Home Computer Safety Basics

Bill Metzker

RAP Safety and Security Committee

Spring 2018

Disclaimer

I don’t consider myself an expert!

What we will discuss today:

- Steps you can take to proactively secure your laptop or desktop device
- Things you can do to protect personal data and confidential information

Introduction

Three recurring themes kept showing up while researching this presentation:

- Be proactive about securing your computer
- Take control over your interactions with the Internet
- Be selective about what information you share in emails or on social media

Only you can prevent computer hacking

Let's keep you from becoming this guy!

Be Proactive

Keep operating system updated!

- Most computer systems can be configured to automatically download updates.
  - Please don't turn this feature off; updates are your friend!
- Download doesn't necessarily mean **install**.

  MircoSoft and Apple let you to control when updates can be installed
- Chrome OS is different: it downloads and installs it updates automatically

What makes updates important?

- New features
- Corrections to old features
- **Addresses vulnerabilities identified between releases.**

Security features only work if they are enabled

Anti-Virus/Anti-Malware Software

Windows and Apple/MAC come equipped with anti-virus tools.

- Tech journals suggest these tools are adequate for most home users, but:
  - It assumes you only access established websites
  - You're careful about what you download and
  - You don't venture into potentially hazardous areas of the web

What about anti-virus tools?

- A number of products are available, including many with free home versions
  - Many offer extensions not available through the OS; tools such as online backup services, flagging questionable websites, browser safe-surfing services and password vaults
  - Most vendors provide products that an run on Microsoft or Apple platforms

Anti-malware tools?

- Tech journals recommend downloading and installing anti-malware packages
  - Malware refers to all forms of malicious code
  - Most vendors offer free versions for home users

Chrome OS is different: Google built anti-virus/anti-malware protection into their operating system. They also maintain strict controls over what can run in their environment.

Control access to your computer

- Create user accounts
- Use strong passwords
  - Minimum 8 characters long
  - Contain upper and lower case letters, numbers, and special characters
  - Hints:
    - Create passwords you can remember without writing them down
    - Us a pattern
    - Use very long string of related characters
  - Never use any personal information, dictionary words, or something easily guessed
  - Never share your passwords
- Other recommendations:
  - Create different passwords when possible.
  - Change passwords periodically
  - OS and Anti-virus vendors offer password manager/vault services that store your login credentials

Backup your system regularly

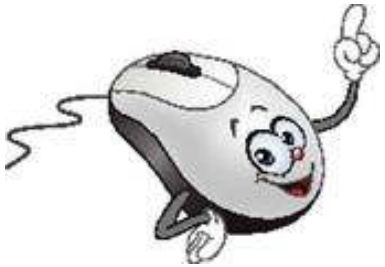
- Routine backups can protect you from the unexpected.
- Cloud vs. local backups
  - Computer manufacturers and anti-virus software vendors may include on-line backup services as part of their installation packages, where your backup is stored on a remote device (a.k.a In the cloud)
  - Backups can be configured to a local device such as large USB flash drive or connected mass storage device
- There is no real difference; both can be used to recover your computer files in the event of a machine failure.

I recommended seeking professional help if you find yourself needing to run an restore.

Taking Control of your Computer

So what are we talking about here?

- Controlling access to your computer
- Using the Internet
- Email and Social Media
- Avoid Phishing scams



Control Access to your Computer

- Be careful when leaving your computer unattended
- Be careful sharing password
  - Never share your password with people you don't know
  - Maintain separate user accounts for your grandkids
- Never grant remote access to anyone you don't know
- Apply parental controls to grandkid accounts
- Be careful when using public networks

Using the Internet safely

Let's review

- The importance of keeping software updated
- The Operating system tools that can mitigate some of the risk
- The importance of user accounts and strong passwords – so what's next?

Things to look for when accessing the internet

- Connect to private networks whenever possible
- Be careful when using public networks
- Look for websites that begin **HTTPS** particularly when access banking or shopping sites
  - This indicates that the website is secure and uses encryption to scramble your data so it can't be intercepted by others.
- See if your online accounts offer **multi-factor authentication**
  - Where the website you are using sends you message or email containing an additional code to enter
- Limit visits to websites you don't know
- Click smartly, we will talk about this next

Email and Social Media

Email:

- Don’t be afraid to hit SPAM (or JUNK)
- Scammers like to hide malware in email attachments, therefore:
  - Be careful where you click
  - Be leery before downloading email attachments
- Limit sharing of personal data

Social Media

- **Be careful about what you write**
  - Don’t share that you will be away from home
  - Don’t write anything you don’t want anyone else to see

Beware of Phishing

What is it?

- Scams designed to trick you into divulging personal information such as your login ID and password, banking or credit card information.
- Phishing scams can be carried out by phone, text, or through social networking sites - but most commonly by email.
- Be suspicious of any official-looking email message or phone call that asks for personal or financial information.

What to do?

- Never divulge personal information
- Assume nothing! Messages from banks, businesses and government agencies can be check d - contact those then directly – do not call the phone number listed in the email, text or phone message.
- Hang up when someone identifies themselves as calling from Windows, Account or email support

Questions

References

- http://www.foxnews.com/opinion/2011/10/29/10-tips-for-safe-computing.html
- https://www.apple.com/macos/security/
- https://security.berkeley.edu/resources/best-practices-how-to-articles/top-10-secure-computing-tips
- https://securingtomorrow.mcafee.com/consumer/consumer-threat-notices/10-tips-stay-safe-online/