Protecting Home PCs

Information Security & Privacy Office

Information Technology Services
"Connecting Phoenix to Information"

Agenda

- Terminology and common security myths
- Practical ways to protect your home computers from threats
  - Shiny new PC
  - Daily workhorse
  - Crusty, slow, obsolete PC

- Note: General info provided is applicable to all personal computers. Examples show Microsoft-specific tools. For other PCs and other operating systems, consult your vendor.

Disclaimers

- It is up to you to make sure you take the proper steps to secure your home PC
  - Information on protecting your home PC is provided as a courtesy by City of Phoenix and is only an introduction
- City of Phoenix is not responsible for personal computers not owned by the City
  - The City's Help Desk cannot answer any questions about computers that are not owned by the City
- City of Phoenix does not endorse any specific vendors or products
  - Vendors and products mentioned are examples only

Terminology

What Is Malware?

- Term for malicious software
- Includes viruses, worms, Trojan horse programs, keystroke loggers, and other malicious software

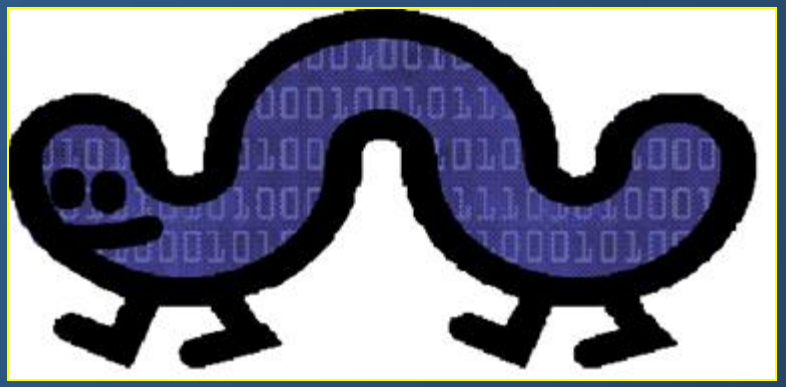
- Most people just use the term, "virus" for all malicious software

What Are Viruses?

- A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes
  - Designed to make copies of itself (replicate), usually without your knowledge
  - **Usually requires user action to run**, such as opening an e-mail attachment
  - Often contains payloads, malicious or annoying actions that the virus carries out separately from replication

What Are Worms?

- Malicious code that requires no specific action on your part to enable infection or to propagate



How Do Worms Spread?

- Worms generally take advantage of a software bug or flaw, called a vulnerability
- A worm is like a zombie looking for "fresh meat"
  - Worms check all devices on a network to see if they're vulnerable
  - If so, the worm infects the computer
  - Now the newly infected computer travels the network asking all connected devices if they're vulnerable

Other Types of Malware

- Trojan horse program: A program that comes into your computer disguised as something else, such as a game or screen saver
- Keystroke logger: A program or hardware device that records all keystrokes
  - Often used by attackers to obtain passwords or personal information, such as bank account numbers
  - Many Trojan horse programs are keystroke loggers
- Spyware: A program that collects information about you and your surfing habits without your knowledge
- Virus Hoax: An intentionally deceptive e-mail warning about a nonexistent computer virus

Scareware aka Rogue Software

- Fake security software
  - Gets you to load malicious software AND
  - Gets your personal / credit card info
- In the first half of 2009, there was a 583% increase in scareware programs

True or False

- I don’t have anything an attacker would want

False

- Bad guys want to control your PC
  - To send spam or distribute malware
- Bad guys want your identity
  - To use for identity theft and fraud

- Most attacks are automated – they simply seek out and compromise all vulnerable systems

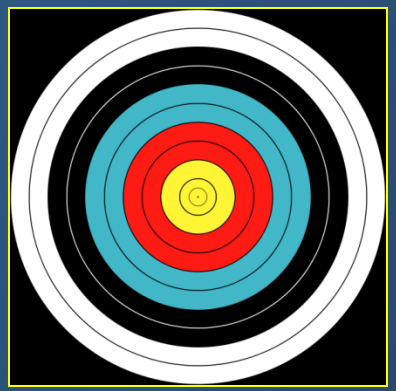
True or False

- Security is a concern only if I use Microsoft Windows

Information Technology Services
"Connecting Phoenix to Information"

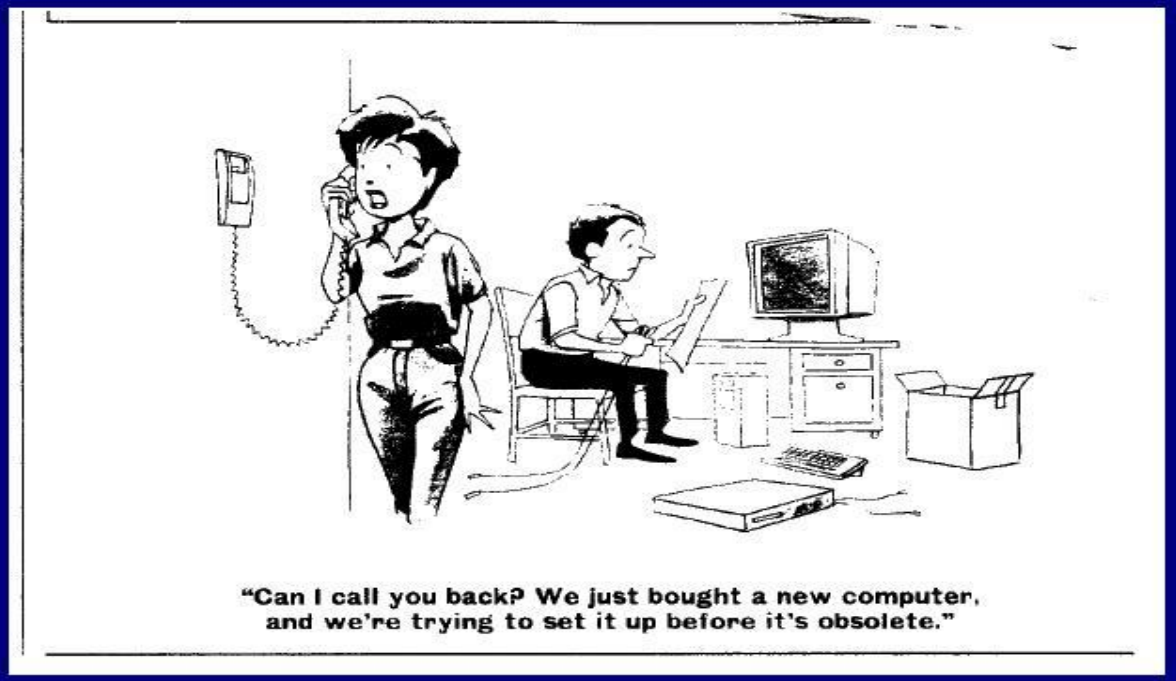
False

- All software has vulnerabilities and flaws that bad guys can take advantage of
  - Including Macs, Linux, Adobe Reader…



- Microsoft products are (currently) the biggest target because they have the most users

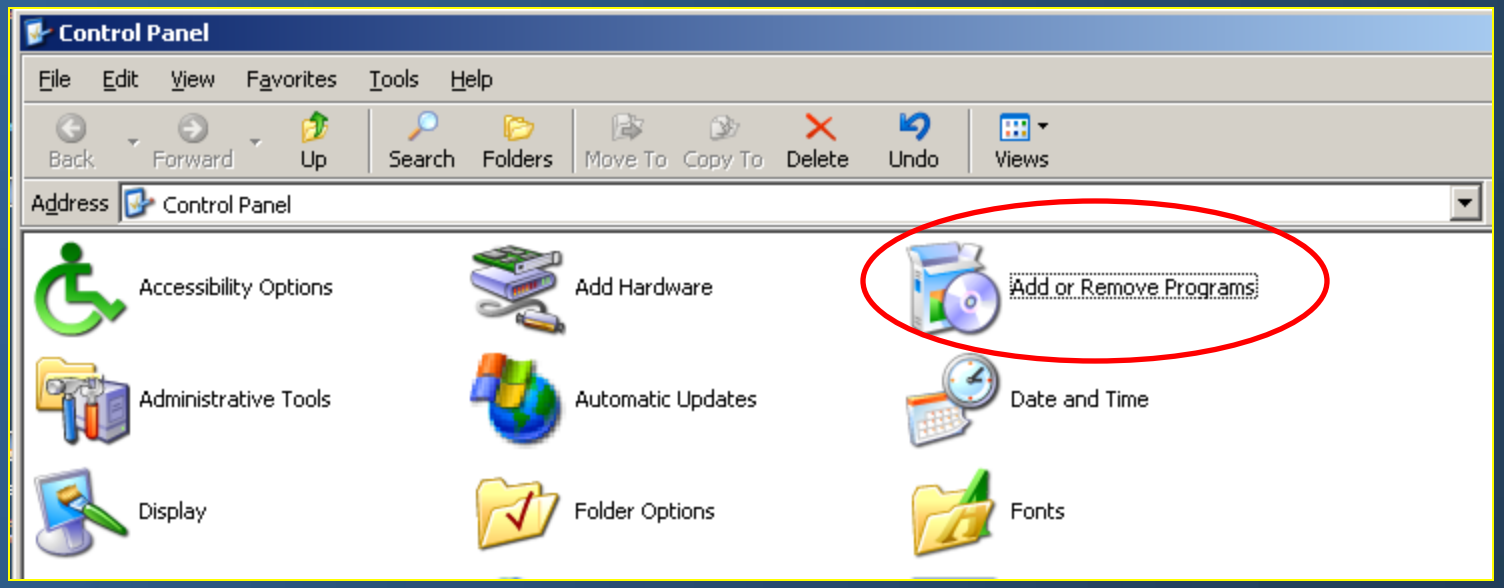
Shiny New PC Protection



"Can I call you back? We just bought a new computer, and we're trying to set it up before it's obsolete."

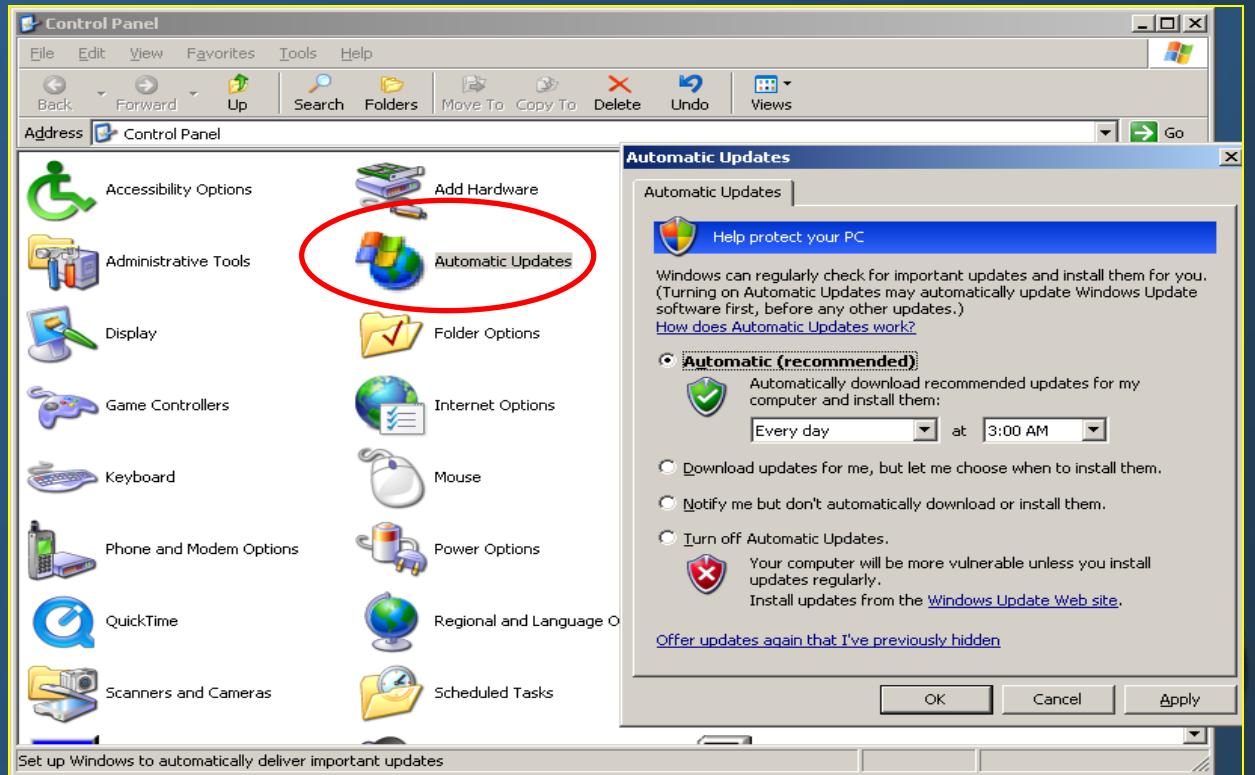
Uninstall Stuff You Don't Need

- PC manufacturers install trial software versions and other unnecessary programs
  - Known as "craplets" or "bloatware"



Install Patches and Set Up Automatic Updates

- While your new PC has been sitting in a box in the store, vendors have issued patches
  - For Microsoft systems, run Windows Update (http://update.microsoft.com)
- Set up automatic updates
- Why? To fix vulnerabilities and prevent worms



True or False

- Having antivirus software installed means my computer is secure

False

- Just having AV installed is not enough
- Update your AV signatures regularly
- Renew your AV software subscription or download free AV
  - Such as AVG Internet Security (http://free.avg.com/us-en/internet-security) or Avast (http://www.avast.com)
- If your AV doesn't detect spyware, add anti-spyware software
  - Such as Lavasoft's Ad-Aware (www.lavasoft.com) or Spybot (http://www.safer-networking.org/en/index.html)

True or False

- I use a firewall, so my PC is protected

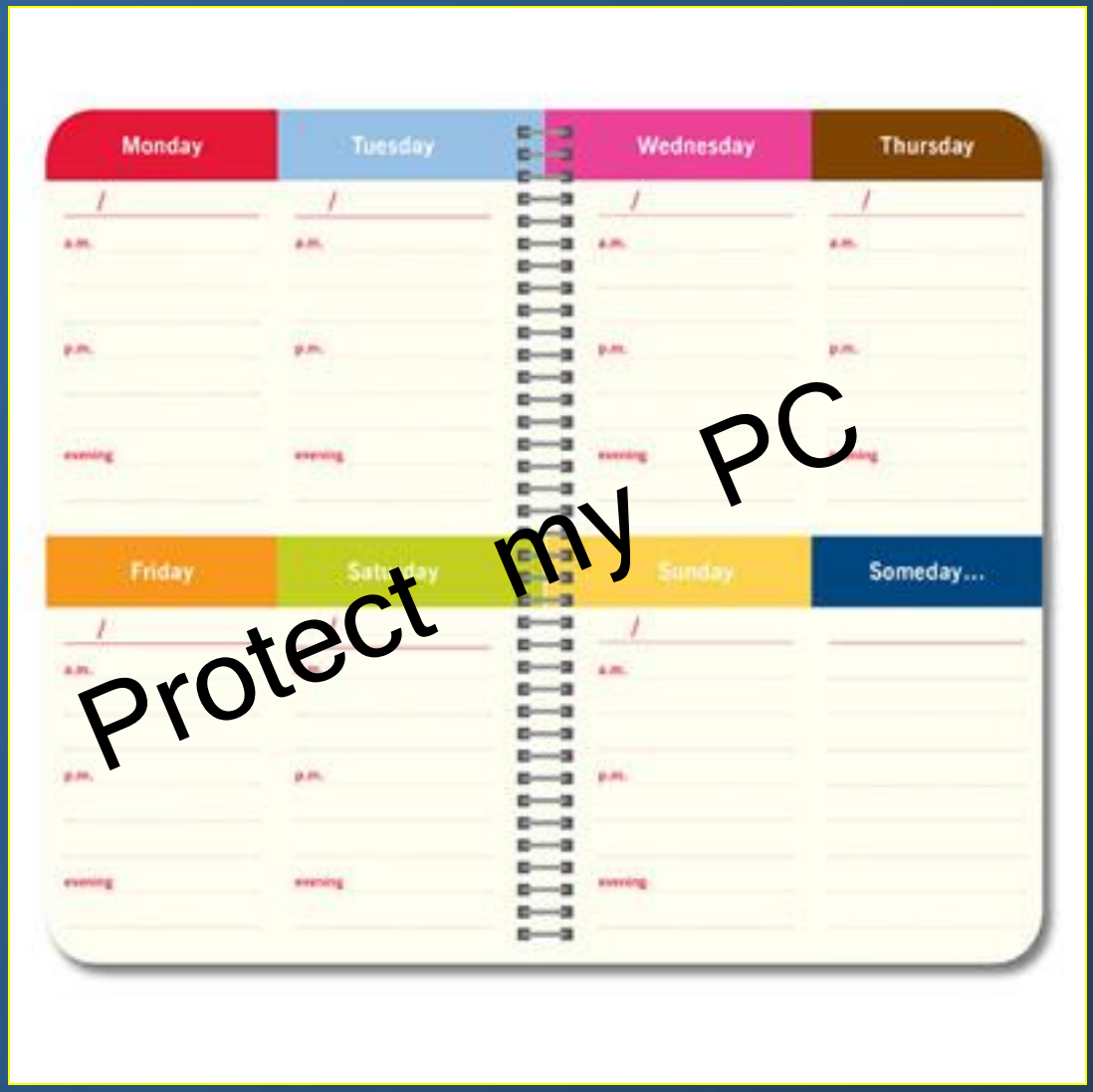
- Firewall: Hardware and/or software designed to prevent unauthorized access to a network

False

- Prevents intrusions and may stop some worms
- Doesn’t stop viruses or Trojan horse programs
- Doesn’t protect you from malicious Web sites or email

- Learn more about firewalls at “Safer Home Networking and Using Wireless Technology”
  - Tuesday, Oct. 26

Tips for Daily Use



Turn Off Your PC

- Turn off the computer when you're not using it
  - Especially if you have an "always on" Internet connection
- Your PC cannot get attacked through the Internet if it's not connected

Don’t Double-Click Everything

- Windows 101: Double-clicking is how you open items in Windows
- It’s not how you open links in your Web browser, click buttons in dialog boxes, or do pretty much anything else
  - If you reflexively double-click, you might accidentally zip past something important or submit a form twice
- If you don’t need this reminder yourself, chances are you know someone who does

Pop Quiz

- 32% American adults would be willing to risk malware by visiting a potentially suspicious website or link

- What tempts them?
  - A friend's link or posting on a social network
  - Entertainment gossip websites
  - Fantasy sports website promising the best statistics
  - Gaming/gambling websites
  - Pornography sites
  - Websites promising a great once-in-a-lifetime deal
  - Websites featuring pictures of a naked celebrity

Pop Quiz

- 32% American adults would be willing to risk malware by visiting a potentially suspicious website or link

- What tempts them?
  - A friend's link or posting on a social network
  - Entertainment gossip website
  - Fantasy sports website promising the best statistics
  - Gaming cheating websites
  - Pornography sites
  - Websites promising a great once-in-a-lifetime deal
  - Websites featuring pictures of a naked celebrity

All of them

Surf “Safe Neighborhoods”

- Visit reputable online stores, news, and entertainment sites
- Porn, gambling, hacker, and “free” sites are more likely to be malicious
  - Adding the word “free” to searches increases the risk of landing on a malicious site
- When doing an internet search, don’t blindly click on search results
  - Bad guys take advantage of current events and celebrity news to create malicious sites

Is Your PC Infected?

- Symptoms: slower processing times, unwanted pop-ups, increased spam, unusual disk activity
- Don’t panic – You should already have anti-malware protection
- If not, here are some free tools
  - Trend Micro’s online malware scanner, HouseCall
  - Microsoft’s Malicious Software Removal Tool
  - PC World’s Additional Security Resources

Be Mindful – Uncheck Boxes

- Lots of apps give you the option of installing search toolbars and add-ons
- Lots of sites offer you free newsletters and email updates
- Just say no – check/uncheck those boxes
  - Don’t know what info the app sends back to its owner
  - Add-ons come with your app because they make money for their owners

No !

Back Up Your Information

- Make regular back-up copies of your info
  - Create backups manually
  - Use an internet service that creates backups and stores them online

- Store your backup copies online or on external hard disk drive, CDs, USB sticks…

Disposing of Obsolete PCs

Information Technology Services
"Connecting Phoenix to Information"

Wipe Your Hard Drive…

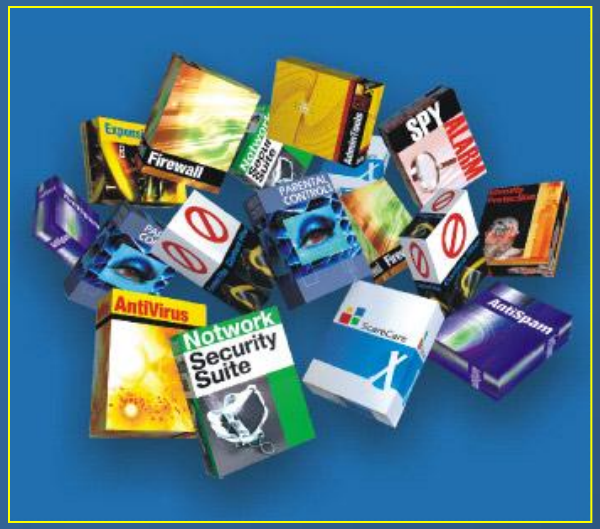
- Deleting files doesn't actually get rid of them
- If you reformat your hard drive, somebody could still use an "undelete" app to recover your data

- Use a special application to wipe your hard drives (and CDs and USB sticks and PDAs…)

- For more info, see http://www.pcworld.com/article/157126/how_to_completely_erase_a_hard_drive.html

Or Destroy Your Hard Drive(s)

Summary



- Think security when setting your new PC
  - Use antivirus and antispyware software and keep it up to date
  - Regularly install security patches
- Practice “safe surfing”
  - Use care when reading email and downloading
- Back up your data, and wipe/destroy old media

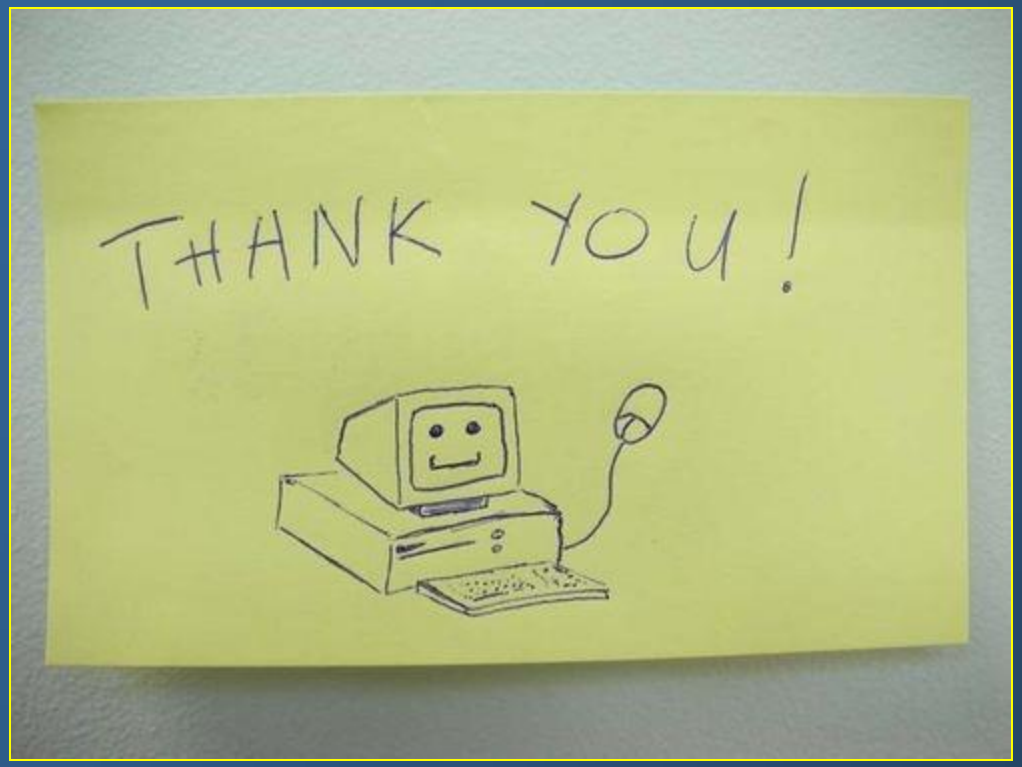
True or False

- Following the recommended protection strategies will 100% protect my PC

Following the recommended protection strategies will 100% protect my PC

False!

There are always new vulnerabilities being discovered and new attacks coming out



Questions? Contact
ispo@phoenix.gov

Information Technology Services
"Connecting Phoenix to Information"