BASIC COMPUTER STUFF
(SECURITY, BACKUPS, ETC.)

As photographers we all use computers regularly to edit our photos. We rely on them and generally are on them several times a week. Between email, web browsing, photo editing, and content creation we find them more and more important in our daily lives, but we sometimes take for granted that they can be targets for bad actors and also can fail for random reasons.

I have been listening to a podcast on computer security for the past 20 years called “Security Now”. It is hosted by Leo Laporte of the TWIT (This Week In Tech) podcast network and produced and presented by Steve Gibson. Steve Gibson runs Gibson Research Corporation. His “bread and butter” is a software program for hard drive maintenance, performance enhancing and recovery called “Spinrite”. He also coined the term “Spyware” and found the first example of it. His site is grc.com and he offers lots of free utilities including one I think is essential for home computer security called “Shields Up”.

Our first line of defense in our home computer setup is our Internet router. We will start there, but first a little background.

NETWORKING

Networking is conceptualized as layers. The bottom layer is the physical network connection, Ethernet. Ethernet can be either wired or wireless. On top of Ethernet is the Internet layer. This includes Internet Protocol (IP (v4)), ICMP IPsec and other protocols. The next layer is the Transport Layer (with TCP or Telecommunications Protocol being the most recognized, but UDP or Universal Datagram Protocol also being very common). The top layer is the Application Layer. This layer includes DNS (Domain Name System), HTTP (hypertext transport protocol), HTTPS (secure hypertext transport protocol), IMAP (mail), SSH, NNTP, etc. Many people think of the Internet being the same as the World Wide Web but that is far from correct, as it also includes Email, network time servers, file transfers, and many other types of communication.

DNS

DNS or Domain Name System is how you find web sites. When you type “microsoft.com" into your browser it doesn’t actually to to “microsoft.com". Instead it sends a request to a DNS server to look up the IP address for that domain, then directs the browser to that IP address. This all happens behind the scene so you don’t see any of that. There is a whole hierarchy of DNS servers. At the top are the authoritative servers for the top level domains (.com, .gov, .org, etc.). A server lower in the stack will query one of them for a record if either it doesn’t have it, or if it’s copy of the record has expired. All records have a maximum TTL or time to live (generally in the range of hours) so changes can be propagated without excessive delay. DNS queries are send

using UDP which is a broadcast protocol with no guarantee of a connection, so if a reply isn't received in an appropriate amount of time the query must be repeated. Also, the source of the DNS query can be spoofed and the reply will go to someone besides the originator of the request.

TCP over IP (TCP/IP)

TCP over IP, usually TCP/IP is how the World Wide Web connections are created. After the IP address is acquired, the browser sends a SYN (synchronize) packet. The remote server responds with a SYN-ACK (synchronize-acknowledge) packet, then the browser sends the final ACK (acknowledge) packet and the three-way handshake is done and the connection is made. Because of the three way handshake, the IP address of the requesting computer cannot be spoofed or the connection won't complete.

Since our browsers don't show the actual IP address (and we wouldn't be able to understand if they did) bad actors can register domains that look very similar to popular web sites (for example Amazun instead of Amazon). If you aren't paying attention you may end up talking to someone other than who you expect.

ROUTER

A router is basically a device that allows multiple computers, tablets, phones or other devices to share one Internet connection. The router has one basic function that provides us with a lot of protection. When a device requests information from a remote server, the router makes an entry into it's routing table. The IP of the requesting device is replaced with the router's IP and the request is sent out. When the reply is received, it looks up the device that made the request, changes it's IP to that of the requesting device and forwards it to that device. If an un-requested packet comes in, there is no entry in the routing table so the router just drops the packet. This simple action protects us from being accessed by malicious actors. However it does require that the router be properly configured and that we do not ask for malicious content ourselves.

ROUTER SELECTION

There are many brands of consumer routers and most are fine. I personally prefer Netgear since they have had fewer vulnerabilities than some other brands, but I have heard good thinks about ASUS. I do not like Plume, since they make managing the router very difficult. I also am skeptical about Eero since it is owned by Amazon and they are pretty aggressive about collecting private information for marketing purposes, but I don't really know they are doing that with their routers.

ROUTER CONFIGURATION

There are a few settings on your router that are critical to check and some that look important but are not really.

One common suggestion is to disable SSID broadcast. SSID broadcast sends the name of your router out to anyone who pings it. Actually hiding the SSID does little or nothing for your router security.

Check for updates to your router firmware regularly, at least a few times a year, and preferably every month. If you stop getting any firmware updates for a full year, it may indicate that your router is out of support. If so it is probably a good idea to consider replacing it. I would recommend buying a new router every 5 to 10 years. This will keep you with a unit that gets updates, and will also have better performance than your old router.

A critical item is to change the default login for managing the router. You can change the user name (typically defaulted to admin) but the important thing is to change the password, and to use something long and strong. I personally like to use a passphrase instead of a password. It is long, very strong, and much easier to type. Not my actual passphrase, but an example might be "My first car, bought in 1967, was a 1956 Chevy Bel Aire." This has upper and lower case, special characters in the numbers, spaces, commas and period, and numbers. It is 57 characters long, thus VERY strong, but still fairly easy to enter. You probably don't need anything this long, but shoot for at least 25 to 30 characters.

Another very important item is to disable "WAN administration". The LAN is short for the local area network and basically means anything in your house connected to the router. WAN is short for wide area network and basically means the whole Internet. You really have no need to administer your router from outside your house, and this setting potentially allows anyone in the world to change your router settings and probe your network if they find a vulnerability.

Unless you really need it, turn off UPNP. UPNP is short for universal plug and play, and was invented to allow Microsoft X-Box gaming to easily connect two people for playing games together. The UPNP protocol allows something inside your network to open ports on your router to allow unsolicited traffic to a specific end point. If something finds a way into your network and this is enabled, it can allow all it's "friends" to come in also.

Do enable the "guest network". Use it to provide Internet connections to untrusted devices such as smart home lighting, door bell cameras, smart power plugs, streaming video boxes (Roku, Amazon fire stick, etc.). Many of these devices never get security updates and many are not really secure, so keep them isolated from your computers, phones, etc. This may mean that if you want to use your phone to control something you will need to change from your regular home network to the guest network, then switch back again when you need to do something else, but the inconvenience will be worth it.

When your are finished, go to grc.com and run "Shields Up". Pick the "All Service Ports" option to scan ports 0 through 1055. If you suspect a problem with a higher

port you can scan any specific port or range of ports with “User Specified Custom Port Probe”. You can also test for the UPnP status. If all comes back green, that is best. There was no response from your router to the probe. Yellow means that a the router said “this port is closed”. It doesn’t let anyone in, but does confirm that your router exists at that IP address. Red means that the port is open and allows unsolicited incoming packets. That is potentially really bad.

BROWSER SELECTION

There are many different web browsers available, but only three browser engines that they all are based on. By far the most popular with over 80% market share is the Chromium engine which is the basis of Google Chrome, Microsoft Edge, and all other browsers except for Apple Safari (which is based on Web Kit) and Firefox (which is based on it’s own engine). All web sites are optimized for Google Chrome due to it’s dominant position in the browser market, so it would seem to be the best choice. However, there are two problems with that selection. First, if a problem is discovered with the Chromium engine it will affect everything except Safari and Firefox. Because Chromium is so dominant it receives more attention from the bad guys. If they can find a weakness they get a much bigger payday. Second, Google makes it’s money pushing ads. On most web sites, you actually make about 80 connections when you connect to that site, and most of those are for advertising or tracking. About half of the total traffic is advertising related.

I use Firefox with a browser plugin in called Ublock Origin. This plugin blocks known malicious connections and blocks advertising and tracking. However, it will not work with the latest version of Google Chrome. It is not available for Apple Safari, but Apple does other things to make it less necessary.

You can install multiple browsers on your computer, though only one can be the default browser. If I have a problem with a site using Firefox, I will try opening the page in Safari or Chrome if I really want to see it. This doesn’t happen very often but I have occasionally had sites not work in Firefox (fairly rare).

PASSWORD MANAGERS and PASSKEYS

Passwords are a big problem. If a password is easy to type and remember it is not secure. One can even say that if you can type a really long password every time, it isn’t secure. Ideal passwords are long (at least 24 characters) combinations of upper case letters, lower case letters, numbers and special characters (punctuation for example). It is also critical to use a different password for every different login. Since we have so many different logins this makes manual (written paper) lists infeasible. Thus the need for password managers to create these long, random passwords and to remember them for us. There are many different password managers out there. I used Lastpass for a long time and they were good initially, but they got bought by an investor company and suffered a serious breach so I would not recommend them.

There are several that are considered good options such as Keypass and 1Password, but my choice is Bitwarden.

Bitwarden is a free, open source, full featured password manager. It is available as a program for all major operating systems, and as a browser plugin for all major web browsers. By default it stores your passwords in an encrypted vault on their servers. However, the vault is encrypted on your local device before it is sent to Bitwarden so they cannot see anything in the vault. The reason they store it is for synchronization. If you make a change on your phone, then later access the same site from your laptop, the vault will be downloaded and decrypted on your laptop and the change will be available. Basically you see the same sites and passwords from all your devices. The only criteria is that all installations will need to use the same username (email address) and the same master password. The only real weakness from a security standpoint is that you need to create a strong master password to be safe. But, since you will only need to remember two passwords (your computer login password and your Bitwarden password) it shouldn't be too bad. Bitwarden will remember all the rest for you.

Passkeys are the replacement for passwords. Passkeys have been around for a few years but are just now seeing more common adoption. Most sites DO NOT support Passkeys but more are coming all the time. So, what are Passkeys?

Passkeys are a login system using the Public Key - Private Key pair system. Basically, a pair of keys are generated. Anything encrypted with the public key can only be decrypted with the corresponding private key, and vice versa. If something is encrypted with the public key, knowing that key provides no help in decrypting.

Passkeys is a system where the web site stores your public key, then when you try to login it sends a challenge and requires you to encrypt it with your private key and send it back. When the site receives your encrypted response it verifies if the public key can decrypt it. If so, it knows it is you and logs you in. When it works, it is nearly instantaneous and you just have to click a button that says "Login using Passkeys". Bitwarden fully supports Passkeys also.

ANTI-VIRUS SOFTWARE

Steve Gibson's recommendation is to not use any third party anti-virus software, but just use Microsoft Defender on Windows machines. Running third party software increases your "attack surface" and if any vulnerability is found in that software, it has so much access that it can do a lot of damage.

Personally I use Apple products most of the time and I don't run any anti-virus software on them. I also run Linux occasionally and don't use anti-virus software on it either.

SOFTWARE INSTALLED AND DOING UPDATES

It is very important to keep your software up to date. However, never trust links to updates in email or text messages. There are lots of modified versions with malware added and they are promoted via email frequently. If you get an email saying you need to update the software, go to the web site of the publisher and check for updates yourself. You don't necessarily need to install a new version of a program if it is a paid upgrade. By update, I am talking about updates that fix software bugs.

If you have software installed that you are not using and know you will not need in the future it is recommended to uninstall it. Every program on your computer is a potential security weakness so the fewer unnecessary programs the better. This applies to apps on your smart phone also.

EMAIL AND TEXT MESSAGES

Email is one of the major conduits for malware infections today. Text messages are the second. It is recommended that you never open links in email. However, with the complicated URL's in use today it is almost impossible to type them correctly. At a minimum, verify the email sender is who they actually appear to be. In most email programs if you hover your mouse over the sender's name, it will show the actual email sender. At least make sure the "@xxx.com" matches the name of the supposed source. You can also hover over the link and see the actual target of the link. It should also match.

If you receive a suspect email or text message, the best practice is to delete it without ever selecting it. If you select it you will see a preview. The act of previewing the text message or email can be enough to trigger the malware. At a minimum it will potentially allow a tracking pixel to verify that you received the email or message.

BACKUPS

I heard that there are two types of storage drives, those that have failed and those that are getting ready to fail. It doesn't matter if they are spinning magnetic platter drives (the old conventional "hard drive") or solid state drives. They all fail eventually.

The best advice I have seen for computer backups has two important features. First, it should be the "3-2-1" backup strategy. This means at least three copies of all data, at least two different backup media or types, and at least one copy off-site. One example would be to back up your files to a local hard drive, and also use a cloud backup solution. Another would be to have two backup drives and keep one at a friend's house or in your safe deposit box.

Secondly, backups should be automatic. If you have to backup manually, you will inevitably be busy and forget to do it for days at a time. When you finally have a failure of your computer storage drive, your backups will be sadly out of date.

Lastly, ransomeware will scan all your connected drives and encrypt your backups along with your main drive, so it is critical that you have at least one backup off-line and not accessible by your computer.

If you keep backup drives off-line, you should store your backup drives in a cool and dry environment, especially solid state drives. When stored in a hot environment SSD's can very quickly become unreadable (even sooner than conventional hard drives). Even with proper storage, the SSD will need to be rewritten at least every few years.

RAID and NAS

A RAID is a Redundant Array of Inexpensive Disks. Basically it is a collection of two or more disks that look like a single drive to the computer. There are many different types of RAID called "levels". For data protection use Raid 1, 5, 6 or 10. Raid 0 is also called "scary RAID" because it writes half of each file to a different disk to increase speed, but if one disk fails you loose all your data - not good.

NAS is Network Attached Storage. It is generally a RAID with an Ethernet port attached directly to your router so that all the computers on the network can access it (if permissions are granted to do so). It is an excellent option for backup due to the redundancy it can offer. If set up as RAID 5 or 6, it offers single or dual drive redundancy, meaning a drive (or two) can fail and all your data is still safe. The disadvantage is that you loose some of the storage capacity. If you have RAID 5 with four 2TB drives you will get 6TB of storage (2TB times 3). If you set up RAID 6 with dual drive redundancy you will get 4TB capacity (2TB times 2). Of course, larger drives means more capacity for any given RAID configuration.

PHONE - BATTERY LIFE AND UPGRADING

Since your phone is on the same network at home as your computer, we need to consider the security of the phone as much as your computer. First line of defense is to keep your phone operating system and software up to date. Also, consider removing all the apps you no longer use or need.

If you are having problems with your phone battery lasting all day, consider uninstalling the Meta apps (Facebook, Instagram, What's App, etc.). They are known battery hogs and will drain your battery faster even if not being actively used.

I have a plan for upgrading my phone. Whenever it won't update to the latest operating system version, I plan to replace it within one to two years. I know the older operating system version will receive security updates for at least one or two versions old, but generally not for versions older than that. I look at the rumors of new features and decide if I want to get the newest phone, or save a little money and get one version older.