WELLESLEY FREE LIBRARY

Keeping Your Computer Safe

Companies are taking many steps to protect your online information but individuals can take steps to ensure the safety and security of information and systems as well. You can take steps, using common sense to identify Phishing and email frauds, running maintenance programs to keep your computer up to date and running fast, and using antivirus programs to prevent, detect and respond to attacks.

What are the types of cyber threats that you face?

- A hacker or intruder can break into your computer
- Malware such as a virus, worm, trojan or spyware can become installed on your computer
- You can become the victim of a phishing scam
- Your accounts can be hacked into, most often, your email account
- Files can be corrupted.

What are the risks to you or your computer if your protections are breached?

- Not much. Many security breaches are fairly harmless
- Your email can become a spamming tool for professional spammers, sending out messages on behalf of someone else
- Files on your hard drive can be altered or corrupted up to and including system files
- Your computer can become a zombie or botnet, and become involved in denial of service attacks (an attacker may be able to prevent you from accessing email, websites, online accounts (banking, etc.), or other services).
- Credit card numbers or account numbers can be stolen, leading to credit card fraud.

What can you do to protect yourself?

- Use Common Sense especially when using Email or Downloading Files or Attachments.
- Do not let yourself be led astray: emails often include fraudulent hyperlinks, beware of unfamiliar websites.
- Do not respond to unsolicited (spam) e-mail.
- Do not click on links contained within an unsolicited e-mail.
- Be cautious of e-mail claiming to contain pictures in attached files; the files may contain viruses. Only open attachments from known senders.
- Avoid filling out forms contained in e-mail messages that ask for personal information.
- Always compare the link in the e-mail to the link you are actually directed to and determine if they match and will lead you to a legitimate site.
- Log on directly to the official website for the business identified in the e-mail instead of “linking” to it from an unsolicited e-mail. If the e-mail appears to be from your bank, credit card issuer, or other company you deal with frequently, your statements or official correspondence from the business will provide the proper contact information.

- If you are requested to act quickly or there is an emergency that requires your attention, it may be a scam. Fraudsters create a sense of urgency to get you to act quickly.
- Avoid becoming a victim of phishing scams: if you receive email requests to verify account numbers, ignore them.
- Create strong passwords: the best passwords use a combination of alpha-numeric characters, avoid real words, and don't follow any sensible pattern.

What can you do to protect your computer?

- Back-up your information including programs and system files. Use a cloud tool such as Dropbox or OneDrive to store files, and use restore tools like Windows Backup and Restore Center.
- Use anti-virus and anti-spyware programs: Windows Defender, Norton, There are many different antivirus and antispyware programs on the market. If you are downloading a new one, use a reputable reviewing source, such as consumerreports.com or consumersearch.com to choose a program. Either download directly from the company's site (and double check the URL!) or download from a source like CNET.com
- Keep your operating system up-to-date: OS makers are constantly testing the vulnerabilities in their systems, and designing patches to fix problems. Install updates to your OS to try to close the gaps
- Double check to make sure your firewalls are on: factory settings will have firewalls turned on, but it can be useful to know where they are on your computer
- Run scans on your computer periodically to make sure that you aren't infected: There are a number of tools on the market, such as the Malicious Software Removal Tool from Microsoft, ccleaner, and malwarebytes to help you clean your computer.

Unfortunately, there's no 100% guarantee that even with the best precautions some of these things won't happen to you, but there are steps you can take to minimize the chances.

Useful sites with additional information

lifehacker.com - LifeHacker is a great site with tips on many different issues, checking in every now and then can point you to great information about security issues and topics.
www.us-cert.gov/ncas/tips/ - United States Computer Readiness Program: Computer security is becoming so important that the Department of Homeland Security is getting involved.
StaySafeOnline.org - The National Cyber Security Alliance: More consumer focused than the site above, this can be a great place to get tips and general information.
Microsoft.com/security or **Apple.com/security -** Reading security tips from the maker of your OS is a great way to keep up with security updates for your device.
fbi.gov/about-us/investigate/cyber - This page is most useful in terms of giving examples of cyber crimes, including phishing scams. If you would like to report an phishing scheme, come here.
topics.nytimes.com/top/reference/timestopics/subjects/c/computer_security/index.html - Stories about cyber security, both for individuals and businesses.
News.cnet.com/security - A good stream of stories about online security and privacy. Great site to check every so often for new information.