THE GEEK PROFESSOR®

Protecting your Identity – Online

STEP 1: PROTECT YOUR PRIVATE ACCOUNTS

Account safety

- Password systems for low-security sites
- Password encryption for important sites
- LOG OUT or use Incognito mode.

Phone/laptop safety

- Use a pin or pattern lock
- Be careful what you install
- Use alternate software or just don't use it (install then delete trick)
- Use traffic encryption (https and/or VPN)

Computer safety

- Keep your OS and browsers updated
- Don't be a sucker! Ignore fake alerts, be careful what you install
- Multiple browsers trick
- Separate machines
- Virtual machines

STEP 2: DOXX YOURSELF

Sample searches:

- "Jeremy Duffy" -lawyer
- Duffy site:somesiteidonttust.com (if you want to monitor just a specific site for a term)

People search

- Whitepage sites
- Online profile search tools

Defenses

- Clean up your old stuff!
- Create positive profiles
- Your own domain
- Post comments and articles under your real name (positive web presence)

STEP 3: MONITOR

Google alerts (https://www.google.com/alerts) – no account required!

- Enter search terms
- Select how often to get the alert
- Enter an email to receive the alert
- Create the alert

THE GEEK PROFESSOR®

Protecting your Identity – Offline

Non-Credit Identity Theft

There is only one defense against this kind of ID theft: protect your data and keep it out of the bad guys' hands.

Adopt a "Need to Know" philosophy and use it in all situations. Even family should be limited in access.

At Home

- Protect your mail
- Store private information securely in your house
- Shred properly (microcut or better)

Elsewhere

- Never give information to a business without knowing why they want it and how they'll use it.
- Use a persona to guard your information from companies that don't need it (as law permits!).
- Avoid data-stealing tricks like surveys, rebates, and warranties.
- If you ask, many stores will give you a discount card without requiring you to fill a form with your data.
- Always assume any company or store that wants your data will lose it at some point (because they probably will). Don't give them more than you have to.
- Avoid new technology (like e-voting, wireless tablet check-in at doctor offices) until you are able to determine conclusively that they are secured properly (don't take their word for it).

Credit Identity Theft

1. Search online for "Credit Security Freeze"
2. Look for links that go to the credit reporting companies themselves (Transunion, Experian, Equifax) and click them to start the process.
3. Follow the directions and provide the information they ask for.
4. IGNORE ANY UPSELL OPTIONS. When they offer you a score or monitoring, refuse (unless you really want a score).
5. Submit payment (varies by state). If you are a prior victim with a police report of identity theft, you may be able to select the option for free lifetime freezes instead.

There should be no expiration for the freeze (if there is, you accidentally did a fraud alert instead). You'll know for sure when you receive your freeze PINs.

These numbers (generally 8 to 12 digits long) must be stored securely (you might receive them immediately online or you may have to wait for them in the mail).

At no point should you **ever** give your PIN to any employer, store, or creditor. You go back to the websites, select a "thaw" or temporary unlock of the freeze. You'll have to pay another fee and select a time period that your credit will be exposed, but it will automatically relock afterwards.

Instruct any potential creditors (or people who you want to view your credit report) to check during the period of time you specified during your "thaw".