Computer Security

Computer security is becoming more and more an issue for organizations and individuals. Below are some thoughts on various aspects.

If you use Apple products — computer, iPhone, iPad, iCloud — Apple provides some features and services to help with some of the issues.. These are mentioned where applicable. Other providers often offer similar products — Google is a prominent example.

Topics

Passwords and 2FA

Most online services require a password as part of your identification for access. An increasing number require or allow Two Factor Authentication (2FA) as further security. 2FA means that after you enter your password you will be asked to provide another element that only you will know. This can be a code that is sent to you, by email, Text message or phone call, or provided by an authentication app that generates a regularly changing code unique to you.

It is important that you create passwords that are unique (not reused among multiple sites or services) and hard to guess. Current advice is that a password contain at least 12 characters, no dictionary words and a combination of upper and lower case letters, numbers and special characters (* $ # @ etc.).

Since you will probably need many unique, hard to guess passwords, thinking them up and remembering them can get to be a chore. Password managers can be very helpful. A password manager will save your user name and password for every site or service, and can automatically enter them when you are logging in. It can also generate a strong password for any new login, if you choose. Cyber security experts recommend use of password managers. There are many available, and an on line search will provide descriptions and ratings

The Apple Keychain app is a free password manager that is easy to use and automatically syncs across all your Apple devices, through Apple's iCloud.

2FA Is a good protection for sites or services that are important to keep secure, such as bank accounts, brokerage accounts, on line purchase accounts, etc. Sites that offer it have a setup procedure that allows you to choose how the code will be sent to you — email, Text or phone call. It’s an easy way to get a big increase in login security.

Backups

It is incredibly important to back up your computers (including smart phones and tablets) regularly. If you ever have a computer or disk failure, any information that is not backed up will be lost. Less probable, but still possible, malicious attacks on your computer could include destroying or encrypting for ransom (ransomware) all your files. Having a secure recent backup can protect you against these losses.

Two common ways to back up your files are to copy them to a separate disk or to upload them to the cloud (internet). Both methods are good, and doing both is even better.

Local backup

Local backups involve copying the contents of your computer files to a disk separate from the one in the computer. Typically, an external disk is connected to the computer, and a software program copies any changes since the last backup to the external disk. This is done in such a way that the program can restore it to the computer when needed, recombining file segments from multiple incremental backups into a complete copy. An alternative is to copy a total or partial computer disk image onto a storage device like a thumb drive or DVD.

Ideally, you will run your backup program regularly, and frequently enough that any loss since the last backup will be acceptably small. Backup programs can often be set to run automatically at acceptable intervals.

For Apple Macintosh users, Apple provides a very nice backup program called Time Machine. When an external hard drive is attached to the Mac, a very simple procedure is offered to make it a Time Machine backup disk. Once set up. it runs every hour, incrementally backing up any changes since the last prior backup. Copies of all backed up files are kept until the Time Machine disk fills up, after which the oldest images are discarded to make room for the latest. In Time Machine, you can access older copies of files and, if ever needed, a complete restoration of the entire computer drive. This is truly a set it and forget it backup solution with many benefits. There is hardly any reason for a Mac user not to take advantage of it.

Cloud backup

Many internet cloud providers offer backup programs where files on your computer can be automatically kept in sync with a copy on the cloud. This is often used for photographs, but can also be used for other files. A benefit of cloud storage is that it is remote from your computer, so it will not be damaged by fire, flood etc. where your computer is kept. There can be a cost associated with cloud storage, but it is usually nominal and doing cloud backups is a good idea even if you also do local backups. Cloud backups also can back up your smart phones and tablets.

Apple's cloud backup product is iCloud. A small amount of iCloud storage is free to any Apple user, and additional storage is nominally priced. Currently, 5 GB is free, and 200 GB costs $2.99/month. You can configure iCloud backups to include a variety of files — photos, music, email, Desktop files, Documents, etc. Once configured, any changes on any included devices are automatically synced to iCloud, and the device is backed up daily to iCloud when it is connected to WiFi. When you buy a new iPhone or iPad, Apple software can completely set it up to download all the relevant iCloud files.

Invisible pixels

Invisible pixels are an insidious way that websites can track you or download malicious code without any action on your part.

When you get an email, it can include loadable attachments or links to images. Clicking on one of these can download malicious code. It also sends the download provider information about your computer that can contribute to an ability to track you. For this reason, many know not to click such links from unknown email senders.

Invisible pixels are small images — one pixel square — that can be embedded in an email. The recipient won't see it. But the email program will automatically attempt to display it, by sending a message to its associated web site requesting that it be downloaded. That is exactly the same action that would occur if you clicked a link on an attachment. It has exactly the same possible negative consequences.

Apple offers an option in its Mail program to not automatically download embedded images in emails. This is a good safeguard to employ — it means that you will be offered the choice of whether to download any images before they download — including invisible pixels.

In its 2021 operating system releases, Apple is also cracking down on email tracking. Most marketing emails contain invisible pixels that can identify when a recipient has opened an email. These trackers also collect information including users' IP addresses that can tell marketers when and where their messages were opened. New Apple Mail releases will default to not automatically download these invisible images..

Virtual Private Network (VPN)

Large organizations often protect their internet traffic from eves droppers by encrypting it, so that an eavesdropper will see only gibberish. They do this by setting up a private network that is only accessible to authorized users. Inside their facilities, the network is over wires, so cannot be tapped. Outside of their facilities, they use a virtual network over WiFi or cellular services. Traffic on this Virtual Private Network (VPN) is encrypted end to end by all the organization's users' devices.

When you use a public WiFi hot spot, all of your messages can be viewed by anyone within range of the WiFi signal. Readily available software can capture this traffic, so that its contents are available to the eavesdropper. It can be particularly interesting to someone with malicious intent if it includes information that could be used for identity theft, black mail or logging into interesting accounts, like a bank or brokerage, or Amazon. This is not good. But you can defend yourself against it. VPNs are available for nominal cost (less than $100/year) to individuals. If you ever use public WiFi services, consider signing up for a VPN. A Google search will provide information and recommendations for dozens of alternatives.

In June, 2021, Apple announced that they will soon include VPN-like software as part of iCloud in a new product named iCloud Private Relay. It will be in iCloud+, a free addition to any iCloud customer who pays for one of the extended iCloud plans, starting a $.99/month. Full details aren't yet available, but this might be an attractive alternative to paid VPN services for iCloud users.

Tracking

How do you feel about corporations knowing where all you have visited on the internet? Quite likely, they can. Web sites can put a "cookie" in your computer when you visit, and check it later. They use this for some reasons that benefit you, like storing information you have given them about your preferences, login credentials, etc. But some also install 3rd party cookies.

Third-party cookies are cookies that are set by a website other than the one you are currently on. For example, you can have a "Like" button on your website which will store a cookie on a visitor's computer. That cookie can later be accessed by Facebook to identify visitors and see which websites they visited. Such a cookie is considered to be a 3rd party cookie.

Another example would be an advertising service (ex: Google Ads) which also creates a third-party cookie to monitor which websites were visited by each user. This is the main technology used to show you products that you previously searched for on a completely different website.

Your computer probably offers you the option of disallowing the use of 3rd party cookies. Choosing this option will not inconvenience you, because the cookies that store information about your logins and preferences at the site you visited will not be affected.

Cookies are not the only way your web visits can be tracked. The apps in your smart phone can also track your internet activity.

IDFA stands for Identifier for Advertisers, which is a unique ID assigned by Apple to a user's device. Android has its own identifier version called Google Advertising ID, or **GAID**. The IDFA or GAID is used for tracking and identifying a user. Advertisers use this to track data so they can deliver customized advertising.

The IP address on your device provides another means of tracking you. An Internet Protocol address (IP address) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. Collecting a history of where your IP address has visited the web provides information about you that you might prefer not to share.

In Apple's recent operating system releases the utility of these tracking methods has been reduced. IOS 14.5 requires all iPhone and iPad apps to offer you the option of disallowing the use of IDFA to track you. Early indications are that about 95% of users have chosen to disallow this tracking. The next operating system releases (not yet released) for iPhone, iPad and Mac will hide your IP address from web sites you browse with Apple's Safari browser,, shutting off this tracking method.

Spam filtering?

Are you not receiving messages? If you don't get messages that you think are being sent too you, check your Junk folder(s) — sometimes messages are erroneously treated as spam.
NOTE that if you download messages to your PC to read them, your mail will be screened by two spam filters — one on your PC by your PC mail program, and one online managed by your email provider. You should check both if you don't get the messages. If you do find messages that were erroneously sent to Junk, you can train your email program by selecting the misclassified message(s) and clicking "Not Junk" or "Not Spam" in your mail program — usually at the top somewhere.

Anonymous credit cards

There are ever increasing ways to buy things on line. sSometimes you may want to make a purchase without establishing a permanent relationship with the seller. In these cases, having a one-time-use or an anonymous credit card can be helpful.Such credit cards enable making a payment without disclosing to the seller any personal information about you.

Apple Pay

Apple Pay is designed to protect your information and enable you to choose what you share.When you use Apple Pay in apps and on the web, information necessary to process the payment is shared with the app or website. Your actual card number isn't shared with the merchant. Apple Pay allows you to make secure purchases in stores, in apps, and on the web, using your debit, credit, and prepaid cards.

Identity theft

If a bad actor obtains enough information about you, he can impersonate you to steal money from you. To do this, he may create a financial account or credit card in your name. Part of the process of creating a financial account involves doing a credit check with one of the credit bureaus.

To prevent this sort of theft, you can request a credit freeze with each of the credit bureaus. The credit freeze is free, and can be terminated or temporarily suspended at any time, using a secure login you establish with each bureau. A credit freeze restricts access to your credit report, which means you — or others — won't be able to open a new credit account while the freeze is in place. You can temporarily lift the credit freeze if you need to apply for new credit. When the freeze is in place, you will still be able to do things like apply for a job, rent an apartment, or buy insurance without lifting or removing it.

Establishing a credit freeze is widely recommended by experts. The three main credit bureaus with whom to establish a freeze are **Equifax, Experian**, and **TransUnion**. You should contact each of them and follow their instructions to set up the freeze. It is a simple process, and can contribute greatly to your peace of mind.

Masked email addresses

Many web sites and apps ask you to sign in to do business. Perhaps you would rather not provide your email address, to avoid being a permanent target of unwanted email. A number of organizations with whom you may already have a relationship offer a sign-in option that keeps your email address hidden, by substituting an alias address just for the sign-in. These include Google, FaceBook and Twitter — you may have seen their SIGN IN WITH **** icons on sign-in pages. These can be useful, provided that you don't mind the company adding your connection to their data base about you.

When you see a Sign in with Apple button on a participating app or website, it means you can set up an account using your Apple ID. No need to use a social media account, fill out forms, or choose another new password. Sign in with Apple is built from the ground up to respect your privacy and keep you in control of your personal information. It works natively on iOS, macOS, tvOS, and watchOS, and in any browser.

Assign access to online accounts after death

In this digital era, if you die or become incapacitated, it is likely that an executor, fiduciary, personal representative or a family member will want access to your online banking accounts, investment portfolio, social media sites, websites, backups, email, etc. If you have not entrusted someone with the usernames and passwords to such accounts, how will your bills get taken care of? Who will monitor or disable your email or Facebook account? Will social media sites allow them access without a court order?

At a minimum, you should have a document that list all your accounts, logins, passwords, etc., made available upon your death to your survivors.

Digital Legacy

Apple announced a new program that is coming with iOS 15, iPadOS 15, and macOS Monterey. Called Digital Legacy, it basically lets you pass down your information to family and friends if you pass away. You'll be able to add "legacy contacts" to your account. So, when you're gone, they can simply request access, and then your information will be handed over. It is not clear yet how much of the need this will meet.

Written: June, 2021