Computer Virus (Malware) Desk Reference Card

What to do if you see a Fake Browser or Fake Antivirus pop-up window

- **Completely power off your computer**
- **Disconnect any network cables from your computer**
- **Call the GETS Consolidated Service Desk at 877-GTA-3233 to report you suspect a virus**

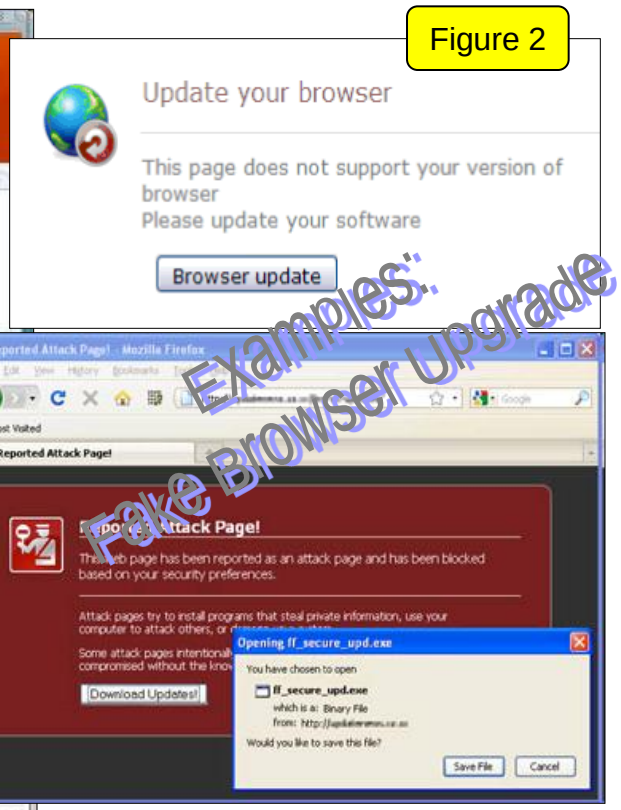
If you're not sure what you see is legitimate, it's best to ask.

Georgia Enterprise Technology Services

Common forms of computer viruses appear as Fake Antivirus (Figure 1) and Fake Browser Upgrade (Figure 2) pop-up windows. They pop up on your computer desktop and prompt you to take action. These windows look legitimate but are not.

Figure 1

Figure 2



Tips to Avoid Computer Viruses

Think Security First: When in doubt, ask. Your job may give you access to sensitive data. You are the first line of defense.

Work E-mail: E-mail attachments requesting installation from unknown sources should not be installed. Links within your e-mail from unknown parties should always be deleted.

Personal E-mail, Social Media Web Sites, Etc: Personal Web browsing should be done at home on a computer you own. Opening these sites at work on a GETS computer introduces another way for computer viruses to be present.

Web Browsing: When visiting a Web site that asks you to install software or download anything, ask yourself "*Do I need this in order to perform my daily work routine?*" or "*Did I actually request this action?*" If the answer is no, do not install or download. If the answer is yes, note where the download is coming from. If it does not look familiar, do not proceed with the installation. If necessary, press ALT+F4 multiple times in order to close the application. Please reboot your computer as soon as possible.

Installation Prompts: If you are prompted to install a piece of software unexpectedly, first ask yourself "Did I request this?" or "Does this look familiar?" If no, press ALT+F4 instead of clicking "No." You may have to do this multiple times. Please reboot your computer as soon as possible.

Links: Links (URLs) you consider suspicious in documents or on a Web site can be verified easily. Place your cursor over the link to reveal the true address you will be taken to. It will display either in the status bar at the screen bottom (left or right side) or through a pop-up window. Examples: