Vesper’s Random Security Tips

As someone who has worked various IT roles and experienced a wide range of random bullshit over the last 20+ years, I’d like to try and provide some tips for people regarding their account security.

I hope it's useful and people can learn something to try and keep themselves safe online.

Two Factor Authentication (2FA)

- Don’t use SMS (text message) based 2FA if you can avoid it. If your account is targeted, a malicious actor won't just try to guess your password; they will target your phone number instead.

- While numbers can be spoofed to trick people into falling for phishing texts, the real danger is a **SIM Swap**. This is where hackers bribe or trick carrier employees into moving your phone number to their own SIM card.

- I know it sounds far-fetched but anyone who’s worked in critical infrastructure or anywhere that handles a lot of data knows the random sketchy “Job offers” they get. They do this to get that access, and once they do that, they get your 2FA messages directly on their device, completely locking you out of the loop.

- Always prioritise 2FA via an app, like Google Authenticator, Authy, or Microsoft Authenticator; whatever works for you. These tokens are tied to the physical device itself, not a phone number, making them infinitely harder to intercept.

- If a site does not use app-based 2FA and only uses email or SMS, then create a separate, dedicated email address for those types of accounts to distance them from your core assets. Then, bug the owners of that site to request they add app-based 2FA for security reasons.

- If a site refuses or gives excuses for not setting up app-based 2FA, consider dropping their services. I personally find this red flag as it usually means they do not care about ensuring user safety on their platform.

Password Management

- Get a password manager and use a **COMPLETELY UNIQUE, complex** password when setting it up. A password manager I personally use is called ‘Dashlane’, but look around for any others or use one you’ve been recommended by a trusted friend or colleague.

- When it comes to making a password, sometimes a phrase can work well, as well as swapping out letters, numbers and unique characters where possible. If you use a password manager as mentioned earlier, these can make passwords for you and are an excellent way of securing your accounts, random gibberish is much harder to crack!

- Never repeat or use the same password over multiple accounts. If your data gets leaked from one poorly secured forum or store, that password is out in the wild, and automated bots will immediately test it against your email, banking, and social accounts.

- Try not to save passwords in your web browser. Sure, it's convenient, but if you accidentally execute any type of infostealer malware, the very first thing it does is silently scrape all saved password files and active session cookies straight out of your browser data folder. It zips them up, ships them back to the hacker, and they can bypass your 2FA completely by hijacking your active login session. **(This is the primary method those Discord "Minecraft Mod"/"I made a game" malware attacks work)**

- Make passwords hard to guess, the logic "If I use 'password' as the password, they won't expect that"; **yes they will**. Malicious actors tend to utilize bots to do the brute force attempts first with the most well known/common passwords, and if you haven't set up 2FA you're just asking for problems.

Passkeys

- Passkeys are phenomenal at providing an extra layer of security. These are effectively digital locks that open using biometric data (your face, fingerprint, or device PIN) instead of using a typical password.

- These work by a classic "lock and key" process, but with a massive upgrade: the key is cryptographically linked directly to the secure hardware it was set up from, such as a physical mobile device or a dedicated chip inside your PC.

- Because they use on-chip cryptography, the site you're trying to access sends your device a unique digital puzzle. Your operating system solves the puzzle locally and sends the answer back. The actual cryptographic key itself is never handed over to the website, meaning it can never be leaked in a database breach or stolen by a fake phishing site.

If you have an option to set up passkeys, I highly recommend doing so.

CRITICALLY IMPORTANT FOR PASSKEYS:

If you plan to upgrade or change devices, do not wipe or get rid of your old device immediately.

If your passkeys are synced to a specific ecosystem (like Apple iCloud Keychain or Google Password Manager), moving to a new device on the same platform is usually seamless.

However, if you are changing architectures (like moving from iOS to Android or vice versa), you will need the old device active and by your side to cross-authenticate and log into your accounts on the new ecosystem.

Always confirm all your accounts work on the new hardware before getting rid of the old one.

Spotting the Traps: Links, Files, and Discord Hijacks

How to spot malicious links:

- Always look at the top-level domain (the text right before the .com or .net).
- Hackers buy domains that look nearly identical to real brands; this is called typosquatting.
- Look for things like micros0ft.com (using a zero), goggle.com (slight typo), or domain extensions that don't make sense for a company (like a banking link ending in .ru or .cc).
- Check hidden links, just because the text on your screen says it's a safe URL doesn't mean that's where the button actually points. Hover your mouse cursor over the link before clicking it to see the true destination address in the bottom corner of your browser.

How to spot dangerous files:

- Beware of "Double Extensions." A file named Invoice.pdf.exe is not a PDF; it is a dangerous Windows executable file.
- Windows hides known file extensions by default, which hackers love. Make sure you turn on "File name extensions" in your operating system settings so you always see exactly what a file is. Steer clear of password-protected archive files (.zip or .rar) sent by unverified sources. Hackers use password protection because it encrypts the payload, making it impossible for your email provider or local antivirus to scan and flag the virus inside until you extract it.

How to tell a Discord message isn't from your friend:

- Watch for sudden, out-of-character shifts in tone. If your friend usually types in casual lowercase fragments and suddenly sends a perfectly punctuated message saying, "Hey, look at this cool game I made, can you test it?" or "Can you vote for my esports team on this link?", your alarm bells should go off.
- Look for mass-distribution scripts. If an account sends you a link or a file and then immediately drops offline, or sends the exact same message chain to multiple shared mutual servers simultaneously, the user's account token has been hijacked by an automated script.
- When in doubt, cross-verify. Reach out to that person through a completely different platform (like a phone call, text, or WhatsApp) and ask, "Hey, did you just send me a link on Discord?" Never use the compromised Discord chat window to verify their identity.
- In the event your friend's alternative contact method has been compromised or you suspect that this has happened, ask them something only they would know, or, say something that didn't happen such as saying "Hey, what do you think of that event last night?", they should respond in such a way that confirms your suspicion, if the event never happened and they act like it did, you've caught them out in a cross referencing trap.

I’ve been hacked, what do I do?

So, you’ve downloaded a random file and suddenly see your accounts logging you out in real-time. Don't panic. You need to act fast, cut the lines, and lock the hacker out. Follow these exact steps:

- **Step 1: Pull the plug immediately**
  The absolute first thing you must do is disconnect the infected device from the network completely. If you are on a wired connection, rip the Ethernet cable out of the back of the machine. If you are on Wi-Fi, turn off your wireless adapter instantly. Do not bother shutting down the PC gracefully first—break its connection to the internet right now to stop the malware from uploading any more of your stolen session cookies or files to the hacker's server.

- **Step 2: Secure a clean machine**
  Grab a separate, non-infected device. This could be your smartphone (as long as it wasn't connected to the PC via USB or file-sharing) or a different tablet/laptop. You need a clean environment that has zero traces of the malware to begin the fight back.

- **Step 3: Time to go nuclear, start resetting passwords.**
  Using your clean device, begin changing the passwords to every single account you can still access. Change your password manager master password first. As you change passwords on your accounts (Google, Discord, banking), look for the option that says **"Log out of all other devices"** or **"Revoke trusted devices"** and click it. This instantly destroys the session cookies the hacker stole, kicking them out of your account.

- **Step 4: Deploy your recovery keys**
  If you saved a hard copy of your emergency recovery keys when you initially set up your high-value accounts, now is the time to dig them out. Find the recovery portal for the specific service, enter your recovery seed, and force an administrative reset. This allows you to override the hacker's changes, resetting the email, password, and active sessions all in one go.

- **Step 5: Contact support and warn your immediate circle/contacts**
  For any accounts you can no longer access, initiate the official support recovery process immediately. Because corporate support can take time, reach out to your friends, family, and colleagues via alternative methods (like a direct text or phone call). Tell them explicitly: *"My accounts were compromised. Do NOT accept any weird links, files, or emergency money requests from me until I tell you otherwise."*

- **Step 6: Post-Incident Cleanup (The Full Wipe)**
  In my experience, the safest option is always a full wipe. Do not rely on the built-in "Reset my PC" menu option. Built-in resets carry a massive risk of advanced malware or rootkits "hiding" within local system recovery images during the setup process, meaning it might not actually wipe the threat.

    - Go to your **clean, uninfected device** and create a fresh USB installation media tool straight from the official OS manufacturer.

    - Plug that clean USB into the infected machine, boot directly from it, completely format and delete the existing drive partitions, and install the operating system from a completely blank slate.

- This entire scenario highlights exactly why users should always maintain safe, detached backups on hand or at least run a strict, regular backup schedule. Having your raw files safely stored elsewhere turns a catastrophic malware event into nothing more than an afternoon of reloading an OS.

I'll add onto this as I think of more, but most of these are generally the "go-to" processes I would recommend at the time.

<u>One last note:</u>

Do not give in to demands from the hacker, they will make threats and try to scare you into giving up or paying them. If you pay them because they will "give your accounts back", chances are they won't, and they'll lock you out more or leave you completely isolated with no means to get your information back