3. W zakładce „**Bezpieczeństwo”** wyłącz zapamiętywanie haseł do witryn.

Dodatkowo:

- **Czyść ciasteczka**
- **Czyść historię przeglądania**
- **Uruchom Adblock Plus i blokuj reklamy**
- **Jeśli coś jest nie tak, zgłoś oszustwo internetowe (zakładka Pomoc)**

Prywatność i bezpieczeństwo w Internet Explorer

Jeśli korzystasz z przeglądarki Internet Explorer zajrzyj do górnego MENU, a następnie:

Narzędzia → Opcje → Zabezpieczenia oraz zawartość

3 Zasady Główne:

1. Ustaw poziom zabezpieczenia w zakładce „**Prywatność”**

2. Włącz opcję przeglądania „**Inprivate”** (Narzędzia → Przegldanie inprivate)

3. Włącz filtr **SmartScreen** (Narzędzia → Filtr SmartScreen).

Co to jest filtr SmartScreen i jak może pomóc mnie chronić?

FILTR SmartScreen – Filtr SmartScreen ułatwia identyfikowanie zgłoszonych witryn Internetu wyłudzających informacje i zawierających złośliwe oprogramowanie oraz podejmowanie świadomych decyzji dotyczących pobieranych plików. Filtr SmartScreen zapewnia Ci ochronę na trzy sposoby: chroni przed stronami wyłudzającymi informacje i rozsyłającymi złośliwe oprogramowanie.

Dodatkowo:

- **Włącz „Filtr rodzinny” w zakładce „Zawartość”**
- **Włącz „Tryb chroniony” w zakładce „Zabezpieczenia”**

Bezpieczne wtyczki

Przeglądarki oferują również wtyczki, które podnoszą poziom bezpieczeństwa. Wtyczki można pobrać ze strony głównej producenta przeglądarki z której korzystasz.

Polecane wtyczki:

GHOSTERY

Ghostery (blokuje wybrane skrypty śledzące) – Firefox

Ghostery rozpoznaje "niewidzialne" sieci poprzez wykrywanie tropicieli, błędów internetowych (web bug), pikseli i internetowych znaków nawigacyjnych (web beacon) umieszczonych na stronach internetowych przez Facebook, Google oraz ponad 500 innych sieci reklamowych, dostawców danych behawioralnych, wydawców internetowych, czyli wszystkich firm, które są zainteresowane Twoją aktywnością.

HTTPS EVERYWHERE

HTTPS Everywhere (automatycznie włącza bezpieczny protokół HTTPS tam, gdzie to możliwe) – Firefox i Chrome

BETTER PRIVACY

Better Privacy (zarządza flash cookies, umożliwia ich skuteczne usuwanie przy zamykaniu przeglądarki) – Firefox

Cyberzagrożenia

Cyberzagrożenia są obecnie jednym z największych wyzwań cyfrowego świata. Już w 2010 roku korzyści materialne wynikające z cyberprzestępstw przewyższyły zyski z pornografii w internecie. Aby w pełni zrozumieć czym jest to wyzwanie musimy poznać definicję „cyberprzestępstwa".

Czym jest cyberprzestępstwo?

Istnieją dwa ujęcia tego pojęcia:

Ujęcie wertykalne – przestępstwa specyficzne dla cyberprzestrzeni, czyli takie, które tylko tam mogą być dokonane np. hacking, sabotaż komputerowy.

Ujęcie horyzontalne – przestępstwa wykonywane przy pomocy technik komputerowych (np. fałszowanie pieniędzy).

Po co przestępcy przenieśli część swojej działalności do Internetu? Dlatego, że mogli! Internet to kopalnia danych osobowych, cennych informacji, o nas, o naszych bliskich, a także tajnych informacji, które nie powinny zostać wyjawiane osobom postronnym. Cyberprzestępcy wchodząc w ich posiadanie mogą bardzo dużo zyskać.

Jakie są motywacje cybeprzestępców

1. Finansowe – liczą na korzyści majątkowe.

2. Sprawdzenie swoich umiejętności – złamanie barier zabezpieczających systemy informatyczne to dla nich wyzwanie!

Zagrożeń czyhających na nas w sieci internetowej jest… mnóstwo! Cyberprzestępcy nie śpią i na bieżąco starają się wymyślać nowe sposoby kradzieży danych w sieci…

Poniżej przedstawiono kilka najczęściej spotykanych zagrożeń internetowych, na które jest narażony.

Phishing

Według słownika informatyki stosowanej „phishing" jest to „*takie* ***wykorzystywanie poczty elektronicznej, które ma na celu kierowanie użytkownika na fałszywe witryny internetowe"****. Strony te złudnie przypominają autentyczne portale, na które użytkownik stara się wejść. Najczęściej proceder ma na celu* ***oszukiwanie i naciąganie klientów oraz zdobywanie poufnych danych na ich temat.***

Informacje zawarte w wiadomości bardzo często odnoszą się do zasad bezpieczeństwa i prawidłowego korzystania z konta!

Cyberprzestępca stara się zdobyć poufne dane wysyłając do użytkowników wiadomości np. podszywając się pod bank lub inną, ważną instytucję. W wiadomości zawarty jest link, na który ofiara ma kliknąć i na fałszywej stronie wpisać dane, które interesują cyberprzestępcę.

Wciąż powstają nowe metody działania mające na celu wyłudzanie danych, a co jakiś czas słyszmy o nowych, urozmaiconych formach ataków. Oto kilka przykładów udoskonalonych ataków phishingowych:

Phishing – instalowanie oprogramowania

Nowa forma phishingu – infekcja komputera następuję po wizycie na specjalnie stworzonej stronie

WWW. Przestępca nie próbuje wskazać ofierze konkretnej strony internetowej. Stara się za to dopisać złośliwy kod do jak największej liczby witryn. Oczywiście najlepiej gdyby była to popularna strona, odwiedzana przez dużą liczbę użytkowników.

Spear Phishing – spersonalizowany atak phishingowy

Podobnie jak w przypadku tradycyjnych ataków phishingowych, ofiary otrzymują e-mail, który wydaje się pochodzić od zaufanej osoby bądź organizacji. W tym przypadku jednak przestępcy starannie dobierają swoje ofiary**. Znacznie zwiększa to szanse na sukces oraz powoduje, że nielegalne działania są trudniejsze do wykrycia.** Celem przestępców wykorzystujących spear phishing jest pozyskanie konkretnych informacji, takich jak np. tajemnice handlowe.

Pharming

Jeszcze bardziej udoskonalona forma phishingu. Głównie wykorzystywana do kradzieży bankowych. Według autorów słownika internetowego I-słownik, Pharming *„**polega na fałszowaniu adresów IP odpowiadających nazwom domen**. Złodziej podstawia swoją stronę WWW, a następnie kieruje na nią ruch atakując system DNS”*.

Czym różni się phishing od pharmingu?

W pharmingu **użytkownik kierowany jest bezpośrednio i samoczynnie na fałszywą stronę internetową**. Dzieje się tak nawet, gdy sami wpisaliśmy adres w okno przeglądarki lub wybraliśmy stronę zapisaną w zakładce „ulubione”. **Phishing natomiast do tego celu używa poczty i fałszywego linku.** (człowiek sam musi kliknąć w link, który przeniesie go do fałszywej strony).

Cracking

Polega na złamaniu zabezpieczeń internetowych poprzez wyszukiwanie luk i tzw. „tylnych furtek” w systemach operacyjnych i przeglądarkach internetowych. Łamanie zabezpieczeń stron i wykradanie z ich informacji bądź włamywanie się na nie dla samego włamania.

Straty z tytułu cyberprzestępczości tylko w USA wynoszą około 100 mld dolarów rocznie! Na świecie może być to suma pomiędzy 300 a 400 mld.

Powyższe zagrożenia to tak naprawdę cząstka całej puli nielegalnych działań cyberprzestępców w Internecie. Cybeprzestępcy prześcigają się w projektowaniu nowych metod działania, łamią najnowsze technologiczne bariery bezpieczeństwa w bardzo krótkim czasie.

Dobre rady czyli co robić by się chronić przed zagrożeniami online?

1. ZASADA OGRANOCZONEGO ZAUFANIA.

2. WZMOŻONA OSTROŻNOŚĆ I RACJONALNE MYŚLENIE. Nawet najlepsze antywirusy nie ochronią nas przed cyberprzestępcami jeśli sami ujawniamy ważne dane o sobie czy swojej rodzinie.

3. PROGRAM ANTYWIRUSOWY – chroni jedynie w 40%, ale zawsze jest to dodatkowe, ważne zabezpieczenie.

Co jeszcze?

- Sami wpisujmy adresy stron, na które logujemy się nawet codziennie. Dzięki temu możemy uniknąć zagrożenia PHARMINGU.
- Sprawdzajmy za każdym razem czy po wpisaniu adresu do przeglądarki i zaakceptowaniu go klawiszem „enter" dany adres nie zmienia się.
- Sprawdzajmy zabezpieczenia stron oraz certyfikaty bezpieczeństwa SSL – zazwyczaj są to ikony zamkniętej kłódki tuż przy pasku adresu, jednak zależy to od zainstalowanej przeglądarki internetowej. Adres powinien zaczynać się od https.
- Dbajmy o ochronę haseł. Im mniej osób zna nasze hasła, tym lepiej.
- Korzystajmy z kilku haseł, do logowania na różne strony.
- Twórzmy mocne hasła – co najmniej 10 znaków zawierające małe i duże litery, cyfry oraz znaki specjalne (np. /,?!#). Hasło nie powinno bezpośrednio kojarzyć się z naszą osobą lub z osobami nam bliskimi.
- Raz na jakiś czas zmieniajmy hasła – mogą to być niewielkie modyfikacje.
- Przy ściąganiu darmowych programów komputerowych sprawdźmy czy dany program figuruje na stronie internetowej jego producenta.
- Ignorujmy wiadomości z załącznikami oraz linkami, gdy nie jesteśmy pewni skąd dana wiadomość pochodzi.
- Ignorujmy i nie odpowiadajmy oraz nie instalujmy aplikacji przysyłanych SMS-ami ze strony banków oraz nieznanych nam instytucji.
- Wyłączajmy programy oraz aplikacje, z których nie korzystamy w danym momencie.

Czasem, nawet mimo stosowania powyższych zasad bezpieczeństwa, zdarza się, że cyberprzestępcy byli sprytniejsi… i wyłudzili od nas pieniądze….

Co robić gdy podejrzewamy, że jesteśmy ofiarą?

- Niezwłocznie poinformujmy o tym instytucję, za jaką cyberprzestępcą się podawał. Jak najszybciej należy powiadomić bank o tym, że otrzymaliśmy fałszywe wezwanie do ujawnienia danych finansowych.
- Regularnie sprawdzajmy swoje konto bankowe – dzięki temu będziemy mieć pewność, że nie została wykonana żadna niezlecona przez nas transakcja.
- W przypadku kradzieży dokumentów tj. dowodu osobistego, paszportu lub prawa jazdy – jak najszybciej należy je zastrzec! Zdarzały się sytuacje podszywania się w sieci internetowej pod osoby, którym skradzione zostały dokumenty!

Na koniec warto przytoczyć słowa najsłynniejszego hakera, który doskonale odzwierciedla nasze starania o zachowanie bezpieczeństwa online. Kevin Mitnick, bo o nim mowa, powiedział, że…"każdy przeciwnik dysponujący odpowiednimi środkami w końcu może włamać się wszędzie…. ale naszym celem powinno być utrudnienie próby do tego stopnia, żeby jej podejmowanie nie było warte czasu". ▪

Bezpieczna e-bankowość

Dzisiaj prawie każda osoba zakładająca konto w placówce banku, wchodzi w posiadanie także konta elektronicznego. Nie jest ważne czy potrafimy z niej korzystać w odpowiedni sposób. Ważne, że mamy dostęp środków na naszym koncie 24 godziny na dobę.

Czy wiemy czym właściwie jest e-bankowość i co dzięki niej zyskujemy?

Bankowość elektroniczna – forma usług oferowanych przez banki, polegająca na umożliwieniu dostępu do rachunku za pomocą urządzenia elektronicznego.

Polskie usługi e-bankowości są jednymi z najbardziej rozwiniętych na świecie!

Według ZBP w Polsce sukcesywnie rośnie liczba użytkowników bankowości elektronicznej. **Na koniec 2012 r. umowę na używanie rachunku bankowego online miało… 20,79 mln osób.**

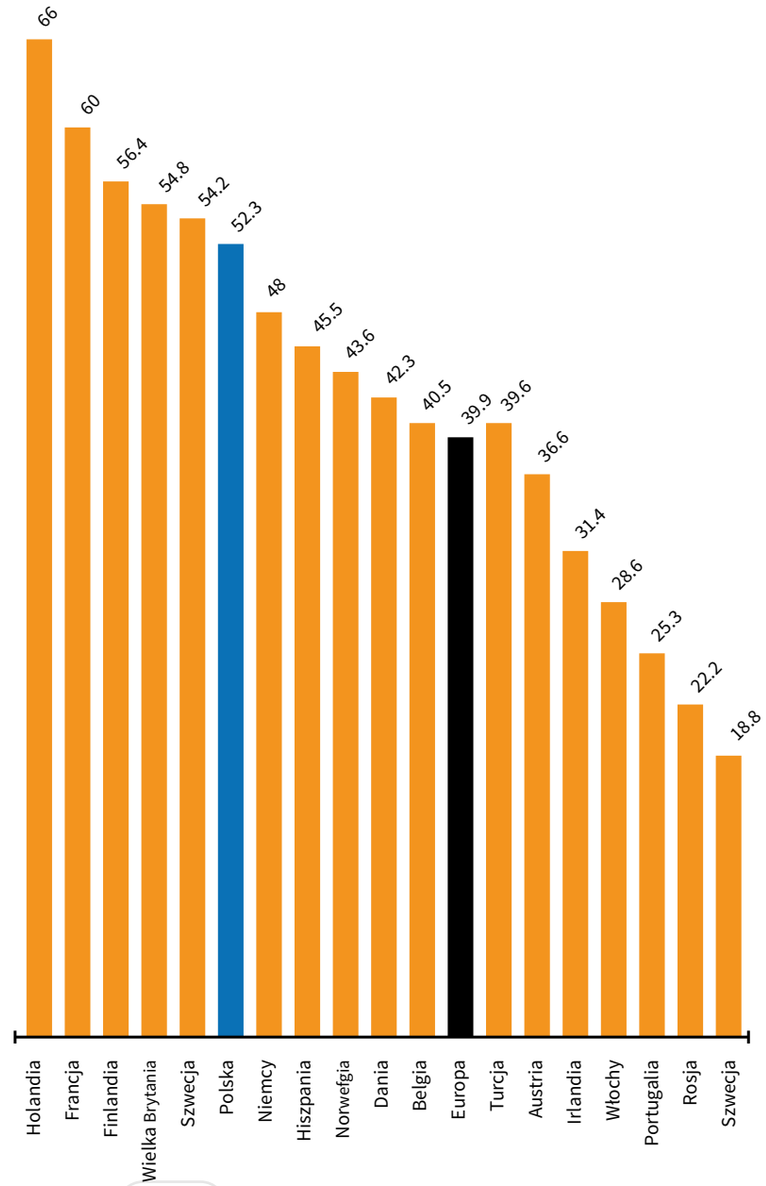
W Europie plasuje nas to na wysokim 6 miejscu!

Co ciekawe…
Polscy klienci jako jedni z pierwszych mogli płacić za zakupy telefonem komórkowym. Przed nami taką możliwość mieli jedynie Francuzi i Brytyjczycy.

Bankowość elektroniczna bez wątpienia ułatwia nam życie. Wyobraźmy sobie, że za każdym razem gdy chcemy wykonać przelew, doładować telefon komórkowy itp. musimy osobiście iść do siedziby banku.

No właśnie, a z jakich możliwości e-bankowości korzystamy najczęściej?

- Sprawdzić stan konta 97%
- Sprawdzić historię konta 95%
- Wykonać przelew jednorazowy 93%
- Doładować telefon komórkowy 50%
- Zrobić zlecenie stałe 45%



Elelektroniczna bankowości w Europie

Z racji tego, że jesteśmy narażeni na działania cyberprzestępcze bardziej niż inne kraje, gdzie poziom bankowości online jest na niższym poziomie, musimy wiedzieć jak chronić siebie i swoje pieniądze!

Co robić by bezpiecznie korzystać z e-bankowości? Oto kilka najważniejszych zasad bezpieczeństwa:

1. Sprawdzaj czy strona transakcyjna jest zabezpieczona (symbol kłódki, protokół https://).

2. Wykonuj przelewy na własnym komputerze. Masz wówczas pewność, że sprzęt posiada legalne oprogramowanie i jest zabezpieczony programami antywirusowymi.

3. Korzystaj z zabezpieczonych łączy internetowych i unikaj tych publicznych – np. w kawiarniach i galeriach handlowych.

4. Nie odchodź od komputera, gdy korzystasz z konta bankowego.

5. Wyloguj się z konta i zamknij przeglądarkę po dokonaniu transakcji. Nie klikaj cofnij/ dalej gdy jesteś zalogowany na stronie swojego konta.

6. Nie udostępniaj osobom trzecim poufnych danych (loginu, hasła czy PIN-u do karty).

7. Nie odpowiadaj na e-maile z prośbą o przesłanie poufnych danych i nie klikaj w aktywne linki w nich zawarte.

8. Nie pobieraj aplikacji bankowości mobilnej z niezaufanych źródeł – aplikacje mobilne możesz pobrać z autoryzowanych sklepów: App Store, Google Play lub Windows Phone Store.

9. Sprawdzaj numer rachunku odbiorcy gdy kopiujesz dane do przelewu.

10. Jeśli korzystasz z jednorazowych kodów autoryzacyjnych SMS – weryfikuj ich treść i zwrócić szczególną uwagę na datę i kwotę przelewu oraz numery rachunków prezentowane w wiadomości.

Uwaga na skimming!

Cyberprzestępcy znaleźli także sposób na kradzież pieniędzy z bankomatów! Jednym z najpowszechniejszych zagrożeń stosowanych z wykorzystaniem bankomatu jest „skimming”.

Skimming – jest to działanie polegające na skanowaniu i kopiowaniu paska magnetycznego karty płatniczej.

Cyberprzestępcy instalują na bankomacie malutki czytnik kart. Jest on niemal niezauważalny. Skanując pasek magnetyczny karty bankomatowej przestępcy kopiują wszystkie informacje na niej zawarte. Jedyne czego potrzebują by bez problemu dostać się do środków zgromadzonych na koncie jest kod PIN. Dlatego cyberprzestępcy zakładają na „zainfekowanych” bankomatach miniaturowe kamery, po to by każdy użytkownik sam podał im odpowiednią kombinację cyfr.

Jak się chronić?

1. Korzystajmy tylko z tych bankomatów, które są przy placówkach bankowych.

2. Zakrywajmy dłonią wybierany PIN (od góry i po bokach).

3. Sprawdzajmy czy bankomat ma zainstalowany czytnik paska magnetycznego. W tym celu dotknij miejsce gdzie wsuwasz kartę bankomatową. ▪

Ochrona danych osobowych w sieci

Ochrona naszych danych osobowych jest jednym z ważniejszych tematów jeśli chodzi o bezpieczeństwo online. Najpierw jednak musimy zdefiniować czym są dane osobowe.

Za dane osobowe uważa się **informacje służące do zidentyfikowania lub możliwe do zidentyfikowania** osoby fizycznej.

Osobą możliwą do zidentyfikowania jest ta, której tożsamość można określić bezpośrednio lub pośrednio, **w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka czynników określających** jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

Szczególną kategorią danych osobowych są DANE WRAŻLIWE (stan zdrowia, poglądy polityczne, orientacja seksualna itp.) Ich przetwarzanie jest poddane szczególnemu trybowi. Istnieje generalny zakaz przetwarzania danych wrażliwych z wyjątkiem sytuacji, gdy zezwalają na to przepisy prawa np. historia choroby, stan zdrowia.

Ochrona danych osobowych w sieci łączy się z ochroną naszej tożsamości.

Czym zatem jest tożsamość w sieci internetowej?

Tożsamość w sieci to nasze zdjęcia, nazwa naszego użytkownika, obrazki, które zamieszczamy w profilu, jest to wszystko co buduje się dookoła siebie". Może być rzeczywista lub wirtualna.

Temat ochrony danych osobowych jak i tożsamości w sieci jest bardzo ważny dlatego, że cyberprzestępcom zależy na wykorzystaniu tych danych w niewłaściwy sposób. Często jest to wymierzone bezpośrednio w nas! Może zdarzyć się, że nasz skopiowany PESEL udostępniony w sieci trafia do sfałszowanego dowodu osobistego. Na czyj rachunek będą naliczane odsetki kredytu, który ktoś wziął „na dowód"? Dlatego dbanie o bezpieczeństwo naszych danych osobowych jest bardzo istotne!

Cena danej osobowej (na nielegalnych rynkach internetowych) w zależności jaka ona jest to od kilkudziesięciu groszy do nawet 100 złotych.

Zdarza się jednak, że cyberprzestępcom trudno jest przełamać bariery bezpieczeństwa w systemach teleinformatycznych. Nie mają wtedy dostępu do wielu pakietów informacji, adresów, pinów i haseł, na którym im zależy... co wtedy?

Wówczas cyberprzestępcy kierują metody swoich działań na najsłabsze ogniwo informacji czyli na człowieka. Jest to tak zwana „socjotechnika".

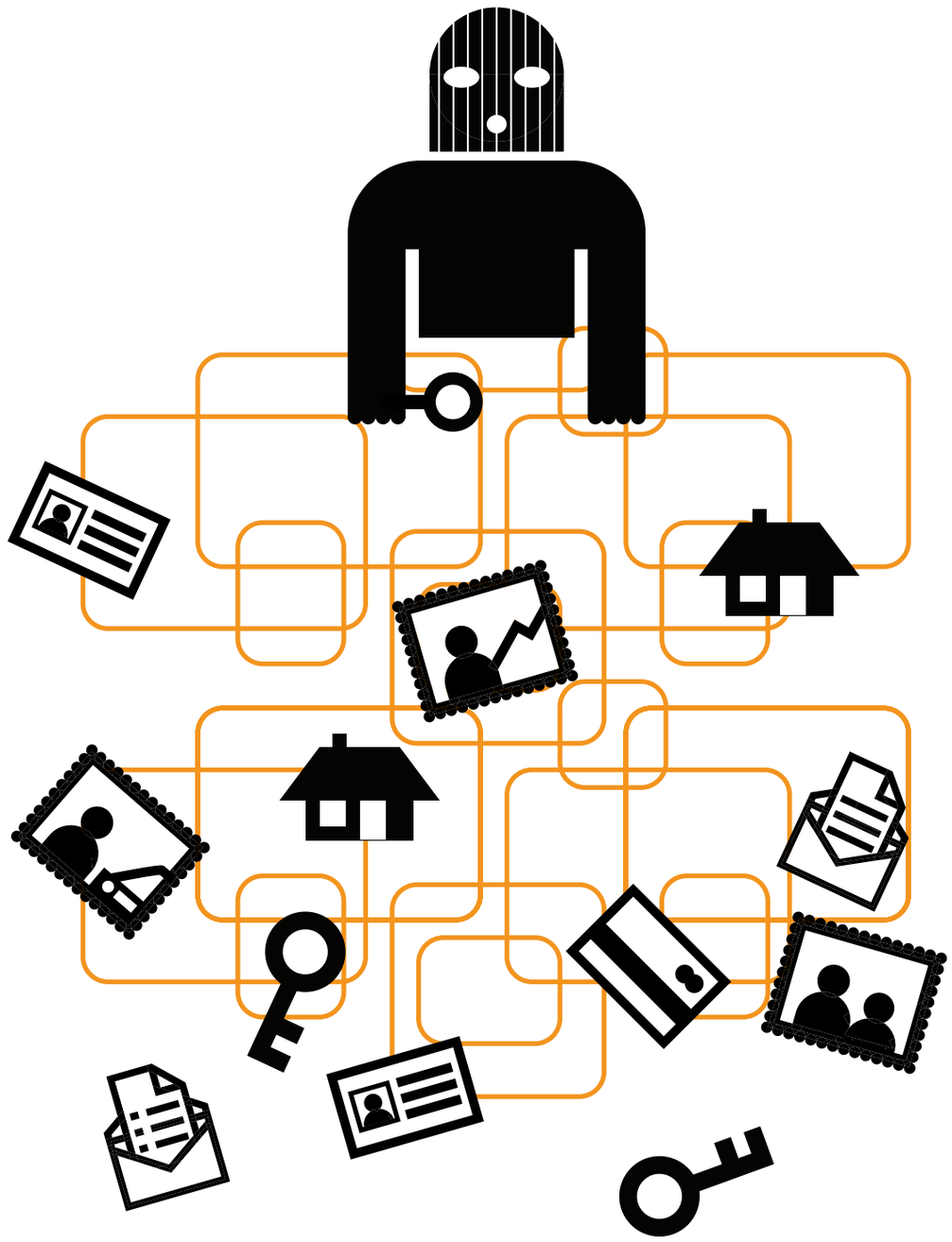
SOCJOTECHNIKA – w bezpieczeństwie teleinformatycznym to zestaw metod mających na celu uzyskanie niejawnych informacji przez cyberprzestępcę. Hakerzy często wykorzystują niewiedzę bądź łatwowierność użytkowników, aby pokonać zabezpieczenia odporne na wszelkie formy ataku.

Istnieje dużo przypadków podszywania się oraz jawnego wykorzystywania kradzionych danych osobowych.

Portale takie jak Pobieraczek.pl oraz Plikostrada.pl nielegalnie wchodziły w posiadanie danych osobowych i wykorzystywały je w zastraszaniu użytkowników do opłacenia abonamentu, na który rzekomo zgodzili się akceptując regulamin.

Jak się chronić przed kradzieżą i nielegalnym wykorzystaniem danych osobowych w sieci?

- Jeśli nie jest to konieczne – nie podawaj w Internecie swoich pełnych danych osobowych (imienia, nazwiska, daty urodzenia, peselu).
- Uważaj komu i jak udostępniasz swój adres e-mail oraz informacje wrażliwe.
- Nie wysyłaj za pośrednictwem Internetu numerów kont, pinów, haseł itp.
- Nie podawaj miejsca zamieszkania.
- Jeśli nie musisz, nie wrzucaj zdjęć przedstawiających Ciebie, Twoich bliskich, miejsc w których bywasz.
- Nie wpisuj danych osobowych, gdy mamy podejrzenie co do rzetelności strony internetowej.
- Dbajmy o dokładne czyszczenie starych komputerów/telefonów itp. z danych, które tam przechowywaliśmy.
- **Zastrzegajmy skradzione dokumenty!** ▪



Bezpieczeństwo urządzeń mobilnych

W dzisiejszych czasach trudno jest znaleźć osobę, która nie posiada telefonu komórkowego. Często nawet nie zdajemy sobie sprawy, że urządzenie w naszej torebce czy kieszeni nie jest już zwykłym telefonem a... smartphonem! (urządzeniem łączącym w sobie funkcje telefonu i komputera kieszonkowego).

Urządzenia mobilne stały się nowym polem działalności cyberprzestępców

Zagrożenia wynikające z korzystania z urządzeń mobilnych łączą w sobie typowe zagrożenia internetowe z funkcjonalnością telefonów komórkowych.

Za pośrednictwem smartphona, cyberprzestępca może mieć dostęp do naszych danych, książki teleadresowej, prywatnych zdjęć, smsów, e-maili itd. Może również nas podsłuchiwać lub zmuszać do wysyłania płatnych smsów bez naszej wiedzy.

Bezpieczeństwo urządzeń mobilnych zależy od rodzaju ich oprogramowania systemowego

Najczęściej występującym oprogramowaniem występującym na rynku są:

1. System IOS – działa na urządzeniach firmy Apple.

W 2013 roku odsetek aplikacji złośliwych w sklepie IStore – platformie do pobierania aplikacji wynosił 0.01%

2. System ANDROID – działa na urządzenia różnych marek m.in. Samsung, LG.

W 2013 roku odsetek aplikacji złośćliwych w sklepie Google Play – platformie do pobierania aplikacji wynosił 10,4%

10 mln aplikacji dla użytkowników androida to w rzeczywistości złośliwe oprogramowanie!

3. System WINDOWS PHONE – działa m.in. na urządzeniach firmy NOKIA

Windows Phone nie udostępnia danych o złośliwych aplikacjach, które można było ściągnąć za pośrednictwem sklepu Windows.

Skąd taka różnica?

W systemie Android nie ma weryfikacji „kto” oraz „co” wstawia do sklepu Google Play. Istnieje także możliwość instalowania aplikacji z innych źródeł niż wspomniana platforma Google Play. W dwóch pozostałych systemach stosowana jest weryfikacja aplikacji przed umieszczeniem jej do ściągnięcia przez użytkowników.

Sposoby zabezpieczania urządzeń mobilnych

Zabezpieczaj telefon oraz PILNUJ GO!

Dobrze jest stosować PIN do telefonu lub blokadę ekranu.

Dzięki temu nawet jeśli nasz aparat dostanie się w niepowołane ręce, złodziej nie będzie mógł wykonywać z niego połączeń, wchodzić do Internetu, nie będzie miał również dostępu do aplikacji oraz naszych prywatnych danych. W zabezpieczenia hasłem, PIN-em lub blokadą wyposażone są wszystkie seryjne modele smartfonów.

1. Szyfruj

Wymaga to włączenia odpowiednich funkcji lub zainstalowania programu szyfrującego. Co ważne, włączenie tych opcji nie wpływa na wydajność (bateria) ani na wygodę obsługi telefonu.

2. Ściągaj odpowiedzialnie

Jeśli jakąś aplikację ściągnęło 8 mln ludzi, to zapewne jest ona bezpieczna. Ale pamiętajmy – przy instalacji programu lepiej czytać wyświetlające się monity, które wskazują, z jakich danych będzie on korzystać. Jeśli zwykła gra w kulki żąda dostępu do naszej poczty, lepiej przerwijmy instalację.

3. Aktualizuj

Nowe aktualizacje uszczelniają nasz system ochrony, likwidując „dziury" w oprogramowaniu. Android i iOS zapewniają aktualizacje automatyczne niemalże bez ingerencji użytkownika, natomiast producenci smartphonów z Windows wymagają, aby użytkownik sam zainteresował się, czy pojawiły się już jakieś aktualizacje i czy pasują do danej wersji urządzenia.

4. Kup program antywirusowy

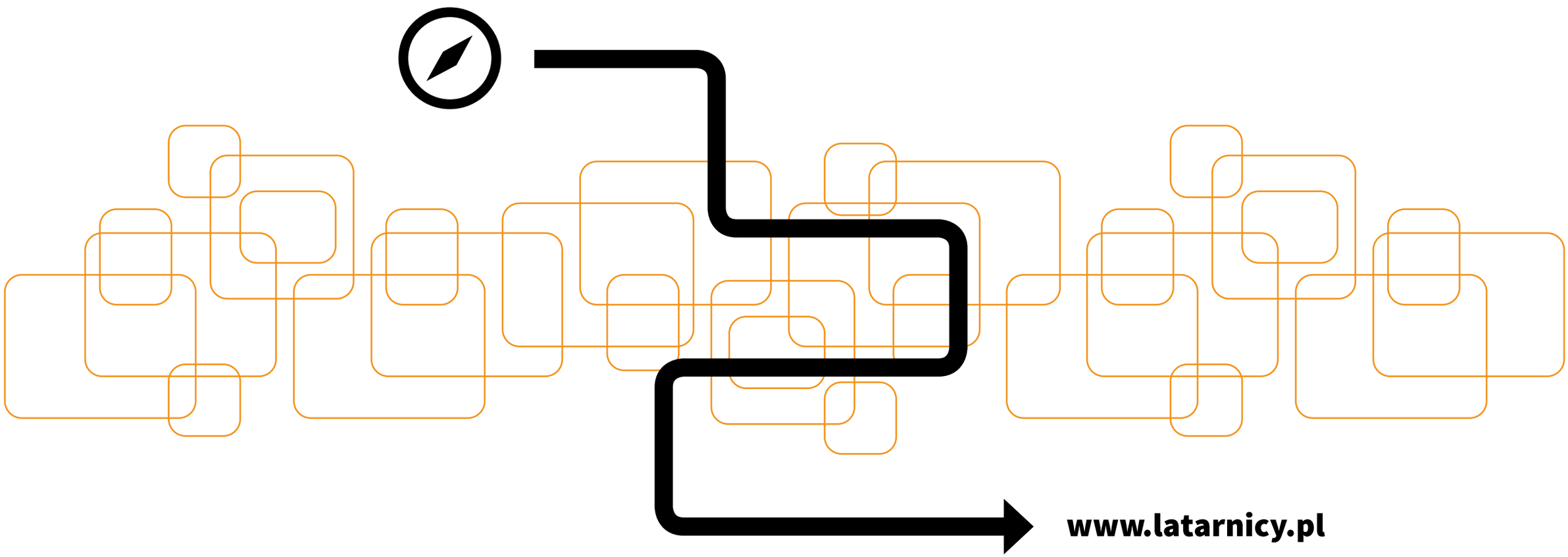
Dobry antywirus będzie nas zabezpieczał przed złośliwym oprogramowaniem i szkodliwymi aplikacjami, ostrzeże przed niebezpiecznymi stronami WWW. Antywirusy mają wbudowaną ochronę przed złodziejami. W przypadku kradzieży telefonu będziemy mogli go nie tylko zdalnie zablokować, ale także namierzyć telefon na mapie, a nawet wykonać zdjęcie z miejsca, w którym się znajduje.

5. Uważaj na wi-fi

Surfowanie po Internecie przy filiżance kawy w kawiarni albo w pasażu handlowym nie naraża nas na ryzyko, pod warunkiem że nie używamy aplikacji korzystających z wrażliwych danych. Logowanie się do banku przez nieznane wi-fi można porównać do przeglądania zawartości portfela na ławce w zatłoczonej dworcowej poczekalni. Dlatego korzystając z Internetu w smartphonie, najlepiej jest stosować te same zasady bezpieczeństwa co przy korzystaniu ze zwykłego komputera, czyli korzystać ze sprawdzonych sieci wi-fi i upewniać się, czy strona internetowa jest szyfrowana (świadczy o tym ikona kłódki przy adresie internetowym). Dobrze jest też wyłączyć opcję automatycznego łączenia smartphona z sieciami wi-fi (lepiej jest mieć nad tym kontrolę) i korzystać z Firewalla, czyli zapory systemowej, która monitoruje połączenia.

6. Rób kopie zapasowe

Odzyskanie danych, które gromadziliśmy na zgubionym urządzeniu, jest możliwe, jeśli robiliśmy regularnie kopie zapasowe (backup). Można to uczynić na dwa sposoby – archiwizując informacje bezpośrednio na komputerze lub korzystając z chmury. Użytkownicy iPhonów mogą korzystać z dostarczanej przez Apple usługi iCloud, która pozwala przetrzymywać w chmurze kopie zapasowe, m.in. kontaktów, wiadomości, e-maili, zdjęć, muzyki. Google Cloud to z kolei bezpłatna usługa tworzenia kopii zapasowych dla urządzeń z systemem Android, swoją chmurę mają także aparaty z systemem Windows Phone. ▪


www.latarnicy.pl