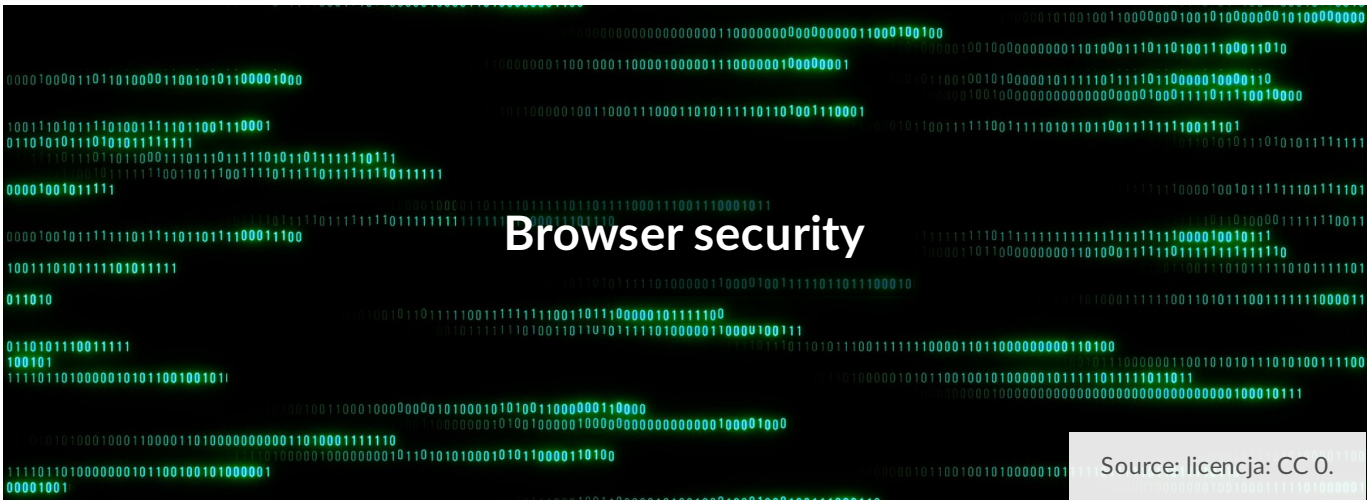
Browser security



Source: licencja: CC 0.

Ochrona przeglądarki

> **You will learn**
>
> - threats associated with using a web browser, how to prevent them,
> - how to use a web browser safely.

Nagranie dostępne na portalu epodreczniki.pl

Source: GroMar, licencja: CC BY 3.0.

nagranie abstraktu

A web browser is a software which is installed on almost every computer, tablet or smartphone. None of web browsers is completely secure. Each of them has security vulnerabilities, which can be eagerly detected by hackers and used to breach the security of your computer. It is crucial to make every effort to ensure that your “favourite” web browser is as secure as possible.

Phishing is an internet fraud, the form of data theft, that is committed by displaying a „malicious website” in order to obtain sensitive information such as passwords, account details or credit card numbers. Phishing attacks are carried out most often with the use of fake email messages which encourage the recipients to update their personal data at fake websites, which usually look identical to the legitimate sites.

Malware is a malicious software. It can be also placed on websites.

The anti-phishing and anti-malware security of web browsers checks every visited website and compares it with the lists of known malicious websites. This feature should be obligatorily enabled. Anti-phishing security that blocks fake websites is one of the features of the majority of available antivirus software. When you use the Internet, make sure that this feature is enabled in your antivirus programme.

Task 1

Nagranie dostępne na portalu epodreczniki.pl

Source: GroMar, licencja: CC BY 3.0.

nagranie abstraktu

In the antivirus software installed on your computer find settings that are responsible for browser security.

Nagranie dostępne na portalu epodreczniki.pl

Source: GroMar, licencja: CC BY 3.0.

nagranie abstraktu

In order to keep your browser security:

- configure the security and privacy settings of your browser,
- keep your browser updated,
- use encrypted connections (the HTTPS protocol),
- be cautious when you install add-ons since every add-on decreases browser security,
- install security plug-ins, e.g. HTTPS Everywhere, Web of Trust (WOT),
- check short links,
- regularly empty the temporary and downloaded files folders of your browser,
- do not save your passwords in web browsers,
- use an account without administrator privileges while browsing the Internet,
- block pop-up ads.

Source: GroMar, licencja: CC BY 3.0.

Task 2

Nagranie dostępne na portalu epodreczniki.pl

nagranie abstraktu

On the Internet find the information about how to remove temporary files from the cache in popular web browsers.

Task 3

Nagranie dostępne na portalu epodreczniki.pl

nagranie abstraktu

Check in the web browser installed on your computer in what location temporary files and files downloaded from the Internet are stored.

Task 4

Nagranie dostępne na portalu epodreczniki.pl

nagranie abstraktu

How can you check to which website a *short* URL leads?

Nagranie dostępne na portalu epodreczniki.pl

nagranie abstraktu

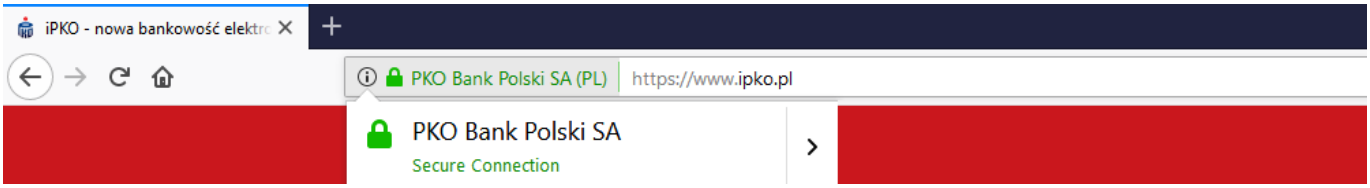
SSL is a protocol used to provide secure data transmission over computer networks by encrypting the data transmitted. It uses certificates issued by trusted certificate authorities. Due to its application, more secure services have been developed, e.g. HTTPS, which is the encrypted version of HTTP.

Nagranie dostępne na portalu epodreczniki.pl

Source: GroMar, licencja: CC BY 3.0.

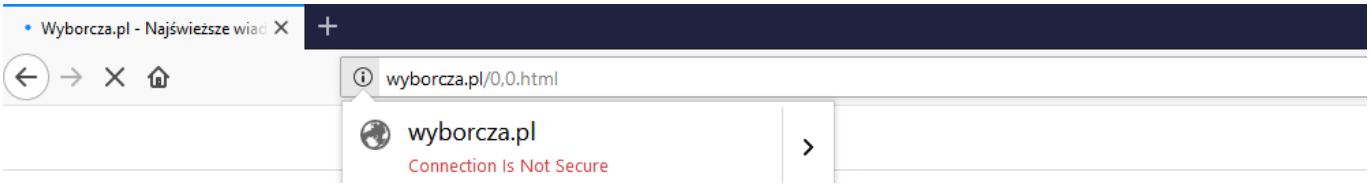
nagranie abstraktu

Most web browsers display information about the type of communication and certificates of websites in their address bar.



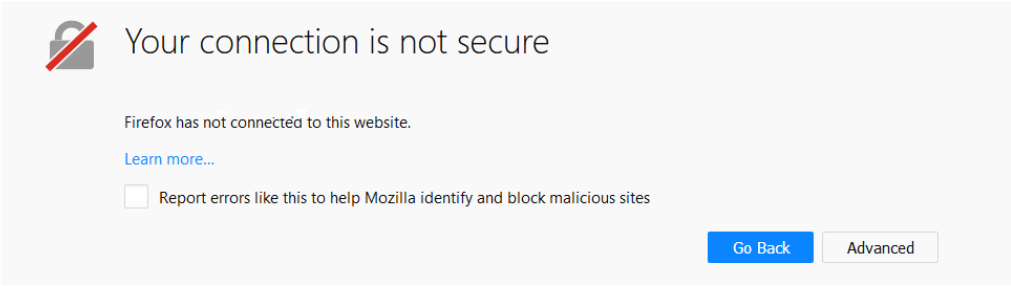
Encryped connection.

Source: GroMar, licencja: CC BY 3.0.



Unencrypted connection.

Source: GroMar, licencja: CC BY 3.0.



No certificate or incorrect certificate.

Source: GroMar, licencja: CC BY 3.0.

Nagranie dostępne na portalu epodreczniki.pl

Source: GroMar, licencja: CC BY 3.0.

nagranie abstraktu

When the computer you are using is not your own, do not perform operations that require transmitting sensitive data. If you have to use this computer, enable private browsing. Using private browsing disables collecting and storing information about the operations of a user. When you leave the privacy mode of your browser, none of the following information should be saved:

- browsing history,
- downloaded files history,
- data in cookies,
- filled-in text boxes in forms,
- search history,
- the temporary files of visited websites,
- website settings.

> **Task 5**
>
> Nagranie dostępne na portalu epodreczniki.pl
>
> Source: GroMar, licencja: CC BY 3.0.
>
> nagranie abstraktu
>
> ---
>
> On the Internet find the information about how to run private browsing in popular web browsers.

Nagranie dostępne na portalu epodreczniki.pl

Source: GroMar, licencja: CC BY 3.0.

nagranie abstraktu

A secure browser:

- enables to download auto updates,
- has the feature that protects against phishing;
- protects data during their transfer by encrypting them.

Exercises

Exercise 1

Determine which sentences are true.

- configure the security and privacy settings of your browser
- do not keep your browser updated
- use encrypted connections (HTTPS protocol)
- be cautious when you install add-ons
- check short links
- regularly empty the temporary files folder of your browser
- do not save your passwords in web browsers
- use an administrator account while browsing the Internet
- do not block pop-up ads

zadanie

Exercise 2

Create a multimedia presentation about browser security. Find the needed information and the comparisons of the features of web browsers on the Internet.

Exercise 3

Visit the Web of Trust (WOT) website. Describe in English its idea.

Exercise 4

Indicate which pairs of expressions or words are translated correctly.

- pasek adresu - address bar
- certyfikaty - certificates
- ciasteczka - cookies
- oszustwo internetowe - Internet fraud
- pliki tymczasowe - pop-up ads
- wyskakujące okna - temporary files

zadanie

Match Polish terms with their English equivalents.

- cookies
- wyskakujące okna
- address bar
- pop-up ads
- odwiedzane witryny
- pasek adresu
- ciasteczka
- certificates
- certyfikaty
- visited websites

Glossary

address bar

pasek adresu

Nagranie dostępne na portalu epodreczniki.pl

wymowa w języku angielskim: address bar

---

certificates

certyfikaty

Nagranie dostępne na portalu epodreczniki.pl

wymowa w języku angielskim: certificates

---

cookies

ciasteczka

Nagranie dostępne na portalu epodreczniki.pl

wymowa w języku angielskim: cookies

Internet fraud

oszustwo internetowe

Nagranie dostępne na portalu epodreczniki.pl

wymowa w języku angielskim: Internet fraud

---

pop-up ads

wyskakujące okna

Nagranie dostępne na portalu epodreczniki.pl

wymowa w języku angielskim: pop-up ads

---

private browsing

tryb prywatny

Nagranie dostępne na portalu epodreczniki.pl

wymowa w języku angielskim: private browsing

---

secure

bezpieczna

Nagranie dostępne na portalu epodreczniki.pl

wymowa w języku angielskim: secure

---

temporary files

pliki tymczasowe

Nagranie dostępne na portalu epodreczniki.pl

wymowa w języku angielskim: temporary files

---

visited websites

odwiedzane witryny

Nagranie dostępne na portalu epodreczniki.pl

wymowa w języku angielskim: visited websites

---

web browser

przeglądarka internetowa

Nagranie dostępne na portalu epodreczniki.pl

wymowa w języku angielskim: web browser

Keywords

certificates

private browsing

secure

web browser

Scenariusz

Temat

Ochrona przeglądarki

Etap edukacyjny

Drugi

Podstawa programowa

Klasy IV–VI

V. Przestrzeganie prawa i zasad bezpieczeństwa. Uczeń:

3) wymienia zagrożenia związane z powszechnym dostępem do technologii oraz do informacji i opisuje metody wystrzegania się ich;

4) stosuje profilaktykę antywirusową i potrafi zabezpieczyć przed zagrożeniem komputer wraz z zawartymi w nim informacjami.

Czas

45 minut

Cel ogólny

Przestrzeganie prawa i zasad bezpieczeństwa.

Cele szczegółowe

1. Identyfikowanie zagrożeń związanych z korzystaniem z przeglądarki internetowej.

2. Określanie metod wystrzegania się zagrożeń związanych z korzystaniem z przeglądarki internetowej.

Efekty uczenia

Uczeń:

- rozpoznaje zagrożenia związane z korzystaniem z przeglądarki internetowej,

- korzysta z metod wystrzegania się zagrożeń związanych z korzystaniem z przeglądarki internetowej.

Metody kształcenia

1. Dyskusja.

2. Uczenie się przez obserwację.

Formy pracy

1. Praca indywidualna.

2. Praca z całą klasą.

Etapy lekcji

Wprowadzenie do lekcji

Nauczyciel przeprowadza krótką dyskusję na temat bezpieczeństwa przeglądarek internetowych.

- Jakie przeglądarki internetowe znacie?
- Jakie funkcje posiadają przeglądarki? (przeglądanie stron, zakładki, historia, pobieranie plików, tryb prywatny)
- Jakie zagrożenia niesie ze sobą korzystanie z przeglądarek internetowych?

Realizacja lekcji

Przeglądarka internetowa jest oprogramowaniem instalowanym niemal na każdym komputerze, tablecie czy smartfonie. Żadna z przeglądarek internetowych nie jest w stu procentach bezpieczna. Każda posiada jakieś luki, które są skrzętnie wykrywane przez hackerów i wykorzystywane do złamania zabezpieczeń naszego komputera. Ważne jest dołożenie wszelkich starań, aby nasza „ulubiona" przeglądarka internetowa była najbardziej bezpieczna, jak to jest możliwe.

Phishing to oszustwo internetowe będące formą kradzieży danych, polegające na wyświetlaniu „szkodliwej witryny" w celu zdobycia poufnych informacji, takich jak: hasła, dane kont czy numery kart kredytowych. Ataki phishingowe najczęściej dokonywane są za pomocą sfałszowanych wiadomości email, nakłaniających adresatów do aktualizacji prywatnych danych na fałszywych witrynach, które zazwyczaj są łudząco podobne do oryginalnych.

Malware to szkodliwe oprogramowanie. Może być ono umieszczone również na stronach internetowych.

Ochrona antyphishingowa i antymalware przeglądarek internetowych sprawdza każdą odwiedzaną stronę i porównuje ją z listami znanych niebezpiecznych stron. Funkcja to powinna być obowiązkowo włączona.

Obrona przed phishingiem blokująca fałszywe witryny jest jedną z funkcji większości dostępnych programów antywirusowych. Korzystając z internetu, bądź pewny, że w twoim programie antywirusowym ta funkcja jest włączona.

Polecenie 1

Odszukaj w programie antywirusowym zainstalowanym na twoim komputerze ustawienia odpowiedzialne za ochronę przeglądarki.

Aby zwiększyć bezpieczeństwo swojej przeglądarki:

- skonfiguruj ustawienia zabezpieczeń i prywatności przeglądarki,
- zadbaj o uaktualnienia przeglądarki,
- stosuj połączenia szyfrowane (protokół HTTPS),
- zachowaj ostrożność przy instalowaniu dodatków, gdyż każdy dodatek zmniejsza bezpieczeństwo przeglądarki,
- zainstaluj wtyczki zabezpieczeń, np. HTTPS Everywhere, Web of Trust (WOT),
- sprawdzaj krótkie linki,
- czyść systematycznie folder plików tymczasowych przeglądarki oraz folder plików pobranych,
- nie zapamiętuj haseł w przeglądarkach,
- korzystaj z internetu na koncie bez uprawnień administratora,
- blokuj wyskakujące okna.

[Slideshow]

Polecenie 2

Znajdź w internecie informację, jak usunąć pliki tymczasowe z pamięci podręcznej w popularnych przeglądarkach internetowych.

Polecenie 3

Sprawdź w przeglądarce internetowej zainstalowanej na twoim komputerze, w jakiej lokalizacji przechowywane są pliki tymczasowe oraz pobrane z internetu.

Polecenie 4

W jaki sposób można sprawdzić, do jakiej witryny WWW prowadzi nas skrócony adres?

Przypomnienie:

SSL to protokół służący do bezpiecznej transmisji danych w sieciach komputerowych, polegający na szyfrowaniu przesyłanych danych. Używa certyfikatów wydawanych przez zaufane urzędy certyfikacji. Dzięki jego użyciu powstały bezpieczniejsze usługi, np. HTTPS będący szyfrowaną wersją HTTP.

Większość przeglądarek internetowych na pasku adresu podaje informacje o rodzaju komunikacji i certyfikatach stron internetowych.

[Ilustracja 1]

[Ilustracja 2]

[Ilustracja 3]

Na nie swoim komputerze nie wykonuj operacji wymagających przesyłania wrażliwych danych. Jeśli już musisz korzystać z takiego komputera, stosuj tryb prywatny przeglądarki.

Stosowanie trybu prywatnego uniemożliwia gromadzenie i przechowywanie informacji o działaniach użytkownika. Przeglądarka internetowa po wyjściu z tego trybu nie powinna zachować żadnej z niżej wymienionych treści:

- historii przeglądanych stron,
- historii pobranych plików,
- ciasteczek witryn,
- wypełnionych pól formularzy,
- historii wyszukiwania,
- plików tymczasowych odwiedzanych witryn,
- ustawień witryn.

Polecenie 5

Znajdź w internecie informacje, jak uruchomić tryb prywatny w popularnych przeglądarkach internetowych.

Podsumowanie lekcji

Bezpieczna przeglądarka to taka, która:

- oferuje automatyczne pobieranie aktualizacji;
- posiada funkcję ochrony przed stronami wyłudzającymi informacje (phishing);
- chroni dane podczas ich przesyłania, szyfrując je.

Lesson plan

Topic

Browser security

Level

Second

Core curriculum

Grades IV–VI

V. Compliance with law and safety principles. The student:

3) identifies threats associated with the common access to technologies and information and describes the methods of avoiding them;

4) uses antivirus preventive measures and can protect the computer and information contained in it against threats.

Timing

45 minutes

General objective

Compliance with law and safety principles.

Specific objectives

1. Identifying threats associated with using a web browser.

2. Identifying the methods of avoiding threats associated with using a web browser.

Learning outcomes

The student:

- identifies threats associated with using a web browser,

- uses the methods of avoiding threats associated with using a web browser.

Methods

1. Discussion.

2. Learning through observation.

Forms of work

1. Individual work.

2. Class work.

LESSON STAGES

Introduction

The teacher initiates a short discussion about the security of web browsers.

- What web browsers do you know?
- What are their functions? (web browsing, bookmarks, browsing history, downloading files, private browsing)
- What threats are associated with using web browsers?

Procedure

A web browser is a software which is installed on almost every computer, tablet or smartphone. None of web browsers is completely secure. Each of them has security vulnerabilities, which can be eagerly detected by hackers and used to breach the security of your computer. It is crucial to make every effort to ensure that your "favourite" web browser is as secure as possible.

Phishing is an Internet fraud, the form of data theft, that is committed by displaying a „malicious website" in order to obtain sensitive information such as passwords, account details or credit card numbers. Phishing attacks are carried out most often with the use of fake email messages which encourage the recipients to update their personal data at fake websites, which usually look identical to the legitimate sites.

Malware is a malicious software. It can be also placed on websites.

The anti-phishing and anti-malware security of web browsers checks every visited website and compares it with the lists of known malicious websites. This feature should be obligatorily enabled.

Anti-phishing security that blocks fake websites is one of the features of the majority of available antivirus software. When you use the Internet, make sure that this feature is enabled in your antivirus programme.

Task 1

In the antivirus software installed on your computer find settings that are responsible for browser security.

In order to harden your browser security:

- configure the security and privacy settings of your browser,
- keep your browser updated,
- use encrypted connections (the HTTPS protocol),
- be cautious when you install add-ons since every add-on decreases browser security,
- install security plug-ins, e.g. HTTPS Everywhere, Web of Trust (WOT),
- check short links,
- regularly empty the temporary and downloaded files folders of your browser,
- do not save your passwords in web browsers,
- use an account without administrator privileges while browsing the Internet,
- block pop-up ads.

[Slideshow]

Task 2

On the Internet find the information about how to remove temporary files from the cache in popular web browsers.

Task 3

Check in the web browser installed on your computer in what location temporary files and files downloaded from the Internet are stored.

Task 4

How can you check to which website a *short* URL leads?

Reminder:

SSL is a protocol used to provide secure data transmission over computer networks by encrypting the data transmitted. It uses certificates issued by trusted certificate authorities. Due to its application, more secure services have been developed, e.g. HTTPS, which is the encrypted version of HTTP.

Most web browsers display information about the type of communication and certificates of websites in their address bar.

[Illustration 1]

[Illustration 2]

[Illustration 3]

When the computer you are using is not your own, do not perform operations that require transmitting sensitive data. If you have to use this computer, enable private browsing.

Using private browsing disables collecting and storing information about the operations of a user. When you leave the privacy mode of your browser, none of the following information should be saved:

- browsing history,
- downloaded files history,
- data in cookies,
- filled-in text boxes in forms,
- search history,
- the temporary files of visited websites,
- website settings.

Task 5

On the Internet find the information about how to run private browsing in popular web browsers.

Lesson summary

A secure browser:

- enables to download auto updates,
- has the feature that protects against phishing;
- protects data during their transfer by encrypting them.

Selected words and expressions used in the lesson plan

address bar

certificates

cookies

Internet fraud

pop-up ads

private browsing

secure

temporary files

visited websites

web browser