

SAFE EMAIL GUIDELINES:

SAFE PRACTICES AND THE CONSEQUENCES OF BEING UNSAFE

What Are Safe Email Practices?

- **Don't open email attachments** unless you know what they are.
- **Don't open, forward or reply** to spam or suspicious emails; delete them
- **Be aware of sure signs of scam email.**
 - Not addressed to you by name
 - Asks for personal or financial information
 - Asks you for password
 - Asks you to forward it to lots of other people
- **Don't click on website addresses** in emails unless you know what you are opening.
- **Use official WSU student email addresses** to communicate with students about grades or to provide feedback on assignments.
- **Use antivirus and firewalls** and update them regularly.
- **Report email security concerns** to the IT Help Desk.

How Do I Recognize Phishing?

- Phishing is a type of email or instant message scam designed to steal your identity.
- Phishing is the act of attempting to fraudulently acquire sensitive information, such as usernames, passwords, and credit card details, by masquerading as trustworthy entity in electronic communication using email or instant message.

How Can I Safeguard Against Phishing?

- Don't reply to email or pop-up messages that ask for personal or financial information.
- Don't click on links in email or instant message.
- Don't cut and paste link from questionable message into your Web browser.
- Use antivirus and firewalls and update them regularly.
- Don't email personal or financial information.

Virus Detection and Prevention Tips

- **Do not open** any files attached to an email from an unknown, suspicious or untrustworthy source.
- **Do not open** any files attached to an email unless you know what it is, even if it appears to come from a dear friend or someone you know. Some viruses can replicate themselves and spread through email. Better be safe than sorry and confirm that they really sent it.
- **Do not open** any files attached to an email if the subject line is questionable or unexpected. If the need to do so is there always save the file to your hard drive before doing so.
- **Delete chain emails and junk email.** Do not forward or reply to any to them. These types of email are considered spam, which is unsolicited, intrusive mail that clogs up the network.
- **Do not download** any files from strangers.
- **Exercise caution** when downloading files from the Internet. Ensure that the source is a legitimate and reputable one. Verify that an anti-virus program checks the files on the download site. If you're uncertain, don't download the file at all or download the file to a floppy and test it with your own anti-virus software.
- **Update your anti-virus software regularly.** Over 500 viruses are discovered each month, so you'll want to be protected. These updates should be at the least the products virus signature files. You may also need to update the product's scanning engine as well.

- **Back up your files on a regular basis.** If a virus destroys your files, at least you can replace them with your back-up copy. You should store your backup copy in a separate location from your work files, one that is preferably not on your computer.
- When in doubt, **always err on the side of caution** and do not open, download, or execute any files or email attachments. Not executing is the more important of these caveats. Check with your product vendors for updates which include those for your operating system web browser, and email. One example is the security site section of Microsoft located at <http://www.microsoft.com/security>.
- If you are in doubt about any potential virus related situation you find yourself in, ask!

Beware of "Spoofed" Email

There are viruses on the internet today that work through the current internal email system. (SMTP / POP protocols.) They "spoof" (pretend / appear to be someone else) an email address to gain your trust and acceptance to do something you ordinarily wouldn't do (and shouldn't do). The latest round of viral produced email attempts to get you to click on attachment. It may be a .zip or a .pif - either way, if clicked on it starts computer code that executes on your PC and can damage your machine or other machines. Or the "spoofed" email may contain a link to a web site that will download viruses or malware/spyware to your computer.

Consequences of Unsafe Practices

If your email account has been compromised:

- The effect on the campus mail servers is a flood of email that can in a short period of time clog up the system enough to slow or stop email services.
- Outside email services (AOL, MSN, Comcast, etc.) can and will blacklist our campus email – their email servers will block and reject email sent from our servers.
- Your personal information that you provided can be used to steal your identity – this can include everything from using your email address to send spam, to using your identity to make purchases in your name causing havoc with your credit.

If your computer gets a virus:

- Your computer may become infected with a virus that can spread rapidly to other people's computers.
- You may lose some or all of the information on your computer.
- Your computer could be used as a "base of operations" for sending spam, downloading illegal internet content and more.