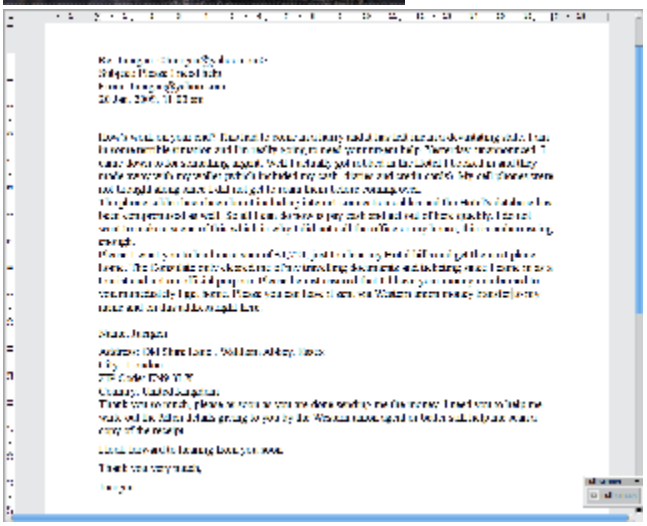
draft Internet lesson 2 - Security



add downloading software free stuff login with picture - add keepassX

Internet lesson 2 - homework

Try to avoid doing the homework in the last minute but rather do them in time and email them to **bluelight.training@gmx.com**. **Please do not use the bluelight@auroville.org.in** address.
This gives us time to look into what you did and give you some feedback. **It is a requirement to do the homework to be able to follow the classes.**
You find all lessons and homework here

How do you recognize a secure website?

What is **Caps Lock**?

What is the master password in the Firefox context?

Sort the passwords in weak and strong ones: greenbelt Dosai1968 auroville SurRenDer Yu6Gfs7 Tuñ88T undercover

How dangerous are your favourite http-cookies? If you have sample cookies bring them to the next class? (The Blue Light team prefers chocolate cookies 🙂)

Name 3 different types of useful pop-up windows?

If you find the following part much too difficult - relax. The aim of this test is not to pass with good results but to see for you how much you know **now** and how secure you feel being confronted with this and how much you know at the end of the next class and how you feel then. Have fun: Go to http://www.sonicwall.com/phishing/ and follow the instructions to do the Phishing test. How many of the 10 examples could you identify correctly?

Question(s)

What is Phishing?

Most probably all of you have occasionally received emails like this one:

This type of mails lead you to fraudulent web sites. In criminal law, fraud is the crime or offense of deliberately deceiving another in order to damage them - usually, to obtain property or services unjustly.

Watch out for this stuff in emails!

Misspelled domains are big deceivers. Phishers will purchase a domain name that resembles the real domain. They will replace letters with numbers or with other letters. Pay close attention to the spelling of a domain name, and learn to spot a fake like paypol.com instead of paypal.com.

An IP (Internet Protocol) address looks something like 102.199.60.250. Bottom line, never trust emails that point you to URLs that only show an IP address.

i.e.: http://102.199.60.250/sample/of/suspicious/address.aspx?ID=7878

Variations of domains should also be a red flag. Don't click on any email that contains URLs like http://center.yahoo-security.net. A legitimate URL should read http://center.yahoo.com if it actually belongs to Yahoo! Anyone could've purchased www.yahoo-security.net for a scam.

Does the sender's mail account match the domain name? i.e. an email from ICICI http://www.icicibank.com/ should be something like support@icicibank.com or customer-care@icicibank.com

Phishers often create the sense of urgency. If you feel under time pressure stop and wait. If it is really urgent they would have phoned you or sent you a regular letter.

Technical language like "We have recently updated our online system to include multi-socket layer secure authentication." tries to impress you.

Logos help to make the email look "real" and "official"

Your name in the email doesn't guaranty authenticity anymore. They are often borrowed from your email address, social networking sites like Facebook, etc.

Cut-and-paste links are the preferred link type in secure emails - "click here" is not a secure way. Click here - If this type of link is used be careful. It offers easy clicking. Secure websites use "copy&paste" links most of the time like this one:

```
Please copy and paste this link into the address bar of you browser

https://link-to-a-bank/example/login.php
```

Make sure the URL of the displayed link matches the URL in the status bar

Most money and login transactions use encrypted https links. You can see them in the status bar at the bottom or the location bar.

Be careful if you find no other means to contact the originator of the email than the email address itself. Why don't they have phone and post addresses?

Grammar and spelling errors are suspicious

"Thank you for requesting ...." - did you request?

Account information displayed matches with your actual numbers? It is not very likely that confidential information is sent to you by email. Generally that shows low security and privacy standards of the sender.

A fraudulent e-mail flooding the Internet claims to have a link to an E-Card from a "family member," "friend," "neighbour," or a first name (i.e., Tom, Sue, etc.) and uses major greeting card company names such as Hallmark. Clicking on the link downloads a virus onto your computer that compromises personal data.

Instant Web Site ID

Want to be extra sure about a site's legitimacy before you make a purchase? Click on a site favicon for an instant identity overview. Another click digs deeper: how many times have you visited? Are your passwords saved? Check up on suspicious sites, avoid Web forgeries and make sure a site is what it claims to be.

Yahoo

Exercise(s)

Open Firefox.
Enter this address paypal.com and load the page.
Then press Ctrl + t to open another tab and enter this address: paypol.com

Check the favicons with a left click. What information do you get?

Exercise(s)

Does the ICICI bank have a security certificate? If not, why? Try to log in under **personal**. What security certificate does this site use?
icicibank.com

Question(s)

What is a security certificate? Where are those certificates stored?

Clear Private Data

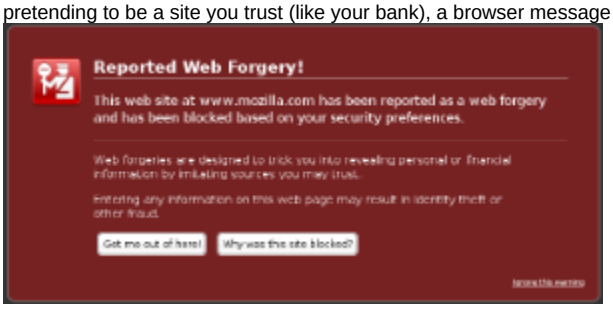
Question(s)
What are your private data on your computer or in your browser?

Exercise/Question
To clear your private data automatically go to TOOLS/CLEAR PRIVATE DATA on your own computer. Do you understand the content of this window?

Anti-Malware

Question(s)
What is malware?

Firefox 3 protects you from viruses, worms, Trojan horses and spyware. If you accidentally access an attack site, you'll receive a full-sized browser message as a warning. A continuously updated list of attack sites tells you when to stop browsing. This tool, called officially Malware Protection, warns you when you steer Firefox to sites that are known to install viruses, spyware, Trojan horses and other malicious code. When you try to reach a site on the banned list, a large red warning appears in lieu of the page. The warning says that the intended destination "has been reported as an attack site and has been blocked based on your security preferences." A button labeled "Get me out of here!" returns Firefox to the browser's original page.
Shop and do business safely on the Internet. Firefox gets a fresh update of web forgery sites 48 times in a day, so if you try to visit a fraudulent site that's pretending to be a site you trust (like your bank), a browser message - **big as life** - will stop you.



Exercise(s)
Search with google the keywords **mozilla trap** and follow the first link.

Automated Update

The open source security strategy finds - and fixes - security issues in record time, making Firefox the safest way to surf. Make sure you always use the latest Firefox copy!

Privacy

Let's have a look what other people know about your computer.
Spyware and viruses can scan your entire hard drive and send this information to people you don't know. They can find out who you are, where you live (address, email, phone etc), your passwords and credit card numbers and much more. They can scan your emails, know about stuff you don't want them to know - business information, secret girl or boy friends, illegal downloads ...

Internet lesson 3 - homework

Try to avoid doing the homework in the last minute but rather do them in time and email them to **bluelight.training@gmx.com**. **Please do not use the bluelight@auroville.org.in** address.
This gives us time to look into what you did and give you some feedback. **It is a requirement to do the homework to be able to follow the classes.**
You find all lessons and homework here

What is a favicon?

What is the Instant Web Site ID?

Explain the difference between http and https?

Name 3 companies which issue internet security certificates. Find out with Google.

Find 3 web sites that use internet security certificates.

You might want to take the time and go once more through the lesson to recall what you learned.

What should you do after browsing in a public place before you leave the computer?

What happens if you accidentally access an attack site (viruses, worms, trojan horses and spyware) with Firefox?

Go to the http://www.icicibank.com bank's website and click on login under personal. Why do you think on-screen virtual keyboards are in use?

Internet lesson 1 - homework

Try to avoid doing the homework in the last minute but rather do them in time and email them to **bluelight.training@gmx.com**. **Please do not use the bluelight@auroville.org.in** address.
This gives us time to look into what you did and give you some feedback. **It is a requirement to do the homework to be able to follow the classes.**
You find all lessons and homework here

You can copy and paste the questions into an email and answer them. In case you don't know the answer you could try to paste the question into google.co.in or the wiki

---

Install Firefox on your computer

How do I set my 'home page'? (Tip: look under the Tools-menu in Windows or under Edit in Linux)

Why will the Internet be important in the near future?

What is a URL?

What is the default browser?

How do you save an interesting link? Check the Bookmarks menu in Firefox ...

Get familiar with **Booksmarks Toolbar** (The personal address bar), **Location bar**, **Integrated Web Search** and the **Status bar**

See this 2 links below. Hoover with your mouse pointer (the arrow you move by moving your mouse) over the link (don't click) and see what information you get in the status bar (in the left bottom corner of Firefox)

http://www.google.co.in

Save your Soul

Read the blue box above about the Mozilla Foundation.

Read at least once the glossary below.

Handy Hint

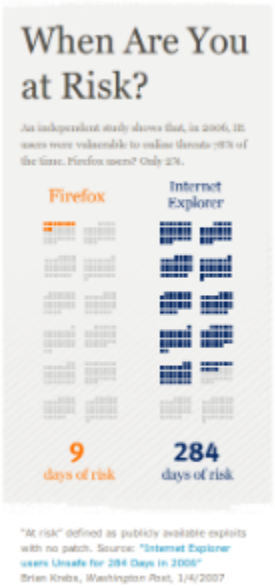
Use the right-click to call the context menu and see what you can do in this moment with your computer while the left-click means action. When you hover over an active link inside Firefox it turns into a hand - you can click then to follow the link. Not Every link is underlined any more. Sometimes words in a different colour are links.

Question(s)

How real is the Internet security problem?

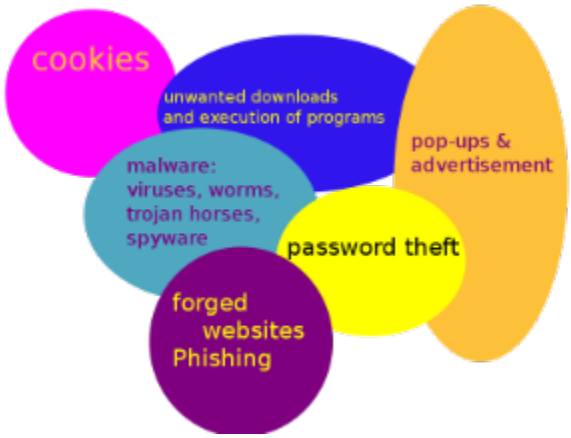
Security News worm

IE security test



Question(s)

What are common problems browsing on the Internet?



Let's have a look how Firefox helps you to be safe on the Internet

Firefox has a lot of inbuilt security like pop-up blockers, Phishing protection, safe password storage to name a few. We will have a closer look into this important aspect of Firefox. One can safely say that Firefox is one of the most secure browsers presently available. Security is the main concern designing Firefox.

Question(s)

What is a pop-up?

Pop-Up Blocker

Pop-Up windows are widely used on the Internet to display optional information and only pops up when needed. However, advertisement uses them to impose the ad on you. Banish those pop-ups (and pop-under windows) from your surfing experience once and for all. Or create an "allow" list of sites whose pop-ups you're okay with seeing. Not all pop-ups are bad...

(Disable the pop-up blocker)

This is an example for a misuse of pop-ups

Exercise(s)
Go to Firefox (Linux/Ubuntu) Edit/Preferences/Content and disable the pop-up blocker. Then press **Close** or Go to Firefox (Windows) Tools/Options/Content and disable the pop-up blocker. Then press **Close**. Open popuptest.com. Try the different pop-up tests in the **Common popup techniques** section and see what happens. Go back to the Firefox configuration panel and enable the pop-up blocker and repeat the test. What do you notice? Try the different pop-up tests in the **Not all pop-ups are bad...** section and see what happens. Tip: some pages are nasty ....

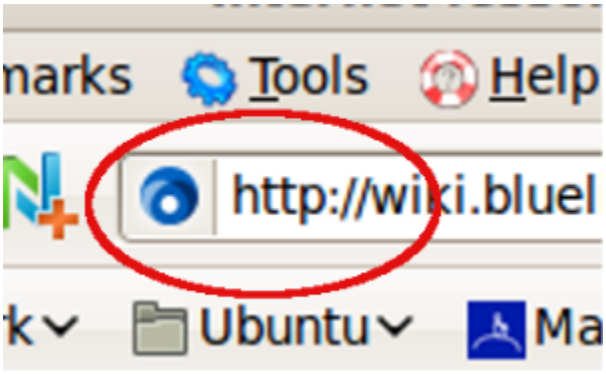
Six monkeys in one boat sail to Sumatra

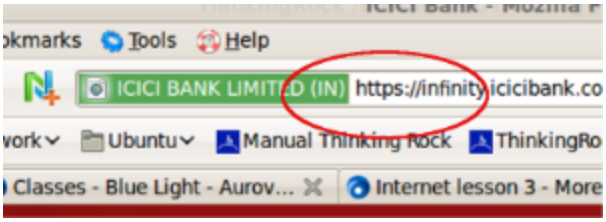
Be Careful

One password to rule them all ...
The truth about passwords - most people have one single all-purpose password for all logins! Is that good?
How many of you use one password for all?

The Firefox password manager is seamlessly integrated into your surfing experience. Intranet

Question(s)
Why are passwords like auroville, mother, surrender, truth, light weak? **Why are passwords like AuR0ville55, 6mi1bstS strong?** **How can you memorize a password like this one: 6mi1bstS ?** **What is the difference between encrypted and unencrypted (http and https) web sites? What difference does that make regarding passwords?**





How Firefox manages your passwords for the Internet

Sample login user: test
Show the saved password.

Exercise(s)

Go to a web site where you log in i.e. Intranet, Google or Yahoo mail etc.

Log in with a fake user name and save a password.

In Linux: Open the passwords preferences in Firefox: EDIT/PREFERENCES/SECURITY

In Windows: Open the passwords preferences in Firefox: TOOLS/OPTIONS/SECURITY

Check out your saved passwords.

Question(s)

What is the a master password?

Useful Information

PaSsWoRds arE cAsE seNsiTive.

Take care of the Caps Lock!

Some web sites use login restrictions: 3 times in 10 minutes or login is disabled for one hour after 5 failed logins. FS

Don't use language specific letters like ä ñ . Why?

Cookies

Question(s)

What is a cookie?

Are they stored on my computer? How long?

What happens if cookies are disabled?

HTTP cookies, or more commonly referred to as Web cookies, tracking cookies or just cookies are used for authenticating, session tracking, and maintaining specific information about users, such as site preferences or the contents of their electronic shopping carts.

Exercise(s)

Click on the favicon on any web page and click on the **More Information** button. Check out the cookies for this web site. Is it useful for you?

For more information go to the Wikipedia. Search for **HTTP cookies**

Internet lesson 2 - homework

Try to avoid doing the homework in the last minute but rather do them in time and email them to **bluelight.training@gmx.com**. **Please do not use the bluelight@auroville.org.in** address.
This gives us time to look into what you did and give you some feedback. **It is a requirement to do the homework to be able to follow the classes.**
You find all lessons and homework here

How do you recognize a secure website?

What is **Caps Lock**?

What is the master password in the Firefox context?

Sort the passwords in weak and strong ones: greenbelt Dosai1968 auroville SurRenDer Yu6Gfs7 Tuñ88T undercover

How dangerous are your favourite http-cookies? If you have sample cookies bring them to the next class? (The Blue Light team prefers chocolate cookies 🙂)

You might want to take the time and go once more through the lesson to recall what you learned.

Name 3 different types of useful pop-up windows?

If you find the following part much too difficult - relax. The aim of this test is not to pass with good results but to see for you how much you know **now** and how secure you feel being confronted with this and how much you know at the end of the next class and how you feel then. Have fun: Go to http://www.sonicwall.com/phishing/ and follow the instructions to do the Phishing test. How many of the 10 examples could you identify correctly?