How to protect yourself against viruses

- Operating systems are not secure, buying and installing virus protection software on your computer is an important safeguard.
- Avoid downloading programs from unknown sources (like the Internet), and instead stick with commercial software purchased on CDs to eliminate most of the risk from viruses.
- Never open an e-mail attachment unless you know what it is- even if it's from someone you know and trust. Contact the sender if you are not sure
- Never double-click on an attachment that contains an executable file that arrives as an e-mail attachment. Attachments that come in as Word files (.DOC), spreadsheets (.XLS), images (.GIF and .JPG), etc., are data files and they typically can do no damage. A file with an extension like EXE, COM or VBS is an executable file, and an executable can do any sort of damage it wants. Once you run it, you have given it permission to do anything on your machine. The VBS is an executable file, and an executable can do any sort of damage it wants. Once you run it, you have given it permission to do anything on your machine. The only defense is to never run executable files that arrive via e-mail.

Additional Websites that may be Useful:

Viruses and Firewalls: www.symantec.com

Spam: www.mailwasher.net

Spyware and removal tools: www.lavasoft.de

How Stuff Works: www.howstuffworks.com

Department of Technology Services

Jack Belcher, CIO

Christopher T. David
Chief Technology Officer

Rob Billingsley
IT Procurement Manager

Denise Hart, PMP
Program Management Officer

David Jordan
IT Security and Privacy Officer

Ajit Arya
e-Government Architect

Lou Michael
Director, Network Infrastructure

Joe Bistany
Telecommunications

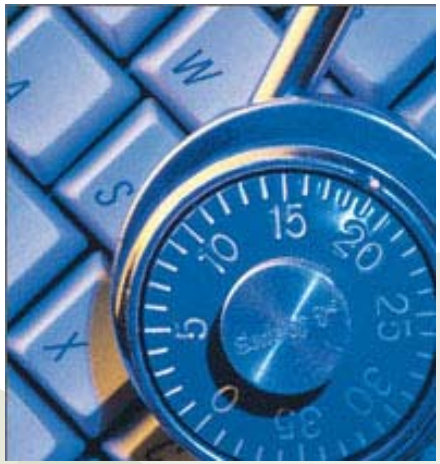
Maria Meredith
ERP Program Manager

George Barusso
Administrative Officer

Steven Fort
IT Budget Officer

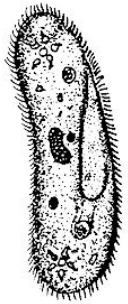
2100 Clarendon Blvd, Suite 612
Arlington, VA 22201
(703) 228-3220
cio@arlingtonva.us

Computer Security for the Home PC



A Quick Lesson for Home Computer Users

ARLINGTON VIRGINIA | DEPARTMENT OF TECHNOLOGY SERVICES



WHAT IS A COMPUTER VIRUS?

Viruses – A virus is a small piece of software that piggybacks on real programs. The virus must piggyback on top of some other program or document in order to get executed. Once it is running, it is then able to infect other programs or documents. It passes from computer to computer like a biological virus passes from person to person.

E-mail viruses – An e-mail virus moves around via e-mail messages, and usually replicates itself by automatically mailing itself to dozens of people in the victim's e-mail address book.

HOW DOES AN E-MAIL VIRUS WORK?

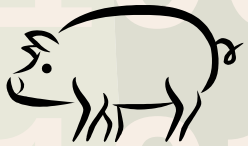
Example: Someone creates a virus as a Word document and uploads it to an Internet newsgroup. Anyone who downloads the document and opens it, triggers the virus.

The virus would then send the document (and therefore itself) in an e-mail message to the first 50 people in the person's address book. The e-mail message would contain a friendly note that included the person's name, so the recipient would open the document, thinking it was harmless. The virus would then create 50 new messages from the recipient's PC, and so on.

WHAT IS A WORM?

Worms – A worm is a computer program that has the ability to copy itself from machine to machine. Worms normally move around infect other machines through computer networks. Using a network, a worm can expand from a single copy incredibly quickly. For example, the **Code Red** worm replicated itself over 250,000 times in approximately nine hours.

WHAT IS SPAM?



Spam is unsolicited "junk" e-mail, usually mass-distributed, to promote products or services. Spam also refers to inappropriate promotional or commercial postings to discussion groups or bulletin boards.

The best technology that is currently available to stop spam is spam filtering software.

WHAT IS A TROJAN HORSE?

Trojan horses – A Trojan horse is simply a computer program. The program claims to do one thing (it may claim to be a game) but instead does damage when you run it (it may erase your hard disk). Trojan horses have no way to replicate automatically.

WHAT IS PHISHING?

Phishing is a form of criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication. Phishing is one way that **identity theft** can be carried out and usually occurs through e-mail or an instant message.

More recent phishing attempts have targeted the customers of banks and online payment services. E-mails supposedly from the Internal Revenue Service have also been used to glean sensitive data from U.S. taxpayers. While the first such examples were sent indiscriminately in the hope of finding a customer of a given bank or service, recent research has shown that phishers may be able to identify the bank a potential victim has a relationship with, and then send a spoofed email to this victim.

Social networking sites are also a target of phishing, since the personal details in such sites can be used in identity theft. Experiments show a success rate of over 70% for phishing attacks based on social networks