Care and Feeding of Your Digital Life

Below are some suggestions for managing the safety and security of your digital life. You likely know nearly all of this – still, it might be worth revisiting – so have some patience with me and read on. A little prevention goes a long way in having a trouble-free modern tech-saturated existence. Am I paranoid and is this list overkill? Absolutely – until a device loss, crash, infection or identity theft causes you discomfort. Stay ahead of the bad luck and the bad people – and here's a short laundry list of how:

Backup, backup and BACK UP

TimeMachine is Apple's built-in backup program. Two of the best features: it is free, and it creates a complete backup of your entire Mac automatically. All you'll need is a spare hard drive accessible to your Mac and to turn TimeMachine on. Large capacity USB hard drives sell well under $100. Check to see your TimeMachine (TM) hard drive is plugged in every few weeks, if not daily. The TM System Preference displays the most recent backup. PLEASE do NOT rely on an iCloud backup as your sole emergency parachute – nothing is as reliable as a complete LOCAL backup of your data.

Other Apple devices can be backed up to your computer, too. Using iTunes or the Finder to back up an iPhone, iPod or iPad – *locally to your computer* and frequently -- is easy. Do you have a website that matters? Download the pages, images, database and content for backup or have your developer provide you annual backups.

If TM isn't your preferred option, consider CarbonCopyCloner, SuperDuper or similar utilities to clone your hard drive. Computer fact-of-life: drives die, all electronics die, and almost always at an inconvenient moment. Rebuilding a Mac drive or recovering an iPhone from a backup takes an hour or two. Recovering all of your data, settings, and even applications from scratch can take many hours; sometimes it is impossible. A backup is your data's best friend – and far cheaper than paying for data recovery.

Have those backups been running for several years? If that backup drive is getting long-in-the-tooth, retire it. We recommend replacing whatever is used for your automated computer backups every year or two with a fresh drive. Label, ziplock, and place the old drive securely in your fire safe or safety deposit box. Plug in the new drive, train TM to start over using this new drive, and let TM do its thing. One large drive can service multiple Macs. When current TM drives are not in use, store them in the firesafe with other vital items.* [*This has the drawback of you, dear user, forgetting to occasionally letting TM run it's updates – set a repeating update reminder in your Calendar.]

What, you're NOT backing up your computer? Please start today. It's cheap and easy with TimeMachine. Data recovery runs $90/hr or more from most firms. [Windows and

Linux folk: *Acronis* or *Clonezilla* are terrific, or learn to use *File Histor*y and/or *Windows Backup and Restore*]. One dead hard drive (or cryptovirus) will ruin more than your day.

Keep it Current

Your Operating System (OS) runs everything on your computer. It's not perfect. Squashed bugs, security updates and even new features are usually part of a System Update. As a rule, applying updates are worthwhile.

Every month or two: After your system is fully backed up, check for System Updates (using the System Preferences/Settings, depending on your OS version) only apply updates within your current OS version, not upgrades. If you are NOT making frequent backups, please read the section above on backups.

System UPGRADES are another matter – check with your IT team or specialist to determine if a System upgrade is appropriate for your needs -- and will not cripple existing tools you use. If you are planning a System Upgrade (e.g., going from Mac OS10.14 Mojave to OS11/Big Sur or Windows 7 Pro to Windows 11), determine what versions of your favorite applications/programs will run on the newer version, and budget accordingly. Note, there are many 'free' versions of productivity software to consider as alternatives. Older vintage System versions **may** require upgrades to run newer browsers for current security certificates, or other desired features. *Note: all hardware will eventually reach a cap on what version of operating system can run on it.*

iOS and portable devices (iPhone, iPad, iPod, AppleTV, & AppleWatch) each have their own OS. Just like larger computers, these devices usually benefit from an update, but go slow on upgrades – let someone else be the 'early adopter' guinea pig. Upgrades may cripple older software/apps you use – research before Upgrades.

Likewise, check your frequently used Applications for updates, and apply. Most have a selection under their File, Preference or Help menus, or on an 'About' screen (e.g., under the *MS Office* **Help** menu, there is 'Check for Updates'; or under the *About Firefox* menu, this browser automatically checks for updates). The App store will update purchased items.

Trust, but Verify

Don't trust any received email with a link to a website unless you specifically requested one. Make it a habit to visit each website manually or use a trusted source (Contacts or AddressBook and Bookmarks). Similarly, eMail spoofing is so common that no unexpected email with an attachment should be believed. If you do receive an attachment from a 'known source', avoid opening the file until you've confirmed that trusted source has sent it. The 'reply address' may be forged, or the sender's account may have been hacked.

While Macs are far less vulnerable to virus threats, historically they have not been completely immune. They can also act as ‘carriers’, a threat included as an email attachment or other shared file with users of other OS systems. Just like washing hands, it’s socially prudent to consider some kind of antivirus tools such as Malwarebytes or Avast to test systems and files periodically. Mobile devices such as iPhones and iPads are less vulnerable, but that does not mean some future threat won’t arise. Practice good app and file hygiene awareness.

How else to practice awareness? When surfing the web, if a pop-up window tells you to update a piece of software to view a feature or an ad states your computer needs Flash, is ‘compromised’, requires ‘routine maintenance’, or is ‘running slow’ and you should download some software, **do NOT**. Certain online ads for software that will ‘optimize’, ‘speed up’ or ‘clean your Mac’ may not just take your money and do nothing for you, but also install Adware or worse. Be VERY careful what ‘free’ programs you download. Nearly all computer infections are due to such scam popups, ads or aforementioned email attachments. ANY computer is vulnerable if the user installs software directly.

Can’t make a popup ad or fake warning go away on a browser? Quit or Force-Quit the browser (Control-click on the browser icon in the Dock, then hold the Option key while selecting Force Quit). If you suspect you actually do need to update the likes of Java or anything else, go to your System Preferences, select Java and use the update tab –or visit the software publisher’s website and download the update manually for your OS version. Note: Adobe retired Flash in 2019 and recommends fully removing it from all devices.

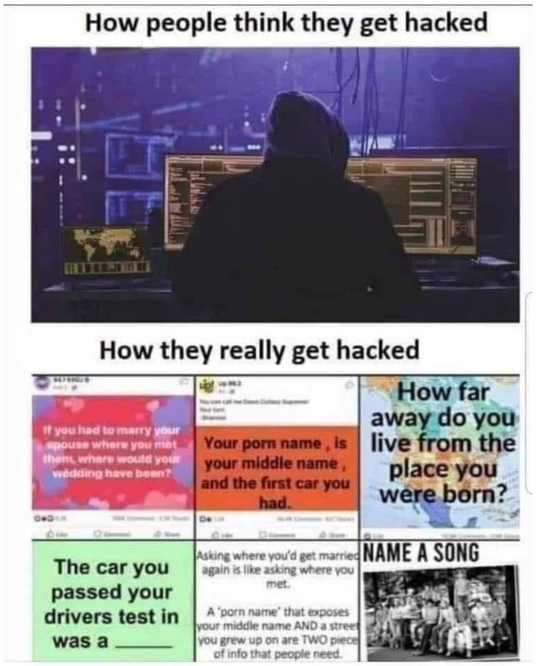
Change is Good

Change login passwords routinely. This should include account or settings access for all computers, tablets, phones, and any other Internet-connected device (thermostats, smart appliances, security systems, home network routers, VoIP/Ooma devices, baby monitors, gaming consoles, TV streaming devices/AppleTV/Roku/Firestick, ATM cards and anything I’ve forgotten here. Even if it’s a 4-digit pin, just do it. Note that EACH password should be unique to a device or account – avoid recycling or reuse.

Why change your passwords? Identity theft and online fraud are now multi-billion-dollar industries. The criminals that perpetrate these acts purchase databases from other bad actors who collect and build them from insecure computer networks and companies. They scour the web for information about you to build a ‘profile’ – remember that online quiz that asked if you could remember your first car, your favorite holiday, or what was the Top-40 song when you graduated? Great – the bad guys know a few potential security question answers now, too. Anything you post on social media, the public neighborhood list serve, discussion and product forums, public shopping site comment sections – anything that is public is potentially problematic.

These profile databases detail user information, particularly a user's name, known addresses, email accounts, common user IDs, telephone numbers, Social Security Numbers, Drivers Licenses, known online accounts (for anything), answers to security questions (favorite color, mother's maiden name, first school, street you grew up on, etc.) and of course account passwords.

The databases are used to test access to websites and accounts with other companies – and if a combination is found, the miscreants will compromise the account to exploit it.


How people think they get hacked
How they really get hacked
If you had to marry your spouse where you met them, where would your wedding have been?
Your porn name , is your middle name , and the first car you had.
How far away do you live from the place you were born?
The car you passed your drivers test in was a ______
Asking where you'd get married again is like asking where you met.
A 'porn name' that exposes your middle name AND a street you grew up on are TWO pieces of info that people need.
NAME A SONG

What's a good password? Some say it should be 10-16 characters minimum, with a mix of upper-case, lower-case, special symbols and numbers. Your choices really depend on what the password is protecting - a local or an online account – and what the website or application allows.

How often? For accounts that matter, at least annually. Typical Internet accounts:

> **eMail** (use of SSL connections when available), **FTP** and **Webhosting Banking, Investing** & **Medical** & **Utility** companies.
>
> **iCloud** / **iTunes**, **Dropbox, OneDrive, GoogleDrive** and other cloud storage.
>
> Other companies wherein service disruption, identity theft or impersonation would be a headache -- **Paypal** / **Ebay** / **Amazon / Facebook / Indeed / Nextdoor /** other sites if CC or address books and personal data is stored.

'Ahem,' you say, 'keeping track of dozens or hundreds of passwords is – a crazy nightmare?' Yes – but even a printed list of them stored in your fire safe is far superior to the best of memories – or one relying on a simple handful for your online life.

Applications such as the built-in **Keychain** in the Apple ecosystem, **1Password, Avast Passwords**, **Dashlane** and others are handy tools for storing passwords on Macs, iPads, iPods and iPhones. Websites such as MacWorld are reliable sources for researching password manager software features for your best solution. Some of these software tools allow for a shared database among all devices, allowing all of your Macs and iPhones/iPads access.

Along with passwords, consider recording serial numbers, version numbers and specs for all of your software and hardware. Is cataloguing non-computer information useful? Car VINs, the models and serials of tools, appliances, paint codes, personal book and entertainment libraries, etc. for insurance? Some will create a detailed video tour of their home, property and possessions for insurance needs. Print out an updated paper copy every year for that fire safe. (Simple fire safes are $20 at stores like Lowe's.)

What happens if you become incapacitated or pass away? Heirs to your estate may need your access list to monitor or close accounts, or at the very least the unlock key to your password manager – so consider how to have that privately accessible from your attorney or in your Will. A current list of all relevant accounts, userIDs, URLs, phone numbers, passwords, etc. are a great addition for the Executor of your estate, too. Even unlocking electronic devices (e.g., turning off Find My features on Apple products) before erasing, reformatting and selling/donating away requires your admin password access.

'Never Say Never' was just a movie

Never trust a phone call purporting to be from a family member in need of money wired to them or a service provider 'helping' with your business, mortgage, or credit card debt. Educate yourself about common phone scams (Rachael from Cardholder Services, Sally from Google placement, your car warranty, a 'nephew stranded in Italy'). That Nigerian Prince is really a scruffy jerk living in his mom's basement. No, really, he is.

Never give out a SSN, Driver's License, Military or Student ID, account numbers or ANY personal information unless YOU have called a known party and you expect they need it for an existing account. We'd like to believe this is 'obvious', but anyone can be caught off-guard and slip up. The Government, Banks, Hospitals, etc. will never CALL YOU and ask for your SSN or credit card/bank account or routing number. Hang up and call the agency back at their known published number (from an account statement or trusted government resource). If the 'IRS' calls, it's not really them. No legitimate agency takes gift cards as a form of payment.

Never blindly pay an unexpected bill for a service or subscription renewal.   E.g., one common scam in the Internet hosting world is an advertisement that looks like an invoice for SEO rankings, domain registration renewal or hosting. Put an alert in your Calendar for recurring bill renewals and complete them online ahead of any expiration dates.

Never use a public computer for private needs – some computers harbor infections that record the screens visited or your keystrokes to harvest login information.

Account takeover fraud is rising fast – other ways to protect oneself:

https://www.usatoday.com/story/money/personalfinance/2017/11/18/this-type-of-fraud-is-rising-frighteningly-fast-heres-how-to-protect-yourself/107704222/

An Ounce of Prevention…

Do you read over your monthly account statements? If not, this might be the easiest way to nip fraud before it does massive harm later. Many miscreants will run test charges on compromised accounts for a small amount to test the waters and wait a few weeks or months. Reviewing your account activity is *situational awareness* – a few minutes each month may save a few years of credit repair or reputational redemption.

Do your financial institutions offer free text and/or email notifications whenever the accounts sees activity? What a handy way to keep tabs on those accounts. Have you reviewed your credit report this year? Download a free credit check report from www.annualcreditreport.com and review it for errors. It's also wise to review your Social Security statement annually, https://www.ssa.gov/ .

https://www.fool.com/credit-cards/2017/09/14/worried-about-the-equifax-data-breach-heres-how-to.aspx

Within the above article about the Equifax data breach of 2017, the salient part is the contact information from the big three credit reporting agencies. The links below visit the pages to 'freeze' your credit reporting for free. Links may change with time – search online for current sources.

To freeze your credit for free, contact each of the three major credit bureaus directly:

- **Equifax** -- 1-800-349-9960 or https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
- **Experian** -- 1-888-397-3742 or https://www.experian.com/freeze/center.html
- **TransUnion** -- 1-888-909-8872 or https://www.transunion.com/credit-freeze/place-credit-freeze2

https://www.fool.com/personal-finance/2017/09/27/how-to-protect-yourself-against-identity-theft.aspx

Luckily, identity theft is not usually the case when folks see an errant charge on a credit card. Most mistakes and issues can be solved by calling the bank that owns the card – ask them about a questioned charge. If it's sketchy but not Identity Theft, request a fresh card with a new number. However, if you believe you are experiencing Identity Theft, here's a good place to start:

https://identitytheft.gov

How else can you protect yourself? Many services online or on the phone now offer 'Two-Factor Authentication', or 2FA. This means not only do you have to provide the proper User or Login name and password, but a separate device will be used to reach you with a special code, such as a telephone call to your known number, an email to the account on your profile, or a text to your smart phone.

Make use of 2FA where offered: your banks and other financial accounts, your medical accounts, at-work accounts, your employment benefits accounts, your government accounts (US Treasury, IRS, SSA, DOR, DOT or any other federal, state or local agency that you use), your life-insurance company website, your digital payment solutions such as ApplePay, PayPal, Venmo, Adyen, Azimo, CirclePay, Intuit, Level Up, Lightspeed, Sage, Samsung Pay, Zelle or the dozens of others. And probably your social media accounts of MySpace, Facebook, Nextdoor, Twitter, Instagram, Snapchat or any online forums group where someone impersonating you could steal your identity or cause reputational harm.

Are all these warnings overly paranoid about security? Only until it happens to you.

And finally, teach your family and friends – share how to protect themselves.

Safe computing, everyone!
Paul Vail -- AfterHoursConsulting.org
paul@AfterHoursConsulting.org – 919-271-7479