Internet safety

On the internet, these must be protected:

* the computer
* the user
* data

# Computer protection

The basic elements of computer protection are firewalls, antispyware, antivirus programs and it is necessary to patch security holes.

***Firewall*** – usually an application protecting the computer from attacks and filtering the network traffic.

***Antispyware* –** protects the computer from spyware.

***Antivirus program*** – a program which detects and removes harmful programs. The effectiveness relies on keeping an updated database.

***Security vulnerability*** – errors in the programming which can be abused to attack the computer. The resolutions to these errors are called **security patches** and are regularly released for operation systems, browsers and other software.

The computer also needs to be protected from malware. Malware is all the malicious software that can be acquired and can corrupt the computer or the data in it.

Malware can be:

* *a computer virus* – a program that latches onto a file, replicates and infects other files on the computer
* *worm* – a program spreading and replicating in networks without a host program and which seeks suitable computers. The goal is to corrupt access to a service or site.
* *trojan horse* - masquerades as benign software but in fact it monitors the user’s activity, sends data and attacks unexpectedly
* *spyware* – gathers information about the computer or its user and sends it to another entity without permission
* *adware* – programs generating advertisement
* *spam –* unsolicited electronic messages, spreads like an avalanche
* *hoax –* deliberately fabricated falsehood
* *phishing* – an e-mail asking to change the login data to a bank account. Sometimes all it takes is to enter one’s login information on a false website linked in the e-mail.

# User protection

# Internet users should be protected as well. They should not publish their personal information to prevent abuse. The forms of abuse on the internet are:

* *cyberbullying* – bullying via IT technologies
* *stalking* – surveillance and harassment
* *slander, intimidation, trolling* (provoking and harassing other users)
* *fraud and scamming*

# Data protection

# In an information society, the protection of data is crucial. That is why users should protect their data from:

* *computer crime* – crime and offenses towards computers or committed using computers
* *computer piracy* – unauthorised use of computer programs, mainly unauthorised entering of other systems
* *social engineering* – a confidence trick on a selected target

**Literature**

Skalka, J. – Klimeš, C. – Lovászová, G. – Švec, P.: Informatika na maturity a prijímacie skúšky, Enigma Publishing, 2017, ISBN 978-80-89132-49-2