Strona internetowa projektu (Internet)

Materiał "Strona internetowa projektu (Internet)" składa się z sekcji: "Wstęp", "Wybór technologii tworzenia serwisów WWW", "Projekt strony", "Tworzenie strony z wykorzystaniem: HTML 5 i CSS3", "Publikacja i administracja strony WWW", "Walidacja stron internetowych", "Zarządzanie kontem pocztowym projektu", "Bezpieczeństwo w Internecie".

Materiał zawiera 47 ilustracji (fotografii, obrazów, rysunków).

Strona internetowa projektu (Internet)

Wstęp

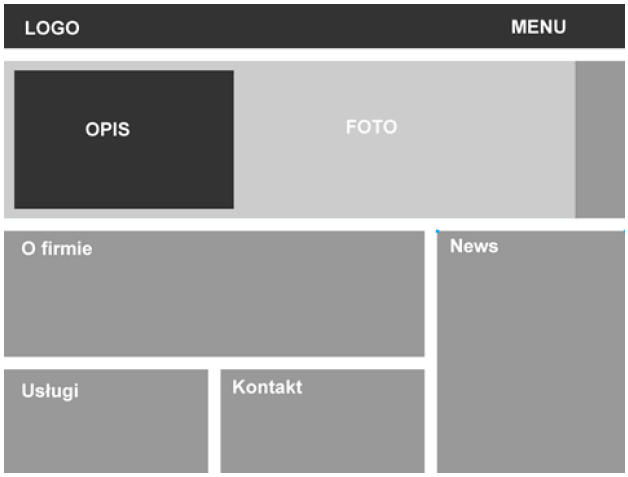
Projekt jest już niemalże skończony. Ostatnim etapem będzie opublikowanie efektów pracy w Internecie. W tym celu należy przygotować prostą stronę internetową prezentującą wykonaną aplikację. Projekt strony internetowej powinien być spójny z wyglądem aplikacji. Potrzebny będzie również dostęp do konta pocztowego, aby zapewnić możliwość komunikacji z użytkownikami stworzonej aplikacji.

Wybór technologii tworzenia serwisów WWW

Należy się zastanowić, jakie informacje i dane dotyczące realizowanego projektu powinno się umieścić na stronie internetowej. Wybór technologii, w jakiej będzie tworzona strona, zależy od rodzaju treści i sposobu ich prezentacji. Najprostszą możliwością jest zapisanie utworzonej wcześniej prezentacji multimedialnej w formacie html.
W ramach realizowanego projektu można utworzyć stronę promującą opracowaną aplikację w technologii HTML5 z zastosowaniem kaskadowych arkuszy stylów. Przed przejściem do implementacji, należy zaplanować układ strony.

Projekt strony

Układ poszczególnych elementów (tzw. layout) strony internetowej w dużej mierze zależy od funkcji jaką będzie pełniła projektowana strona. Jeśli ma ona zaprezentować zrzuty ekranu ze stworzonej gry komputerowej lub fotografie z multimedialnego przewodnika geograficznego, konieczne będzie zaplanowanie dostatecznej przestrzeni lub nawet osobnej podstrony na galerię. W przypadku symulatora lotów kosmicznych najważniejsze mogą być zebrane dane statystyczne osadzone na stronie w postaci tabelki.



Źródło: Piotr Napieralski, licencja: CC BY 3.0.

Tworzenie strony z wykorzystaniem: HTML 5 i CSS3

Stronę internetową można napisać wykorzystując zwykły notatnik. Edytory tekstu mają możliwość zapisu pliku w formacie html. Dzięki tej opcji można zaprojektować stronę internetową bez znajomości html, jednak bardzo pomocne jest wykorzystanie podstawowych poleceń i tagów języka html.
W Internecie można znaleźć wiele darmowych edytorów html do projektowania stron WWW. Bardzo pomocną opcją jest możliwość kolorowania składni oraz sprawdzanie poprawności kodu. Rozwiązania te pomagają sprawnie edytować tworzoną stronę. Tworząc stronę w języku polskim, ważne jest by edytor miał możliwość kodowania polskich znaków w standardzie ISO i UTF. Znaczniki html, w większości składają się ze znaczników otwierających i zamykających, dlatego bardzo pomocną opcją jest ich domykanie. W sieci można znaleźć także edytory wizualne oraz kreatory szkieletu strony, które w sposób automatyczny są w stanie wygenerować szkielet

projektowanej witryny
W tabeli zestawiono nazwy popularnych edytorów dla różnych systemów operacyjnych

Nazwa	System operacyjny
Adobe Dreamweaver	Windows
Ager Web Edytor	Windows
Bluefish	Windows, Linux, Mac OS X
CoreEditor	Windows
EdHTML	Windows
HateML Pro 2	Windows
kED	Windows
KompoZer	Windows
Microsoft Expression Web	Windows
Pajączek	Windows
nvu	Windows
PSPad	Windows
Web Edit	Windows
Notepad++	Windows
NetBeans	Windows
Kate	Linux
Quanta Plus	Linux
getedit	Linux
Geany	Linux
Smultron	Mac OS X
Taco HTML Edit	Mac OS X
Fraise	Mac OS X

Źródło: Piotr Napieralski, licencja: CC BY 3.0.

Jednym z polecanych edytorów jest Bluefish, gdyż stanowi wolne oprogramowanie. Dzięki wieloplatformowości, pozwoli na sprawną naukę edytora przez użytkowników różnych systemów operacyjnych. Program posiada szereg przydatnych funkcji, takich jak kolorowanie składni HTML, PHP, C, Javy, JavaScriptu, JSP, SQL, XML, Pythona, Perla, CSS, ColdFusion, Pascala, R i Octave/Matlab, automatyczne zamykanie znaczników HTML I XML. Ma wbudowane funkcje kreatora stron (np. automatyczne generowanie galerii obrazów). Adres z którego można go pobrać:
http://www.bennewitz.com/bluefish/stable/source/
Aby móc obejrzeć zaprojektowaną stronę WWW należy ją otworzyć w przeglądarce. Przeglądarki internetowe do niedawna komunikowały się z serwerem za pomocą protokołu HTTP, choć obecnie najpopularniejszym protokołem staje się HTTPS. Najpopularniejsze przeglądarki na rynku światowym (dane z grudnia 2015 według serwisu www.w3schools.co) to:

- Google Chrome – 66,5%
- Internet Explorer – 6,9%
- Mozilla Firefox – 20%
- Safari – 3,6%
- Opera – 1,4%

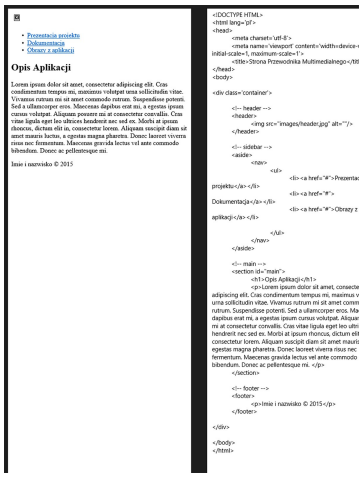
Większość przeglądarek (w najnowszych wersjach) wspiera HTML5 i CSS3.
HTML to język do oznaczania składni (markup), który pozwala klasyfikować zawartość dokumentu z rozszerzeniem .html lub .htm. Pojedynczy element HTML nosi nazwę Taga lub znacznika. Każdy znacznik może zawierać skojarzone z nim atrybuty.

Konstrukcja HTML5 różni nieco od konstrukcji strony w HTML czy XHTML. Każdy dokument będzie się zaczynał od wpisu określającego rodzaj języka. Jest to informacja dla przeglądarki w jaki sposób interpretować występujące na stronie znaczniki. Dla HTML5 znacznik otwierający to
<!DOCTYPE html>.
Następnym elementem wspólnym dla wszystkich języków html jest znacznik
<html></html>.
Wewnątrz tego znacznika tworzona będzie treść projektowanego dokumentu czyli właściwa zawartość strony WWW.
W strukturze strony można wyróżnić dwie zasadnicze części. Części te zdefiniowane są odpowiednio w znacznikach *<head></head>* oraz *<body> </body>*. Pierwszy znacznik odpowiada za określenie podstawowych właściwości strony (tytuł, strona kodowa, informacje o autorze, słowa kluczowe itp.).
Druga część zamknięta w znacznikach *<body></body>*, jest to ciało strony czyli to co zostanie wyświetlone w oknie przeglądarki.
Podstawowy szkielet strony HTML5 jest następujący:

```
1  <!DOCTYPE html>
2  <html>
3  <head>
4  <meta charset="utf-8" />
5  <title>To jest przykładowa strona</title>
6  </head>
7  <body>
8  A tutaj treść strony
9  </body>
10 </html>
```

Źródło: Piotr Napieralski, licencja: CC BY 3.0.

Poniżej znajduje się przykładowy szkielet ze zdefiniowanym układem strony i podstawową treścią.



Źródło: Piotr Napieralski, licencja: CC BY 3.0.

Na projektowanej stronie internetowej powinny znaleźć się informacje na temat stworzonej aplikacji. Na stronie głównej można umieścić logo projektu i podstawowe informacje na temat funkcjonalności i charakterystyki autorskiej aplikacji. W menu nawigacyjnym powinny znajdować się odnośniki do podstron zawierających dokumentację projektu oraz podstron zawierających prezentację zrzutów ekranowych z aplikacji.
Podstrony, z którymi będą się łączyć hiperłącza projektowanej strony wykonane zostaną z dokumentów powstałych podczas realizacji projektu, to znaczy:

- prezentacja będzie wcześniej stworzoną prezentacją zapisaną w formacie html,
- dokumentacja będzie linkiem do pliku dokumentacji zapisanego w formacie pdf,
- obrazy to podstrona stworzona w html, zawierająca zdjęcia z aplikacji.

Szkielet strony jest już gotowy, więc można zająć się jej stylem z wykorzystaniem CSS, aby nabrała ona odpowiedniego wyglądu. Ponieważ szerokość została ustalona na 1050px, tak więc kod CSS będzie wyglądał następująco:

```
* {padding:0;margin:0;}

html {width:100%;height:100%;}
body {font-family:Arial, Helvetica, Sans-serif;font-size:14px;line-height:1.5;font-weight:400;color:#4

.container {margin:0 auto;}

header {margin:25px 0;}
header img {width:100%;}

aside {float:left;margin:0 0 25px;}
aside nav ul {list-style:none;}
aside nav ul li {margin-bottom:1px;}
aside nav ul li a {display:block;text-decoration:none;color:#000;background:#ff0040;padding:8px 20px;}
aside nav ul li a:hover{background:#212121;color:#FFF;}

#main {float:right;margin:0 0 25px;}

footer {clear:both;color:#FFF;background:#FF0000;padding:15px 0 15px 30px;margin:0 0 25px;}
```

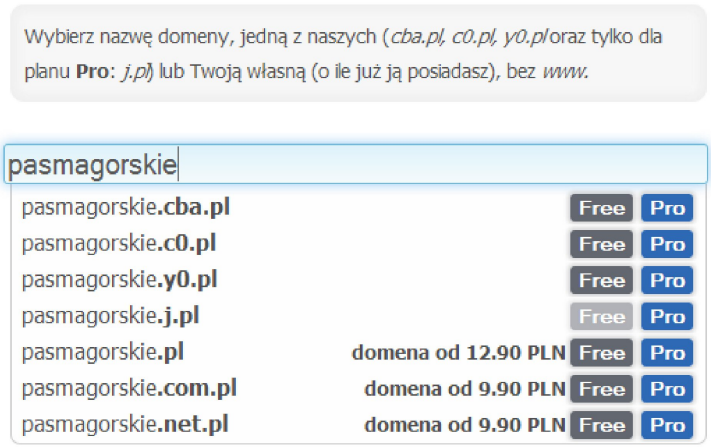


Źródło: Piotr Napieralski, licencja: CC BY 3.0.

Szablon można rozbudować o kolejne podstrony.

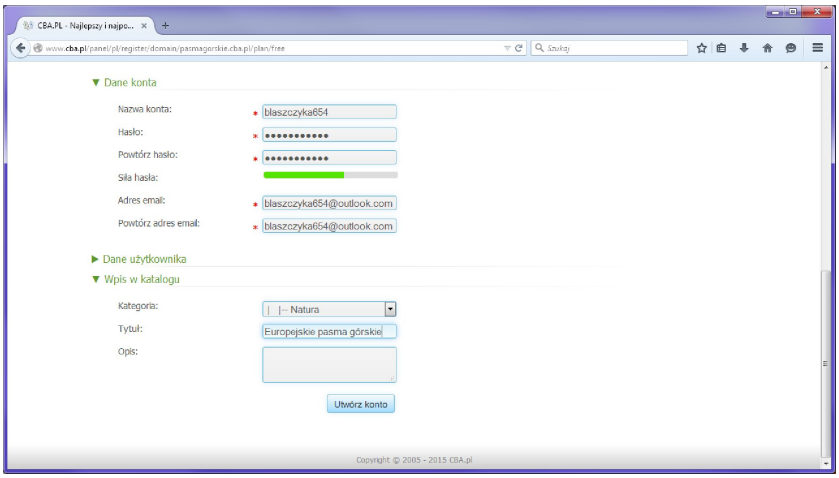
Publikacja i administracja strony WWW

Po utworzeniu stron internetowych, ważnym zadaniem jest pokazanie ich internautom. W celu udostępnienia strony internetowej publicznie, można skorzystać z darmowych usług hostingu. Takie możliwości daje np. portal „cba.pl". Aby z nich skorzystać, wystarczy zarejestrować się na stronie *www.cba.pl*, podając potrzebne dane.
W miejscu nazwy domeny należy podać nazwę, która będzie w adresie strony. To może być nick, w przypadku strony domowej, lub fragment opisujący zawartość np. „pasmagorskie". Domena może składać się z małych liter, myślników i cyfr:



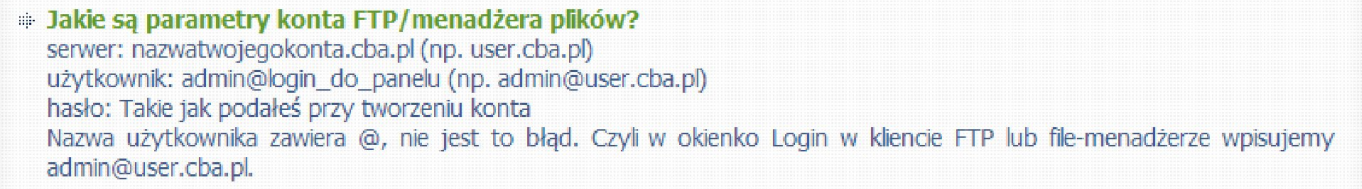
Źródło: Sławomir Szaruga, licencja: CC BY 3.0.

W celu utworzenia darmowego konta należy wybrać opcję „Free" spośród bezpłatnych domen. Następnie podać nazwę użytkownika, hasło do konta i adres e-mail. Dodatkowo można wprowadzić szczegóły odnośnie stworzonej strony, takie jak kategoria i tytuł, aby łatwiej byłą ją znaleźć w wyszukiwarce internetowej.



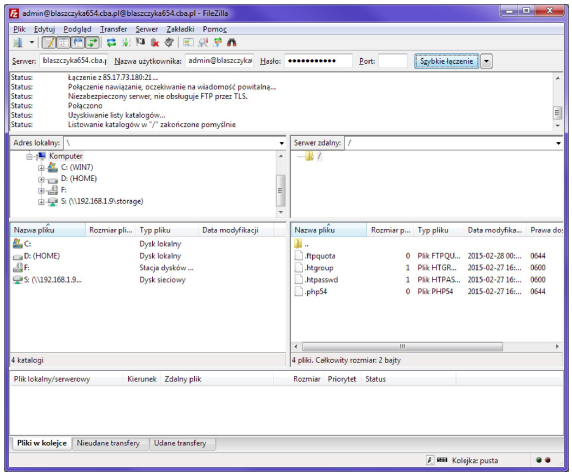
Źródło: Sławomir Szaruga, licencja: CC BY 3.0.

Dostęp do serwera przechowującego pliki strony u większości usługodawców jest możliwy za pomocą protokołu transferu plików – FTP (File Transfer Protocol). Wygodnym sposobem na przesłanie danych jest wykorzystanie, na przykład, programu FileZilla, dostępnego dla różnych systemów operacyjnych. W głównym oknie programu można wprowadzić adres serwera i dane logowania, które będą opisane w szczegółach lub pomocy na portalu usługodawcy.



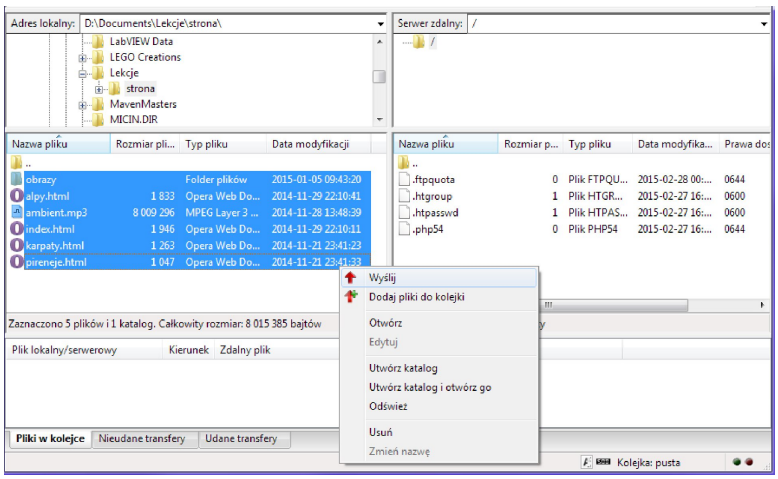
Źródło: Sławomir Szaruga, licencja: CC BY 3.0.

Po pomyślnym połączeniu, po prawej stronie programu pojawią się pliki przechowywane na serwerze:



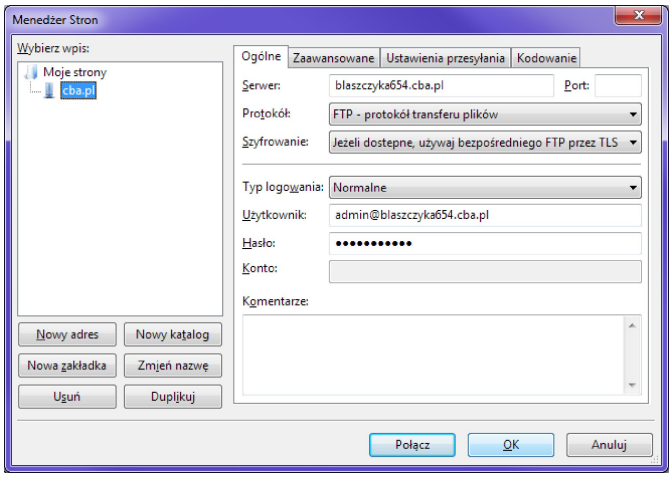
Źródło: Sławomir Szaruga, licencja: CC BY 3.0.

Po pierwszym połączeniu może być widoczna przykładowa zawartość strony oraz pliki konfiguracyjne. Jeżeli wśród elementów na serwerze znajduje się folder „public_html", to w nim należy umieszczać pliki strony. W innym wypadku można je kopiować bezpośrednio do katalogu głównego, jednak zawsze warto się upewnić, sprawdzając w pomocy na portalu usługodawcy.
W celu przesłania plików należy znaleźć folder ze stroną na swoim komputerze, nawigując w lewej części okna programu do miejsca zawierającego plik „index.html". Następnie trzeba zaznaczyć wszystkie elementy i przeciągnąć do okna po prawej stronie, lub klikając na nie prawym przyciskiem myszy wybrać „Wyślij":



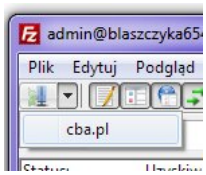
Źródło: Sławomir Szaruga, licencja: CC BY 3.0.

Postęp widoczny będzie na dole. Przesyłanie może potrwać dłużej, w zależności od rozmiaru plików.
Po skończeniu przesyłania, należy wpisać w przeglądarce adres strony, w celu sprawdzenia czy działa ona poprawnie.
Głównym plikiem strony jest „index.html". Jest on wczytywany po wpisaniu bezpośredniego adresu w przeglądarce. Przykładowo:
http://www.pasmagorskie.cba.pl/
jest odpowiednikiem:
http://www.pasmagorskie.cba.pl/index.html
Dotyczy to również podkatalogów na stronie:
http://www.pasmagorskie.cba.pl/podkatalog/
odpowiada adresowi:
http://www.pasmagorskie.cba.pl/podkatalog/index.html
Jeżeli wszystko odbyło się bez problemów, można zapisać połączenie do serwera FTP w pamięci programu FileZilla. Z menu „Plik" należy wybrać „*Kopiuj aktualne połączenie do Menedżera Stron*", podać jego nazwę i zatwierdzić przyciskiem OK.



Źródło: Sławomir Szaruga, licencja: CC BY 3.0.

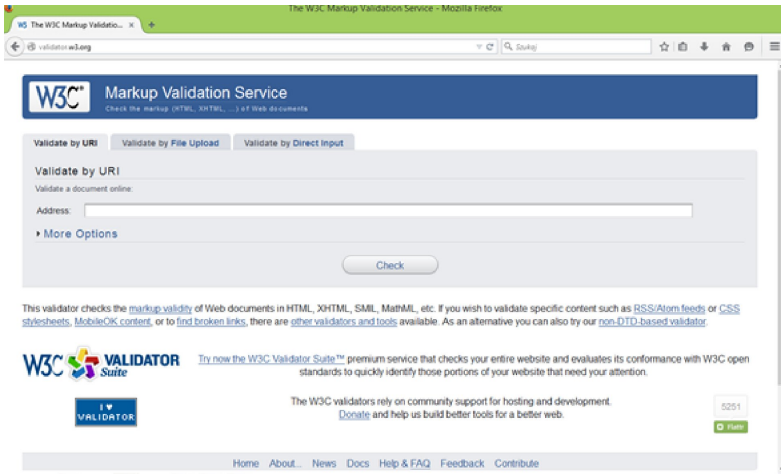
Później można skorzystać z zapisanego połączenia, wybierając je z rozwijanego menu obok pierwszego przycisku na górze.



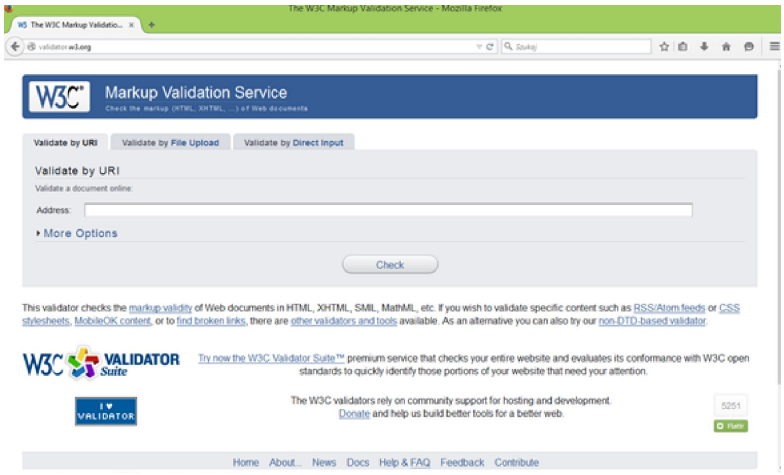
Źródło: Sławomir Szaruga, licencja: CC BY 3.0.

Walidacja stron internetowych

Przed opublikowaniem strony w sieci należy upewnić się, że jest ona poprawnie skonstruowana. Pomimo dobrego wyglądu, może zawierać błędy znajdujące się w jej kodzie. Aby nie publikować wadliwych dokumentów (ładują się dłużej), należy sprawdzić poprawność kodu strony pod kątem jego zgodności ze specyfikacją języka. Do tego celu służą specjalne aplikacje, tzw. walidatory, które dodatkowo zwracają uwagę na brakujące lub źle użyte znaczniki, błędne ich zagnieżdżanie oraz na złe użycie stylów.
Jedną z nich jest aplikacja udostępniona przez organizacje W3C (World Wide Web Consortium) na stronie pod adresem *http://validator.w3.org*

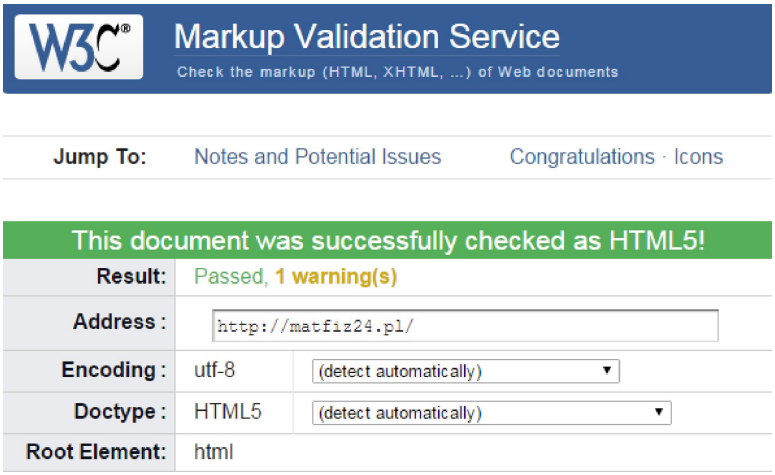


Źródło: Sławomir Szaruga, licencja: CC BY 3.0.

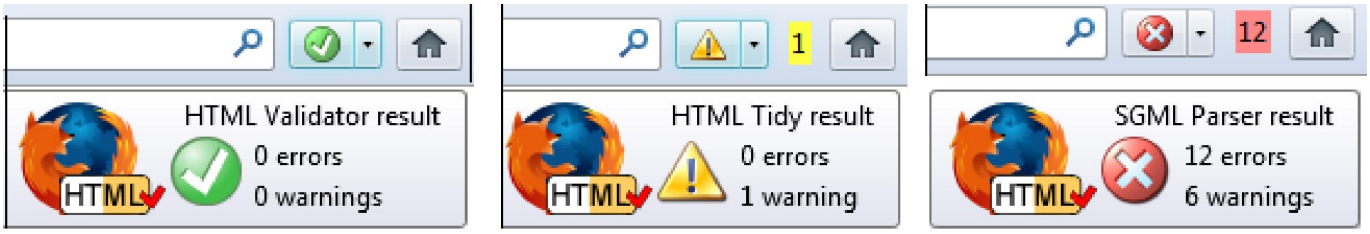


Źródło: Sławomir Szaruga, licencja: CC BY 3.0.

Umożliwia ona sprawdzenie kodu strony poprzez podanie adresu strony internetowej, załadowanie pliku HTML strony lub wklejenie bezpośrednie jej kodu HTML. Po wybraniu jednej z powyższych możliwości, po kliknięciu „Check" zostanie ukazany wynik.



Źródło: Sławomir Szaruga, licencja: CC BY 3.0.



Źródło: Sławomir Szaruga, licencja: CC BY 3.0.

Zielone kółko oznacza poprawność kodu HTML, pomarańczowy trójkąt, że na stronie znajdują się drobne zastrzeżenia, a czerwone kółko, że strona posiada poważne błędy. Za dopuszczalny można uznać wynik z maksimum 3 błędami.

Będąc pewnym, że strona jest poprawnie zbudowana, można śmiało udostępnić ją w sieci internetowej.

Zarządzanie kontem pocztowym projektu

Korzystając z projektowego konta pocztowego (np. konta Microsoft) należy pamiętać o omówionych w poprzednich klasach zasadach netykiety, czyli swoistego kodeksu zachowania obowiązującego wszystkich użytkowników sieci.
Obecnie, netykieta uznana za formę kodeksu Internautów, pełni rolę pośrednią między zwyczajem a prawem.



Źródło: Sławomir Szaruga, licencja: CC BY 3.0.

Treści netykiet znajdują się od niedawna w Kodeksie Cywilnym i dotyczą: tajemnicy korespondencji, plagiatu, używania niewłaściwego języka. Z kolei w polskim Kodeksie Karnym (k.k.) z 1997 roku znajdujemy je w treściach dotyczących:

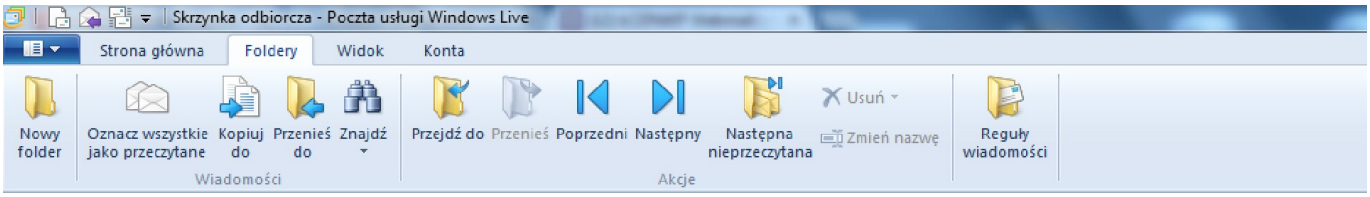
- ochrony prawa własności (wszystkie zasoby sieciowe znajdujące się na serwerach),
- tajemnicy korespondencji znajdującej się w skrzynkach poczty elektronicznej.

W przypadku prawa karnego, praktyka dowodzi, iż popełniane przestępstwa można rozpatrywać w oparciu o ustawy takie jak: Ustawa o świadczeniu usług drogą elektroniczną czy Ustawa o prawie autorskim.
Innymi regulacjami dotyczącymi funkcjonowania Internetu są regulaminy tworzone przez firmy udostępniające bezpłatne korzystanie z kont e-mail i www, a także regulaminy kawiarenek internetowych.
Jak widać, netykieta i prawo wzajemnie się uzupełniają. Netykieta może być więc uznana za część norm życia społecznego, ale rzadko spotykamy odwoływanie się do jej zasad w orzecznictwie sądowym. W polskim prawie nie ma ich spisanych w formie jednolitego „prawa internetowego", ale kwestie ewentualnych przestępstw są uwzględniane we wspomnianych kodeksach (karnym, cywilnym) oraz w prawie pracy, prawie podatkowym i prawie prasowym.

Pamiętając o przestrzeganiu zasad netykiety można przystąpić do wykorzystywania serwisów pocztowych i klientów poczty elektronicznej do usprawnienia codziennej pracy. W gimnazjum wykorzystywany był program pocztowy, tzw. klient, **Windows Live Mail**. Pozwala on odbierać pocztę z wielu kont e-mail równocześnie. Uruchomienie programu powoduje połączenie go z serwerem poczty przychodzącej i odebranie poczty. Odebrane listy zapisywane są w folderach: **Szybki podgląd**, **Nieprzeczytane wiadomości** oraz w folderze **Skrzynka odbiorcza**.
Dobrze jest jednak znać i korzystać z przedstawionych poniżej, bardziej zaawansowanych możliwości programu, przydatnych podczas pracy nad realizowanym projektem.

- Zarządzanie informacjami na koncie pocztowym poprzez tworzenie układu folderów

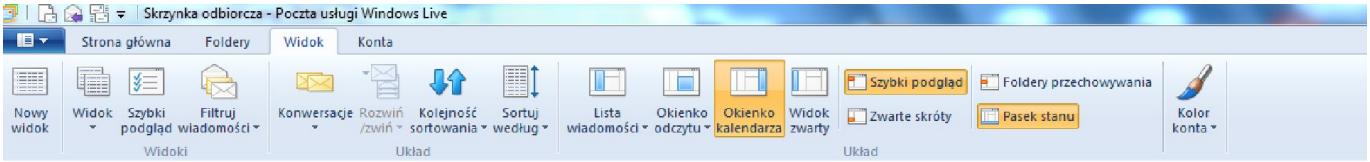
Z biegiem czasu liczba e-mali zwiększa się. Porządkując je, można niektóre z nich przenieść do utworzonego folderu o samodzielnie wybranej nazwie. Wystarczy na karcie poleceń **Foldery** kliknąć ikonę **Nowy folder**. Możn również przenieść wybrane listy do innego folderu korzystając z Ikon **Kopiuj do** i **Przenieś do** widocznych na karcie **Foldery**.



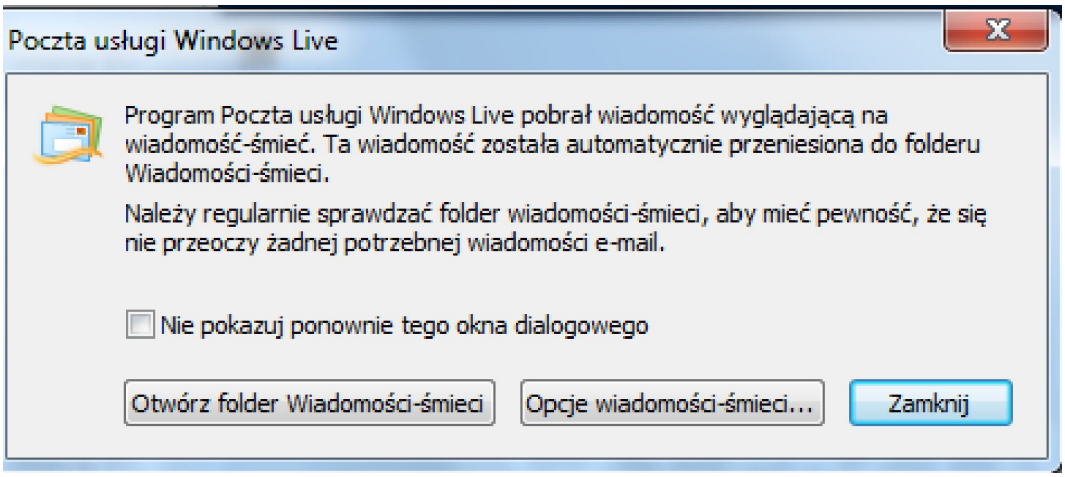
Źródło: Sławomir Szaruga, licencja: CC BY 3.0.

- Filtrowanie korespondencji

Program jest wyposażony w filtr nazywany filtrem spamu. Przegląda on treść nadesłanych wiadomości i przenosi podejrzane do folderu wiadomości-śmieci.

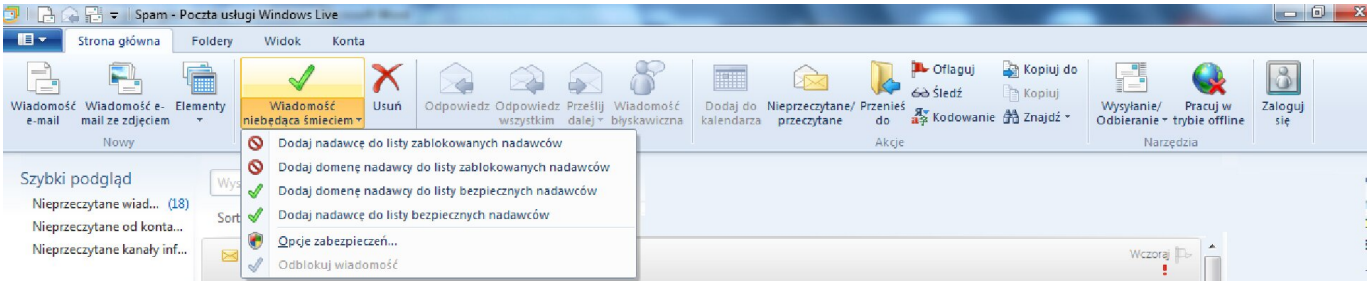


Źródło: Sławomir Szaruga, licencja: CC BY 3.0.



Źródło: Sławomir Szaruga, licencja: CC BY 3.0.

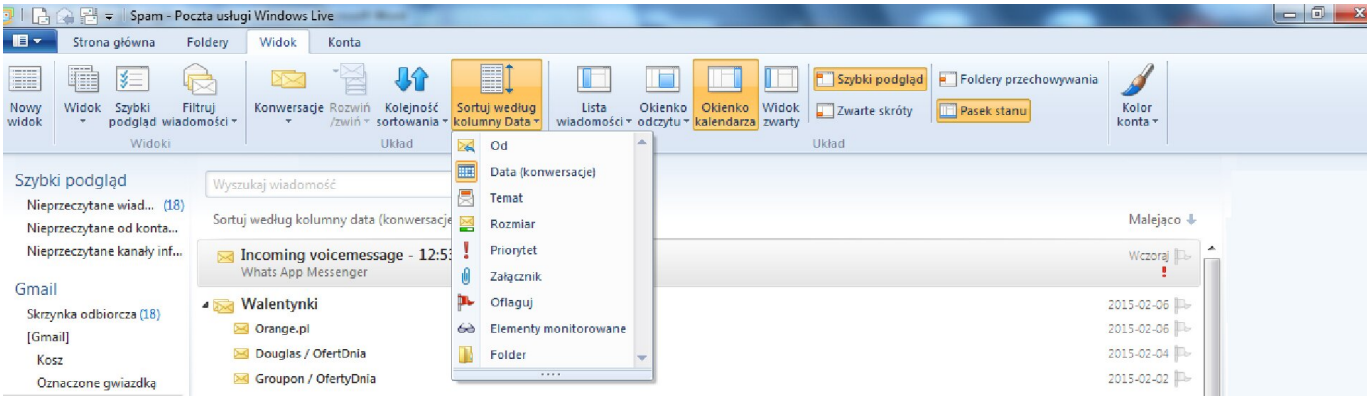
W dowolnym czasie można je przejrzeć i te naprawdę podejrzane usunąć definitywnie.



Źródło: Sławomir Szaruga, licencja: CC BY 3.0.

- Sortowanie wiadomości

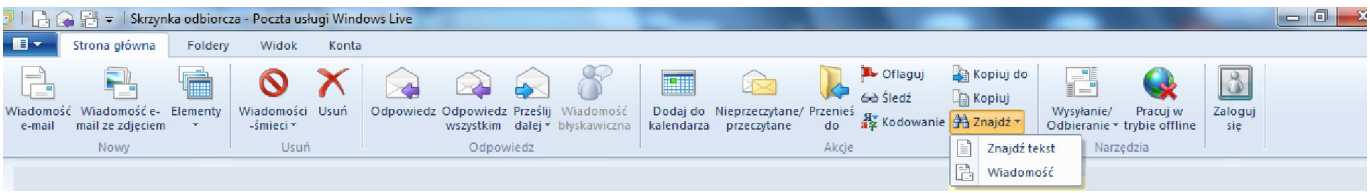
Układ wiadomości w skrzynce odbiorczej można zmienić dokonując czynności sortowania. W tym celu należy zaznaczyć wybraną kolumnę i klikając kartę poleceń **Widok** wybrać **Kolejność sortowania**, rosnąco lub malejąco. Podobny efekt otrzyma się dwukrotne klikając nagłówek kolumny, np. *Temat*, *Data* lub *Rozmia*r. Zmianie ulegnie sposób sortowania z rosnącego na malejący i odwrotnie. Można również dokonać wyboru kolumny korzystając z polecenia **Sortuj według kolumny** ...



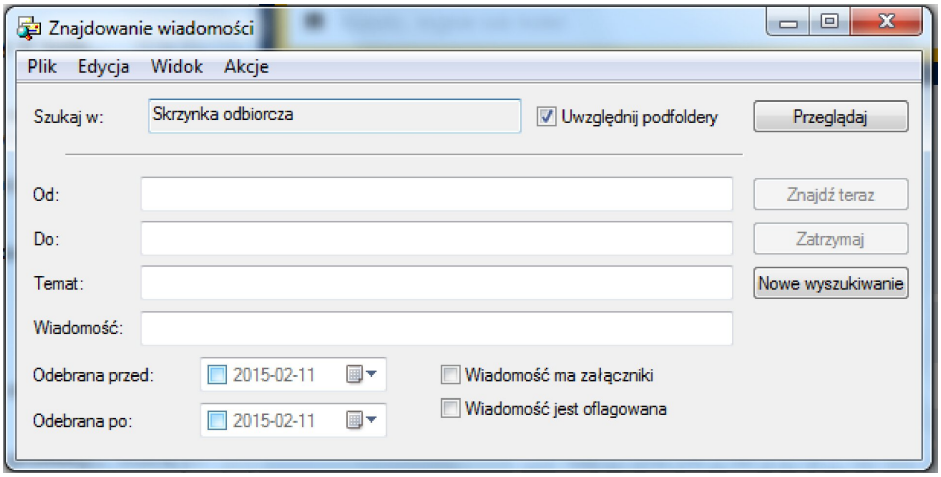
Źródło: Sławomir Szaruga, licencja: CC BY 3.0.

- Znajdowanie wiadomości

Można przeszukać skrzynkę odbiorcza w poszukiwaniu konkretnego listu. W tym celu wystarczy kliknąć ikonę **Znajdowanie wiadomości** i w ten sposób uzyskać możliwość odnalezienie e-maila według nadawcy, tematu i treści wiadomości.



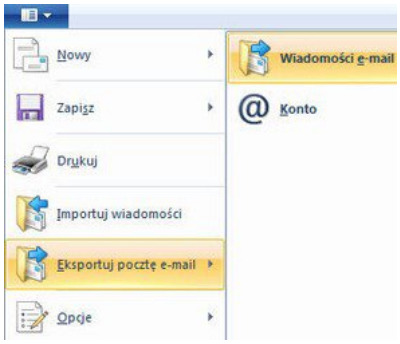
Źródło: Sławomir Szaruga, licencja: CC BY 3.0.



Źródło: Sławomir Szaruga, licencja: CC BY 3.0.

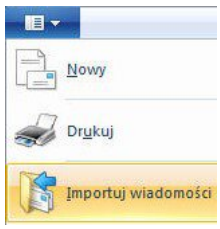
- Importowanie i eksportowanie wiadomości

Przy wymianie komputera, wiadomości znajdujące się w skrzynce odbiorczej każdy chce przenieść do programu pocztowego w nowym komputerze. Należy więc wykonać operację wykonywania kopii zapasowych. Przed jej rozpoczęciem trzeba utworzyć folder w wybranej lokalizacji. Po jego utworzeniu można przystąpić do wyeksportowania wiadomości. W tym celu w menu **Plik**, trzeba kliknąć polecenie **Eksportuj pocztę e-mail**, a następnie wybrać pozycję **Wiadomości e-mail**.



Źródło: Sławomir Szaruga, licencja: CC BY 3.0.

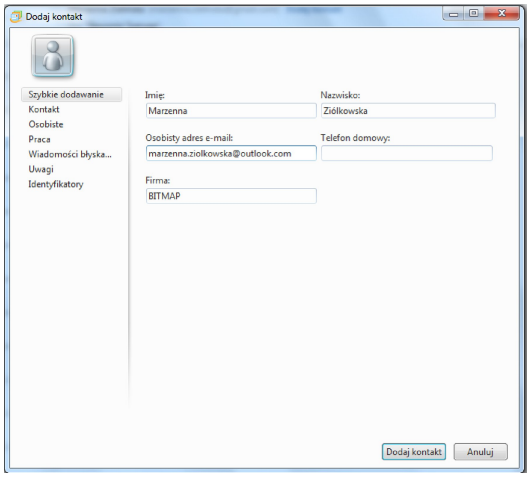
Najlepiej jest wybrać format eksportu w postaci „**Poczta usługi Windows Live firmy Microsoft**”.
Następnie należy wskazać folder, w którym mają być zapisane wiadomości i ponownie kliknij **Dalej**.
Kolejnym krokiem jest zaznaczenie elementów, które mają być wyeksportowane, po zaznaczenie odpowiednich folderów należy kliknąć przycisk **Dalej**.
Jeśli wszystko przebiegło pomyślnie. powinien pojawić się komunikat o powodzeniu operacji eksportu. Wystarczy teraz zakończyć operację odpowiednim poleceniem.
Jeśli chcemy otworzyć pocztę w nowej lokalizacji należy dokonać importu. Trzeba w tym celu wybrać z menu **Plik** polecenie **Importuj wiadomości**.
Następnie należy zaznaczyć format pliku w którym zarchiwizowane zostały wiadomości i kliknąć polecenie **Dalej**. Należy zlokalizować folder w którym znajduje się zapisane archiwum za pomocą polecenia **Przeglądaj**, i znowu kliknąć **Dalej**. Jeśli operacja przebiegła pomyślnie, można będzie podejrzeć zaimportowane wiadomości.



Źródło: Sławomir Szaruga, licencja: CC BY 3.0.

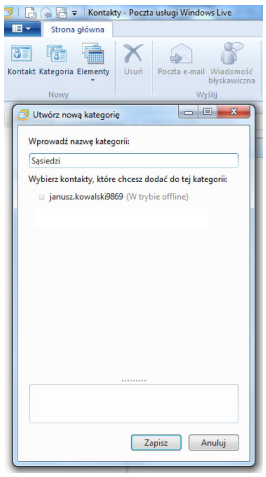
- Książka kontaktów

Przy prowadzeniu rozbudowanej korespondencji przydatna jest **Lista kontaktów**, która ułatwia adresowanie korespondencji. Wystarczy pisząc nowy list kliknąć DO, DW lub UDW a następnie wybrać kontakt, jako adresata wiadomości Dostęp do niej można uzyskać, klikając w ikonę **Kontakty**. Książkę kontaktów można aktualizować ręcznie lub automatycznie. W tym drugim przypadku automatycznie dodany do listy zostanie adres pocztowy, na który trzykrotnie została wysłana odpowiedź.



Źródło: Sławomir Szaruga, licencja: CC BY 3.0.

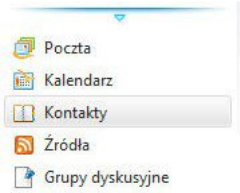
Można w książce kontaktów utworzyć tzw. listy dystrybucyjne, czyli grupy kontaktów. Uzyskuje się wówczas możliwość wysyłania jednocześnie jednego listu do grupy odbiorców. Listę dystrybucyjną można utworzyć klikając ikonę **Kategoria** karty poleceń **Strona główna kontaktów**. W otwartym oknie należy wpisać jej nazwę i wybrać kontakty, które powinny się w niej znaleźć. Po zakończeniu pracy nad kompletowaniem adresów trzeba kliknąć **Zapisz,** a nowa lista zostanie utworzona.



Źródło: Sławomir Szaruga, licencja: CC BY 3.0.

- Importowanie i eksportowanie kontaktów

Równie cenne jak wiadomości są informacje znajdujące się w książce kontaktów. Można je wyeksportować, klikając pozycję **Poczta usługi Windows Live,** a w niej **Kontakty**.



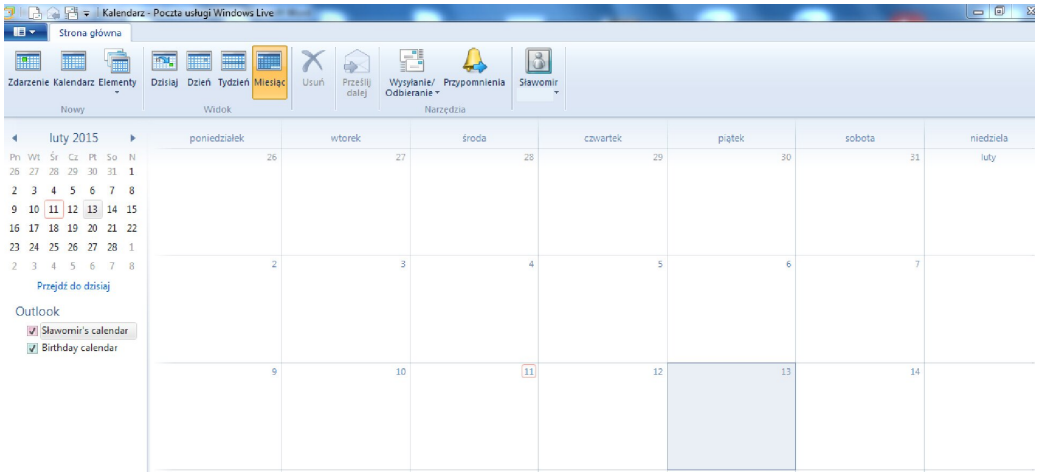
Źródło: Sławomir Szaruga, licencja: CC BY 3.0.

Na ukazanej wstążce należy kliknąć przycisk **Eksportuj**, w menu rozwijanym zaznaczyć format pliku (.vcf dla jednego lub dwóch kontaktów, .csv przy większej liczbie), wskazać miejsce zapisu kontaktów korzystając z przycisku **Przeglądaj**. Następnie należy nazwać powstały plik i kliknąć **Zapisz**. Po kliknięciu przycisku **Dalej**, trzeba zaznaczyć pola, które chce się wyeksportować i kliknąć **Zakończ**. Aby zaimportować kontakty trzeba również skorzystać z pozycji **Kontakty** poczty Windows Live Mail z tym, że teraz ze wstążki należy wybrać przycisk **Importuj**. Następnie zaznaczyć format wyeksportowanych kontaktów i korzystając z przycisku **Przeglądaj** znaleźć folder

zawierający kontakty. Podobnie jak poprzednio trzeba kliknąć **Dalej** i zaznaczyć pola do zaimportowania. Na koniec należy kliknąć **Zakończ**.

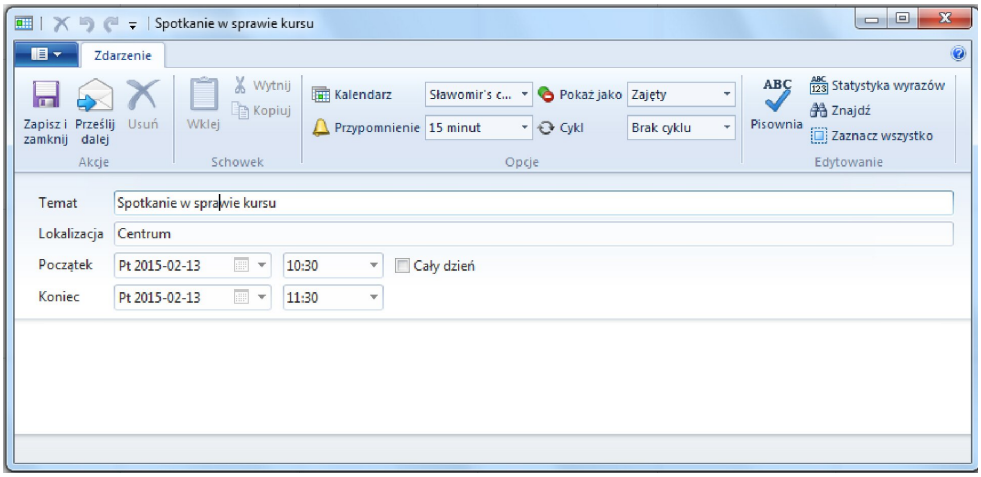
- Kalendarz usługi Windows Live Mail

Ikona Kalendarza (lewy dolny róg programu) umożliwia korzystania z kalendarza w układzie dziennym, tygodniowym lub miesięcznym.



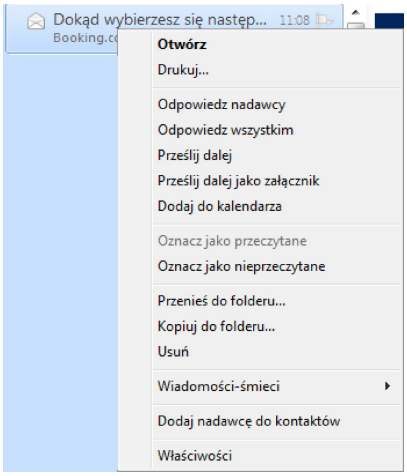
Źródło: Sławomir Szaruga, licencja: CC BY 3.0.

Kliknięcie w datę lub godzinę umożliwia edycję informacji o zdarzeniu. Podwójne klikniecie otwiera okno w którym można wpisać dodatkowe informacje np. początek i koniec imprezy. Każdy wpis można usunąć poleceniem **Usuń** z menu podręcznego.



Źródło: Sławomir Szaruga, licencja: CC BY 3.0.

> **Ważne!**
>
> Umieszczając wskaźnik myszy na dowolnym e-mailu znajdującym się w skrzynce odbiorczej i wybierając z menu podręcznego polecenie Dodaj do kalendarza możesz dodać go do kalendarza.



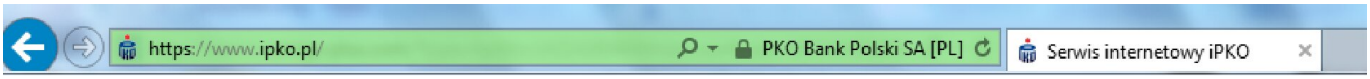
Źródło: Sławomir Szaruga, licencja: CC BY 3.0.

Bezpieczeństwo w Internecie

Bezpieczeństwo w internecie było wielokrotnie omawiane w poprzednich klasach, jednak ze względu na wagę problemu, przypominamy kilka podstawowych zasad.
Internet umożliwia zdobywanie informacji, dokonywanie zakupów, operacji finansowych oraz współpracę z innymi jego użytkownikami nad tworzeniem nowych treści. Korzystając z niego można się jednak natknąć na wiele niebezpieczeństw. By się przed nimi uchronić należy pamiętać o zachowaniu ostrożności. Poniżej przedstawione porady pozwolą poruszać się bezpiecznie w sieci internetowej, podczas korzystania z usług internetowych oraz administrowania stroną WWW.

Logowanie się i wylogowywanie

Powszechnie stosowanym sposobem zabezpieczania dostępu do strony internetowej jest logowanie, które pozwala na autoryzację użytkownika. Wcześniej administrator powinien w procesie rejestracji przydzielić każdemu użytkownikowi niepowtarzalny w serwisie login oraz hasło. Bezpieczeństwo w sieci zwiększa korzystanie z bezpiecznych stron internetowych oraz wylogowanie się z nich po zakończeniu pracy.
Na przykład w przeglądarce IE połączenia z bezpieczną witryną sygnalizowane są zielonym kolorem paska adresu.



Źródło: Sławomir Szaruga, licencja: CC BY 3.0.

Reputację strony można również uzyskać korzystając z poznanego w gimnazjum bezpłatnego programu WOT (Web of Trust) służącego do określenia witryn internetowych pod względem zaufania, wiarygodności i bezpieczeństwa dzieci.



Źródło: Sławomir Szaruga, licencja: CC BY 3.0.

Ważne!

Zawsze, po zakończeniu lub przerwaniu na jakiś czas pracy z komputerem stacjonarnym, laptopem lub tabletem, należy zablokować ekran. Sprzęt powinien być tak skonfigurowany, aby w chwili przejścia w tryb uśpienia blokował się automatycznie, a wznowienie

pracy było możliwe po wprowadzeniu stosownego hasła.

Zabezpieczanie haseł

Korzysta się z nich w rozwiązaniach zapewniających bezpieczeństwo kart bankomatowych, kont bankowych, telefonów, haseł komputerowych. Jednak często hasła i kody są ustawione w dość przewidywalny sposób. Najczęściej są to informacje takie jak data urodzenia, czy imię dziecka. Czasami jedno hasło i stosuje się w wielu miejscach, np. do karty bankomatowej, telefonu czy laptopa. Ktoś kto pozna to hasło ma wówczas dostęp do wszystkich chronionych nim kont. Z reguły strony internetowe banków, czy sklepów internetowych, dają swoim użytkownikom możliwość zmiany hasła i należy z tej możliwości korzystać. Nie powinny to być jednak hasła, które są bardzo popularne i w związku z tym łatwe do odgadnięcia. Powinny być odpowiednio długie min. osiem znaków, a idealne to hasło około czternasto znakowe, zawierające wielkie i małe litery oraz symbole.

Najpopularniejsze hasła bezpieczeństwa na świecie w 2014 roku

Lp.	Hasło	Lp.	Hasło
1.	123456	11.	1234567
2.	password	12.	monkey
3.	12345	13.	letmein
4.	12345678	14.	abc123
5.	qwerty	15.	111111
6.	123456789	16.	mustang
7.	1234	17.	access
8	baseball	18.	shadow
9.	dragon	19.	master
10.	football	20.	michael

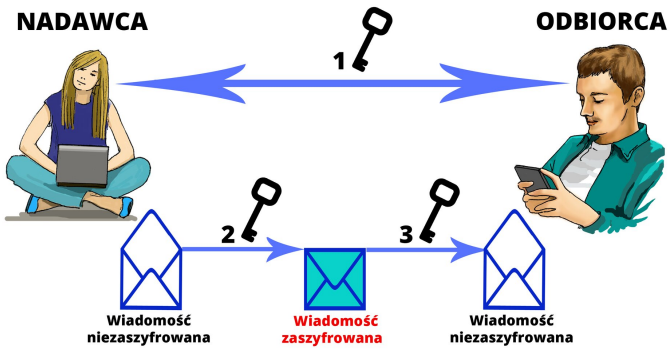
Źródło: Piotr Napieralski, licencja: CC BY 3.0.

Uwaga!

Przy wpisywaniu hasła bezpieczniej jest używać klawiatury ekranowej, ponieważ istnieją programy tzw. keyloggery, które rejestrują klawisze naciskane przez użytkownika.

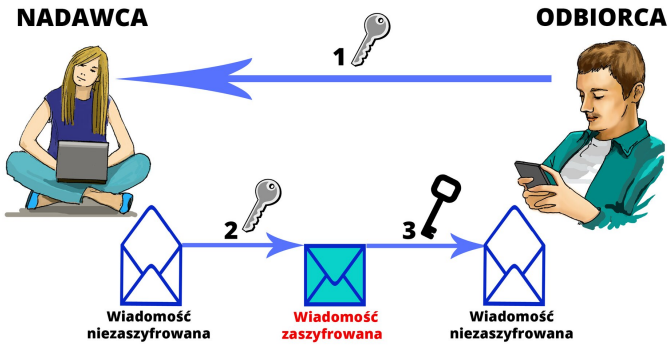
Połączenia szyfrowane

Podczas korzystania z Internetu przekazywane informacje przechodzą przez wiele komputerów i są narażone na przeczytanie przez osoby do tego nieupoważnione. Aby chronić przesyłane w sieci dane, wykorzystywane są metody kryptografii. Kryptografia jest dziedziną obejmująca zagadnienia związane z utajnieniem (zaszyfrowaniem) danych w przesyłanych wiadomościach i zabezpieczaniem przed niepożądanym do nich dostępem. Rozszyfrowanie wiadomości będzie możliwe tylko przez osobę znająca specjalny klucz rozszyfrowujący. Dla osób nie znających klucza rozszyfrowującego wiadomość będzie wyłącznie niezrozumiałym ciągiem znaków.
Prawie codziennie korzystając z Internetu wykorzystuje się rozmaite kody i szyfry, a także algorytmy autoryzacji. Wszystkie wcześniej stosowane szyfry miały charakter symetryczny czyli taki, w którym nadawca i odbiorca używali tego samego klucza, którego znajomość była niezbędna do zaszyfrowania jak i odszyfrowania wiadomości. Czyli szyfrowanie symetryczne jest skuteczne o ile klucz nie wpadnie w niepowołane ręce.



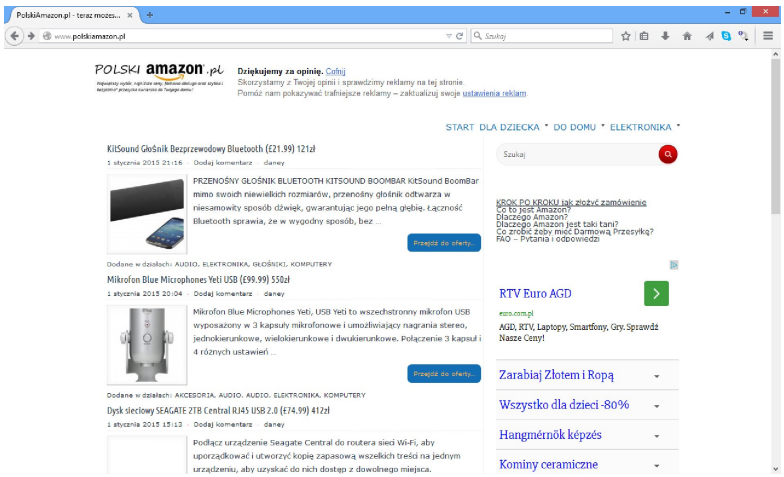
Źródło: Ewa Dobrzyńska, licencja: CC BY 3.0.

Szyfry symetryczne są również i obecnie wykorzystywane do przesyłania wiadomości przez Internet. Do tego rodzaju szyfrów należy, opracowany przez firmę Netscape Communications, protokół kryptograficzny SSL (Secure Socken Layer). SSL jest najczęściej kojarzony z protokołem HTTP (HTTPS) i jest obsługiwany przez większość przeglądarek internetowych. W kryptografii istotną rolę odgrywa również długość wykorzystywanych kluczy, czyli w tym przypadku liczby składających się nań bitów. Klucz długi jest trudniejszy do złamania. Współcześnie używane klucze liczą 128-bitów.
Od końca lat siedemdziesiątych XX wieku stosowana jest kryptografia asymetryczna oparta na dwóch kluczach: publicznym, służącym do szyfrowania i rozprowadzanym wśród użytkowników oraz kluczu tajnym, prywatnym – służącym do odczytywania wiadomości. Klucz który stosowany do szyfrowania wiadomości nie daje możliwości jej odszyfrowania. Szyfrowanie bazujące na kluczu asymetrycznym zapewnia wysoki poziom bezpieczeństwa. Znacznie wyższy niż w metodzie stosującej jeden, wspólny klucz.



Źródło: Ewa Dobrzyńska, licencja: CC BY 3.0.

Nadawca szyfruje wiadomość kluczem publicznym otrzymanym od Odbiorcy, który następnie otrzymuje zaszyfrowaną wiadomość i rozszyfrowuje ją kluczem prywatnym.
Protokół SSL używany jest przede wszystkim przez witryny sklepów internetowych, zapewniając możliwość dokonania zakupów bez obawy o przechwycenie poufnych danych (np. numerów kart kredytowych.). Przed uzyskaniem możliwości zakupu należy wypełnić formularz zgłoszeniowy, w którym będzie zawarta prośba o podanie adresu e-mail i domowego. Adres poczty elektronicznej będzie potrzebny do potwierdzenia zamiaru dokonania zakupu, a zakupiony towar zostanie przesłany na adres domowy za pośrednictwem tradycyjnej poczty. Zakupy można dokonywać w wielu sklepach, a nawet w największym sklepie internetowym na świecie (własność amerykańskiego przedsiębiorstwa Amazon), działającym w naszym kraju pod adresem **www.polskiamazon.pl**.

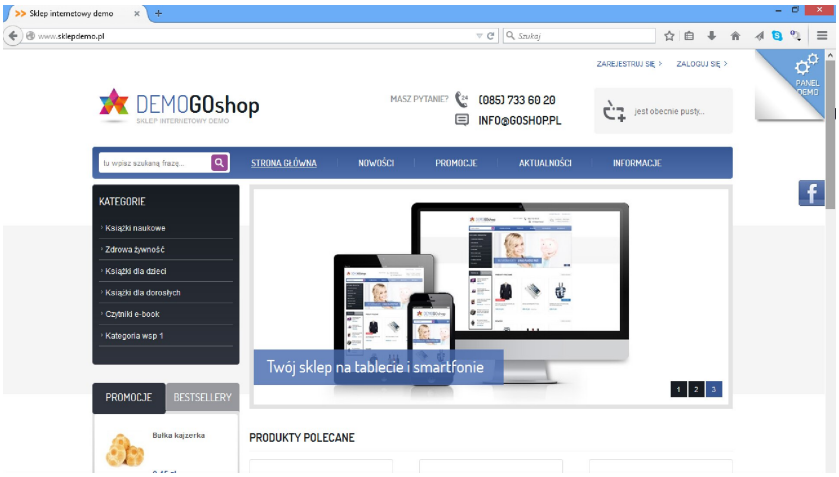


Źródło: Sławomir Szaruga, licencja: CC BY 3.0.

Dokonując zakupów poprzez Internet należy pamiętać o:

- korzystaniu z tego typu serwisów sklepowych ze swojego domowego sprzętu,
- zachowaniu w tajemnicy haseł dostępu i danych osobowych,
- wyborze sposobu płatności, np. gotówką przy odbiorze lub z posiadanego przez ciebie rachunku bankowego,

Sposób dokonywania zakupu w sklepie internetowym można prześledzić na demonstracyjnej stronie WWW: **http://www.sklepdemo.pl/**



Źródło: Sławomir Szaruga, licencja: CC BY 3.0.

Niestety przy zastosowaniu szyfrowania asymetrycznego istnieje możliwość zastąpienia klucza publicznego kluczem nie należącym do danej firmy. Wysyłając wiadomości warto sprawdzić, czy klucz publiczny jest kluczem prawdziwym. Dlatego wprowadza się tutaj cyfrowe certyfikaty wydawane przez instytucję zaufania publicznego. Przeglądarki internetowe są przygotowane do obsługi cyfrowych certyfikatów, które w protokole SSL zawierają m.in. nazwę domeny, dla której zostały wystawione. Chcąc sprawdzić, czy strona jest zabezpieczona certyfikatem bezpieczeństwa, wystarczy kliknąć podwójnie w ikonę kłódki na pasku adresowym. W ten sposób są chronione strony poważnych instytucji finansowych, takich jak np. banki.
Po przejściu do zakładki **Połączenie** można uzyskać informacje o certyfikacie potwierdzającym, że połączono się z właściwą stroną internetową, na przykład z bankiem, a nie udającą go witryną. Kliknięcie polecenia **Informacje o certyfikacie** pokaże okno umożliwiające sprawdzenie autentyczności i daty ważności certyfikatu.
Uwaga

> **Uwaga!**
>
> Zawsze przed przystąpieniem do sesji należy sprawdzić czy:
>
> - W przeglądarce jest włączona obsługa szyfrowania.
> - W pasku adresowym przeglądarki adres internetowy banku jest poprzedzony skrótem „https". Litera „s" oznacza wspomniane wcześniej szyfrowanie protokołu komunikacji a zatem wprowadzony przez ciebie login i hasło nie dadzą się odczytać przez inne osoby.
> - Pasek adresowy jest zabarwiony na zielono.
> - W polu adresu jest kłódka sygnalizująca, że strona jest zabezpieczona certyfikatem bezpieczeństwa.
> - Data logowania jest datą faktycznego korzystania z usługi w e-banku.

Sposób przeprowadzania operacji bankowych można prześledzić na demonstracyjnych wersjach stron banków internetowych, np. banku ipko http://demo.ipko.pl/html/login.html

- Sprawdzanie autentyczności dokumentów przesyłanych drogą elektroniczna

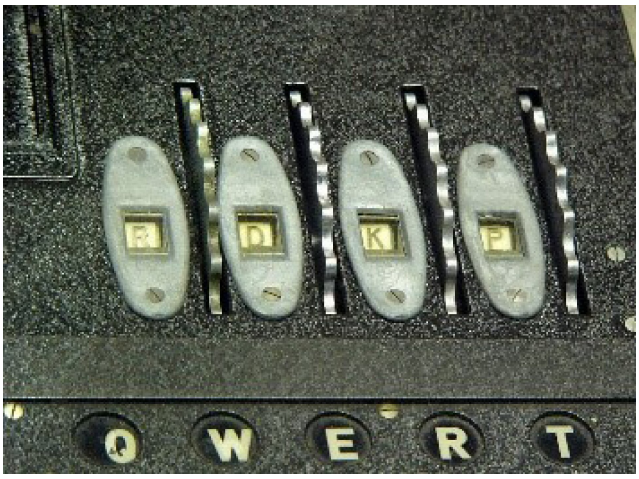
Coraz częściej pojawia się z możliwoscć przekazywania dokumentów drogą elektroniczną. Istnieje wiele sposobów, dzięki którym można stwierdzić, że dana osoba jest autorem przekazywanego dokumentu. Taką osobę może np. charakteryzować podpis elektroniczny oraz informacja biologiczna.

- Podpis cyfrowy (z ang. DSA - Digital Signature Algorithm) to dane w postaci elektronicznej, pozwalające na identyfikacje osoby składającej podpis na dokumentach elektronicznych. Są one przedstawione w postaci ciągu cyfr powstającego w wyniku wykorzystania technik kryptograficznych utajniających dane poprzez ich szyfrowanie. Dzięki nim możemy przekształcić normalny tekst w taki sposób, iż stanie się on niezrozumiały dla nieupoważnionego odbiorcy. Osoba otrzymująca wiadomość tego typu jest w stanie przekształcić ją do pierwotnej czytelnej postaci. W podpisach cyfrowych stosuje się kryptografię asymetryczną.

Kolejność czynności przy tworzeniu dokumentu z podpisem cyfrowym jest następująca:

- nadawca pisze wiadomość,
- nadawca wytwarza wiadomość,
- nadawca podpisuje wiadomość za pomocą algorytmu podpisu cyfrowego (używając swojego prywatnego klucza),
- nadawca łączy wiadomość i podpis w celu uzyskania nowej, podpisanej wiadomości,
- nadawca tworzy losowy klucz szyfrujący do zaszyfrowania podpisanej wiadomości,
- nadawca szyfruje wiadomość za pomocą klucza i algorytmu konwencjonalnego,
- nadawca pobiera jawny klucz odbiorcy,
- nadawca szyfruje pobranym kluczem wygenerowany przez siebie losowy klucz szyfrujący,
- nadawca łączy zaszyfrowaną widomość z zaszyfrowanym kluczem,

- nadawca wysyła zabezpieczoną wiadomość.



Źródło: Sławomir Szaruga, licencja: CC BY 3.0.

- U podstaw identyfikacji biometrycznej leży fakt, że pewne cechy ciała ludzkiego są przypisane do konkretnej osoby i są niezmienne. Stosowane sa następujące metody identyfikacji biometrycznej:
    - skanowanie linii papilarnych,



Źródło: Sławomir Szaruga, licencja: CC BY 3.0.

    - skanowanie tęczówki,
    - identyfikacja głosu,
    - rozpoznawanie twarzy.

Wyłudzanie informacji

By chronić się przed wyłudzaniem informacji poprzez Internet dobrze jest poznać najpopularniejsze z tych sposobów. Należą do nich phishing i pharming.

- Phishing polega na przekonaniu użytkownika do podania danych osobowych poprzez fałszywą stronę.
- Pharming obejmuje modyfikację wpisów DNS, co powoduje przekierowanie użytkownika do niewłaściwej strony, kiedy odwiedzi pewien adres WWW.

W przypadku phisingu oszuści wysyłają e-maile, które wydają się pochodzić z legalnych stron internetowych np. instytucji bankowych. W treści e-maila może być zawarta np. prośba o podanie nazwy użytkownika i hasła motywowana koniecznością aktualizacji konta. Dysponując tymi informacjami oszust może uzyskać dostęp do większej ilości informacji (numeru telefonu, numeru PESEL czy numeru karty kredytowej) logując się do udostępnionego konta.
Fałszywe e-maile często wyglądają zaskakująco zgodne z prawdą, a fałszywe strony internetowe, mogą wyglądać jak prawdziwe. Po otrzymaniu e-maila z prośbą o zaktualizowanie informacji należy przejść do strony internetowej, wpisując ręcznie adres URL w polu adresu przeglądarki, zamiast klikania w link w wiadomości e-mail. Jeśli po wpisaniu adresu WWW zostanie wyświetlona prośba o aktualizację danych, to e-mail był prawdziwy. W przeciwnym wypadku e-mail był najprawdopodobniej próba zdobycia informacji przez tzw. phishera.



Źródło: Sławomir Szaruga, licencja: CC BY 3.0.

Ochrona przed phishingiem

- Nie należy otwierć hiperłączy bezpośrednio z otrzymanego e-maila.
- Prośby o podanie hasła i loginu w mailu należy zignorować i zgłośic odpowiednim osobom (firmie).
- Jeśli strona z logowaniem do instytucji finansowej nie zawiera w adresie nazwy protokołu HTTPS, nie powinno podawać się na niej żadnych danych.

W pharmingu, podobnie jak w przypadku ataków typu „phishing", użytkownicy wabieni są do fałszywych witryn internetowych. Strony te do złudzenia przypominają strony oryginalne. W przeciwieństwie do phisingu w pharmingu użytkownik przekierowany jest na fałszywą stronę nawet jeśli wpisze prawidłowy i prawdziwy adres strony www.



Źródło: Sławomir Szaruga, licencja: CC BY 3.0.

Działanie takie powoduje wpisanie przez użytkownika haseł, numerów kart bankowych i innych poufnych danych. Pharming przekierowuje użytkowników do fałszywych stron internetowych, bez wiedzy użytkownika Internetu. Po wpisaniu adresu jest on tłumaczony na adres IP za pośrednictwem serwera DNS. Przeglądarka internetowa łączy się z serwerem tego adresu IP i ładuje daną stronę WWW. Wpis DNS dla tej witryny jest często przechowywany na komputerze użytkownika, w cache . W ten sposób komputer nie ma dostępu do serwera DNS i odwiedzając stronę internetową korzysta z tego przechowywanego w cache komputera. Komputer ofiary zostaje najczęściej zainfekowany tak, by lokalne pliki odpowiedzialne za rozpoznawanie nazw DNS zostały zmodyfikowane przez hakera. Można chronić się przed wirusami zmieniającymi pliki na komputerze, instalując program antywirusowy z aktualna baza wirusów.
W przypadku zaobserwowania znaczących różnic w wyglądzie strony internetowej, należy uruchomić ponownie komputer i ponownie połączyć się z tą samą witryną. Jeśli strona nadal będzie budziła podejrzenie, należy skontaktować sięz dostawca usług internetowych.
Celem drugiej odmiany ataku typu „pharming" są serwery DNS należące do firmy lub usługodawcy internetowego. Haker musi włamać się do serwera DNS, z którego korzystają pracownicy firmy i przekierowywać połączenia, bez potrzeby włamywania się do ich komputerów. W tym przypadku użytkownik nie może nic zrobić: zapewnienie właściwej ochrony serwera należy do pracowników działu informatycznego firmy, lub usługodawcy internetowego.
Aby upewnić się, czy wyświetlana strona jest prawdziwa można sprawdzić jej certyfikat SSL. Aby się o tym przekonać wystarczy kliknąć symbol kłódki w pasku adresowym przeglądarki. W wyświetlonym oknie pojawi się informacja, kto jest właścicielem strony.

Zabezpieczanie przed niepożądanym i treściami

Można spotykać się również z próbami umieszczania na naszych stronach WWW niepożądanych treści. Istnieje wiele sposobów, dzięki którym można stwierdzić, że ktoś ma prawo wejścia, czyli, że jest autoryzowanym użytkownikiem danego serwisu. Jednym z nich jest system anty-robotowy, np. reCAPTCHA. Standardowe rozwiązania CAPTCHA wykorzystują losowo generowane znaki, które po pewnych zniekształceniach należy przepisać z ukazanego obrazka do pola tekstowego. Dopiero po poprawnym wpisaniu wygenerowanych znaków uzyskuje się dostęp do danego serwisu.



Źródło: Sławomir Szaruga, licencja: CC BY 3.0.

Postęp badań nad sieciami neuronowymi spowodował opracowanie systemów praktycznie bezbłędnie rozpoznających tekst. Z tego powodu postanowiono zmienić formę reCAPTCHA na numerację domów, znajdujących się na zdjęciach ulicy Street View. Przykładowy formularz zawiera wycięty numer ze zdjęcia oraz dla dodatkowej weryfikacji numer wygenerowany losowo.



Źródło: Sławomir Szaruga, licencja: CC BY 3.0.

Taka weryfikacja pojawia się między innymi podczas zakładania poczty elektronicznej, aby chronić się przez nadmiernymi spamerami, rozsyłającymi niechciane e-maile.