|  |
| --- |
| **TECHNOLOGY PLUG-IN T1 – Personal Productivity Using IT** |

**LEARNING OUTCOMES**

1. **Describe the four steps you can use to create a strong password.**

* **Create strong passwords that you can remember**. A strong password is one that is at least eight characters, includes a combination of letters, numbers, and symbols and is easy for you to remember, but difficult for others to guess. The easiest way to create a strong password that you will not have to write down is to come up with a *passphrase*.
* **Keep your passwords a secret**.
* **Manage your passwords.** A strong password is one you change every few months.
* **Monitor your accounts**.

1. **Identify three tips you can use to manage your files.**

* Use My Documents
* Limit file name lengths
* Archive completed work
* Use shortcuts instead of multiple copies
* Use abbreviations
* Use thumbnails
* Do not save unnecessary work.

1. **Explain why you would use Microsoft’s backup and recovery utility.**

The Backup Utility in Windows XP helps protect data if a hard disk fails or files are accidentally erased due to hardware or storage media failure. The Recovery Console is used to perform many tasks without starting Windows XP, including starting and stopping services, reading and writing information on a local disk drive, and formatting drives.

1. **Describe the six common e-mail mistakes.**

* Failing to follow e-mail etiquette
* Attempting anonymity
* Sending e-mail to the wrong person
* Using one e-mail address for everything
* Clicking send to fast
* Forgetting the attachment

1. **Explain spam and phishing and identify three ways that you can prevent each.**

**Spam** is received junk e-mail. Tips to stop spam include:

* Delete junk e-mail messages without opening them.
* Do not reply to spam.
* Think twice before opening attachments.
* Do not buy anything through spam.
* Do not forward chain e-mail messages.

**Phishing** is a type of deception designed to steal your identity. In phishing scams, scam artists try to get you to disclose valuable personal data, such as credit card numbers, passwords, account data, or other information, by convincing you to provide it under false pretenses. Tips to stop phishing include:

* Report suspicious e-mail.
* Be wary of clicking on links in e-mail.
* Type addresses directly into your browser or use personal bookmarks.
* Check the security certificate when you are entering personal or financial information into a Web site.
* Do not enter personal or financial information into pop-up windows.

1. **Explain the primary uses of spyware and adware.**

**Spyware** is a general term used for software that performs certain behaviors such as advertising, collecting personal information, or changing the configuration of your computer, generally without appropriately obtaining your consent. Spyware is often associated with software that displays advertisements (called **adware**) or software that tracks personal or sensitive information.

1. **Identify three things you can do to maintain your computer and keep it running smoothly.**

* Free disk space.
* Speed up access to data.
* Detect and repair disk errors.

1. **Explain why you would install anti-virus protection software.**

**Anti-virus (AV)** is a term applied to either a single program or a collection of programs that protect a computer system from viruses. Anti-virus software is designed to keep your PC free of computer viruses and worms. It does so by scanning your PC’s file system looking for known viruses; if a virus is found, the software will inform you and then take steps to remove the virus threat.

1. **Describe the need for a personal firewall.**

A **firewall** is simply a program or hardware device that filters the information coming through the Internet connection into a computer. If an incoming packet of information is flagged by the filters, it is not allowed through.

**CLASSROOM EXERCISE**

**Cell Phones, Spam, Phishing, and Viruses**

As next-generation cell phones grow in popularity and function more like PCs, digital intruders are targeting them with viruses, spam and phishing schemes. There are several mobile phone viruses in the wild at the moment, including Skulls, Cabir, and Fontal. And, like many PC-based viruses, each has its own set of variants.

When you contemplate the possibilities, the concept of Cabir gets pretty scary. The number of computer users who are already targets of virus infections pales in comparison to the number of mobile phone users out there.

Ask students…

1. How many use Bluetooth?
2. How many know what Bluetooth is?
3. How many check for cell phone security updates?
4. How many install some type of security software on their phone?

As a side note to mention to your class…

**That Thing With Paris Hilton's Phone**

Remember when someone got his hands on Paris Hilton's star-studded contact list? It was not the result of a virus, and nobody hacked into Hilton's phone. Mobile phone servers hold on to certain types of information, such as contact lists (in case the user's phone locks up) and recent calls (for billing purposes). The enterprising hacker got into T-mobile's servers and stole the information from there.

**Internet Resources:**

* [How Cell-phone Viruses Work](http://electronics.howstuffworks.com/cell-phone-virus.htm)
* [The 10 Biggest Security Risks You Don't Know About](http://www.pcworld.com/article/id,126083-page,8/article.html)

**EXTENDING THE CORE MATERIAL**

**Google puts up 'Beware of malware' signs**

Google has started warning people when search results could potentially lead them to malicious code.

The search giant is using data from the Stop Badware Coalition to flag sites that are potentially host to malicious software. Google, along with Sun Microsystems and Chinese PC maker Lenovo, announced support for the group.

People who attempt to go to a Web site that has been identified as risky by the coalition are taken to a warning page.

"Warning--the site you are about to visit may harm your computer!" the page states in bold type, then suggesting users can "learn more about malware and how to protect yourself at StopBadware.org."

The interrupt page suggests that users can try returning to the search page and choosing a different result, trying another search or they can continue to the potentially malicious site.

**Windows Vista**

Not all students have Microsoft Vista unless they bought a new laptop or PC recently. Chances are you (the instructor) may not have it either, as many schools have been reluctant to migrate (as of this writing). It may be worth taking a straw poll in class to see how many students are using Windows XP and how many have Vista. For those that have Vista, ask how they would rate their experience (good, fair, great).

* For those students who have yet to upgrade, you might want to have students tour the Microsoft Vista Web site for a closer look. <http://www.microsoft.com/enable/training/windowsvista/>

**MAKING BUSINESS DECISIONS**

1. **Third-Party Backup Utilities**

**Project Purpose:** To begin to understand the various types and choices of backup software available.

**Potential Responses:** Although there is no right or wrong answer here, students responses should be pragmatic to their needs and budget. Some of the more popular utilities that students should find are: Norton Ghost, Keepsafe, and AutoSave.

1. **Spybot Search & Destroy**

**Project Purpose:** To begin to understand one tool to assist in eradicating spyware and adware.

**Potential Responses:** Although there is no right or wrong answer here, this exercise should provoke some interesting results. Some students may be familiar with this utility and use it regularly. However, for those students who have never use this tool or any other anti-spyware or adware, they will be amazed at the amount of malicious software hiding on their system.

1. **Firewall Utilities**

**Project Purpose:** To begin to understand use of a personal firewall utility.

**Potential Responses:** Although there is no right or wrong answer here, this exercise should be monitored so that firewalls don’t block student’s basic Internet access, including Web surfing and e-mail retrieval.

1. **Testing Your Setup**

**Project Purpose:** To begin to understand the different types of online resources to use for personal computer safety.

**Potential Responses:** There is no right or wrong answer with this exercise; however, it would be worth noting which students found vulnerabilities and with what product/utility.

1. **Scanning From The Web**

**Project Purpose:** To begin to understand how an online free virus scan operates.

**Potential Responses:** There is no right or wrong answer with this exercise; however, it would be worth noting which students found vulnerabilities using the PC-cillin product.