



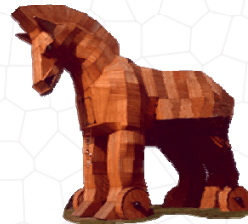
Intentional misuse of your computer

The most common methods used by intruders to gain control of home computers are:

- Trojan horse programs
- Denial of service
- Being an intermediary for another attack
- Mobile code (Java, JavaScript, and ActiveX)
- Email spoofing
- Email-borne viruses
- Hidden file extensions
- Chat clients

Trojan Horse Programs

Appear to be useful utilities or games, but when installed will allow hackers access to a user's system via "back doors."



Denial of Service

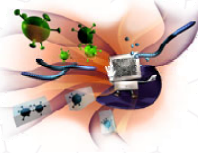
This type of attack causes your computer to crash or to become so busy processing data that you are unable to use it.



Mobile code (Java/JavaScript/ActiveX)

You can potentially expose your web browser to malicious scripts by:

- following links in web pages, email messages, or newsgroup postings without knowing what they link to
- using interactive forms on an untrustworthy site
- viewing online discussion groups, forums, or other dynamically generated pages where users can post text containing HTML tags

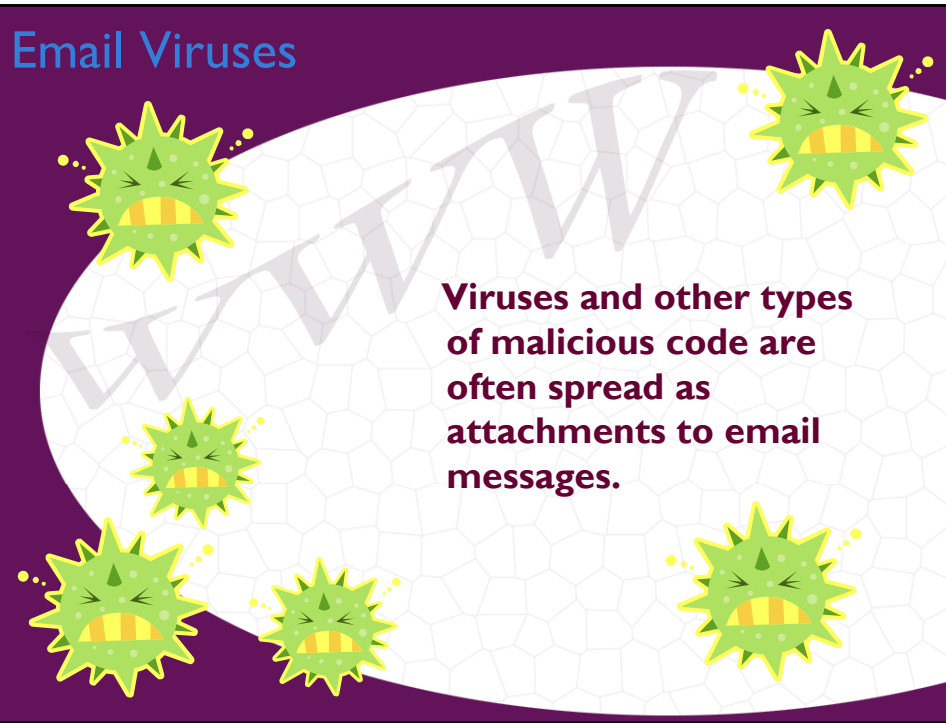


Email spoofing

Email “spoofing” is when an email message appears to have originated from one source when it actually was sent from another source.

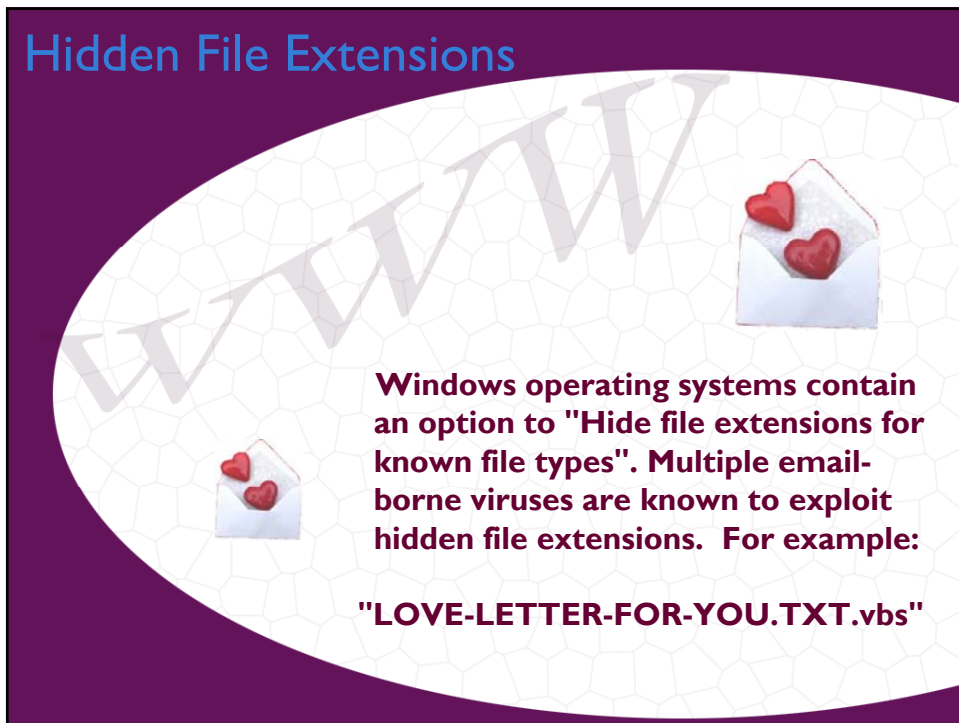


Email Viruses



Viruses and other types of malicious code are often spread as attachments to email messages.

Hidden File Extensions



Windows operating systems contain an option to "Hide file extensions for known file types". Multiple email-borne viruses are known to exploit hidden file extensions. For example:

"LOVE-LETTER-FOR-YOU.TXT.vbs"

Protecting Your System



- **Use virus protection software**
- **Use a firewall**
- **Don't run programs of unknown origin**
- **Keep all applications (including your operating system) patched**
- **Turn off your computer or disconnect from the network when not in use**
- **Make regular backups of critical data**

Protecting Yourself while On-line

- **Establish another e-mail address for use with news groups and 'strangers'**
- **Surf anonymously**
- **Don't open unknown e-mail attachments**
- **Disable hidden filename extensions**
- **Disable scripting features in e-mail programs**
- **Disable Java, JavaScript, and ActiveX if possible**
- **Use mail screener techniques during high virus threat times**

Avoid Adware, and other Snoops

- **Lavasoft's Ad-Aware Remover** (<http://www.lavasoftusa.com/>)- Ad-Aware will safely remove all sorts of spyware programs you may have innocently downloaded into your system along with shareware. They provide a free Personal Edition.
- **SpyChecker** (<http://www.spychecker.com/>) A database of known spyware/software titles and how to get rid of them.

Identity Theft and On-line Shopping

- **Cancel your credit cards immediately**
- **File a police report immediately**
- **Call the three national credit reporting organizations immediately**
- **Alert your bank**
- **Request a change of PIN and new password**
- **Contact the Social Security Administration's Fraud Hotline**
- **Contact DPS**

