Internet Security

Internet security is a very complex issue. Today, I am going to go over the high level concepts and review the types of threats you will experience on the Internet and steps you can take to minimize your risk.

There are many types of attacks you may face when using the Internet:

- **Malware** - programs added to your computer usually through email attachments
- **Phishing** - links in bogus email messages that take you to websites that try to get your information or load malware on your computer
- **Network** (aka. “Man in the Middle”) - stealing your network traffic when you use an unsecure public WIFI to connect to the Internet
- **Password** - people guessing your passwords on websites

We will talk about each of these types of Internet Security Issues

Enjoying the Internet is a bit like moving from a remote island to a big city. On the island, you don’t need to worry as much about security but the advantages of the city also mean you have to be more careful and take actions to prevent problems.

If your computer is not connected to the Internet, the problems we are talking about today will likely never happen but you cannot use email, the World Wide Web or many other wonderful features of the Internet. Some simple measures can help prevent most security problems.

Malware

Malware (**MAL**icious soft**WARE**) is a program that is installed on your computer, often without you knowing about it. A common source of malware is opening email attachments in bogus emails. Never open an attachment in an email unless you are sure who sent it to you. This will be described in more detail below in the phishing section.

Malware programs can do a lot of harmful things, such as:

- Delete files on your computer
- Take over your computer and hold it for ransom ("**ransomware**")
- Steal your data
- Steal your keystrokes (often used to steal your passwords)
- Track what you do and where you go on the Internet ("**spyware**")
- Popup ads on your computer ("**adware**")
- Infect other computers on your local network
- Use your computer as a robot ("**botware**") to attack other computers or send phishing emails.

Malware can happen on any device. Most smartphones, tablets and computers have detailed security and privacy settings that let you control which apps can get access to your files, camera, microphone, etc. When you install an app you are often asked for permission for the app to access protected items on your phone or computer. Read these carefully and don't automatically press OK. You should also review your security settings periodically to make sure apps can only access what they need.

Some devices (e.g. iPhone and iPad) do not let you install apps except through an App Store which makes sure the apps do not contain malware. They do a very good job, but this is not perfect on any of the app stores.

On other devices, like Android phones, you can install apps (software) though the Google Store or download apps directly from web sites. The Google Store, just like the Apple App Store should protect you from adding malware to your device. The Mac computer also lets you use an App Store or download directly and most PC software is installed directly from Internet websites.

App stores are normally a safest way to install software. If you download and install software (aka “apps”, “applications”, “programs”) directly from websites, make sure the website is legitimate, e.g. microsoft.com which is Microsoft website. If you are not sure, don’t download the app.

There is software available for computers and some portable devices which can scan for malware. These are called “**antivirus**” or “**security**” software.

This type of software regularly scans your device for malware and can quarantine or isolate any problems that it finds. It can also automatically check any software you download and try to install on your device. Some of these systems also protect you from malicious websites.

The PC comes with anti-virus software called “Windows Defender”. You can also install software from many different vendors to help protect your computer.

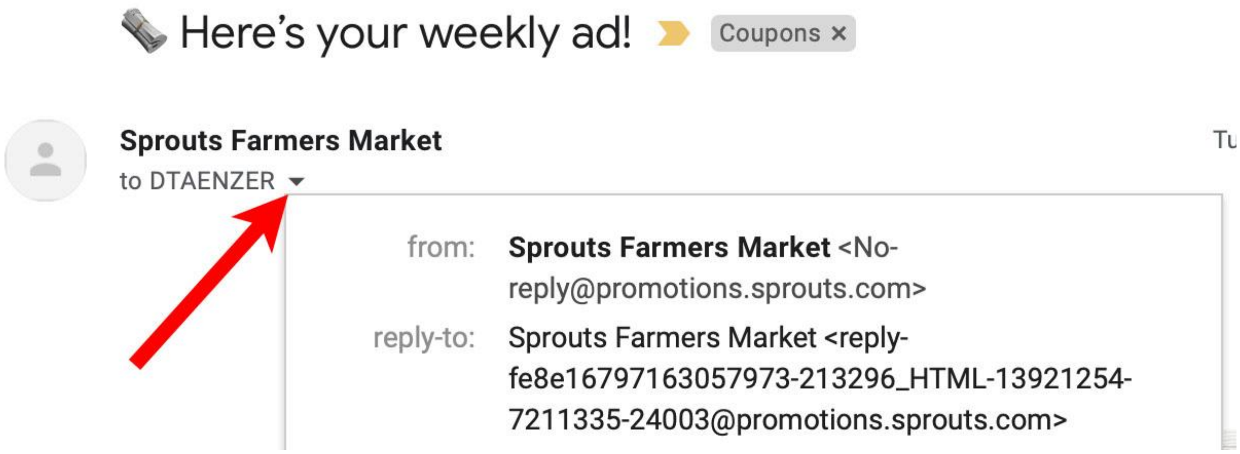
Mac computers have less malware problems but they are not unknown. Traditionally most malware targeted Windows PC computers because there were many more of them. There are a variety of security systems you can use to help protect your computer.

Phishing

Phishing is the term commonly used for malicious emails that either try to get you to download attachments that contain malware or give you links to websites that try to steal information like passwords.

These often look legitimate, but before you download an attachment or follow a link, take a close look at who sent you the email. The way this works varies from one email program to another, but try to see the email address of the sender.

If you use Gmail on a browser, there is an arrow that you can click to see this information:



Here's your weekly ad!

Sprouts Farmers Market
to DTAENZER

from: **Sprouts Farmers Market** <No-reply@promotions.sprouts.com>
reply-to: Sprouts Farmers Market <reply-fe8e16797163057973-213296_HTML-13921254-7211335-24003@promotions.sprouts.com>

On portable devices, you can tap on the From field in the email message to see this information in a popup window.

Make sure the email address of the sender matches their organization (e.g. sprouts.com) in this case. If you get an email that says it's from Verizon but the email came from a yahoo.com email address, it is a phishing email and you should be very, very careful with it.

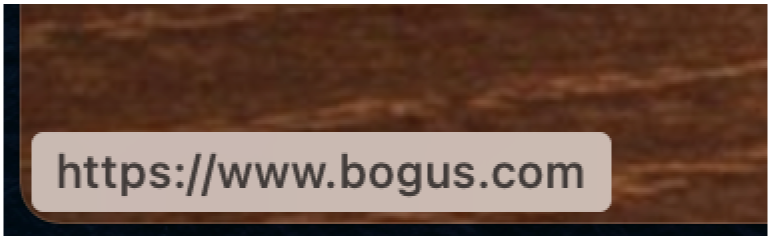
A common trick is for a phishing email to send you to a website that looks very similar to what you expect but the web address at the top of the browser does not match the company or organization that you expected.

Emails may contain links that look the web addresses, e.g.

https://www.seniorplanet.org

But actually link to a completely different address. The text for this link is “https://www.seniorplanet.org” but it goes to “**https://www.bogus.com**".

On a computer based browser, when you move the cursor over a link, the web address the link will take you to is displayed in a status bar at the bottom left corner of the browser window:



https://www.bogus.com

You may need to enable the display of the status bar either through a menu or setting depending on the browser you are using.

On iPhones and iPads, you can view a link in the browser by pressing and holding down on a link. A preview pane appears with the URL at the top. Make sure the link goes to where you expect it to take you before clicking on it. After you click on a link, check the browser address bar to make sure you are where you think you are on the web.

It is not difficult for a bogus website to look like a legitimate one but the web address cannot be faked so always check the address at the top of the browser window.

Network Attacks

Your home network should use a strong password for your WIFI router. This is the simplest way to protect yourself. It may be convenient to have a simple password you can give to guests to let them use your network but this puts your network and all the computers attached to it in danger. Always use a long, complex password with combinations of upper and lowercase letters and numbers.

You can also enable or add “**firewall**” software to your computer that can prevent someone from certain types of access if they do compromise your network. This software often comes included with antivirus security software.

The Mac operating system offers a built-in firewall and one is also included in Windows Defender for PCs running Windows 10.

When you are using a portable device like a phone or laptop, beware of using public WIFI networks, particularly ones that do not need a password to sign into them. A common network attack, called “**Man in the Middle**” is a router that looks OK but is actually connecting you to a computer that can steal your data as you use the Internet.

One option if you want to use a tablet (e.g. iPad) while on the go, is to set up a WIFI hotspot on your phone and connect the tablet to that network. This turns your cell phone into a portable WIFI network which is a safer way for you to access the Internet. Keep in mind that this uses data on your cell phone, so only use this option if you have a cell phone data plan with enough data to use your phone as a WIFI hotspot. You should also make sure you choose a complex password for your phone hotspot.

There is a type of software called a Virtual Private Network (“**VPN**”) that can be used to increase your security and privacy when using networks, particularly outside your home.

A VPN encrypts (scrambles) your network traffic and also hides the IP address of your computer (which can be used to roughly indicate your location).

This software is not normally necessary for most users since most websites these days whose addresses start with “**https://**” already cause your network data to be encrypted. Some browsers also offer “**private”** windows which hide some of your identity.

If you frequently use public networks, a VPN may be helpful but be very careful about choosing a good vendor. There are many “free” VPN services that may be selling your information.

Most companies that collect information about you (e.g. Facebook and Google) are doing this to provide targeted ads on the websites you visit. They do not directly sell your information but use it to target advertising based on the information they know about you.

The information they collect is concerning, particularly after the Facebook Cambridge Analytica scandal a few years ago. Facebook had set up a way for researchers to get its information on some people and the Cambridge Analytica company used this to steal user information and to spread conspiracy theories.

Password Attacks

I have done several Lunch and Learn talks on passwords. There are a few simple rules to keep in mind:

1. Never use simple passwords. Always use a long sequence of upper and lower case characters, numbers and special characters. Longer passwords are much safer than shorter ones.
2. Never use the same password on multiple sites
3. Let your browser create complex passwords for you and save them so you don’t need to type them in on websites. This is much easier and safer than writing down passwords on paper. If you use multiple browsers on various devices, you can use a password manager to create and save passwords for you.
4. Make sure the password you use to access your email is long and complex. The reason is that if someone can access your email account, they can change all of your passwords by requesting this on websites which will send you an email which they can access.
5. Make sure your passwords to access Internet storage (“**cloud accounts**”) are long and complex. Examples are Apple iCloud, Google Drive, Dropbox, etc. These companies keep your data encrypted on the “cloud” but if someone can guess your password they can get access to this data.
6. Make sure your passwords to access financial websites and to log into your browser are long and complex.
7. Use **two factor authentication** on sensitive websites (e.g. financial and email). The website will send you a code on your phone that you must enter to log into the site.

You normally don’t need to change your passwords if you follow these steps. If you hear about a data breach at a company where you have a password, you should definitely change that password immediately.

Conclusion

I hope these suggestions will help you stay safe when using the Internet. If you follow these basic steps you should not have to worry about using your email or web browser. Use common sense and if something does not feel right, trust your instincts.

Just like with bogus phone calls, if you get an email or message that seems unusual or suspicious, do not download any files or follow any links. Simple contact the company directly to make sure the message is legitimate.

References

Is Public WIFI Safe Video
https://www.youtube.com/watch?v=bdVkkRmJEeM

CISA (Cybersecurity and Infrastructure Security Agency)
https://us-cert.cisa.gov/ncas/tips/ST15-002
https://us-cert.cisa.gov/ncas/tips/ST04-014

Network Security Threats
https://securitytrails.com/blog/top-10-common-network-security-threats-explained

Mac Firewall
https://www.macworld.com/article/2940180/fire-up-your-macs-firewall.html

When Do You Need a VPN
https://defendingdigital.com/when-do-you-need-a-vpn-virtual-private-network/

My Lunch and Learn Videos and Documents
http://davetaenzer.com/docs/

Antivirus Software Reviews

CNET: https://www.cnet.com/how-to/best-antivirus/
PC Magazine: https://www.pcmag.com/picks/the-best-antivirus-protection
Macworld:
https://www.macworld.com/article/3263722/best-antivirus-for-mac.html
Consumer Reports:
https://www.consumerreports.org/cro/antivirus-software.htm

How to Recognise a Phishing Email
https://www.mcafee.com/blogs/consumer/phishing-email-examples-how-to-recognize-a-phishing-email/

Privacy Settings

How to Manage App Permissions on your iPhone or iPad
https://www.howtogeek.com/211623/how-to-manage-app-permissions-on-your-iphone-or-ipad/

Change App Permissions on your Android Phone
https://support.google.com/android/answer/9431959?hl=en

Change Privacy Settings on Mac
https://support.apple.com/guide/mac-help/change-privacy-preferences-on-mac-mh32356/mac

How to Change Privacy Settings in Windows 10
https://windowsradar.com/change-privacy-settings-in-windows-10/