
Welcome to the Mac SIG Meeting
November 28, 2017

Types of security attacks and what to do about them

TERMS USED IN THIS TALK

★ COMPUTER in this presentation refers to an Apple laptop or an Apple desktop.

★ OPERATING SYSTEM or “OS” is the main software allowing an iPhone/iPad or computer to run:
for an laptop/desktop it is designated OS X 10.xx.xx.x or macOS *name* *Version* xx.xx.x
for an iPhone/iPad it is designated by iOS xx.x.x

★ iOS DEVICE therefore means an iPhone, iPad (or iPod)

★ BROWSER is the program that allows you to surf the internet

★ SAND BOXING is a way to keep the main OS safe while using apps. iOS devices use this method to protect their operating systems.

★ SSD stands for Solid State Drive. An SSD device uses only micro chips and no hard disk at all.

TYPES OF SECURITY ATTACKS

Computer Based:

- SOCIAL ENGINEERING
- PHISHING
- SOCIAL PHISHING
- MALWARE/VIRUSES
- RANSOM WARE
- ID THEFT
- PASSWORDS

Network Based:

- Eavesdropping
- Data Modification
- Identity Spoofing (IP Address Spoofing)
- Denial-of-Service Attacks
- Man-in-the Middle Attacks
- Compromised-Key Attacks
- Sniffer Attacks

SPECIFIC ATTACKS

➤SOCIAL ENGINEERING

Using psychology to trick people into giving their personal information to the attacker. Oftentimes, the attacker will pretend to be somebody else such as a friend or an official of some company thus trying to convince the victim that they are legitimate.

What can be done?

- Be self vigilant and be wary of anything that looks strange.

SPECIFIC ATTACKS

➤PHISHING

“Fishing” for information. This type of attack uses social engineering to gain the wished for information. A common situation is to send out an email that looks like it’s coming from your bank. It asks for you to click on a link to confirm account information, address, email, account numbers etc. Sometimes there is an included threat saying that the accounts will be closed unless the information is received.

What can be done?

- Be familiar with your usual websites such as for banks or credit card companies.
- Also be familiar with what legitimate emails look like from these companies.
- Look for bad syntax.
- Does the email appear to be over threatening?

SPECIFIC ATTACKS

➤SOCIAL PHISHING

Phishing attacks can take place on social media websites such as Facebook or Twitter.
It might include pictures or a phrase to entice the person to click on a link that sends them to a malicious website. At this website it asks the person to login thus stealing their login credentials.

What can be done?

- As usual be self vigilant. Look for unusual postings, odd buttons to click on etc.
- If asked to click on a link, copy the text of the link directly into the address bar of your browser and then go to that website. Sometimes illegitimate web addresses are hidden behind benign looking addresses.

SPECIFIC ATTACKS

➤MALWARE

A contraction of "Malicious Software"; It is a general term that refers to viruses, worms, trojans, ransomware, spyware, adware etc.

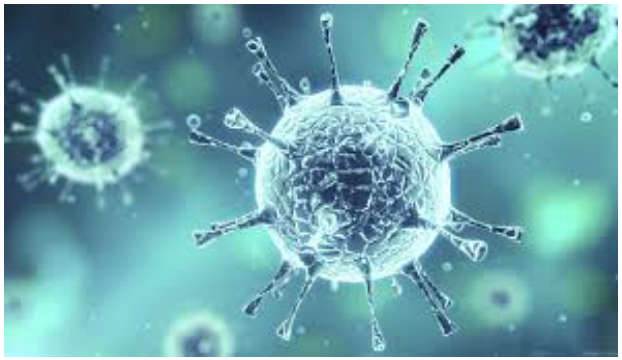
It's main function is to cause operational disruption to a computer by using malicious code. In the past it was mostly to annoy people. Now it's much more criminal in intent often concentrating on the stealing of money.

SPECIFIC ATTACKS

➤VIRUSES

As the name indicates, it's a malicious code that is written so as to spread from computer to computer. In the meantime the code infects one's computer in order to corrupt or delete stored information or in the worst case to cause non-operability of the computer.

It is spread mostly by email but also by interconnected networks as used by businesses. Social engineering can be a part of the attack since the attacker may try encourage you to click on a malicious link. Black hats (bad people) are constantly looking for OS vulnerabilities to exploit.



SPECIFIC ATTACKS

➤VIRUSES

What can be done?

- Definitely have an anti-malware program on the computer which can detect external threats and also fix them. Note: you can have more than one program.
- Update constantly. This includes apps as well as the OS updates.
- Turn on Firewall which limits the number of ways an attacker can get into your computer.
- Turn on FileVault which prevents an attacker from reading data stored on the computer.
- Watch what sites you download from. Downloading from the App Store is safe.

SPECIFIC ATTACKS

➤RANSOMWARE

Definition: A type of malicious software designed to block access to a computer system until a sum of money is paid.

Ransomware locks up the computer by encrypting it whereby only the attacker has a special key to unlock the encryption. Fortunately, anti-malware software has started to include protection against ransomware.

What can be done?

- Make sure that the anti-malware program also has ransomware protection.
- In case ransomware protection does not work, it is essential that you back up your data onto an external flash drive, hard disk or SSD with at least one device not connected to the computer.

SPECIFIC ATTACKS

➤ID THEFT

Definition: The fraudulent acquisition and use of a person's private identifying information, usually for financial gain.

Typically the criminals collect various pieces of information about individuals through any means that they can. Once they have enough information they can pretend to be that person when applying for a loan, open a credit card account or have money transferred to a different account all in that person's name.

SPECIFIC ATTACKS

➤ID THEFT

What can be done?

- If asked to click on a link, copy the text of the link directly into the address bar of your browser and then go to that website. Sometimes illegitimate web addresses are hidden behind benign looking addresses.
- Look for “http**s**” or a lock symbol in the address bar before sending critical personal information to a website. This means it will be encrypted.
- Possibly purchase identity theft protection such as Identity Guard or Life Lock.
- Every 3 months or so personally check on your credit rating and credit score.
- Put a credit freeze on your files in one of the credit reporting agencies if your are not about to get a loan.

SPECIFIC ATTACKS

➤PASSWORDS

There are three main methods used to break into a password protected system:

a. Brute Force Attack
b. Dictionary Attack
c. Key Logger Attack

Brute force uses a computer program to search for possible password combination. Dictionary attacks try various combinations of words found in the dictionary with combination of numbers. Key logger is a malware program that has gotten into your computer via a virus which transmits your keystrokes to an attacker including your passwords and login information.

SPECIFIC ATTACKS

➤PASSWORDS

What can be done?

- Use strong passwords. 12 to 16 digits of non-related alpha-numeric and miscellaneous symbol characters.
- Use two-factor authentication whenever it's offered. Facebook, Google, PayPal, Apple and many others are now using this method in order to protect you. Even if an attacker can get through your first wall of defense, it would be very difficult for them to get through the second.

IN SUMMARY

- ★ Be vigilant
- ★ Be careful about opening unsolicited email. If not sure, don't open it.
- ★ Double check links that are you sent to you before using them.
- ★ Use a good anti-malware program
- ★ Perform updates as soon as possible
- ★ Use built-in computer protection such as FireWall and/or FireVault
- ★ Use the App Store for downloading apps or software
- ★ Back up your computer or iOS device
- ★ Periodically check on your credit at the major credit bureaus
- ★ Use excellent passwords
- ★ Use two-factor authentication