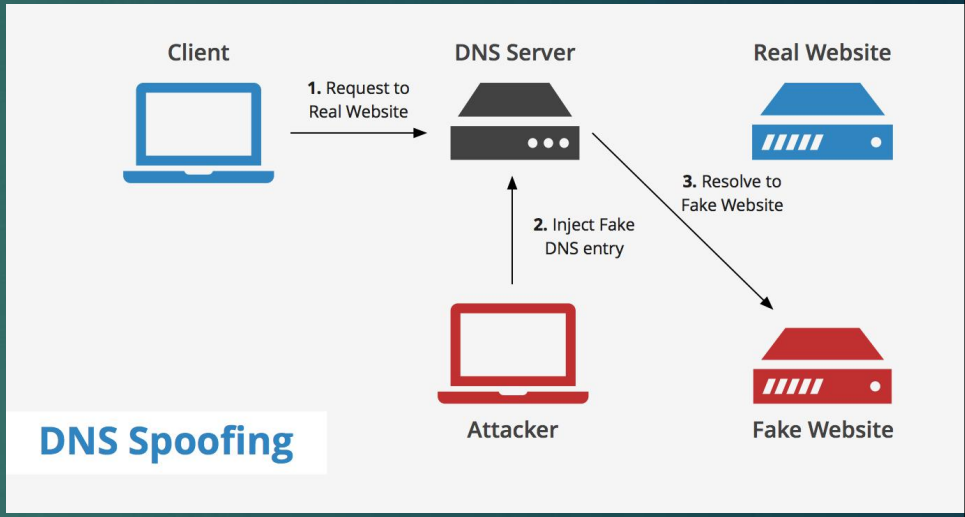
Zasady cyberbezpieczeństwa

Rodzaje ataków hakerskich

- Spoofing – metoda dla doświadczonych hakerów
- Spoofing polega na podszyciu się pod jednego użytkownika, który ma swój numer identyfikujący. Dzięki temu haker może ominąć wszystkie zabezpieczenia administratora. Spoofing udaje dowolnego użytkownika i wysyła mu sfałszowane informacje. Jest to bardzo trudny do wykrycia mechanizm. Aby się przed tym uchronić, nie powinno się włączać pakietów zawierających adresy komputera źródłowego, które znajdują się w lokalnej domenie. Warto też filtrować dane wchodzące przez router oraz wybierać zaufaną domenę, którą można znaleźć na stronie https://www.kylos.pl.



Rodzaje ataków hakerskich

- Phishing i pharming – podszywanie się pod zaufane osoby
- Phishing to udawanie osoby godnej zaufania w celu pozyskania poufnych danych, takich jak hasła czy numer karty kredytowej. Często wykonuje się to za pomocą prośby o zweryfikowanie hasła lub potwierdzenia informacji w rachunku. Gdy ofiara podaje hasło, przestępcy wykorzystują je w celach zarobkowych. Pharming natomiast polega na fałszowaniu adresów IP, które są przypisane do nazwy domen, a następnie wprowadzaniu tych danych do serwerów DNS. Gdy klient zechce wejść na witrynę swojego banku, zostanie przekierowany na złodziejską stronę. Podstawiona witryna będzie niemal identyczna jak prawdziwa.

Rodzaje ataków hakerskich

- Sniffing – podsłuchiwanie transmisji w sieci

- Sniffing to monitorowanie i zapisywanie haseł, które są używane do logowania się do zabezpieczonych systemów. Programy monitorują nazwy użytkowników i hasła, a bardziej złożone sniffery rejestrują cały ruch sieciowy. Haker korzystający ze sniffingu ma dostęp do wszystkich danych, które może odebrać w swoim zasięgu.

Rodzaje ataków hakerskich

- DDoS – blokada systemu
- DDoS to atak hakerski, który ma na celu zablokowanie określonego serwera sieciowego lub awarii całej sieci. Ten rodzaj ataku hakerskiego uniemożliwia wykonanie przez serwer jakichkolwiek usług. Program ten wykorzystuje protokół IP, który jest pokazywany publicznie. Obecnie ten rodzaj ataku jest rzadko stosowany, ponieważ łatwo się przed nim uchronić, instalując aktualizacje systemu oraz najnowsze wersje antywirusów.

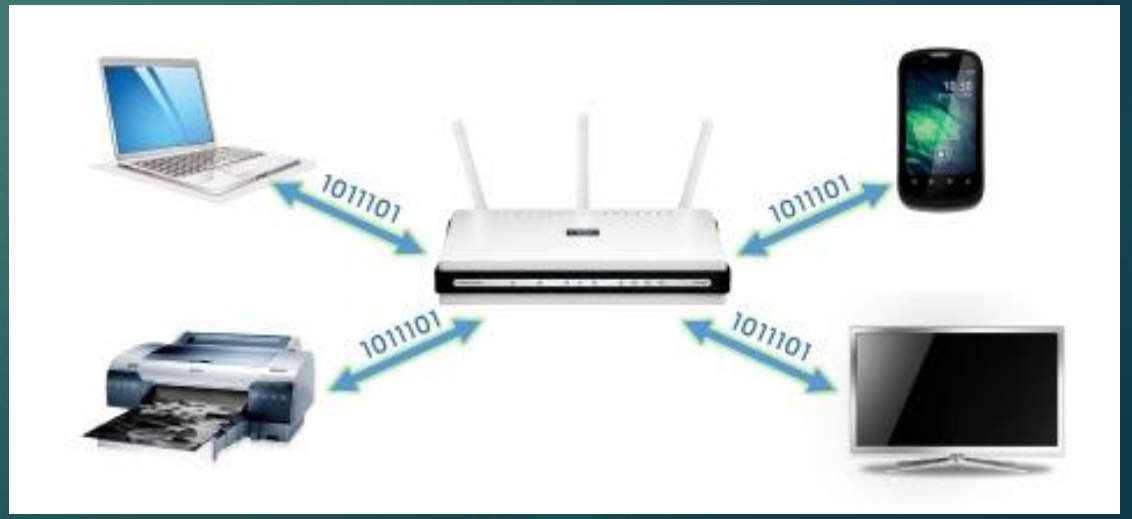
Rodzaje ataków hakerskich

- SYN flooding – „zalewanie" systemu fałszywymi informacjami
- Głównym skutkiem ataku SYN flooding jest zablokowanie usług całego serwera za pomocą protokołu TCP. Polega to na sfałszowaniu adresu IP nadawcy i wysłaniu dużej liczby pakietów z flagą SYN w nagłówku. Pakiety TCP z flagą SYN sygnalizują, że użytkownik chce się skontaktować z odbiorcą. Protokół TCP powoduje, że serwer odpowiada na każdą informację od fikcyjnych komputerów. To znacznie zwiększa natężenie przesyłu informacji i obciąża sieć. Nieprzerwany atak powoduje spowolnienie serwera, brak odpowiedzi lub nawet zawieszenie systemu. Jednym ze sposobu zabezpieczenia się przed atakiem jest używanie najnowszego firewalla, który posiada mechanizmy ograniczania pakietów SYN.

Środki zabezpieczeń przed złośliwym oprogramowaniem oraz atakami hakerskimi

- Aktualizuj system operacyjny komputera i jego oprogramowanie
- Gdy tylko możesz, korzystaj z konta bez uprawnień administratora
- Dobrze się zastanów, zanim klikniesz linki lub cokolwiek pobierzesz
- Zachowaj ostrożność, otwierając załączniki lub obrazy otrzymane w e-mailu
- Nie ufaj wyskakującym okienkom z prośbami o pobranie oprogramowania
- Uważaj podczas korzystania z usług wymiany plików
- Stosuj programy antywirusowe

Zagrożenia dla sfery psychicznej (emocjonalnej), fizycznej, społecznej, poznawczej, wynikające z przebywania w cyberprzestrzeni



Zagrożenia fizyczne

- Z danych statystycznych wynika, że ok. 30% osób pracujących przy stanowisku komputerowym cierpi na różne dolegliwości nabyte w przebiegu wykonywanej pracy. Najbardziej narażone części ciała na problemy zdrowotne to:
  - nadwyrężenie mięśni nadgarstka
  - naprężony kark
  - skrzywienia kręgosłupa, bóle dolnych jego części,
  - zanik mięśni pasa biodrowego,
  - oczy (niewłaściwe oświetlenie powoduje męczenie się wzroku),
  - bóle głowy,
  - brak apetytu,
  - nadpobudliwość psychoruchowa lub wręcz przeciwnie, apatia i depresja
  - ogólne zmęczenie organizmu.

Zagrożenia psychiczne

- Bardzo niewielu ludzi uświadamia sobie, że komputer może uzależnić podobnie jak alkohol czy narkotyki. Proces ten początkowo jest niezauważalny lecz wraz z rozwojem powoduje wyraźne szkody. Najpierw można zaobserwować postępującą izolację, która sprawia, że uzależniony zastępuje maszyną związki z innymi ludźmi. Tworzy się silny związek emocjonalny z komputerem co z kolei osłabia wciąż emocjonalną z otoczeniem, zaburza wzajemną komunikację, a życie powoli zaczyna przebiegać w oderwaniu od realnego świata.

Zagrożenia moralne

- W obecnych czasach dość powszechna jest fascynacja Internetem, oferującym łatwy i szybki dostęp do olbrzymich zasobów informacji. Wielokrotnie nie są to treści wiarygodne i pożądane z punktu widzenia interesów rodziny i szkoły mogące zagrozić moralnemu rozwojowi dzieci i młodzieży.

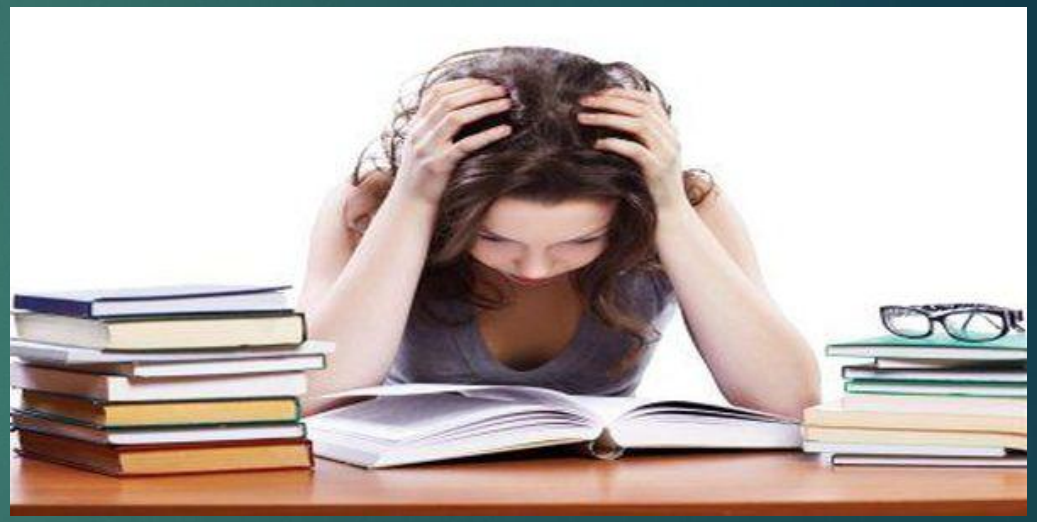
Zagrożenia społeczne

- Anonimowość i brak hamulców przy komputerze i w sieci często powodują zachowania nieetyczne. Zdarza się, że na co dzień grzeczni i dobrzy uczniowie prowadząc internetowe pogawędki wypluwają z siebie stek okropnych przekleństw i wulgaryzmów, których nie odważyliby się powiedzieć na głos nawet przed samym sobą. W sieciowych kontaktach nikt nas nie kontroluje, nie widzi. Można zmienić swoją tożsamość, płeć, wiek, zawód, możemy udawać kogo chcemy. Tak samo w sieciowych grach typu fantasty, w których gracz jest zupełnie inną osobą niż w realnym świecie.

Zagrożenia intelektualne

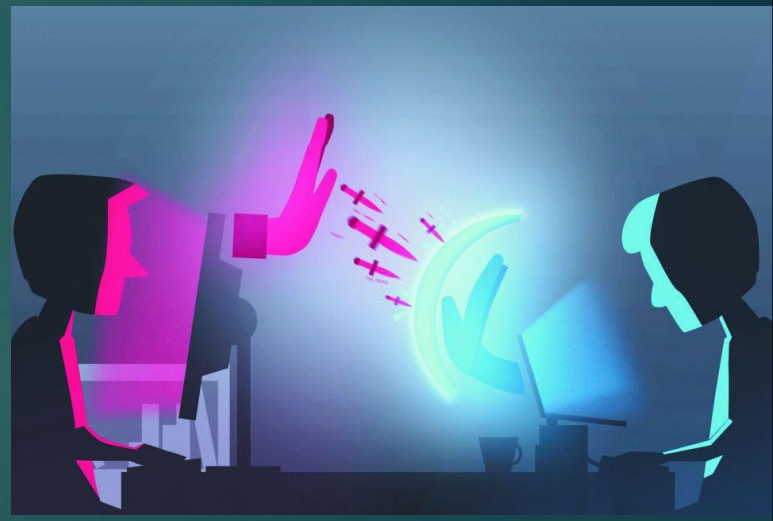
- Skupiają się w dwóch nurtach. Jeden z nich to problem bezkrytycznego zaufania do możliwości maszyny.

- Wśród młodych ludzi panuje przekonanie, że komputer jest dobry na wszystko, wszystko może i nigdy się nie myli. Może to wynikać z faktu przypisania zwykłej maszynie cech, których ona w sposób oczywisty nie posiada, tj. zdolności do poprawiania pomyłek człowieka, obdarzania zwykłych ludzi nadnaturalną charyzmą, czynienia życia szczęśliwym, itp.



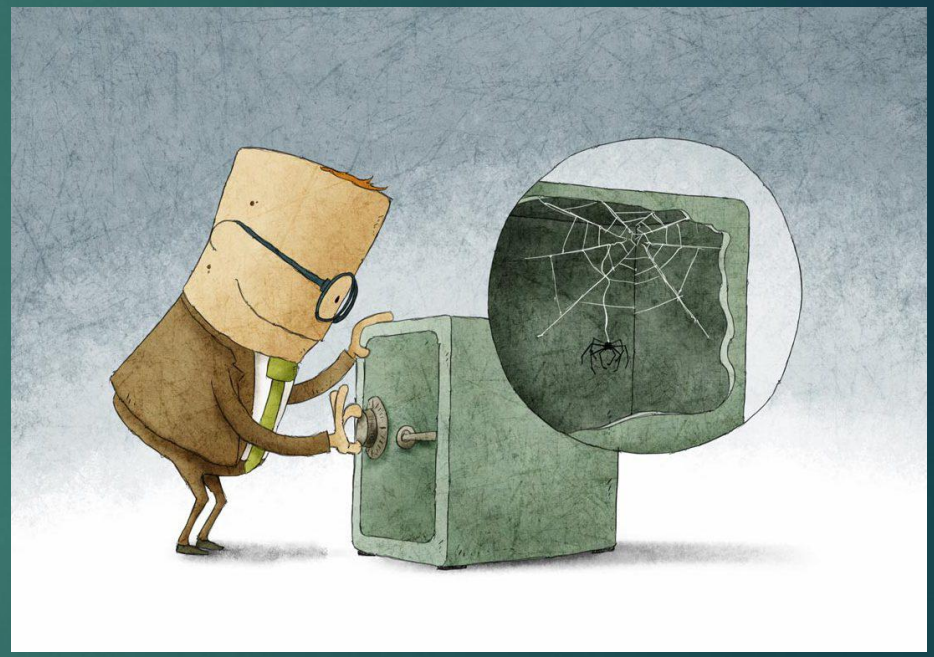
Sposoby przeciwdziałania zagrożeniom wynikającym z przebywania w cyberprzestrzeni

- konsekwentne stosowanie zasady: najpierw obowiązki, później rozrywka,
- bezwzględne ograniczenie czasu spędzanego przy komputerze do 1-4 godzin dziennie w zależności od wieku dziecka,
- proponowanie innych, atrakcyjnych form spędzania wolnego czasu (sport, turystyka, hobby niezwiązane z komputerem),
- poświęcanie dziecku jak najwięcej czasu i zainteresowania,
- czasami wprowadzanie okresów całkowitej abstynencji,
- bezwzględny zakaz korzystania z Internetu dla dzieci do lat 12 bez nadzoru dorosłych.



Zasad bezpiecznego przechowywania danych

- 5 zasad bezpiecznego przechowywania danych
  - Zasada 1: Chroń swój komputer.
    - Zasada 2: Walcz ze złośliwym oprogramowaniem.
  - Zasada 3: Rób kopie zapasowe.
    - Zasada 4: Myśl o przyszłości.
  - Zasada 5: Trzymaj kopie plików w kilku miejscach.



Zasady bezpieczeństwa swojego cyfrowego wizerunku i tożsamości

- Zwykle przejmujemy się tym, co myślą o nas inni. Opinia na nasz temat zależy od wielu czynników. Może mieć na nią wpływ nasze zachowanie, ubiór czy zainteresowania. Wszystko to składa się na nasz wizerunek.

- We współczesnym świecie internet stał się ważną przestrzenią tworzenia naszego wizerunku. Nasze aktywności w sieci mają na niego duży wpływ.

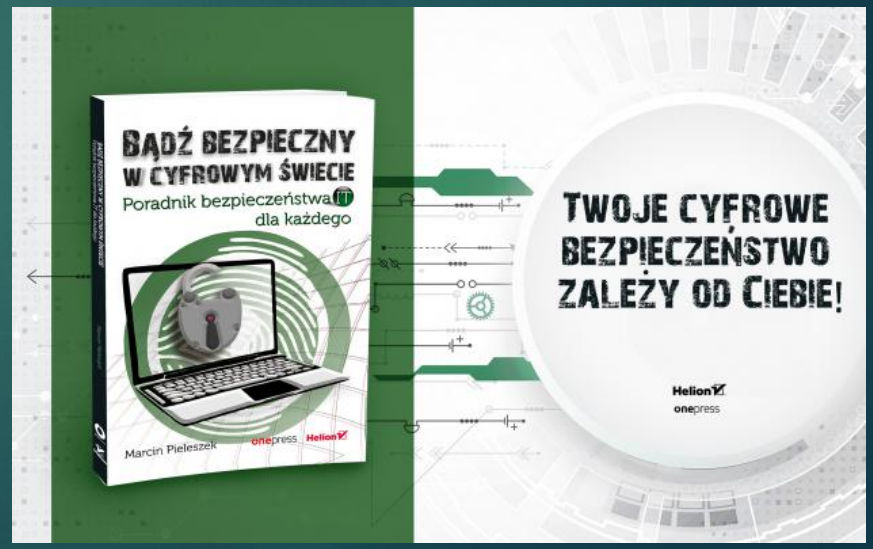
Zasady bezpieczeństwa swojego cyfrowego wizerunku i tożsamości

Na twój wizerunek w sieci wpływają m. in.:

- Twój sposób wyrażania się — to, czy piszesz zgodnie z zasadami poprawnej polszczyzny, czy przeklinasz, jak dużym zasobem słownictwa się posługujesz;
- profile na portalach społecznościowych, a w szczególności:
- zdjęcia, na których jesteś i które udostępniasz,
- informacje „o mnie”,
- twoje statusy,
- strony, które „lubimy”,
- nasze komentarze pod artykułami i wypowiedzi na forach,
- forma adresu mailowego i sposób pisania maili.

Zasady prywatności w cyfrowym świecie

- Dbaj o swoje dane osobowe
- Używaj różnych adresów e-mail
- Korzystaj z różnych komputerów lub urządzeń do różnych celów
- Używaj bezpiecznych haseł i oprogramowania zabezpieczającego
- Chroń swoje najważniejsze dane poprzez szyfrowanie
- Kasuj dane bezpowrotnie



Podstawowe pojęcia związane z ochroną danych osobowych, ochroną informacji

- „dane osobowe” – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

- Przykładowe inne dane osobowe to: adres, PESEL, adres e-mail, numer telefonu, adres IP komputera, numer konta bankowego.

Podstawowe pojęcia związane z ochroną danych osobowych, ochroną informacji

- „przetwarzanie" oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany.
- Najczęściej wykonywane przetwarzanie danych osobowych to: zbieranie, utrwalanie, przeglądanie, rozpowszechnianie lub innego rodzaju udostępnianie, usuwanie lub niszczenie

Podstawowe pojęcia związane z ochroną danych osobowych, ochroną informacji

- „profilowanie” oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się
- „administrator” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych

Podstawowe pojęcia związane z ochroną danych osobowych, ochroną informacji

- „podmiot przetwarzający” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora

- „zgoda” osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych

Podstawowe pojęcia związane z ochroną danych osobowych, ochroną informacji

- „naruszenie ochrony danych osobowych" oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych
- ABI - Administrator Bezpieczeństwa Informacji
- ADO - Administrator Danych osobowych
- ASI – Administrator Systemów Informatycznych

Podstawowe pojęcia związane z prawami autorskimi i własnością intelektualną

- Cytat Przytoczenie drobnych utworów lub fragmentów utworów, bez dokonywania zmian, w odrębnym dziele. Przytaczany utwór lub jego fragment musi pozostawać w takiej proporcji do wkładu twórczości własnej, aby nie było wątpliwości co do tego, że powstało własne dzieło. Cytat powinien być tak oznaczony, by czytelnik wiedział, kiedy ma do czynienia z tekstem autora posługującego się cytatem, a kiedy z samym cytatem. Cytat nie może naruszać normalnego korzystania z utworu ani godzić w słuszne interesy twórcy.

- Plagiat Przywłaszczenie cudzego autorstwa. Plagiat popełnia nie tylko ta osoba, która przejmuje cudzy utwór w całości, ale również ta, która przywłaszcza sobie jedynie fragmenty dzieła.

Podstawowe pojęcia związane z prawami autorskimi i własnością intelektualną

- Prawa majątkowe Prawo do decydowania o sposobach korzystania z utworu na wszystkich polach eksploatacji. Łączy się ono z czerpaniem korzyści finansowych przez osobę, która takie prawo posiada (prawo do wynagrodzenia). Z reguły przysługuje ono twórcy, jednak może też przysługiwać wydawcy, producentowi lub pracodawcy. Jest ono zbywalne (z wyjątkiem niektórych przypadków prawa do wynagrodzenia), ograniczone w czasie (co do zasady wygasa po upływie 70 lat od śmierci twórcy) i podlega dziedziczeniu.
- Prawa osobiste Prawa, które są na stałe związane z twórcą i nie są ograniczone w czasie. Prawo Autorskie mówi m.in. o takich prawach osobistych, jak prawo do: autorstwa utworu; oznaczenia dzieła własnym nazwiskiem, pseudonimem lub udostępnienia go anonimowo; decydowaniu o pierwszym udostępnieniu utworu publiczności.

Podstawowe pojęcia związane z prawami autorskimi i własnością intelektualną

- Licencja Umowa, której istotą jest zezwolenie na korzystanie z utworu na określonych w niej polach eksploatacji. Umowa licencyjna nie przenosi na na licencjobiorcę autorskich praw majątkowych – do tego konieczne jest zawarcie umowy o przeniesienie praw.

Podstawowe pojęcia związane z prawami autorskimi i własnością intelektualną

- Autorskie prawa majątkowe są ograniczone w czasie, i trwają:

- przez cały czas życia twórcy i 70 lat po jego śmierci;
- jeżeli twórca nie jest znany – 70 lat od daty pierwszego rozpowszechnienia utworu.

Podstawowe pojęcia związane z prawami autorskimi i własnością intelektualną

- Autorskie prawa osobiste są prawami „ojcostwa utworu” i obejmują przede wszystkim prawo autora do wiązania z dziełem jego nazwiska. Prawo to nigdy nie wygasa i jest, z natury rzeczy, niezbywalne, nie można się go zrzec ani przenieść na inną osobę

Potrzeby ochrony danych osobowych, ochrony informacji, praw autorskich i własności intelektualnej

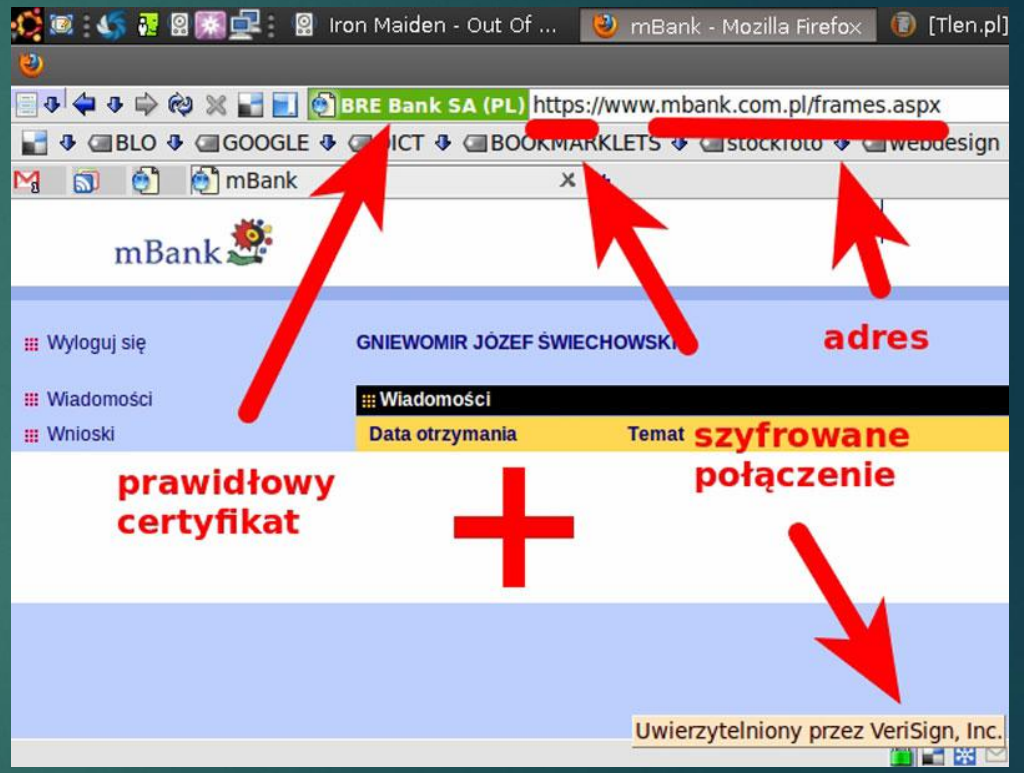
- Dlaczego gromadzimy dane osobowe:

- Kiedy użytkownik tworzy konto przetwarzamy dane osobowe (takie jak imię i nazwisko, adres e-mail, nazwę stanowiska pracy czy nazwę szkoły), by można było prawidłowo zarządzać kontem użytkownika i zapewniać najlepszą możliwą obsługę klienta. Wszelkie dane osobowe, jakie są przetwarzane, bezpośrednio łączą się z konkretnym celem np. prośba o treści internetowe (np. biuletyn informacyjny, plik wideo itp.).

Potrzeby ochrony danych osobowych, ochrony informacji, praw autorskich i własności intelektualnej

- Użytkownik może w dowolnej chwili uzyskać dostęp do swoich danych osobowych, zaktualizować je, poprawić lub usunąć przez zalogowanie się do swojego konta lub kontaktując się z obsługą klienta. Bardziej szczegółowe informacje na temat tego, w jaki sposób chronione są dane umożliwiające identyfikację osobistą, można znaleźć w Polityce prywatności danej firmy.

Zasady dokonywania bezpiecznych transakcji w internecie



- Korzystaj wyłącznie z pewnego komputera
- Uważaj na oszustów w sieci
- Chroń swoje dane logowania do bankowości elektronicznej
- Sprawdź wiarygodność sklepu internetowego
- Wybierz optymalny dla siebie system płatności on-line