SECURITY

by: Jonathan Gorman of iCreative
2/12/2020

There are a lot of bad people out there, the so called "Black Hat Hackers" who thrive off stealing data from the Internet. Fortunately many of them are not necessarily malicious, they apparently do so for the fun of it and bragging rights with their equally anonymous networks of odd friends. And the really bad characters are going after far bigger financial targets than any of us. But any of the multiple viruses they create every day can cause you plenty of trouble - think about having to spend a fortune on consultants to reformat your hard drive, perhaps losing all your data and the potential for the lesser villains out there trying to tap into your finances.

There are four primary ways you get 'hacked'. 1) You are manipulated by a phone caller into giving them access to your computer or passwords. 2) The website storing your information (store, bank or utility company) was compromised. 3) You have an insecure email service. 4) You were tricked into clicking on something bad in an email or on a website that downloads a virus. Fortunately Apple makes it very hard for you to download any files containing viruses as they restrict your ability to download anything not from their App Store and identified developers.

LOG IN INFORMATION:

Because our email addresses are now used by a lot of websites as our User Names, it is essential that we keep their access secure. We need to change email passwords on an ongoing basis to keep them secure. Also, if you use AOL, you are basically waving a red flag that you are an older, perhaps less computer savvy user. And you are much more likely to be hacked as many AOL passwords were stolen at the server level, so get rid off your AOL account and go with your existing iCloud email address. Gmail, Yahoo & MSN have no customer service and although they are also free, this lack of service can be quite irritating. By comparison, you can call APPLECARE at: 800-275-2273 at any time for help. iCloud email is safer because of Apple's encapsulated hardware and software, plus they host all their own services, creating a more cohesive and secure network.

When traveling, be careful of unprotected internet connections, including hotel WiFi systems or even Starbucks. Try to never access your financial websites with a public WiFi. Instead, try to get permission to access private WiFi networks. Best is to use a VPN (Virtual Private Network), that is very much more secure than our cells or WiFi. It spoofs off other networks so that your browsing is vastly more secure. They basically 'tunnel' through the Internet protecting your data along the way. One of the best VPNs is NordVPN as they always seem to perform well and they have great customer service. Right now they have a 3-year deal going for $3.49/month. If you must use public WiFi, keep it to safer subjects, like news & weather webpages and social networks.

It's also a good idea to use Private Browsing when surfing the Internet when you want to be 'invisible' - if for no other reason than it helps hide your activity from the bad guys. There are many reasons for anonymous browsing, perhaps best explained by this article from Apple:

https://support.apple.com/guide/safari/browse-in-private-ibrw1069/mac You can also browse in private on an iPhone/iPad by following these Apple instructions: https://support.apple.com/en-us/HT203036 Look for the search window turning black to confirm Private Browsing.

Automating access to your (hopefully) varied login information for various websites can be done one of three ways: 1) write them all down in a Secure Note - see next section for details. 2) use a third party password managing app like 1Password and Dashlane or 3) use Apple's very own Keychain in conjunction with their Safari browser. Make sure that Keychain is synced across all of your devices by going, on a Mac, to System Preferences -> Apple ID and confirm that Keychain is enabled to sync. On your iPhone or iPad, go to Settings -> Apple ID -> iCloud and make sure that Keychain is enabled. You must also be on the SAME Apple ID for all your Macs and mobile devices, which means your passwords won't be accessible on your spouse's iPad unless you share the same Apple ID.

Keychain is free. To set it up to work properly with Safari, open Safari preferences -> Autofill and check all the boxes. To set this up on your iOS devices, go to Settings -> Passwords & Accounts -> Website & App Passwords and enable it. As mentioned above, you also need to make sure that Keychain is synced in iCloud so that the logins are also on all your synced devices. Whenever you are asked to log in by a site, Keychain will remember your user name and password for that website as it keeps track of that site along with your user name and password.

To update and maintain the data in Keychain on a Mac, do NOT use the Keychain app in the Utilities folder. INSTEAD, go to Safari Preferences -> Passwords. You will then be asked to enter your password for your computer. Once you have done so, you will see the list of all your saved login information. You can now edit or delete any of them and you should do this if you discover you've setup two different log-ins for the same internet account. A tip is to use the same four or six digit code on both you iPhone and Mac so you don't get frustrated remembering them - but it also means a theft who learns your code is in to everything, so guard it carefully!

SECURE NOTES:

Using the Notes app is a great way to keep sensitive information private by creating "Secure Notes" (password protected notes). You need to make sure that your Notes are synced across all your devices just like with Keychain (see the directions above) so you can access everywhere.

You can put all kinds of sensitive information into a Secure Note. On a Mac, all you need do is create a new note and click on the little lock icon at the top of the note. You can create a different passcode for each note or you can use a single passcode for all notes you want to secure. To do the latter, open Note Preferences and at the bottom you can set (or change) to a single password. Do not forget this password as if you do, you will not be able to open those notes. On your mobile device, you create a locked note by creating a new note -> the share icon (box with arrow pointing to the top) and then "Apply Lock Note". For more information, see: **https://support.apple.com/en-us/HT205794**