

Safe Computing Practices

Email Safe Practices

NEVER....give out personal information upon request in an email. This includes your username, password, address, phone or account numbers, and especially your Social Security number. Email is not secure, and reliable companies will never send out email asking for this information.



Phishing Emails: These messages will ask for personal information, especially passwords and account numbers. The sender will forge the email address to look genuine. Links will be added that appear to connect to the real company but instead go to the counterfeit site. Hinds' users have received a number of these recently. **Never respond to them!!**

NEVER...open unexpected or suspicious email attachments. This may execute a disguised program (e.g. adware, spyware, or viruses) and may damage or steal your data. If in doubt, call the sender and verify.

NEVER...call company numbers in emails if the email looks suspicious. Always check a reliable source such as a phone book or credit card statement.

ALWAYS....be diligent and use common sense. If it looks suspicious, it probably is. Do not open it! **Delete it!**

Internet



Even though newer browsers offer added security, you can never be too careful. Be wary of links on websites. While they may seem harmless, they could be littered with pop-ups that may lead to unwanted harmful software called malware. Pop-ups today have changed from new

browser windows to ads that look like windows or graphics that dance across your screen, but they are actually designed to lure you into clicking them. Free screensavers, music and game sites, and even surveys for gifts are common things that people click on.

Dangers of DownloadingIf you do download software in the form of games, screensavers, music, videos, internet toolbars, etc., they may be infected with malware. When malware is downloaded, it can embed and remain on your system even if the original software is uninstalled. Toolbars downloaded from various sites such as Yahoo, Google, etc. will give you increased functionality in browsing, but the site that allowed you to download the toolbar can now also track your browsing movements. Nothing, especially freeware, comes without a price today.

Definitions of Malware



Adware: A form of malware that collects information about the user in order to display advertisements in the Web browser based on the information it collects from the users browsing patterns.

(<http://www.webopedia.com>)

Spyware: Any software that covertly gathers user information through the internet connection without his or her knowledge, usually for advertising purposes, is typically bundled as a hidden component of freeware or shareware. Once installed, the spyware monitors user activity on the internet and transmits that information in the background to someone else. (<http://www.webopedia.com>)

If you need help, call the Support Center at 601-857-3344.