Fairfax County
PUBLIC SCHOOLS
ENGAGE • INSPIRE • THRIVE

Tip Sheet

Malware and Data Theft Tip Sheet

#FCPSDigCit

Malicious code can be spread through just about any computer medium, including email, infected files, instant messages, file-sharing services, or pop-up ads.

Turn on your computer’s firewall, keep the operating system up to date, and use up-to-date antivirus and antispyware software.

1. **Install antivirus software, and update it regularly.** Set antivirus software to auto-start when the computer is on and auto-update from the manufacturer’s web site. If virus protection is out of date, it cannot detect the newest viruses, worms, and Trojan horses being created daily.

2. **Do not open e-mails, attachments** from persons or businesses you do not know.

3. **Always scan incoming e-mail attachments** before opening them. Save attachments to your desktop, then scan with your virus protection software before opening.

4. **Be extra careful when downloading** freeware, screensavers, games, and other **executable programs** (files with extensions like .exe, .pif, or .scr). Save files to your hard drive, and virus scan before opening.

5. **Keep your operating systems patched.** Operating system vulnerabilities are discovered almost daily. Windows updates should be set to update at least weekly to make sure your computer is protected.

6. **Never click “Yes”** when prompted to install or run content from a web page that you are not sure you can trust. If given the option, save to your hard drive and virus scan before opening.

7. **Install antispyware tools** in addition to your virus-protection software. Spyware is designed to hide on your computer and monitor and report your personal information and Internet activity to the remote attacker.

8. **Always read the user agreements, privacy statements, or other disclaimers** before downloading or installing programs. Programs that you install can contain spyware. By accepting the user agreement, you are giving permission to download spyware to your computer.

9. **Use a firewall** to further protect your computer from intrusions.

Recognizing phishing attempts:

1. **Watch for bad spelling and grammar. S**cammers often makes spelling and grammar mistakes that would otherwise be caught by a legitimate company's proofreaders.

2. **Be aware of generic greetings.** Most companies will address you by your name when corresponding with you. Generic greetings, such as "Dear Valued Customer," should raise a red flag.

3. **Be wary of** messages containing **urgent requests for personal information.**

4. **Look out for account suspension or cancellation warnings.** Scammers often use these scare tactics to trick their victims into disclosing personal or financial information.

Respond appropriately to e-mail threats:

1. **Avoid giving your personal e-mail address** to anyone other than family, friends, or business associates.

2. Create and **use a separate e-mail address for public use or to set up accounts.**

3. Before registering on a web site, **read the site's privacy policy** to ensure that your e-mail address will not be shared or sold to a third party and that you retain intellectual property rights to what you create.

4. **Do not display your e-mail address openly** online, such as on public forums or in profiles.

5. Use technology to **block spam.**

6. **Never respond to spam.** Ignore "Unsubscribe" links in spam e-mails. By clicking this link, you are essentially validating that your e-mail address is active and being read.

7. **Never directly respond to messages or e-mails asking for personal or financial information.** Contact the organization via telephone, or go to the organization’s Web site to verify your updated information. Legitimate companies never ask for customer information by way of pop ups or e-mails.

8. **Never click on links within e-mails.** Open a new browser window, and directly type in the organization’s web site address. Never copy and paste the link. Phishers create links that look like legitimate web site URLs and then redirect their victims to phony web sites.

9. **Never use e-mail to provide personal or financial information** to an organization. E-mail is not a secure method of transmitting personal data. Instead go to the organization’s web site and look for the lock icon, or the “https” in the URL address bar, to ensure it is a secure web site.

10. **Act immediately if you believe you have been hooked by a phisher!** Notify your account providers immediately. Don’t forget to contact the credit bureaus and request a fraud alert on your credit files.

Works Cited

Collier, A. and Magid, L. (2012). *A Parents’ Guide to Facebook.* <http://www.connectsafely.org/pdfs/fbparents.pdf>.

"Guidelines on the Use of Social Media and Related Electronic Communication Tools." *Guidelines on the Use of Social Media and Related Electronic Communication Tools*. FCPS, 31 July 2015. Web. 17 Mar. 2016. <http://fcpsnet.fcps.edu/cco/web/socialmedia/>.

"Best Practices for Students Using Social Media to Communicate with FCPS." *Best Practices for Students Using Social Media to Communicate with FCPS*. FCPS, 23 Nov. 2015. Web. 17 Mar. 2016. <https://www.fcps.edu/node/32059>.