Nonnie Markeset
Mac Meeting Presentation
September 18, 2017

Finding Security in an Insecure World©

There are two types of risk we face

1- **Outside our control**
   - A hack has occurred on a company or organization that has our sensitive information.
   - It could be the IRS, Equifax, a bank, a credit card company, a lending company, a mortgage holder, an investment institution. Any entity we deal with and to which we have given our name, address, and social security number.
   - The use of this information by the hackers can be difficult to find and can last for years.
   - Some of what hackers can do with this information is take out credit cards in our name, apply for loans or mortgages, commit crimes and even be convicted, and change our address so that we won't receive any notifications of what has been done.

2- **Within our control. This list is long!**
   a. Have weak passwords for websites we visit
   b. Use the same password for multiple sites
   c. Visit suspicious sites
   d. Download apps , movies, from unauthorized sites
   e. Click links in emails and enter our sensitive information on the website without ascertaining it is a valid site
   f. Post too much information about ourselves on social networks
   g. Use public wifi networks to visit sites that have our sensitive information
   h. Not secure our computers, phones, iPads with strong passwords
   i. Not have "Find My iPhone/Mac/iPad on in our iCloud account
   j. Not install the latest updates to our operating system
   k. Not install the updates to our applications

Nonnie Markeset
Mac Meeting Presentation
September 18, 2017

What you need to do NOW to protect yourself after the Equifax breach

1-You can go to this website, enter your last name and the last six digits of your social security number to see if your information has been compromised. Unfortunately it will only tell you that it MAY have been breached. Equifax has no idea at this point whose info was stolen. But try it anyway. Maybe by the time you do, they will have more information.

https://www.equifaxsecurity2017.com/potential-impact/

2-Sign up for one free year of credit monitoring at Equifax.

https://www.equifaxsecurity2017.com/trustedid-premier/

This is available to every American. But this is incomplete because there are two other main credit companies that thieves could access, Experian, and TransUnion. And also another little known company called Innovis.

3-This is one of the two most important steps to take. Sign up at each of these sites for them to put a permanent freeze on your credit files.

https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp

https://www.experian.com/freeze/center.html

https://www.transunion.com/credit-freeze/place-credit-freeze

https://www.innovis.com/personal/securityFreeze

Each company will charge you about $10 to institute the freeze. DO IT! It is money wisely spent.

Once you do (and it may take a little time to complete the process), the bureaus are not supposed to release your credit report to any company except the ones that already have you as a customer. Why is this important? When a thief shows up with your Social Security number and address to apply for credit in your name, the lender will go to fetch your credit report before anything else happens. If it can't retrieve the report because of the freeze, then the thief can't set up an account in your name.
You still can apply for new credit when you need to. You will be given a personal identification number by each of the credit companies to use to unfreeze your account. This too will cost you a few bucks!!
4- The second important step is to set up fraud alerts at each credit company. These are different from credit freezes. So you should have both. Once these are in place, potential creditors will contact you directly to confirm that it is you who wants to open an account.

https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp

https://www.experian.com/fraud/center.html

https://www.transunion.com/fraud-victim-resource/place-fraud-alert

5- Check your credit a couple of times a year.

https://www.annualcreditreport.com/index.action

If this is too overwhelming, you can always sign up with a credit monitoring company like LifeLock. But be forwarned, you will get a ping every time there is a change in your credit report. That can be nerve wracking.

If you have just finished reading this and are ready to say the hell with it, think of this. If you are one of the ones whose data has been breached, a thief can file a phony tax return in your name on January 2 and claim a big refund. Guess who gets stuck with the bill? YOU.

Safe Sex and Safe Surfing: The two are kissing cousins

Here are the things we need to do NOW to protect ourselves.

1. Buy a good password management application and use it. I recommend 1Password but also good are Dashlane and LastPass.
2. Create a unique password for each site you visit. Your password management app will help you create good passwords and record them for you.

   You can also test your password's strength at this site: http://www.takecontrolbooks.com/resources/0148/zxcvbn/

3. Sear on your brain these three passwords: your computer password, your AppleID password, your password management app password. Forgetting these will give you endless headaches.
4. Passcode protect each of your iOS devices and choose a 6 digit code instead of a 4 if you can.
5. Set up two step verification for your iCloud Account and for sites that have that feature.
6. Make sure in your iCloud Account Settings on each device that "Find My Mac/iPhone/iPad" is turned on and learn on to use it.
7. Tighten up your Facebook and social media passwords and remember that every time you post a pic from your phone it has location data in it. If you don't want to be geolocated, scrub your pics or turn this off.
8. Download and install a good VPN on each of your devices to use when you are on public networks. And use it even if you are just surfing the web. Otherwise it's like being upstairs in the shower when your front door is unlocked.
9. Don't visit porn sites or suspicious sites.
10. Don't download apps from unknown sites. If you want to download a new app, try to find it in the App Store or make sure the site you download from is "clean". That way you know you won't be downloading malware with it.

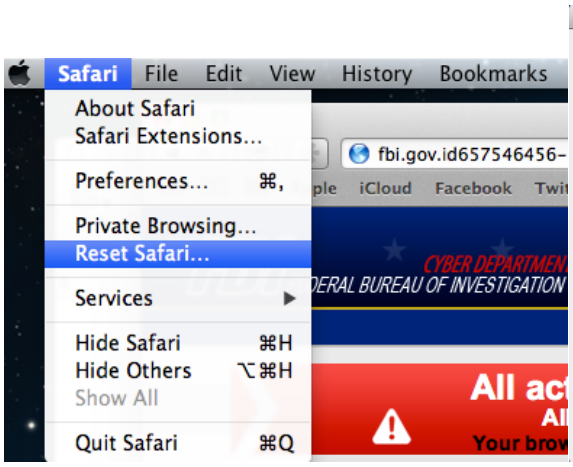
11. Keep your devices operating systems up to date. Many of the updates plug vulnerabilities.
12. Keep your apps up to date. Again many of the updates plug vulnerabilities and correct errors.
13. Don't download "free stuff"
14. Don't click on links in emails and if you send friends links to sites, make sure the site is valid. I recommend if it is an article that you copy the article into the body of the email along with the link..
15. Don't buy things on Safari. Instead download the Amazon App and buy through it.
16. Buy a good malware protection app. Derek recommends Malwarebytes. You can buy and download it from the following (verified) site.

    https://www.malwarebytes.com

17. If your browser freezes when you are on a site and a message comes up telling you you have been infected with a virus and you should download "this app" or call "this number", DON'T.

    Do the following:

    Option 1:
    1. Click on the **Safari menu** and then choose **Reset Safari**
    2. In the new windows, make sure all items are marked and click on the **Reset** button.



OPTION 2:

a. Press **Command** + **Option** + **Escape** simultaneously. This will open the **Force Quit** Applications window.
b. Select Safari, Chrome, Firefox or any other browser in which you're seeing the Your Browser Has Been Blocked Up ransomware notification.
c. Click the button that says "**Force Quit**". This will forcefully end your browser program, thus removing the Your Browser Has Been Blocked Up browser hijacker. If you cannot switch from the unresponsive app, press **Command** + **Option** + **Shift** + **Esc** for **three seconds** to force it to quit. This key combination tells OS X to force quit the front most app.
d. Your browser should be closed now. Open the web browser again, then quickly close it again by using the button in the corner of the browser.
e. I recommend going through Option 1 now to clear everything.