«Drive-by Infections» Information and Prevention

Threats posed by drive-by infections:

- Drive-by infections infect a computer with malicious code when merely visiting a website, i.e. visitors don't need to start a download or explicitly install anything.
- Even legitimate, well-known and frequently-visited websites could have become infected with malicious code.
- Firewalls don’t offer any protection against this.

The best ways to protect yourself:

- always use the latest version of your browser, including plug-ins (e.g. Adobe Flash Player, JavaScript etc.)
- always keep your operating system and all installed programs up-to-date (e.g. Adobe Acrobat Reader)
- always update your virus scanner
- regularly check your hard disk for viruses
- if possible, deactivate scripts (JavaScript, ActiveX etc.) in your browser

Drive-by infections

The term «drive-by infection» describes the process of malware (e.g. viruses, Trojans) infecting a user’s computer merely by visiting a website. Just surfing to an affected website is sufficient to infect a computer, exploiting security gaps in browsers and plug-ins.

To protect yourself, make sure to always use an up-to-date operating system and programs (browser, incl. plug-ins and other software).

Checking websites

On their https://safeweb.norton.com website, Norton (Symantec) offer a service to establish the security status of well-known websites (and any threats they may face).

Further information: www.ebas.ch/drivebyinfection

«eBanking – but secure!» is offering helpful security hints for e-banking users

eBanking but secure!

You will find further practical information on measures and approaches required to ensure that e-banking applications are used securely under **www.ebankingbutsecure.ch**. The use of this website is free.

Hochschule Luzern – Informatik
Campus Zug-Rotkreuz, Suurstoffi 41b
CH-6343 Rotkreuz