

## Safe E-mail Practices

Listed here are definitions of spam, scam and e-mail viruses and some tips on how to deal with these common threats.

### **Spam**

Spam is a form of advertising on the Internet similar to telemarketing. It involves sending out e-mail messages to as many e-mail addresses as possible in the hopes that someone will respond to the message by going to the sender's Web site and buying their product.

#### Dangers:

- Large amounts of spam can fill up e-mail boxes quickly, creating the need to delete or filter the spam.
- Spam can contain viruses.
- Not all spam messages are from legitimate businesses.

#### How to Identify:

- Looks presentable, no spelling errors, good formatting.
- Sender's address often shows up as a business rather than a plain [name@domain.com](mailto:name@domain.com) type e-mail address.

### **Scam**

Scam e-mails are sent out in an attempt to get the recipient to provide some sort of personal confidential information, such as credit card numbers, bank account information or other account information. This is also known as "phishing," and is one of the leading causes of identity theft.

#### Dangers:

- Identity Theft resulting in the loss of personal assets, and damage to credit ratings.
- Can result in a home network or business network being "hacked."
- Can result in more unwanted spam.

#### How to Identify:

- Attempts to look formal, usually will have spelling errors or not look like a standard e-mail from that organization.
- Will ask "to verify" account information. (No official company or organization will contact clients to ask for verification of account information.)
- Usually asks the recipient to open an attached file.

### **E-mail Viruses**

E-mail viruses are simply any virus spread by e-mail. A virus can perform various different kinds of tasks, based on what it was designed to do once it is on a computer system. Some viruses are spread by downloading attachments, while others infect systems when an e-mail message is opened.

#### Dangers:

- Can cause loss of data on system attacked and spread to other systems.
- Can record activities and report them back to the programmer of the virus. (These are known as Trojans.)
- Can cause loss of performance on the computer by using its resources.

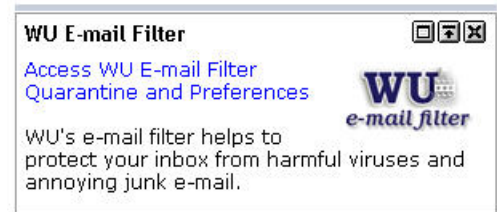
#### How to Identify:

- By subject line, will often be passed around as a joke e-mail.
- Sender's address is often not familiar, but because viruses sometimes reach into address books and files on a system, there is the possibility that the sender's address will be an acquaintance or colleague.
- Text in the e-mail is illegible.
- Attachment has a .exe file extension.

Please see the other side for tips on how to deal with these nuisances.

There are a lot of hazards out there, but almost all of them can be avoided by using the following guidelines regarding e-mail.

- Use the WU e-mail filter available from the Support tab on My Washburn.



Verify that the “Log on to:” pull-down is set to **MyWashburn**.

Log in with the same username and password used to log in to MyWashburn.

- If the sender’s address does not look familiar, do not open the e-mail. Just delete it.
- Scan attachments for viruses. Do not open any .zip or .exe attachments without knowing what they are.
- Only provide personal e-mail addresses to trustworthy people/businesses. Read the privacy policy for online businesses. There are a few companies that sell addresses to spammers.
- Use a ‘disposable’ e-mail address, such as a free account from Yahoo! or Hotmail, for online purchases.
- NEVER give out account information by e-mail. When providing credit card or bank account information to an online vendor, make sure the vendor’s site is secure. Before pushing the button to send this confidential information, look for https:// at the beginning of the address instead of just http:// .
- If an e-mail looks suspicious, just delete it. If it was important and legitimate, the sender will determine some other way to disseminate the information.

Remember, you are the first line of defense in preventing these attacks!