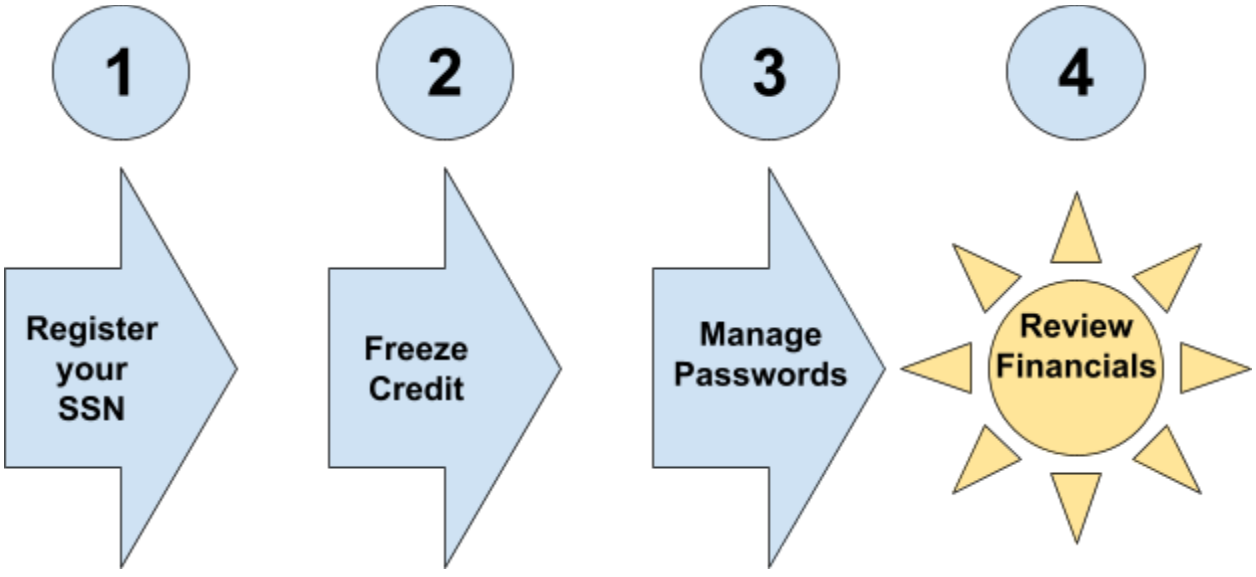
JACK's SECURITY & FRAUD GUIDELINES

http://bit.ly/34FnIYb

Disclaimer: This content is intermittently updated, and every effort is made for accuracy. It's more of a technical reference than an essay for end users. Send questions to security@leadershipbynumbers.com, and I'll answer as I am able.

TABLE OF CONTENTS

Provided below is an action checklist that will minimize the risk from identity theft and prevent compromised financials.



SOCIAL SECURITY

Register your on-line access with Social Security, as that's the best way to ensure no one does it before you do. Because this registration process relies on a credit check, it's important to have it completed before freezing credit.

- Social Security
  http://www.ssa.gov/myaccount/

FREEZE CREDIT ON ALL FOUR AGENCIES:

The ***cornerstone*** of protecting against identity theft is freezing credit access. Credit freezes are frequently viewed as the most effective way to prevent financial identity theft. By freezing credit, no one can open a bank account in your name, or take out a loan. Frozen credit ensures your identity has no financial value to a thief.

However, freezing credit is not without detractors. For instance, the OPM will provide monitoring for federal employees identified in their massive data breach. The free monitoring, though, requires that credit remains open.

Here's the summary recommendation from security analyst, Brian Krebs, for freezing credit checks:

> If you have **already** been victimized by identity theft (fraud involving existing credit or debit cards is *not* identity theft), it might be worth signing up for these credit monitoring and repair services. *Otherwise, I'd strongly advise my US readers to consider freezing their credit files at the major credit bureaus.*

"In ITRC's opinion, a freeze is the best form of financial identity theft protection currently available. . . " (http://www.idtheftcenter.org/Fact-Sheets/fs-124.html)

Reference:
http://uspirg.org/reports/usf/why-you-should-get-security-freezes-your-information-stolen
http://krebsonsecurity.com/2015/06/how-i-learned-to-stop-worrying-and-embrace-the-security-freeze/
https://www.chexsystems.com
https://consumersunion.org/research/frequently_asked_questions_about_security_freeze/
http://www.consumerprotect.com/protect-against-identity-theft/
http://www.nytimes.com/pages/your-money/identity-theft/index.html
https://en.wikipedia.org/wiki/Credit_freeze

A few caveats about credit freezing:

- There may be a one-time, per-agency, charge of around ten dollars to apply the freeze. The rates vary by state.

- Most of the agencies will give you a PIN or require a passcode. **Be sure to have it safely recorded.**
- Once the credit is frozen, it can be temporarily unfrozen, without a charge. To lift a freeze, you access your individual agency accounts to select one of several choices (depending on the agency).
    - Temporarily lift the freeze for a specific duration.
    - Temporarily lift the freeze for a specific duration, and require a passcode.
    - Lift the freeze for an indeterminate time, and then return to the account to have it frozen.

Does locking credit hurt your credit score ?

No.

In fact, your FICO score can be lessened by too many “hard” credit inquiries.
http://www.investopedia.com/terms/h/hard-inquiry.asp
http://www.myfico.com/credit-education/credit-checks/credit-report-inquiries/

For example:

If I have frozen my credit on all four agencies, I’ll need to lift it to apply for a new credit card, car, mortgage or even a job application. Usually, I’ll ask which credit agency is being referenced. Then, I’ll go online to the agency (say, Transunion), return to my account and lift the freeze for a week. I’ll contact the requester (e.g., for a car loan) and let them know my credit is ready to be checked.

Is this a big hassle ? Absolutely. But, think of the alternative--your SSN can be assumed to be widely distributed. With minimum effort, your identity can be compromised, and health bills, unknown credit cards, loans, etc can all be created under your name. **When you lock your credit, you turn the valuation of your identity to zero, on a need-to-know basis.**

Here are the links for freezing your account with the major credit agencies. Or, you can do it old-school with postal mail:

Equifax:
https://www.equifax.com/personal/credit-report-services/credit-freeze/

Transunion:

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

Experian:

http://www.experian.com/freeze

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

PASSWORD MANAGEMENT:

Password management is a significant concern, because there are many different on-line sites that contain financial or personally sensitive information. Unique and difficult passwords are required for each one. There are several commercial offerings.

Use a password manager.

- https://thewirecutter.com/reviews/best-password-managers/ Pick one, use it.
    - I've been using LastPass (w/2FA), but am now considering other options (https://infosec.exchange/@epixoip/109585049354200263, https://www.forbes.com/sites/barrycollins/2022/12/29/leaving-lastpass-heres-where-to-go-next/?sh=430f93fb3974).

- **UNIQUE PASSWORDS:** In other words, choosing to ***avoid*** password management usually indicates that a few passwords are used repeatedly for many sites. Once a password is compromised for one site, then it can be tried out on all your other known sites. Because a browser contains a readable trail of your history (using cookies), it's not difficult to sift out your frequented sites.

  Some websites are moving proactively, and insisting on measures that reduce identical passwords being used across multiple accounts. (http://krebsonsecurity.com/2016/06/password-re-user-get-to-get-busy/)

  Relying on a Password Manager encourages uniqueness, as most Password Managers will provide suggestions and analysis for appropriate password use. They will notify the account holder if duplicate passwords are being used across multiple sites, or if the password is too simple.

  Let's put this into perspective. The odds are, at least one of your online accounts has been compromised, and your authentication details are known. Check https://haveibeenpwned.com/ .

  A Google funded study has demonstrated that data breaches have exposed millions of accounts. No matter how complicated the password, having a single password for all accounts guarantees a security compromise.

  > "... credential leaks pose a broader risk to the online ecosystem due to weak password selection and re-use...Das et al. examined the password strategies for users who appeared in multiple credential leaks and estimated 43% of

passwords were re-used, while Wash et al. found users re-used 31% of their passwords…."

https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/46437.pdf

UNICODE PROTECTION: There is a second use of password managers--they will automatically serve up the credentials on a matched website. For instance, if I have an account with Apple, my name and password will be presented at the web site by the password manager. Some sites are fake, and they look authentic because they rely on unicode.

Look at https://www.xn--80ak6aa92e.com/

UPDATE: fixed in Chrome, but not in Firefox.

By relying on a password manager to administer the credentials input, I'm assured that only a correctly matched URL will receive an account and password.

- **MINIMIZE FEDERATED TRUSTS.** Vendors would prefer that you use federated trusts between their sites to make it simpler in tracking your behavior. I use Google sign-in only for Google services, not to authenticate to other sites (e.g., Feedly). By using a Password Manager, I can easily rely on unique identifiers and passcodes for each site.

ADDITIONAL REFERENCES:

https://www.m3aawg.org/Password-Managers-BP

PHISHING PROTECTION:

A compromise to a workstation or device OS can easily occur when accessing compromised Internet sites. A popular means for compromising your mail account is to redirect you to a fake Google login site. https://www.wordfence.com/blog/2017/01/gmail-phishing-data-uri/

Here are the recommended protections against phishing:

HTTPS

Learn to recognize when a valid HTTPS connection is in use.

DNS FILTERING

DNS filtering is probably the most effective defense, as it will block access to suspicious sites.

OpenDNS/Cisco filters all queries for content, and can be configured on home routers and workstations.

- https://www.opendns.com/home-internet-security/

  OpenDNS provides a free home version

SafeDNS

- https://www.safedns.com/

  Commercial

Google DNS

- https://developers.google.com/speed/public-dns/

  Free home use

Norton

- https://dns.norton.com/

  Free home use

TWO-FACTOR AUTHENTICATION (2FA)

Take a minute and think of all the financial information, medical sites, and personal, on-line, resources that require your email address for authentication. Most of them, right ? Now, how do these sites accommodate a user who happens to forget their password to one of these accounts ? They send a reset link to the email address. If your email is compromised, then in very short order, you'll find all your account passwords have been reset--and you will be locked out.

2FA protects your email.

Adding Two-Factor authentication requires the integration of a trusted device which can supply a one-time secure token. This means that alongside with a password, a one-time use token is required. It's an extra step, but effective. In the event that your account password is compromised, the hacker will also need to physically access your device.

In my personal usage, I installed Google Authenticator on my smartphone for my email authentication.

I love everything about 2FA except …. many users will find it cumbersome.

https://krebsonsecurity.com/2017/08/is-your-mobile-carrier-your-weakest-link/

Google offers this service (no cost), as the Google Authenticator app and it is integrated into their application suite.

Microsoft can also integrate with the Google Authenticator application

- https://www.google.com/landing/2step/

DNS

DNS filtering was reviewed under protection against phishing. But, there are other DNS options.

ANONYMOUS DNS

It's common practice for ISPs to track all DNS queries. Basically, it means that all of your Internet activity is being logged, tracked, and then packaged for analysis by retailers, et al. If you want to minimize your web presence, then change your DNS servers to https://1.1.1.1

DNS PROTECTION

If you own a URL, then it's possible to be attacked with DoS and other DNS specific manipulations. https://www.cloudflare.com/galileo/ will provide protection on behalf of the arts, human rights, civil society, or democracy, at no cost.

FINANCIAL MANAGERS

It's essential to monitor the activity of all financial investments. The simplest method is to use a financial manager, and have one dashboard view for all of your different accounts, etc.

- Mint or Personal Capital
  https://www.mint.com/
  https://www.personalcapital.com

RESTRICTING FINANCIAL TRANSFERS

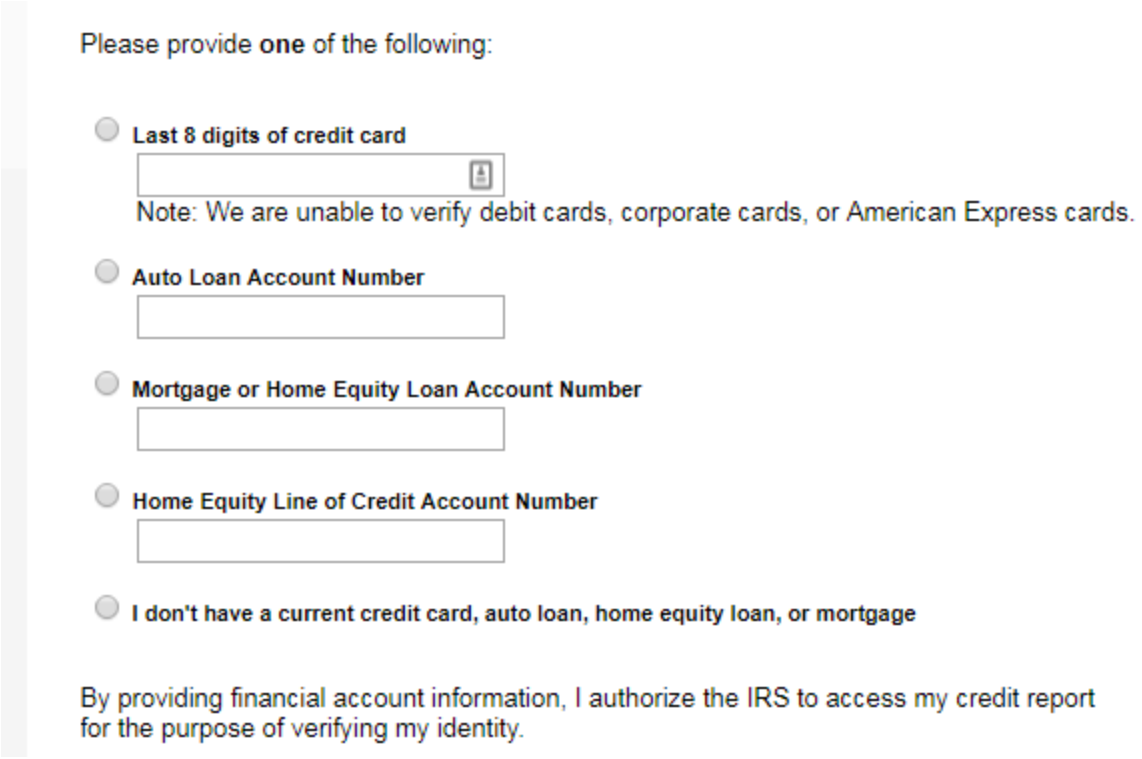
https://thefinancebuff.com/brokerage-account-acats-transfer-fraud.html

https://thefinancebuff.com/fidelity-proof-of-funds-balance-confirmation.html

IRS

It's important that you own access to your IRS account.

https://www.irs.gov/payments/view-your-tax-account



MANUAL PASSWORD MANAGEMENT

It's not always possible to use a password manager (like LastPass) to assist in creating and tracking the use of a passcode. I recommend the application of a "compound" password, that makes it simpler to remember a complex value and to still support scheduled changes. I use compound passwords for system access to workstations, devices, etc.

- Compound Password (http://web.archive.org/web/20090210142452/http://www.leadershipbynumbers.com/MS.nsf/d6plinks/BMMA-5UW4GP)

ROBO-CALLS

Once robo-calls were merely a nuisance that would ruin dinner time. Don't answer.

1. Register your number as do-not-call: https://www.donotcall.gov/confirm/Conf.aspx
2. NEVER SAY 'YES': If you do answer the suspicious call, or respond to a voice message from an unsolicited caller, do not answer "yes" or offer any personal information during the conversation.
3. Install an app: https://moneyish.com/ish/heres-why-youre-getting-so-many-spam-phone-calls/

PERSONAL EMAIL

Use Gmail (https://myaccount.google.com), and set up with two-factor authentication and accept text alerts for odd logins, etc. Gmail has strong security features that can be easily configured.

Microsoft has similar security levels (https://account.live.com/Activity)

For whatever reason, a truly secure email is required, the steps are more complex. Hidester has a solid overview: https://hidester.com/blog/how-create-anonymous-email-account/

DEVICE AND CELL PHONE MANAGEMENT

ENCRYPT DEVICE

After applying an access password, any device should be fully encrypted. This means that all data-at-rest is encrypted. On most devices, if the device is compromised and reset to factory defaults then it is effectively wiped. For maximum security, do not use a fingerprint mechanism.

http://jolt.law.harvard.edu/digest/telecommunications/court-rules-police-may-compel-suspects-to-unlock-fingerprint-protected-smartphones

- Phone passwords are entitled to protection under the Fifth Amendment's promise that no person "shall be compelled in any criminal case to be a witness against himself."
- Fingerprint protection does not qualify for the Fifth Amendment privilege. Producing a fingerprint does not require the communication of knowledge, but is rather analogous to being ordered to produce a DNA sample or a key, which is constitutionally permissible.

VPN

ProtonVPN - Unlimited Free VPN made by ProtonMail
https://play.google.com/store/apps/details?id=com.protonvpn.android

CELL CARRIERS

1. Secure your cell phone

Make sure the password, unique pin, and security codes are long, secure, and unique. It turns out that I had treated my own account like any other utility (i.e. a gas bill) where I should have been treating it like my most valuable financial account.

2. Call your carrier and set up “a port freeze”

From the Coinbase blog (and they know a thing or two about hackers):

Call your cell phone provider and set up a PIN or password, ask for a port freeze and ask to lock your account to your current SIM. Not all providers will do all of those things. If yours won’t, consider changing to one that will.

It took two attempts to do this with my carrier, it’s definitely not one of their common requests.

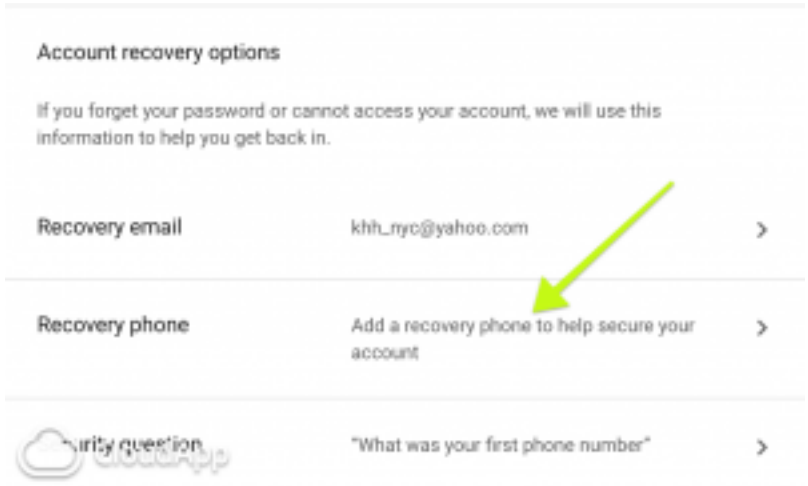
3. Update your 2-factor authentication away from SMS

Many accounts let you use a non-SMS based authentication, with Google Authenticator being the most popular. This helps sever the links between your cell phone number and your accounts.

4. Disable SMS-password recovery on your email accounts

Once again, this severs the link between your phone and your email account. Go to your:

Google account settings -> Sign in & Security -> Recovery phone



Remove any cell phones from the recovery options

https://radreads.co/protect-your-accounts-using-a-port-freeze/

BROWSERS:

Current versions of Edge and Chrome are the most secure, with each tab isolated in a distinct memory segment.

CHROME ADD-INs:

Security and privacy are usually different sides of the same coin. Here are several recommendations, but note that occasionally there will be sites that won't load unless the add-in is temporarily disabled.

Ad Block
https://chrome.google.com/webstore/detail/adblock/gighmmpiobklfepjocnamgkkbiglidom

HTTPS
https://www.eff.org/https-everywhere
Many sites actually have https (for encrypted connections) but do not default to it. This add-in will attempt to default to a secure connection whenever possible.

Privacy Badger
https://www.eff.org/privacybadger
Terrific tool for blocking sites from reading where you've been. You can test the utility of this add-on with https://panopticlick.eff.org

- This add-on is terrific for blocking most tracking technologies. There is a caveat: lots of

legitimate sites rely on tracking, as you select choices or move around to different pages on a site. If you find that, for example, your banking site doesn't seem to be accepting your inputs, then you likely need to provide an exception to that domain.
- Unfortunately, it's very, very difficult to completely remove any identifying trace of your presence. A fingerprint of your browser can be built from several different exposed parameters. So, if you are trying to be invisible to the Internet, these tools are not sufficient.

OPERATING SYSTEMS:

Linux, and OS X are statistically less attractive targets than is Windows. Additionally, Linux and OS X have more security safeguards and can be secured at a lower cost. All modern Linux versions support automatic and free security patching. Windows 11 is the most secure Microsoft version.

AntiVirus

AntiVirus (A/V) software is not likely to ensure the prophylactic protection that is promised.

- The addition of AV software frequently introduces new vulnerabilities, because it is installed throughout the OS, monitoring as much activity as possible.
- AV software increases application failures
- AV software increases system latency, creating a poorly responsive system.
- AV software is primarily effective against signature based malware that has already been identified. Windows Powershell attacks are especially difficult to prevent.

https://arstechnica.com/information-technology/2017/01/antivirus-is-bad/

https://www.scmagazine.com/hackers-hide-base64-encoded-powershell-scripts-on-pastebin/article/579321/

https://www.scmagazine.com/hackers-hide-base64-encoded-powershell-scripts-on-pastebin/article/579321

Virus Removal

After an infection, there are tools which may be successful for removing the infection.

https://www.av-test.org/en/news/news-single-view/put-to-the-test-for-12-months-this-is-how-well-security-packages-and-special-tools-help-after-an-at/

Ransomware

In some instances, it may be possible to remove ransomware.

https://www.nomoreransom.org/

RATING DEVICE SECURITY

https://foundation.mozilla.org/en/privacynotincluded/

SMALL ORGANIZATION RECOMMENDATIONS

https://www.belfercenter.org/cyberplaybook

PRIVACY

Doxxing is a difficult activity to block (and deserves its own section), here's a starting outline: https://www.infoworld.com/article/3168318/how-to-scrub-your-private-data-from-people-finder-sites.html

ANONYMITY GUIDELINES FOR EVENTS & INTERNET

https://docs.google.com/document/d/1615pZB11BhsR0KtvyiXfzfMUBlxZi47HzzhWHIRpxwU/edit

FRAUD

Identity Theft Resource Center https://www.idtheftcenter.org/ is the default, go-to, site for dealing with identity theft and fraud.

MEDICAL FRAUD

It's important to generally monitor the notices and bills received from insurers and providers and contact them immediately about anything suspicious. For Medicare see https://smpresource.org/you-can-help/read-your-medicare-statements/

- Go to the FTC's identity theft site to learn about next steps and file an identity theft report, if appropriate.
- If someone has used your name, contact every provider who may have been involved and ask for a copy of your medical records, then report any errors to your medical providers.
- Notify your health plan's fraud department and send a copy of the FTC identity theft report.

- File free fraud alerts with the three major credit reporting agencies and get free credit reports from them.
- Consider filing a police report. If your health plan offers free credit or identity theft monitoring following a breach, take advantage of it.

“It’s best to proceed as if your data has been compromised and will be for sale,” said Velasquez, whose organization offers free assistance in recovering from identity theft. “Don’t be afraid to ask for help.”

MEDICARE FRAUD

https://www.medicareinteractive.org/get-answers/medicare-fraud-and-abuse

https://smpresource.org/

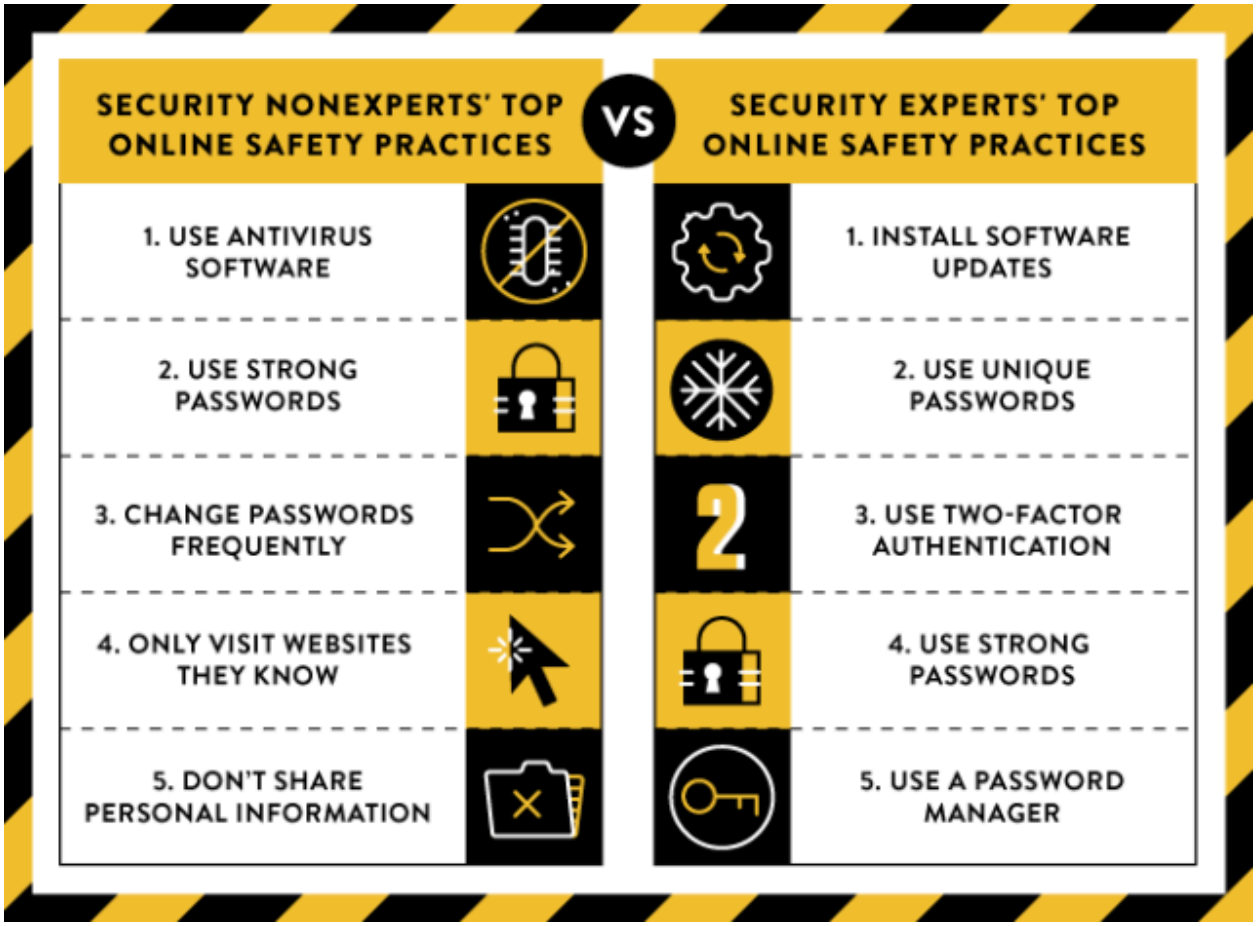
To report fraud, contact 1-800-MEDICARE (633-4227), the Senior Medicare Patrol (SMP) Resource Center (877-808-2468), or the Inspector General’s fraud hotline at 1-800-HHS-TIPS (447-8477). Medicare will not use your name while investigating if you do not want it to.

REFERENCES:

Password creation patterns
https://www.usenix.org/system/files/conference/soups2015/soups15-paper-ur.pdf

Google Research on difference between security pros and consumers
https://www.usenix.org/system/files/conference/soups2015/soups15-paper-ion.pdf

National Cybersecurity Alliance
https://staysafeonline.org/resources/



Personal Accounts are worth ~$20
http://qz.com/460482/heres-what-your-stolen-identity-goes-for-on-the-internets-black-market/

> Prices for stolen identities vary based on factors like quality, reliability, robustness, and the seller's reputation. The most expensive fullz we examined, from a vendor called "OsamaBinFraudin," was listed at $454.05. The vendor explained in the listing that this was a premium identity with a high credit score. . .

https://www.av-test.org/en/
The AV-TEST Institute is a leading international and independent service provider in the fields of IT security and anti-virus research.

Dial One for Scam: A Large-Scale Analysis of Technical Support Scams
https://www.internetsociety.org/doc/dial-one-scam-large-scale-analysis-technical-support-scams

US-CERT TIPS
https://www.us-cert.gov/ncas/tips

> Avoiding Social Engineering and Phishing Attacks
> https://www.us-cert.gov/ncas/tips/ST04-014

NIST Special Publication 800-63B, Digital Identity Guidelines, Authentication and Lifecycle Management
https://pages.nist.gov/800-63-3/sp800-63b.html