

Security Awareness - E-mail & Web Security

Last Updated: 04/25/2013

Overview

Sending and receiving e-mail, file sharing and browsing websites may seem innocuous on the surface, but if you're not careful these activities can open your computer to countless vulnerabilities. E-mail messages can easily be forged and they're often used to launch malware. Malicious web sites can install software on your computer or collect personal information from your computer.

E-mail and Web Security

Here are a few basic things to keep in mind:

- Don't give out confidential information in response to any e-mail. Messages that try to persuade you to send your password or credit card number are forged, even if they appear to be from the your bank or system administrator.
- Be wary of any e-mail attachment that you weren't expecting (this also applies to Web downloads). It's very easy for a computer virus to be present in an e-mail that appears to be from a friend. It is strongly suggested that anti-virus software be used to scan anything that you receive in your e-mail.
- If you receive e-mail from from and CABQ location which you feel violates the City's Acceptable Use policy, it should be reported to the ITSD Service Desk at Helpdesk@cabq.gov or call 768-2930 so action can be taken. It is suggested you do not delete the message, as it can often be useful in tracking down the incident.

Use Secure Clients

Access to CABQ systems requires the use of secure clients and encrypted authentication. These best practices help protect our network from malicious computer attacks and stolen logins, passwords, etc.

Desktop Management including antivirus and patches

Every desktop computer must have current and up-to-date anti-virus software and security patches. Contact the ITSD Service Desk for assistance in obtaining these updates

The operating system on every desktop must be kept up-to-date. ITSD has documentation on configuring your Windows system for automatic updates. ITSD also has documentation for running Windows Updates manually.

File Sharing - a setting on your computer that lets hackers into your computer unless they are disabled or fixed

- City policy is to block peer-to-peer applications as these applications by default, when loaded, share files. Because there are business needs for some peer-to-peer (p2p) file-sharing and social media applications such as Drop Box, Facebook, CABQ does not ban them all from its network. However, we recognize that most p2p activity consists of copying music and video files for personal enjoyment. Music and videos are copyrighted.
- File-sharing may put your personal computer data at risk. Because there are file-sharing application being developed continuous, ITSD suggests that you not run p2p types of programs. If you feel you must do so, at minimum, disable the uploading features. Doing this should NOT affect your ability to copy files to your computer from other locations. It will prevent others from copying files from your computer.

Issues when using public computers

- Always remember to log off when you finish with secure web sites. If you do not, the next person to use the computer will have access to your personal information.
- Public computers that may not always be securely configured pose a threat to your privacy by storing your password or web cookies. Think twice about going to a secure site if you can not verify the security of the computer.

Here are some helpful tips for hardening computers:

- Patch Microsoft Windows automatically.
- Use strong passwords or pass phrases for all Windows user accounts on your PC. See [CABQ Password Standard](#)
- Use and properly maintain good anti-virus software, and optionally anti-spyware software.
- Use a firewall, such as Windows XP's built-in software firewall.
- Do not open suspicious email attachments or respond to suspicious requests.
- If you're not using it, disable the Windows File and Printer Sharing service.
- Disable any unneeded user accounts.
- Lock your PC's screen when you step away, and shut down your computer when you'll be gone for more than 6 hours.
- Where possible, consider using a web browser other than Internet Explorer, and treat "free" software with suspicion.

For Additional information and best practices of email and internet usage see [Internet and email safety](#).