Mac Security Mac Group Presentation February 15, 2016 Nonnie Markeset

How to Secure your Mac and iDevices and Avoid Common Vulnerabilities

What are vulnerabilities?

1. Viruses
2. Malware
3. Trojan Horses
4. Weak Passwords
5. Sharing too much personal information on public websites, like Facebook
6. Visiting sites that contain your sensitive information on a public computer or on a public website
7. Visiting "bad sites". Ones that offer free movies, music, cheap goods and services.
8. Clicking on links in emails you receive
9. Not having your computer/iDevices password or passcode protected and/or having a weak password/passcode for your device.
10. Having the same password or similar for all sites.
11. Not keeping your OS/iOS and apps up to date
12. Spilling coffee on your keyboard
13. Dropping your device

Of all the vulnerabilities listed above, your greatest vulnerability is your passwords.

How do you create a strong password?

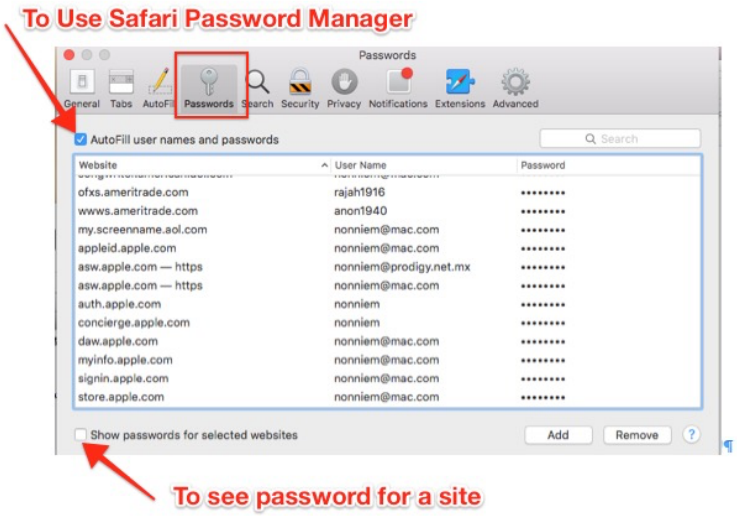
A password should be at least 12 characters. It should contain letters, numbers and symbols and preferably not contain words found in a dictionary.

To check the strength of your password:
http://www.takecontrolbooks.com/resources/0148/zxcvbn/

Each site should have a unique password

How do you remember all your passwords?

1. In Safari, turn on AutoFill (This I do not recommend as it is the least secure of all the options.)



2. Use Keychain Access (User→Applications→Utilities→Keychain Access)
3. Use a third party Password Manager (Your best option.)
   - 1Password
   - LastPass

Here are some examples of weak passwords:
- 123456
- jack0322
- w0nd3r
- pr1ncess
- samkenmary
- 122940

Here are some examples of strong passwords:
- wHx9vm5Gs7zR
- vxqCIKypD7”

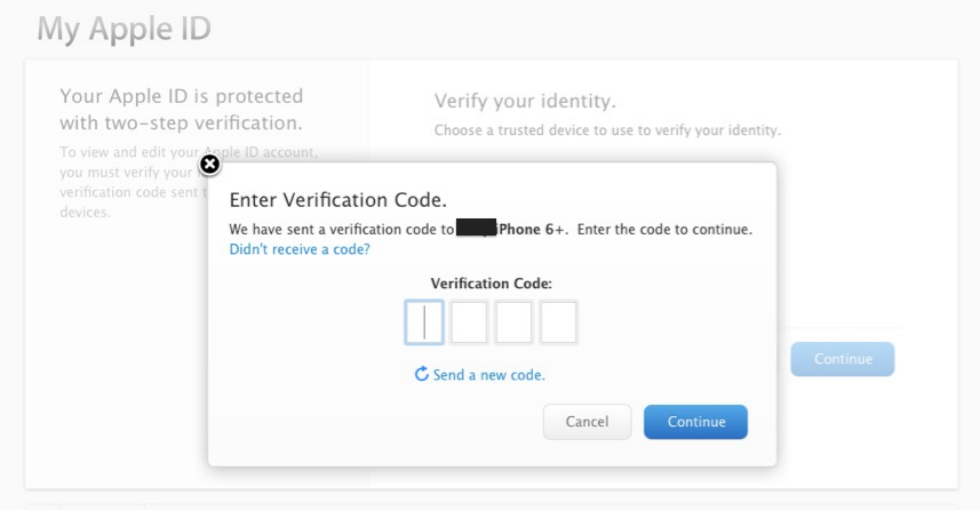
You should also set up 2-step verification for any site that has this feature.
This, however, requires you to have a mobile device on which you can receive a generated code to complete the sign in process. This code will be sent to you via a special app on your iDevice or via an SMS message if you are using an iPad.
How it works:

1. Go to the site.
2. Enter your password.
3. Receive a randomly generated code on your phone.
4. Enter that as a second password on the site.

Here are some sites that offer 2-step verification:

Google/Gmail -- https://www.google.com/landing/2step/
Facebook -- Go to Settings, Security and select Login Approvals
Apple/iTunes/iCloud -- https://support.apple.com/en-us/HT204152

Example of what you will see on the Apple Sign-In Site.



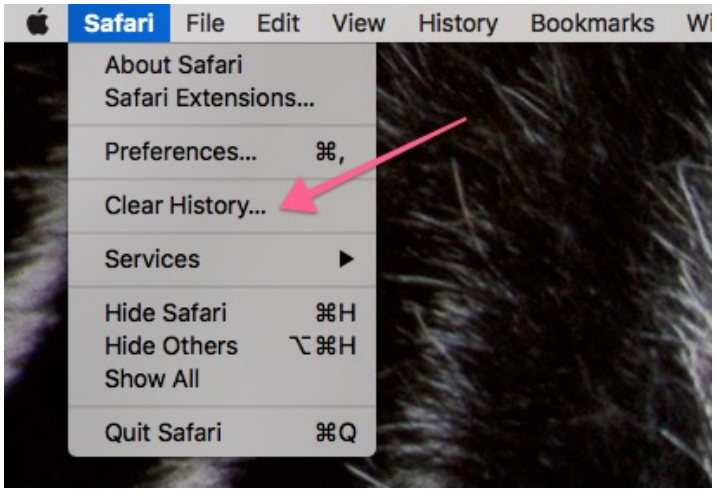
Steps to take if you think you have been compromised.

1. Change the password for the compromised site.
2. Change the questions and answers to the security questions for that site.
3. Change the passwords for other sites.
4. Set up a prioritized list of sites that need to have passwords changed
   - All your email account passwords
   - Bank and investment accounts
   - Facebook and other social sites
   - Amazon, Netflix
   - eBay/PayPal
   - AppleID/iCloud

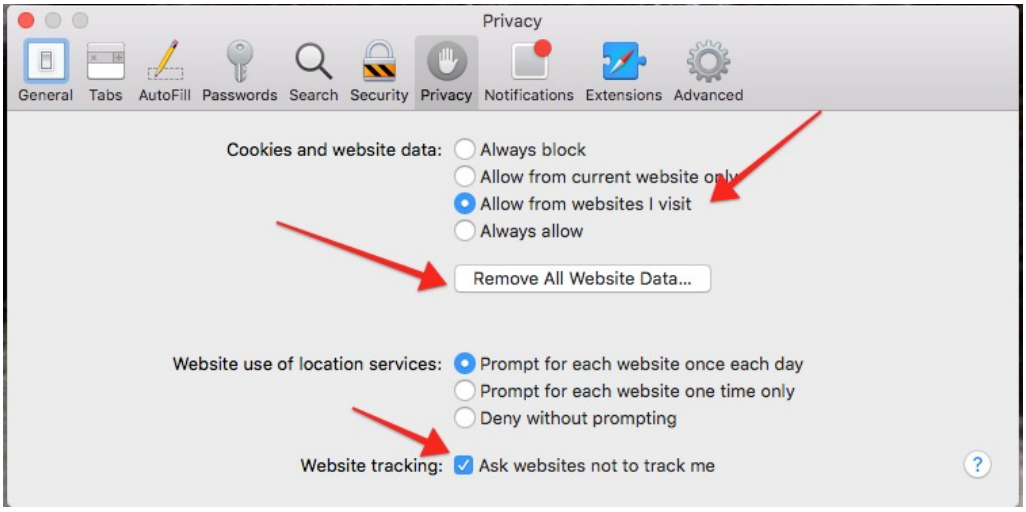
I also recommend that you set up a schedule to change passwords every six months, at least for your most important sites.

<u>What to do if you get constant pop-ups in your web browser warning you that your computer has been compromised. DO NOT CLICK ON THE LINK. DO NOTDOWNLOAD THE SUGGESTED APP THAT CLAIMS IT WILL CLEAN YOUR COMPUTER.</u> Instead:

1. In Safari (Firefox and Chrome have similar procedures) "Clear History" in the Safari drop down menu

i. 

2. In Safari Preferences, go to "Privacy"



Malware, Viruses, Trojan Horses and Hackers

These are vulnerabilities that come from external sources.
Viruses are a type of malware that get installed on a computer without permission and have the ability to create havoc with your computer. This type of malware is at this point "non-existent" on Macs because of the safeguards Apple sets up.
The types of malware that Mac users must be aware of are called Trojan horses. They are pieces of software that can piggyback on other software to get into your computer. Basically you give them permission without knowing it.
Do you need Anti-Virus software to protect yourself from these? Most Mac pundits will say no. Instead follow these 4 rules.

1. Keep your Mac updated
    a. Make sure you have the latest OS and when incremental updates come through make sure to install them
    b. Update the apps you use when you are notified of updates.
    c. Turn on Auto-Update if you want, in System Preferences-App Store

2. Download software only from trusted sites. Here are some safe sites

Mac App Store	Microsoft
Adobe	Agilebits

    If an offer is too good to be true, it is usually too good to be true!
3. Stay informed and research an unknown site before you download from it. Search the web to see if there is any info on the company.
    2 good sites to check and to keep you informed are:
    MacRumors.com
    CultOfMac.com
4. Do not click on links contained in emails you receive.
    - As frustrating as this is you are safer if you open your web browser and manually put in the address…not copy it.
    - Gmail has two new symbols to inform you if your email is being sent encrypted and if the person you are receiving the email from is the actual person sending the email. The first is represented by a lock and the second by a question mark.

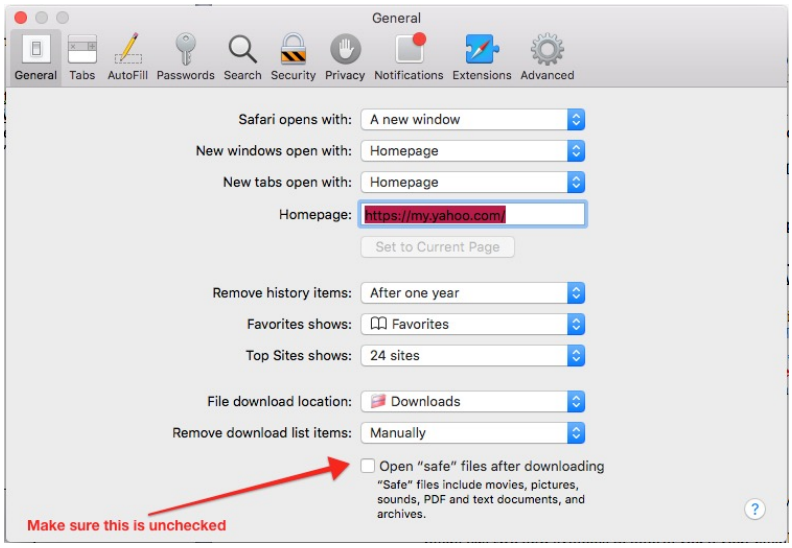
Extra Protection

1. In Safari Preferences under General make sure "Open Safe Files" is unchecked*
2. In System Preferences under Security and Privacy, chose "Mac App Store and Identified Developers".**

Firewall

The firewall lets you block incoming traffic to particular programs, meaning it is only useful if there are programs on your computer that you want to restrict in terms of incoming information.
If that's not the case, and if you use the Internet primarily behind a secure router, you probably don't need to enable a firewall at all.

*In Safari Preferences under General make sure “Open Safe Files” is unchecked.



In System Preferences under Security and Privacy, chose “Mac App Store and Identified Developers”.