Zajęcia 6. Środki ostrożności
(materiał zawiera informacje zgodne z Syllabus e-Citizen v. 1.0)

2.2. Środki ostrożności
Zarówno w świecie realnym jak i wirtualnym – Internecie powinniśmy czuć się bezpiecznie. Jednak w jednym i drugim spotykamy zagrożenia, których istnienia powinniśmy mieć świadomość, aby uchronić się przed ich skutkami, często tragicznymi.
Jesteśmy świadkami postępującej kryminalizacji Internetu. Tworzone, rozwijane i wykorzystywane są nowe złośliwe technologie. Użytkownicy indywidualni coraz częściej stają się obiektem ataków mających na celu kradzież danych, a także ofiarami oszustw i innych przestępstw o charakterze finansowym.
Przez Internet przepływa coraz więcej pieniędzy. A tam, gdzie są miliardy, nie brakuje też przestępców. Drogą elektroniczną można ukraść łatwiej i więcej niż tradycyjnymi metodami, a i trudniej wykryć sprawcę kradzieży. Cel rabusiów to przejęcie kontroli nad naszym komputerem.

2.2.1. Zrozumienie problemu i ryzyka niepożądanej poczty i umiejętność podjęcia zapobiegawczego działania
Pocztę elektroniczną należy często sprawdzać i usuwać niepotrzebne e-maile, aby nie zajmowały miejsca na dysku i utrudniały wyszukanie konkretnego listu.
Można skonfigurować program pocztowy w taki sposób, aby tzw. śmieci (np.: **spam**, reklamy itp.) kierował do utworzonych w tym celu folderów. Przed opróżnieniem takiego folderu warto przejrzeć jego zawartość bo mogą tam też trafić ważne e-maile.

Spam – niechciane lub niepotrzebne wiadomości elektroniczne. Najbardziej rozpowszechniony jest spam za pośrednictwem poczty elektronicznej. Zwykle (choć nie zawsze) jest wysyłany masowo.
Istotą spamu jest rozsyłanie dużej ilości informacji o jednakowej treści do nieznanych sobie osób. Nie ma znaczenia, jaka jest treść tych wiadomości.
Od 2002 roku polskie prawo zabrania wysyłania do użytkowników **niezamówionej** korespondencji handlowej. Zamiast tego, otrzymujemy najczęściej skróconą informację o produkcie, z prośbą o zgodę na wysłanie oferty handlowej dotyczącej tego produktu lub kliknięcie linku.
Obecnie istnieje cały przemysł wysyłania ludziom reklam wbrew ich woli. Najczęstszą metodą używaną przez spamerów jest skanowanie sieci w poszukiwaniu adresów poczty elektronicznej i wysyłaniu danej wiadomości na wszystkie znalezione adresy. Ze względu na ogólne potępienie tych metod, poważne firmy praktycznie nie korzystają z usług spamerów.

Większość współczesnych spamerów, zwłaszcza komercyjnych, wyspecjalizowało się w **oszukiwaniu potencjalnych ofiar**. Jednym z najczęstszych chwytów jest **prośba spamera o odesłanie e-maila**, jeśli ofiara nie życzy sobie otrzymywać od niego więcej wiadomości. Zwykle spamerowi wcale nie chodzi o wykreślenie danej ofiary ze swojej listy, a wręcz przeciwnie – weryfikuje on w ten sposób poprawność adresu ofiary, bowiem adresy potencjalnych ofiar są często generowane np. od imion czy też popularnych nicków, pozyskiwane ze stron WWW lub wymieniane pomiędzy spamerami.

Najbrudniejszym chwytem spamerów jest przysłanie maila z **wirusem typu koń trojański**. Wirus ten instaluje się na komputerze użytkownika i następnie automatycznie przesyła do spamera wiele cennych informacji, np. zawartość książki adresowej. Pod kontrolą spamerów pracuje wiele komputerów zwykłych użytkowników, tworząc sieć zwaną **botnetem**.

Oprócz reklamowania różnych usług i produktów, tego rodzaju przesyłki mogą wiązać się z oszustwami i próbami wyłudzeń:
- Spam na bankowca (**phishing**) – spamer podszywa się pod bank i prosi o podanie hasła. Ten sposób może też służyć do przejęcia naszego konta bankowego, konta w aukcjach internetowych, itp.
- Spam na **urząd** np. bezpieczeństwa, skarbowy, ZUS itd. – żartowniś podszywa się pod urząd próbując wyłudzić dane osobowe lub pieniądze.
- Spam na **spadek** – inaczej spam afrykański lub nigeryjski szwindel. Odbiorca dostaje wiadomość, że otrzymał spadek, ale musi opłacić koszty notarialne i operacyjne.
- Spam na **wygraną** – wygrałeś milion dolarów, samochód lub inną nagrodę. Następnie po kliknięciu linku i wejściu na stronę instaluje się trojan wyszukujący informacje o naszym koncie bankowym.

Adres podany jako **adres nadawcy** nie jest prawdziwym **adresem spamera**, ale adresem innej jego ofiary. Ważne jest, aby **nigdy nie reagować na spam odpowiedzią**, np. nie odwiedzać zawartych w nim adresów, nie podawać swoich danych, itp. W przypadku pojedynczego spamu z jednego miejsca najlepiej jest go po

prostu zignorować. W przypadku, gdy spam jest systematycznie wysyłany z jednego adresu można zawiadomić administratora domeny i założyć **filtr** na ten adres.
Należy unikać podawania adresu poczty elektronicznej tam, gdzie nie jest to konieczne. Jeśli konieczne jest podanie adresu wprost, to przeznaczmy na to dodatkowe konto lub alias pocztowy.
Serwisy internetowe (np.: www.wp.pl, www.onet.pl, www.o2.pl, itp.) mające w swojej ofercie konta poczty elektronicznej posiadają **filtry antyspamowe**, które zapobiegają dostaniu się **spamu** do skrzynki odbiorczej klienta. Takie odfiltrowane wiadomości najczęściej trafiają do specjalnego folderu o nazwie **Spam**.
Żadne z rozwiązań filtrujących nie jest doskonałe i te, które filtrują dużą część spamu, mogą też niezamierzenie odfiltrować list wysłany w dobrej wierze.
Bomba pocztowa (ang. *Email bomb*) – żargonowe określenie masowej wysyłki poczty elektronicznej do jednej osoby lub systemu, czego celem jest załamanie systemu lub utrudnienie jego działania, zwłaszcza przez przekroczenie pojemności skrzynki pocztowej lub zajęcie dysku.
Bomba pocztowa jest zwykle złośliwym działaniem w stosunku do jakiejś osoby. Stanowi często naruszenie zasad sieciowych lub przestępstwo. Do wysyłania bomb pocztowych służą specjalne programy ukrywające prawdziwy adres pocztowy nadawcy.

Ze względów bezpieczeństwa lepiej korzystać z poczty elektronicznej za pośrednictwem strony internetowej (**webmail**), zamiast z programu pocztowego zainstalowanego na komputerze.

Dostępne na rynku **pakiety antywirusowe** (np.: Kaspersky Internet Security, ESET Smart Security, avast! Internet Security, Bitdefender Internet Security i inne) zawierają zintegrowane mechanizmy filtrowania spamu sprawdzające każdą wiadomość. Chronią też przed różnymi **złośliwymi programami szpiegującymi.** Taki pakiet powinien być obowiązkowo zainstalowany na naszym komputerze.

2.2.2. Zrozumienie problemu i ryzyka zagrożeniem wirusem i umiejętność podjęcia zapobiegawczego działania

Korzystając z poczty e-mail, należy zachować szczególna ostrożność. W korespondencji bardzo często rozsyłane są wirusy komputerowe. Najczęściej spotykanym sposobem na rozprzestrzenianie się wirusów mogą być niebezpieczne dla naszego komputera **pliki zawarte w podejrzanych wiadomościach e-mail**. Wtargnięcie takiego wirusa do naszego komputera odbywa się zazwyczaj przez uruchomienie **załączonego do listu pliku**. Jeżeli więc otrzymamy list od nieznajomej osoby, najlepiej jest go usunąć.

Komputery zombie – maszyny, nad którymi dzięki **trojanom** kontrolę przejęli hakerzy. Najczęściej służą do ataków typu DoS (Denial of Service), w których na dany adres wysyłana jest w jednej chwili gigantyczna liczba zapytań, by go zablokować. Ich inne zastosowanie to rozsyłanie spamu. Obecnie pod kontrolą spamerów pracuje wiele komputerów zwykłych użytkowników, tworząc sieć zwaną **botnetem**.

Koń trojański, trojan – określenie oprogramowania, które daje hakerowi możliwość kontrolowania komputera bez wiedzy jego użytkownika. Trojan podszywając się pod przydatne lub ciekawe dla użytkownika aplikacje dodatkowo implementuje niepożądane, ukryte przed użytkownikiem funkcje (programy szpiegujące, bomby logiczne, furtki umożliwiające przejęcie kontroli nad systemem przez nieuprawnione osoby itp.). Nazwa pochodzi od mitologicznego konia trojańskiego.

Malware, złośliwe oprogramowanie, (z ang. *malicious software)* – wszelkie aplikacje, skrypty itp. mające szkodliwe, przestępcze lub złośliwe działanie w stosunku do użytkownika komputera.

Programy szpiegujące (ang. *spyware*) to programy komputerowe, których celem jest szpiegowanie działań użytkownika w pamięci komputera i w Internecie. Programy te gromadzą informacje o użytkowniku i wysyłają je często bez jego wiedzy i zgody autorowi programu. Do takich informacji należeć mogą:
- adresy URL stron internetowych odwiedzanych przez użytkownika,
- dane osobowe,
- numery kart płatniczych, hasła,
- zainteresowania użytkownika (np. na podstawie wpisywanych słów w oknie wyszukiwarki),
- adresy poczty elektronicznej.

Robaki – programy, których działanie polega na tworzeniu własnych duplikatów. Nie atakują one żadnych obiektów jak to czynią wirusy, a jedynie same się powielają. Oprócz replikacji i zajmowania miejsca na dysku niekiedy wywołują również negatywne skutki uboczne, takie jak niszczenie plików, wysyłanie poczty (z reguły spam) lub pełnienie roli **backdoora** albo **konia trojańskiego**. Robaki są najbardziej popularne w sieciach, gdzie mają do dyspozycji różne protokoły transmisji sieciowej, dzięki którym mogą się rozprzestrzeniać przez wykorzystanie luk w systemie operacyjnym lub naiwność użytkownika.

Rootkit – program, który w systemie ukrywa obecność swojego i innego oprogramowania hackerskiego. Zazwyczaj blokuje oprogramowanie antywirusowe. Ukrywa on niebezpieczne pliki i procesy, które umożliwiają utrzymanie kontroli nad systemem. Może on np. ukryć siebie oraz konia trojańskiego przed administratorem oraz oprogramowaniem antywirusowym. Rootkit może się dostać do komputera użytkownika wraz z aplikacją będącą w rzeczywistości trojanem.

Oprogramowanie szpiegujące (ang. *spyware*) – programy komputerowe, których celem jest gromadzenie informacji o użytkowniku, a także ich przesyłanie bez jego wiedzy innym osobom.
Programy te gromadzą informacje o użytkowniku i wysyłają je często bez jego wiedzy i zgody autorowi programu. Do takich informacji należeć mogą: adresy www stron internetowych odwiedzanych przez użytkownika, dane osobowe, numery kart płatniczych, hasła, zainteresowania użytkownika, adresy e-mail.

Keylogger (ang. „*key*" – klawisz, „*logger*" – rejestrator) – rodzaj oprogramowania lub urządzenia rejestrującego klawisze naciskane przez użytkownika. Na ogół są spotykane w wersji programowej, rzadziej w sprzętowej. Prostym i skutecznym sposobem jest logowanie się do serwisów, przy wykorzystaniu klawiatury ekranowej (**Windows +U**).

Wirus komputerowy – krótki program komputerowy, zwykle szkodzący systemowi operacyjnemu lub utrudniający pracę użytkownikowi komputera. Każdy wirus ma zdolność powielania się bez zgody użytkownika. Wirusy przenoszone są w zainfekowanych wcześniej plikach (wirusy plikowe) lub w pierwszych sektorach fizycznych (na zerowej ścieżce) dysku twardego (wirusy dyskowe). Zainfekowaną ofiarę nazywa się **nosicielem**, a proces samopowielania **replikacją**. Wirusy wykorzystywały słabość zabezpieczeń systemów komputerowych lub właściwości systemów oraz niedoświadczenie i beztroskę użytkowników. Aktualnie są już nie spotykane.

Wyłudzacze – oszuści, podający się za pracowników banków czy firm ubezpieczeniowych, wyłudzają poufne dane lub pieniądze.

Wymuszenia online – organizacje przestępcze przeprowadzają ataki na strony firm (np. serwisów bukmacherskich), a następnie żądają pieniędzy za ich zaprzestanie.

Sposoby zabezpieczenia przed wirusami komputerowymi:

- **Aktualna ochrona antywirusowa.** Nawet najlepszy program zabezpieczający nie ochroni naszego systemu, jeśli nie przedłużymy **subskrypcji** i nie mamy nowych **aktualnych definicji wirusów**.
- **Zainstalowany pakiet antywirusowy** (instalujemy tylko jeden na danym komputerze). Jeśli na naszym komputerze jest zainstalowany **pakiet antywirusowy** (np.: Norton Internet Security, Kaspersky Internet Security, ESET Smart Security, avast! Internet Security, Bitdefender Internet Security i inne) to powinien on **chronić komputer przed szkodliwym oprogramowaniem**, w tym przed wirusami, robakami, trojanami, programami szpiegującymi, rootkitami, botami i innym zagrożeniem.
  Oczywiście można w każdej chwili wykorzystać te programy do skanowania wszystkich nośników, wybranych partycji, folderów lub plików.
  Aby przeskanować dany nośnik, folder lub plik, należy kliknąć na jego ikonę lub nazwę prawym przyciskiem myszy i z menu kontekstowego wybrać nazwę pakietu antywirusowego, a następnie opcję **Skanuj** lub **Skanuj teraz**.
- **Dodatkowe zabezpieczenia**. Sam program antywirusowy nie wystarczy. Należy korzystać z dodatkowych zabezpieczeń w postaci **firewalla** (**zapory sieciowej**), czy ochrony prywatności w przeglądarce, aby zabezpieczyć się przed **malware**. **Zapora** może uniemożliwić uzyskanie dostępu do komputera przez **hakerów** lub złośliwe oprogramowanie (takie jak **robaki**) za pośrednictwem sieci lub Internetu. Zapora może też pomóc w uniemożliwieniu komputerowi wysyłania złośliwego oprogramowania do innych komputerów. Można skorzystać z **Zapory systemu Windows** lub zapory (firewall) wbudowanej w **pakiet antywirusowy**.

Dobre **oprogramowanie antywirusowe** powiadomi użytkownika o **wykryciu wirusów** podczas skanowania i zaproponuje sposoby postępowania z zainfekowanymi obiektami.

W ogromnej większości przypadków, komputery osobiste infekowane są **robakami** lub **końmi trojańskimi**. Jednak, najczęściej możliwe jest odzyskanie większości danych. Musimy liczyć się też z faktem, że niektóre **robaki** i **trojany** mogą uszkodzić lub zablokować komputer (zaszyfrować dyski). Wówczas niezbędna będzie wizyta w serwisie.

Co należy zrobić w przypadku wystąpienia oznak infekcji?
Jeżeli komputer zachowuje się w nieprzewidywalny sposób:

- Nie należy wpadać w panikę! W ten sposób można uniknąć utraty ważnych informacji przechowywanych w komputerze oraz niepotrzebnego stresu.
- Należy odłączyć komputer od Internetu.
- Jeśli komputer podłączony jest do sieci lokalnej, należy ją odłączyć.
- Jeśli nie można uruchomić komputera z dysku twardego (błąd przy starcie), należy spróbować uruchomić system w trybie awaryjnym lub przy użyciu dysku startowego systemu Windows.
- Przed podjęciem jakiejkolwiek czynności należy skopiować (o ile to możliwe) wszystkie ważne dane na dysk zewnętrzny (płytkę CD, DVD, pamięć flash itd.).
- Należy zainstalować płatny program antywirusowy, jeśli nie jest on jeszcze obecny w systemie.
- Należy pobrać najnowsze uaktualnienia antywirusowych baz danych. W miarę możliwości nie należy pobierać baz przy użyciu zainfekowanego komputera, lecz skorzystać z innego komputera. Jest to istotne, ponieważ jeżeli zainfekowany komputer jest podłączony do Internetu, wirus może wysłać ważne dane osobom trzecim lub próbować wysłać się pod wszystkie adresy zawarte w książce adresowej. Uaktualnienia programu antywirusowego można otrzymać na płycie CD-ROM od producenta oprogramowania antywirusowego lub autoryzowanego dystrybutora.
- Należy wykonać pełne skanowanie systemu.

W przypadku, gdy jesteśmy przekonani, że nasz komputer padł ofiarą **ataku hackerskiego**, powinniśmy tylko odłączyć go od Internetu i wezwać policję, która podejmie właściwe kroki. W innym przypadku możemy zatrzeć ślady, którą uniemożliwią złapanie sprawcy, a w następstwie otrzymanie odszkodowania.

2.2.3. Zrozumienie potrzeby bezpiecznego dostępu do Internetu wraz z opisaniem dowolnej metody zastosowania środków bezpieczeństwa

Co zwiększa ryzyko w Internecie?
Z winy użytkownika komputera często dochodzi do infekcji systemu przez **trojana** lub innego naruszenia bezpieczeństwa. Niewłaściwe postępowanie może sprowadzić na nasz system komputerowy wiele poważnych zagrożeń.

1. **Oczywiste, łatwe do odgadnięcia hasła dostępu.** Złamanie hasła utworzonego w oparci o proste ciągi cyfr 123 456, imiona, daty urodzin własne i dzieci, banalne pytania resetujące hasło, zajmuje hakerowi chwilę. Jeśli używamy go także w innych serwisach, z łatwością przejmie naszą cyfrową tożsamość.
2. **Brak aktualizacji systemu operacyjnego** i zainstalowanych **aplikacji**. W systemie operacyjnym **Windows 10** nie można wyłączyć automatycznych aktualizacji.
3. **Ujawnianie informacji osobistych online.** Ujawnianie zbyt wielu informacji o swoim życiu na niezabezpieczonych stronach społecznościowych (np. Facebooka, Naszej klasy, Fotki.pl) umożliwia hakerowi przeprowadzenie skutecznego spersonalizowanego ataku.
4. **Nadmiar zaufania.** Jeśli ufamy wszystkim komunikatom wysyłanym przez pocztę elektroniczną czy komunikatorami (np. gg), łatwiej padniemy ofiarą szkodników, które po zainfekowaniu komputera rozsyłają tą drogą linki do swoich kopi.
5. **Brak lub nieaktualna ochrona antywirusowa.** Nawet najlepszy program zabezpieczający nie ochroni naszego systemu, jeśli nie przedłużymy **subskrypcji** i nie mamy nowych **aktualnych definicji wirusów**.
6. **Nie zdeinstalowane nieużywane oprogramowanie** (nieużywane aplikacje, gry, itp.).
7. **Brak dodatkowych zabezpieczeń**. Należy korzystać z dodatkowych zabezpieczeń w postaci **firewalla** (**zapory sieciowej**).
8. **Ignorancja i liczenie na cud** bo „mnie to się nigdy nie przytrafi” to najcięższy, ale często spotykany grzech, jaki może popełnić użytkownik.
9. **Przekonanie, że w moim systemie nie ma nic, co mogłoby zainteresować cyberprzestępców.** Przeciętni użytkownicy uważają, że dane zgromadzone w ich pecetach mają wartość tylko dla nich, więc nie wymagają ochrony przed intruzami. Ta hipoteza kryje w sobie aż trzy błędy.
    - Cyberprzestępcom nie zawsze zależy na danych. Bardzo często chcą przejąć kontrolę nad komputerem, aby użyć go np. do hostowania złośliwego oprogramowania lub do rozsyłania spamu.
    - Agresor może wykorzystać pozornie banalne informacje, takie jak twoje imię, nazwisko, adres zamieszkania i data urodzenia, aby ukraść ci tożsamość.
    - Większość ataków jest przeprowadzana automatycznie w poszukiwaniu wszystkich komputerów podatnych na nie. Wartość komputera czy zgromadzonych danych przeważnie nie stanowi kryterium wyboru potencjalnych ofiar.

Sieć bezprzewodowa może być **zabezpieczona** i **otwarta** (niechroniona).
Nośnikiem informacji w każdej sieci bezprzewodowej są fale radiowe, a to oznacza, że utworzona w domu (biurze) sieć Wi-Fi często ma zasięg wykraczający poza powierzchnię naszego mieszkania (biura). W przypadku braku ochrony dostępu do sieci Wi-Fi każdy, kto dysponuje urządzeniem wyposażonym w interfejs bezprzewodowy, może się do takiej sieci podłączyć. Konsekwencje zaniedbań w zakresie zabezpieczenia dostępu do sieci Wi-Fi mogą być poważne. Nie chodzi tutaj tylko o to, że osoby z zewnątrz mogą korzystać z opłacanego przez właściciela niechronionej sieci łącza internetowego, ale głównie o to, że **sieci pozbawione ochrony mogą być wykorzystywane do popełniania przestępstw**. Agresor może z łatwością nie tylko wykorzystywać otwartą sieć i łącze Wi-Fi na przykład do wysyłania spamu czy złośliwego oprogramowania. Haker może również wykradać dane z komputerów i urządzeń podłączonych do danej sieci, podsłuchiwać całą komunikację, odczytywać wpisywane hasła do odwiedzanych przez domowników serwisów internetowych itp. Pozostawienie niechronionej sieci Wi-Fi to **skrajna nieodpowiedzialność**. Domową (firmową) sieć bezprzewodową trzeba więc skutecznie chronić.

Zabezpieczenie sieci w znacznym stopniu ułatwiają producenci ruterów bezprzewodowych. Każde tego typu urządzenie podczas pierwszego uruchomienia wymusza przeprowadzenie wstępnej konfiguracji. Podczas tego działania, niezależnie od producenta rutera, **użytkownik musi najpierw ustawić hasło ochronne do panelu administracyjnego** – co najmniej 11 znakowe (małe i duże litery, cyfry i chociaż jeden znak specjalny). W dalszej kolejności dokonuje wyboru typu łącza internetowego, które ma być rozdzielane przez konfigurowany ruter, i wreszcie definiuje parametry zabezpieczeń sieci bezprzewodowej. We wszystkich nowoczesnych ruterach proces wstępnej konfiguracji wymusza ustawienie optymalnego poziomu ochrony.

W przypadku już działającej sieci warto upewnić się, czy ustawienia zabezpieczeń są optymalne, a także sprawdzić, w jakie funkcje zwiększające bezpieczeństwo sieci dany ruter jest wyposażony. Należy najpierw zalogować się do **panelu konfiguracyjnego rutera** przez przeglądarkę WWW (adres najczęściej to: http://192.168.1.1 lub http://192.168.1.1/), a następnie wywołać stronę z ustawieniami zabezpieczeń.

Jeżeli wybrany standard to **WPA2-Personal** lub **WPA2-PSK** – dostęp do sieci jest optymalnie chroniony, natomiast jeżeli jest to szyfrowanie **WEP** czy nawet **WPA** z protokołem zabezpieczającym TKIP, należy zmienić ustawienia, wybierając **WPA2-Personal/PSK** z szyfrowaniem **AES**.

Podstawowe zasady, których powinien przestrzegać każdy właściciel domowej sieci Wi-Fi:
- nigdy nie ustawiaj domowej sieci jako tak zwanej **sieci otwartej** (niechronionej),
- wybieranym standardem zabezpieczeń w domowych sieciach Wi-Fi powinien być zawsze standard **WPA2-Personal** (inna nazwa: **WPA2-PSK**),
- nigdy nie używaj standardu **WEP** – współcześnie nie zapewnia on żadnej ochrony,
- w razie konieczności udostępniania łącza internetowego obcym korzystaj z funkcji „sieć dla gości”,
- jeżeli to możliwe: wyłącz funkcję **WPS** ułatwia ona podłączanie, ale obniża bezpieczeństwo.

2.2.4. Rozumienie potencjalnego zagrożenia przy wprowadzaniu do Internetu informacji poufnych i osobowych oraz umiejętność podjęcia środków zapobiegawczych

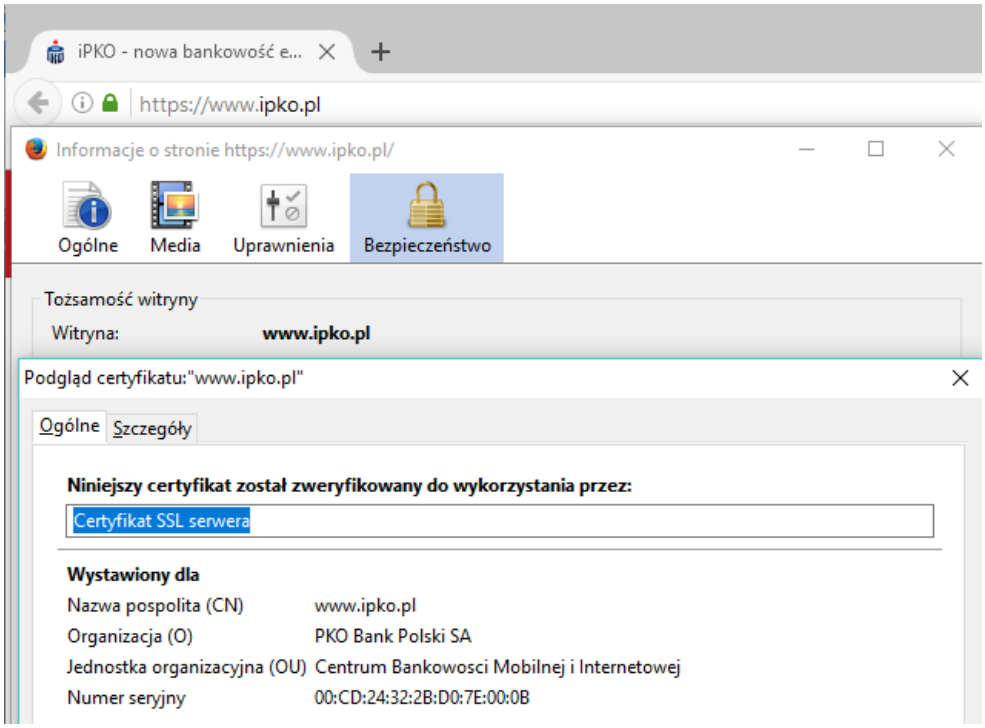
Do najczęściej kradzionych użytkownikom informacji należą dane potrzebne, aby uzyskać dostęp do różnych serwisów finansowych (bankowość internetowa, usługi związane z kartami, zakupy w e-sklepach), stron aukcji internetowych, komunikatorów internetowych, skrzynek poczty elektronicznej, gier internetowych.

Oto kilka podstawowych porad:
- Przed dokonaniem zapłaty lub wprowadzeniem danych, należy sprawdzić co inni użytkownicy sądzą o danej witrynie internetowej. Nie należy ufać jednak komentarzom pozostawionym na stronie, ponieważ mogły zostać napisane przez **cyberprzestępcę**. Lepiej zapytać o opinię osoby, które znamy.
- Jeśli musimy dokonać płatności za pośrednictwem Internetu, lepiej postarać się o osobną kartę lub konto i przelać na nią tylko niezbędną kwotę tuż przed dokonaniem zakupu.
- Zapisywanie danych karty płatniczej na później to jedno z najwygodniejszych rozwiązań **e-commerce**. Zwłaszcza, jeśli często robione są zakupy w danym sklepie. Minus jest taki, że nawet najlepszy sklep może mieć luki w zabezpieczeniach. Dane konta mogą być wykradzione, a zabezpieczenia złamane. Lepiej poświęcić chwilę na wpisywanie numeru karty, niż potem walczyć z bankiem o zwrot środków.
- Nie przepłacaj. W polskim Internecie jest mnóstwo usług, które za ciebie sprawdzą cenę danego produktu. Mowa oczywiście o porównywarkach cen (np.: http://www.ceneo.pl/, http://www.skapiec.pl/).
- Jeśli sklep internetowy ma stronę WWW w domenie drugiego lub trzeciego poziomu (np. firma.a.b.pl) lepiej zrezygnować z zakupów. Szanująca się firma zawsze znajdzie pieniądze na zarejestrowanie domeny pierwszego rzędu (np. sklep.pl).

- Jeśli mamy wątpliwości co do uczciwości transakcji, to nie należy wpłacać pieniędzy z góry, nawet za dostawę kurierską. Za usługi powinniśmy zapłacić dopiero po otrzymaniu towarów.
- Nigdy nie należy odpowiadać na e-maile od banków, funduszy inwestycyjnych czy innych organizacji finansowych. Takie organizacje nigdy nie prowadzą masowych wysyłek. Jeśli mamy wątpliwości, powinniśmy zadzwonić i sprawdzić, czy otrzymana wiadomość rzeczywiście pochodzi od tego nadawcy. W ewentualnej korespondencji nigdy nie należy podawać danych dotyczących logowania się na konto (nazwy użytkownika, numeru ID, identyfikatora i hasła).
- Po zakończeniu pracy w danym serwisie należy się **wylogować**.

Uwierzytelnienie oraz **autoryzacja** są wymagane dla stron WWW, które powinny mieć **ograniczony dostęp** dla pewnych osób. **Uwierzytelnienie** dotyczy weryfikacji czy ktoś jest tym za kogo się podaje. Zazwyczaj używa się do tego **nazwę użytkownika** oraz **hasło** (logowanie). **Autoryzacja** jest znajdywaniem czy osoba raz zidentyfikowana (np. uwierzytelniona), posiada uprawnienia do posługiwania się określonym zasobem.

Bezpieczne logowanie



Rysunek 3. Podgląd certyfikatu oraz ikona kłódki i protokół **https** na witrynie banku www.ipko.pl

- Sprawdzić, czy w obrębie okna przeglądarki internetowej znajduje się **ikona zamkniętej kłódki**. Pojawienie się tej **kłódki** sygnalizuje, że **strona jest zabezpieczona certyfikatem bezpieczeństwa i połączenie jest szyfrowane**.
- Sprawdzić poprawność **certyfikatu bezpieczeństwa**. Dane o certyfikacie dostępne są w przeglądarce po kliknięciu w **ikonę kłódki**. Po kliknięciu w kolejnym oknie zobaczymy szczegóły dotyczące certyfikatu.

2.2.5. Znajomość praw konsumenta i środków ochrony dostępnych dla obywatela podczas zakupów w Internecie

Sposób nabywania towarów w e-sklepach jest bardzo wygodny i często tańszy niż tradycyjny. Polski rynek **e-commerce** jest wciąż bardzo młody, zdecydowana większość e-sklepów funkcjonuje na rynku nie dłużej niż pięć lat i jest obsługiwana przez jedną – dwie osoby.

Wielu konsumentów unika **e-zakupów** ze strachu przed **oszustwem**, **niedostarczeniem towaru**, otrzymaniem **wadliwego** lub **uszkodzonego przedmiotu** albo obawia się innych problemów.
Gdy dochodzi do **sporu** z przedsiębiorcą w związku z **transakcją online**, kupującemu pozostaje złożenie **sprawy w sądzie**. Lepiej szukać rozwiązań polubownych, które dają szansę na szybsze i tanie załatwienie sprawy bez sądowego stresu. Przecież obu stronom kontraktu zależy na tym, by móc później dalej z sobą handlować. Szczególnie mali i średni przedsiębiorcy podkreślają to, że w rozwiązaniach polubownych jest wielka szansa na to, że nie stracą klienta.

Prawa konsumenta podczas zakupów w sieci
Prawa konsumenta reguluje:
- ustawa z dnia 2 marca 2000 r. o ochronie niektórych praw konsumentów oraz o odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny (Dz. U. z dnia 31 marca 2000 r.),
- regulaminy sklepów internetowych – rejestrując się na danych serwisie aukcyjnym czy sklepie, należy dokładnie przeczytać regulamin danego serwisu.

Bardzo przydatne witryny to:
- **Federacji Konsumentów** (http://www.federacja-konsumentow.org.pl/),
- **Poradnik konsumenta** (http://sprzedaz.konsumencka.edu.pl/federacja.html),
- **Urząd Ochrony Konkurencji i Konsumentów** (http://www.uokik.gov.pl/).

Znajduje się na nich wiele informacji oraz publikacji na różne tematy związane z kupnem i sprzedażą. Można także zasięgnąć bezpłatnych pomocy prawnych.

Zasady bezpiecznego płacenia
1. **Dbaj o połączenie**: aktualizuj swoją przeglądarkę, sprawdzaj szyfrowanie, certyfikaty oraz adresy WWW, na które zostajesz przekierowany.
2. **Ukrywaj informacje**: nie podawaj swoich danych i numeru karty w sklepach lecz wyłącznie na witrynach znanych pośredników: Dotpay, Płatności, eCard, Przelewy24, PayU czy PayPal.
3. **Ustalaj limity dzienne** na karcie kredytowej.
4. **Uważaj na oszustów**. Bank nigdy nie prosi o dane do przelewów czy numery kart w e-mailach. Nie wchodź na strony z odnośników zawartych w listach.
5. **Chroń swoje dane**. Nie wykonuj płatności na komputerach publicznie dostępnych, np. w kawiarniach internetowych, centrach handlowych.

2.2.6. Zrozumienie zagadnienia potencjalnej nieuwierzytelnionej natury witryn internetowych i ryzyka napotkania nieprawdziwych i niesolidnych informacji; możliwość podjęcia środków ostrożności

W Internecie znajduje się wiele informacji **nieaktualnych**, a nawet wręcz **nieprawdziwych**, za których umieszczanie nikt nie ponosi odpowiedzialności. Zamieszczone informacje często bardzo szybko się **dezaktualizują**, a autorzy czasami nie usuwają ich, ani nie aktualizują.

Znaleziony materiał należy poddać **krytycznej ocenie**. Zbadać przede wszystkim, czy jest **wiarygodny** (m. in. zawiera odwołania do **źródeł**, **autora**, **datę publikacji**, **wydawnictwo**, **referencje**, itp.) i czy przyda się w dalszej pracy.

2.2.7. Zrozumienie problemu i zagrożenia niekontrolowanego dostępu do Internetu przez dzieci i zdolność do ustanowienia rodzicielskiej kontroli dostępu

Informacje dostępne w Internecie, umieszczone na stronach WWW są najczęściej **dopasowane** do **odpowiednich grup użytkowników**. Aby uchronić dzieci i młodzież są celowo generowane ostrzeżenia przed treściami zawierającymi sceny tylko dla dorosłych – np. „*Czy masz 18 lat*?”

Internet nie jest prze nikogo cenzurowany. Eksperci alarmują: **brak zainteresowania rodziców** tym, co robią ich pociechy w **Sieci**, naraża je na liczne niebezpieczeństwa. Zdarza się, że **dzieci** trafiają na **niewłaściwe strony WWW** lub stają się obiektem **cyberprzemocy**, z którą nie potrafią sobie poradzić. Trzeba ostrzec je i uświadomić im czyhające na nich w wirtualnym świecie niebezpieczeństwa.

W Internecie można spotkać wiele witryn poświęconych problemowi bezpiecznego korzystania z tego źródła informacji. Poniżej zamieszczam hiperłącza do tych najbardziej znanych.
- http://www.necio.pl/,
- http://www.sieciaki.pl/,
- http://dzieckowsieci.fdn.pl/
- http://www.bezpiecznypc.pl/.

Jednym ze sposobów zabezpieczania stanowisk internetowych przed przeglądaniem treści uznawanych powszechnie za szkodliwe społecznie jest instalowanie wyspecjalizowanych programów, do których należą:
- Beniamin – http://www.beniamin.pl/,
- Cenzor – http://www.cenzor.pl/,
- Opiekun – http://www.opiekun.pl/,
- Opiekuna Ucznia w Internecie – http://www.opiekunucznia.pl/.

Systemy operacyjne (Windows 10) oraz pakiety antywirusowe również posiadają funkcję zarządzania **kontrolą rodzicielską** umożliwiającą monitorowanie stron odwiedzanych przez dzieci i ich działań w Internecie, zapewniając im ochronę przed zagrożeniami pochodzącymi z sieci. W/w oprogramowanie umożliwia również ograniczenie w dostępie do gier komputerowych oraz czasu używania komputera.

Filtry **SafeSearch** w wyszukiwarce **Google**

Filtr SafeSearch pomaga blokować grafikę, która jest nieodpowiednia lub ma charakter wyraźnie seksualny, tak aby nie pojawiała się w wynikach wyszukiwania Google. Filtr nie jest dokładny w stu procentach, ale wychwytuje większość materiałów propagujących przemoc i większość treści przeznaczonych dla dorosłych.

Informacje zamieszczone w powyższym materiale zostały opracowane na podstawie treści zawartych w:

- Syllabus e-Citizen v. 1.0,
- Podręcznik: Informatyka. Podstawowe tematy. Nowe wydanie. Autor: G. Koba. WSZ PWN 2009,
- Podręcznik: ECDL Przeglądanie stron internetowych i komunikacja. A. Żarowska – Mazur, W. Węglarz, WNPWN 2011,
- Podręcznik Od Zera Do e-Obyw@tel@, R. Bury, Ł. Galos, Wydawnictwo ITStart 2013,
- PC Format 4 / 2016. Test pakietów Internet Security 2016. Windows 10 w praktyce. Surfowanie na podsłuchu,
- PC Format 12 / 2016. Bezpieczne płatności,
- Chip. 05 / 2010. 11 zagrożeń, o których nie wiesz,
- Chip 01 / 2013. Uważaj na dzieci,
- Chip 02 / 2017. Vademecum bezpiecznego komputera,
- PC Format 6 / 2010. Płać online,
- PC Format 4 / 2010. Poznaj swojego wroga,
- witryny pakietów antywirusowych,
- http://pl.wikipedia.org/,
- https://www.google.pl/,
- http://www.komputerswiat.pl/nowosci/bezpieczenstwo/2013/40/te-wirusy-najczesciej-infekuja-polskich-internautow.aspx,
- http://securelist.pl/threats/18,co_nalezy_zrobic_gdy_komputer_zostal_zainfekowany.html,
- http://windows.microsoft.com/pl-pl/windows7/using-windows-defender,
- http://m.wyborcza.biz/biznes/1,106622,14257377,E_handel_moze_byc_jeszcze_latwiejszy.html,
- https://www.ipko.pl/,
- http://tech.wp.pl/kat,1009785,title,W-2014-r-ponad-22-tys-internetowych-oszustw,wid,17219886,wiadomosc.html,
- witryny, których adresy URL zostały umieszczone w tym opracowaniu.