Security Best Practices

1. Keep a strong password:
   A strong password:
   - Is at least eight characters long.
   - Does not contain your username, real name, or company name.
   - Does not contain a complete word.
   - Is significantly different from previous passwords.
   - Contains characters from each of the following four categories: uppercase letters, lowercase letters, numbers and symbols
2. Don't reuse your passwords.
3. Don’t share your password.
4. Avoid websites that you may suspect provide pirated material.
5. Think before you click.
6. Use a pop-up blocker.
7. Do not open an email attachment from somebody or a company that you do not know.
8. Do not open attachments in unsolicited emails, even if they come from people in your contact list.
9. Never click on a URL contained in an unsolicited email, even if you think it looks safe. Instead, close out the email and go to the organization’s website directly.
10. Always hover over a link (especially one with a URL shortener) before you click to see where the link is really taking you.
11. If you have to download a file from the Internet, an email, FTP site, or a file-sharing service, etc., scan it before you run it.
12. If you travel back and forth using a USB key, scan the USB on a regular basis. A good anti-virus software will scan your links and your USB automatically, but make sure it is being done.
13. Keep Your Operating System Current - Whether you are running Windows or Mac OS X, keep it up to date at home and at work.
14. Keep your antivirus software up to date.
15. Only download software—especially free software—from sites you know and trust (malware can also come in downloadable games, file-sharing programs, and customized toolbars). Poor browsing habits are a leading contributor to malware infections.

Prevent Malware With Smart Online Behavior

The single biggest factor in preventing a malware infection on your PC is you. You don't need expert knowledge or special training. You just need vigilance to avoid downloading

and installing anything you do not understand or trust, no matter how tempting, from the following sources:

From a website: If you are unsure, leave the site and research the software you are being asked to install. If it is OK, you can always come back to site and install it. If it is not OK, you will avoid a malware headache.

From e-mail: Do not trust anything associated with a spam e-mail. Approach e-mail from people you know with caution when the message contains links or attachments. If you are suspicious of what you are being asked to view or install, don't do it.

From physical media: Your friends, family, and associates may unknowingly give you a disc or flash drive with an infected file on it. Don't blindly accept these files; scan them with security software. If you are still unsure, do not accept the files.

From a pop-up window: Some pop-up windows or boxes will attempt to corner you into downloading software or accepting a free "system scan" of some type. Often these pop-ups will employ scare tactics to make you believe you need what they are offering in order to be safe. Close the pop-up without clicking anything inside it (including the X in the corner). Close the window via Windows Task Manager (press Ctrl-Alt-Delete)

From another piece of software: Some programs attempt to install malware as a part of their own installation process. When installing software, pay close attention to the message boxes before clicking Next, OK, or I Agree. Scan the user agreement for anything that suggests malware may be a part of the installation. If you are unsure, cancel the installation, check up on the program, and run the installation again if you determine it is safe.

From illegal file-sharing services: You're on your own if you enter this realm. There is little quality control in the world of illegal software, and it is easy for an attacker to name a piece of malware after a popular movie, album, or program to tempt you into downloading it.

If you have any questions about this email or this list of best practices, please send an email to bbowers@lexington1.net.

Thank you.

Lexington One Information Technology Department