USING A MAC COMPUTER SAFELY

Bob Kapell - March 3, 2014
(areynolds319B@iCloud.com)

"APPLE COMPUTERS HACKED" This has already happened. On September 22, 2013, Reuters News Service reported that Apple admitted publicly that unknown hackers infected the computers of some Apple workers when they visited a website for software developers that had been infected with malicious software. "Apple, Macs hit by hackers who targeted Facebook" was the title of the Reuters story 9/22/13).

According to this article, the malware used had been specifically designed to attack Mac computers. The same software, which infected Macs by exploiting a flaw in a version of Oracle Corp's Java software used as a plug-in on Web browsers, was also used to launch attacks against Facebook, which the social network disclosed. The malware was also employed in attacks against Mac computers used by "other companies," Apple said without elaborating on the scale of the assault.

Some industry watchers have estimated that 700,000 Macs may have been infected by the "Flashback Trojan" malware, but there is really no way to know how many machines were actually affected. These machines were probably all using an out-of-date version of the Java browser add-on. Unfortunately, getting updates to Java can take several months.

***This recent hacking of Apple computers does **NOT** mean that Apple computers are no longer safe. It does mean that we can no longer assume that if we are using an Apple computer that nothing can infect our computer. Because there are now tens of millions of iPads, iPhones, and iPads that run apps that are sold in the App Store, the people who write malware are now writing malware for Apple computers and other Apple devises. So, **we need to be careful**. (OX10 bugs/iOS7 security issues)

This presentation attempts to cover a fairly comprehensive list of security topics and precautions that users can take to make their computing as safe as possible. Not everything in the presentation is applicable to everyone. Take out of it what is appropriate to you.

Apple Support: If you own a MAC there is a wealth of security information available on the Apple web site.
1) Open Safari and type "Apple" in the search bar on top.
2) On the right side, click on the "Support" tab.
3) In the top right hand corner is a search bar. Type in "MAC security" and click.

You will immediately see a list of topics that will address different aspects of MAC security. If you go to the bottom of the screen you will see a button that says "Load More Results." Press this button to get more topics. The list of topics will keep getting longer and longer if you keep pressing the button.

This presentation in based on many of the items from this MAC Security list, and also from a variety of magazine and Internet articles and books about the subject of computer security. Of particular interest are three books: Dark Market: Cyberthieves, Cybercops and You by Misha Glenny, The Internet Police by Nate Anderson, and Cybersecurity and Cyberwar: What Everyone Needs to Know by Peter Singer and Alan Friedman.

OUTLINE: This program will cover the following topics

The OSX operating system
OSX Settings: System Preferences
- **Updates**
- **User Accounts**
- **Administrative Account**
- **Log Out**
- **Lock Out**
- **Firewall**
- **Open Safe Files**
- **Firevault2**
- **Location Services**
- **Bluetooth**
- **Wifi**
- **Passwords**

Installing programs on your computer
Using iCloud
Setting up your router
Safe Use of the Internet: web surfing and emailing
Safari Settings: Preferences
- **Open safe files**
- **Autofill**
- **Cookies**
- **Bonjour**

Review: Web Sites and Email

THE OSX OPERATING SYSTEM

Your Apple computer comes with the operating system (OSX) pre-installed. Do NOT attempt to install a new or updated operating system unless it comes from the App Store. Do NOT buy an OSX or iOS operating system on eBay or any other online place and install it on your machine.

SYSTEM PREFERENCES

Most of the settings that are important for using your computer safely are located in the System Preferences area.

1) Click on the black Apple in the top left hand corner of the screen
2) Click on the fourth item down – System Preferences

Updates: Update your Apple software regularly, especially the security updates. Update your software once a week, or **preferably**, put it on automatic update.

On older operating systems:

1) Click on the Apple logo on the top left-hand corner of your screen.
2) Click on Software Updates.

On the newer operating systems:

1) Click on system preferences
2) Go down to the fourth row and click on the App Store.
3) Make sure that "Automatically check for updates" is checked.
4) Below, check either Mac App Store or Mac App Store and identified developers.

User Accounts: Set up different user accounts for your self and for anyone else that you plan to let use your computer. Each user account should have a password. **Do NOT give any of these user accounts "administrative privileges." "Allow this user to administer this computer."**

1) Click on System Preferences and then, in the fourth row down,
2) Click on Users & Groups

Remember when you are setting up the user accounts to keep a written record of the list of the user accounts and the passwords for each account.

Administrative account: There should be only one account that has administrative privileges. This administrative account should NOT be used for anything except for making changes to the system.

When you are using your computer to do email and surf the Internet use a "user account" that you have set up for yourself that does NOT have administrative privileges. That way if you accidently download any malware you will limit the amount of damage that can happen. "Non-administrative" user accounts do not have access to programs or the operating system, only to the data in that user account.

Log Out: If you leave your computer around where other people may have access to it then you might want to log out of your computer when you are done using it. This is actually not a security measure. It is an energy saving measure.

1) Click on the Apple logo on the top left corner of your screen.
2) Select system preferences.
3) Select Energy saver.
4) Then, depending on the level of security that you need and the potential danger of having someone getting access to your machine, set either the Computer or the Display (or both) to "go to sleep" after a specified number of minutes.

Lock out: If you are really concerned about other people having access to your computer or your data, then you should set your computer up to "lock" when it "goes to sleep" (when it's been inactive for a certain period of time) or when you close out your user account. This provision ("lock out") will require that the password be used to access all user accounts once they have gone to sleep or have been closed. This is a security measure.

To set up the "lock out" feature:
1) Click on the Apple logo on the top left corner of your screen.
2) Select system preferences.
3) Select Security and Privacy.

4) Select the "General" tab.
5) On the upper half of the screen where it says "A login has been set for this user,"
6) Click on the box that says "Require password" and select immediately.
7) Click on the box that says "Disable automatic login".

This measure will require you to re-enter your password every time you want to use the computer. There is some inconvenience to this. However, it will make it very difficult for anyone to use your computer or steal your data without your knowledge.

Firewall: Make sure that the system firewall is on. This puts your computer in "stealth mode."
1) Click on system preferences.
2) Click on Security & Privacy.
3) Click on firewall. Make sure that the firewall is on.
4) Click on firewall options
5) Select the Enable Stealth Mode checkbox. This makes it impossible for other computers to "see your computer"

Open Safe Files: **Turn this off**. This was something that dates from the era when there were no apple viruses.
1) Click on Safari Preferences.
2) Click on General.
3) **Uncheck** "Open safe files."

FileVault2: This program can be used to encrypt your entire hard drive. This will protect you if your computer is lost or stolen. To run FireVault 2 you'll need OS X Lion (or higher), as well as Recovery HD installed on your hard drive as well as your user account. You should also research this further before you enable this feature.

Enable Location Services: When you turn on Location Services, you allow apps and websites to use your computer's current location (identified by GPS) to provide information, services, and features appropriate to where you are. If you **don't** want people on the internet to know where you are, disable this feature. (If you go to visit your children and take pictures of them and their children with a digital camera, the camera automatically "embeds" the GPS location in the picture. If you then post these pictures on Facebook you have just let the world know the exact GPS location of your grand children.) This is a "trade-off" measure.
1) Click on System Preferences.
2) Click on Security and Privacy.
3) Click on Privacy.
4) Disable location services.

Bluetooth: It allows you to access your computer "through the air." It is extremely helpful at home, and in the right circumstances. However, when you are not using them it might be a good idea to **turn it OFF.** If you are in a public place (like a coffee shop or an airpoort) someone might be able to access your computer through bluetooth if it is turned on. (2011 London car thefts.)

Wifi: The same as Bluetooth. If you are in a public place and you are not using wifi you might want to turn it off. If you are using wifi in a public place be careful only to login to safe accounts. Airport "SCRAMBLE"

Passwords: The subject of passwords requires some special attention. (MI 5)

1) **P**asswords should be at least eight characters long. They should contain lower case and upper case letters. They should also contain numbers and symbols (#, %, &, *).
2) You simply **must** use **different passwords for different services**.
3) Turn **off** automatic logins. If you don't, your passwords are useless.
4) Do NOT check "remember me" when logging on to a web site.
5) Keep all of your passwords on paper in a safe place.
6) If you don't want to have to look up and re-enter your passwords when you use your computer there are "password manager" programs that you can use. "Keychain" comes free with Mac OS X. Only use programs that you download from the App Store.

INSTALLING PROGRAMS ON YOUR COMPUTER

There are basically two ways that your computer can become infected.

One way your computer can become infected is by your installing an infected program. A program can be installed by inserting a disk, a "sim" card, or a thumb drive into your computer. (2008 "candy drop" agent.btz)

The other way that your computer can become infected is by your opening an infected program that comes to you on the Internet.

1) You can receive an email that contains an infected file. If you open the file, your machine becomes infected. You need to be careful. Don't open attachments from people or organizations that you don't know. If the email is from someone that you do know, first contact that person and make sure that they actually sent you the file. Many people have had their entire address books "stolen." The person who stole the addresses then sends out email to everyone in the address book.

2) You can click on an Internet site that is not safe. That site can send you a file or application that infects your computer. Be careful not to go to unsafe sites on the Internet. Use common sense.

The best way to protect yourself from unwanted malware is to only install programs from the App Store or a trusted site.
1) Click on the Apple logo on the top left corner of your screen.
2) Select "System Preferences."
3) Select Security and Privacy.
4) Select the "General" tab.
5) On the lower half of the screen where it says "Allow applications downloaded from" select either "Mac App Store" or "Mac App Store and identified developers." **Do NOT select "Anywhere.**"

Be wary of Scripps, Web Archives and Java Archives that you see on the Internet.

Your machine will "ALERT" you when you are trying to download something from the Internet. Do NOT install programs from a source that you are not absolutely sure is safe.

To be safe you should follow these rules:

1) Do NOT let anyone else install programs on your computer; not your children, not your friends, and especially not your grand children.

2) Do NOT install computer games that do not come from the App store.

3) Do NOT install a "pirated" copy of a program. No mater what the cost, the price is too high.

4) Do NOT download programs from sites that you visit on the Internet.

5) Do NOT install an anti-virus program that comes to you by email. More likely than not, the program you are being offered IS a virus. **Mac Defender** (also known as **Mac Protector**, **Mac Security**, **Mac Guard**, **Mac Shield**, and **Fake Mac Def**) is a rogue security program that can be installed by unwitting users of computers running the Mac OS X operating system. **If you insist on putting any anti-virus program on your computer you should download it from the App Store.**

6) Do NOT open attachments that come to you in an email unless you are sure that they are safe and that they have actually been sent to you by a person that you know and trust. It is just like the emails that say: "Hi, this is Bill. We are in France and my wallet was stolen. I don't have my passport or credit cards. Please send me $2,000 fight away."

USING ICLOUD

iCloud is encrypted. It is safe to use to send and receive files. It can also be safely used to store files.

You cannot move or store Microsoft word or excel files as such on iCloud. But, you can save them as Pages or Numbers files. Then move them to iCloud. You can move the files back to your computer and then re-convert them back to Word or Excell. Remember, the easiest way to send files from one computer to another is to simply email them.

With iCloud you are allowed to create three (3) different email alias "identities." These email identities enable you to send email to different people or organizations and hide your true identity and email address. For example, you can create an alias to use when you shop online. Keep your personal (true) identity for use in communicating with family and friends.

With your email identities you can temporarily disable the identity. When an alias is "disabled," the email sent to that address is automatically sent back to the sender as "undeliverable". You can "re-enable" the alias anytime you want to.

SETTING UP YOUR ROUTER

1) Make sure to set up your router to use WPA2 encryption.
2) Set up a secure network with a secure password.
3)Set up a guest network that you will have available for people to use where you will be able to change the password when you no longer want them to have access to your secure network.

USING THE INTERNET

For the average person, there are **two serious potential problems** relating to using your computer on the Internet.

The first potential problem is that your important information might be stolen. Your bank account numbers, your financial records, your passwords could be taken and your assets could be stolen online, and you wouldn't even be aware of it until it was too late.

There are two ways that you can prevent having your important information from being stolen. The first is to be very careful whenever you use the Internet. Be careful when using email and the Web so that you don't download any malware or accidently "give away" the information. **Don't respond to emails or requests for information and include your passwords or personal information. The single biggest danger to your security is lack of awareness and your own carelessness.**

The second way to avoid having your financial information stolen from your computer is extremely simple. Never record your account numbers and account passwords on your computer. Also, don't leave any records of your financial information on the computer where it could be seen or stolen. You should keep this information on written records, or on a thumb drive, but don't save it to the computer hard drive. If your important financial information is not on the computer it can't be stolen from the computer. (Except in the case when someone has managed to install a "keystroke logger" program on your computer.)

It may be inconvenient to have to "look up" your financial account numbers and password numbers and manually type them in whenever you want to bank on the Internet. However, it does provide an important layer of security.

An additional level of security can be achieved, if you feel that you need it, by using a different computer that you use only for your financial transactions. Do not use this computer for anything else – no email, no web searching, etc.

The second potential problem when using the Internet is that your computer could be "hijacked" and taken over by someone, somewhere in the world.

In some cases the hijackers use the computers that they have taken over (tens of thousands) to launch computer attacks on large computer systems (DOS attacks).

The person who has invaded your computer can access any information on your computer. They can "steal" your address book. They could install a "key-stroke logger" on your machine

and would have a record of every key-stroke that you make. They could also take over you computer and use it to spy on you. They could turn on your web cam or your microphone so that they can see and hear everything that is going on in your house or office that is in view of the computer.

SAFARI SETTINGS: PREFERENCES

There are some settings in Safari that are important to do. Open Safari and click on "System Preferences."

Open Safe Files:
1) Click on General.
2) At the bottom, UNCHECK "open safe files."

Java Code is a potential danger. If you want to, you can: (a trade-off issue)

1) Click on Security.
2) Disable java script.

Cookies: clean out cookies regularly.

1) Click on Privacy
2) Either remove all website data once a month, or check the "details" of the cookies stored on your computer once a month and remove the ones that you don't recognize.
3) Make sure that cookies from third parties and advertisers are blocked.

Bonjour:
1) Click on Advanced.
2) Make sure that "Bonjour" is unchecked.

The point of this is very simple. In the past we could all "safely assume" that if we used an Apple computer we simply did not have to worry about malware on the Internet. That is no longer true. This year there have already been several large-scale assaults on Mac computers by hackers who are now writing sophisticated malware that are designed specifically to attack Mac computers. We need to be careful.

REVIEW OF SAFE INTERNET USE

VISITING WEB SITES

It is important to be careful when using the web. There are a few simple rules that you should follow. They will help.

1) Be careful which web sites you visit. Many web sites contain malware. **Some will actually send malware to your computer just for visiting the site. You don't even have to click on any programs on the site. Be particularly wary of porn sites.**
2) Do NOT go to a financial web site by clicking on a "button" contained in an email that you receive. **Go to the web site from your own bookmarks.**
3) Be careful when your browser is "redirected" to another web site. Carefully read the name of the website in the address bar. If the title is not **absolutely identical** to what you have in your bookmarks it may be a "bogus" or fraudulent wed site designed to steal your information. This is especially true of anything to do with financial web sites. For example, what is the difference between www.paypal.com and www.paipal.com? Would you notice the difference if you were not aware that you needed to be especially careful? This could be a serious and costly mistake.
4) When you are dealing with any sensitive information, always make sure that the web site is secure**: https. It is the "s" following the http that indicates that the web site is secure. When you connect to a secure web site a "Lock" icon will appear after the https to show that it is secure and the source of the site has been verified by a Certification Authority.**

USING EMAIL

It is important to be careful when using email. There are some things that you can do that will help you protect your security.

1) Set up your email to take full advantage of the filter that Apple builds into the system. Monitor your "junk" mail and make adjustments when necessary.
2) Don't open **attachments** from people or organizations that you don't know.
3) If there is an attachment from someone that you do know, ask that person if they sent you the attachment. Many people have had their email addresses stolen and the hackers send out malware to everyone who was in their address book. (Certainly you have already heard about this common scam: "I am in Europe and I have been arrested. My wallet and passport were stolen and I need money to post bail. Please send me $2,000 immediately.)
4) Pay very careful attention to the return address of incoming email. It might look like a legitimate company but be only one letter or symbol different. If it is not exactly correct, it might be from a hacker. "Social Engineering" is a term that refers to "phishing" attacks. These are attempts to get people to respond to an email or an inquiry and give out critical information such as a password or an account number. "Phishing" attacks can be general or targeted. A targeted attack is one in which the person conducting the attack does some research in order to learn personal information about you so that they

can gain your confidence or be able to threaten you. In the age of Facebook this is way too easy.

5) Never respond to incoming email and give out any important information, personal or financial. It is exactly like receiving a phone call from someone who calls you and says that they are from the security department of your bank and they want to verify your that you have your credit card in your possession. They ask you for your account number or the security code on the back. Hang up and call the bank on a phone number that you know is really the bank's number. The bank's phone number is on the back of your credit or debit cards. **Financial institutions never send out emails asking for specific information to be sent back by email**
6) Never open an email that comes to you claiming that you may have a virus on your computer and if you open the attached file, the program will scan your computer to detect known viruses or malware. The program that is attached to the email probably IS THE MALWARE. It will compromise your computer. If you really want to use an anti-malware/virus program on your computer download it from the App Store. That way you know that the program is actually safe. (Incidentally, at the present time most of the anti-malware programs that are sold for Macs actually find malware that is designed to attack Windows programs. If you use these programs they will actually help you protect anyone that you sent an email to who is using a "Windows" computer. They don't actually do anything for you.)

"SOCIAL NETWORKING"

If you join any of the social network sites, have the courtesy to your fellow human beings **not** to give them permission to look at your address book. They will ask you if you want to know if any of your friends or contacts are already on their web sight. If you say yes, they will copy your entire address book and you will have sentenced everyone in your address book to an avalanche of unsolicited email saying that YOU invited them to join the network.

If you send, or resend, email to multiple people, please learn to put all of the addresses in the BCC ("blind carbon copy) pane of the email program. If you put the addressed in the recipient pane or the CC (carbon copy) pane, you will be sending every single person every one else's email address. Do we actually need to **help** wipe out privacy completely?