infosec@pjlhuillier.com
ICT GROUP
INFOSEC101
CONFIDENTIALITY • INTEGRITY • AVAILABILITY

November 7, 2014 Release # 291

Begin Transmission…

How to avoid Viruses, Trojans, Worms and Spyware

Use Antivirus or Endpoint Security Software - Install antivirus or endpoint security software on all your desktops and servers, and make sure to keep them up to date. New malware can spread extremely quickly, so have an infrastructure in place that can update all the computers in your organization seamlessly, frequently and on short notice. To protect against email-borne viruses, spam and spyware, run email filtering software at your gateway. And don't forget to protect laptop computers, desktop computers and mobile devices used by employees who telecommute.

Block File Types that often carry malware - Block executable file types from being received by email or downloaded from the Internet. It is unlikely that your organization will ever need to receive these types of files from the outside world.

Use a Firewall on All Computers - Use a firewall to protect computers that are connected to a network. Many worms can enter even a closed network via USB drives, CDs and mobile devices. Laptops and telecommuters will also need firewall protection.

Stay up to date with Software Patches - We encourage using automatic (patch) updating, especially in the case of Windows computers. Patches often close loopholes that can make you vulnerable to malware threats.

Back up your Data Regularly

- Make regular backups of important work and data, and check that the backups were successful. You should also find a safe place to store your backups, preferably off-site in case of fire. If your computer is infected with malware, you will be able to restore any lost programs and data. Any sensitive backup information should be encrypted and physically secured.

Implement Device Control

- Prevent unauthorized devices from connecting to your computers. Unauthorized devices such as USB drives, music players and mobile phones can carry malware that will infect a computer when plugged in.

End of Transmission…

Information Security: It's a Shared Responsibility
REFERENCE(S): Sophos Threatsaurus : The A-Z of Computer and Data Security Threats
INTERNAL USE ONLY: For circulation within the PJ Lhuillier Group of Companies only.