

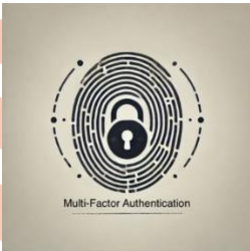


Cybercrime on the Dark Web is now costing over \$12 trillion annually. If it were a country, its 'GDP' would rank third in the world. Cybercriminals don't care about your status, your job, or your wealth—what they care about is your vulnerability. To protect myself, I've created a top ten list to become a harder target. These steps are essential to safeguard yourself and contribute to a safer world against cyberattacks.



1. Use Strong, Unique Passwords for Everything

Craft passwords with a wild mix of letters, numbers, and special characters that only you can decode. Think of it as digital armor – no "1234" or "password" nonsense! Aim for at least 12 characters. Or better yet, create phrases that are meaningful but hard to guess. Reusing passwords is like giving a thief your keys to every lock. Resist the temptation.



2. Enable Multi-Factor Authentication (MFA)

Passwords alone won't cut it; cybercriminals crack them faster than we can say "breach." MFA, often a simple app-based code, adds another lock to your digital door. Wherever possible, activate MFA on accounts that matter most: email, banking, and social media. It's like putting a security guard outside your digital front door.



3. Stay Updated – Religiously

Software updates are often security updates. Cyber attackers love exploiting outdated systems because, well, they're easy. Set your devices to auto-update so you're always patched against the latest threats. This small habit is one of the easiest ways to stay ahead of attackers.



4. Invest in Quality Antivirus Software

Reliable antivirus isn't just an added expense; it's your early warning system. Good antivirus software detects and blocks malware before it can wreak havoc. Check your software daily for updates and make sure it's running properly – and if it's a no-name free version, consider an upgrade.



5. Back Up Your Data Like It's Your Life

Losing all your data is devastating. Back up regularly to an external drive or a secure cloud service. If ransomware ever locks you out of your files, having a recent backup means you can walk away without paying a ransom. Set a reminder and automate backups if possible.

Bring Eric to your organization: Contact@EricONEill.net



6. Encrypt Sensitive Data

Encryption is like locking your data inside a virtual vault. If someone does get into your device, encryption keeps them from accessing your most private information. Most devices and software offer easy options for this – take a few minutes to activate it, especially for any sensitive files.



7. Use a Password Manager to Keep Your Sanity

Creating strong, unique passwords is exhausting unless you have a password manager. Think of it as a secure vault that handles the heavy lifting, so you can remember just one password instead of fifty. It's one of the easiest ways to make your online life more secure and manageable.



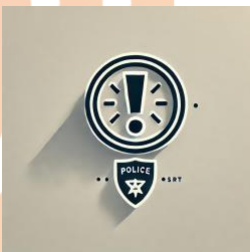
8. Be Wary of Public Wi-Fi – It's Often a Trap

Free Wi-Fi sounds great, but it's an open playground for hackers. When using public networks, avoid accessing sensitive information (like banking). If you must, use a VPN to mask your traffic. Public Wi-Fi can quickly become a hacker's front-row seat to your data.



9. Beware of Suspicious Links and Attachments

Phishing scams are craftier than ever – even those emails that look like they're from your best friend might be hiding a nasty surprise. Hover before you click, and when in doubt, don't. Double-check URLs, especially if they look slightly off, like "amazon.com" instead of "amazon.com."



10. Report Suspicious Activity Immediately

If something feels off – strange charges, weird emails, or your account acting funny – report it. Contact your bank, the platform's support team, or cybersecurity authorities if necessary. Early reporting can prevent further damage and might even help track down the attacker.

Bonus: Stay Ahead with Insider Intel

Keep your defenses sharp and stave off the wild world of cyberattacks, identify spy intrigue, and high-stakes cybercrime? It's all in [Eric's exclusive newsletter!](#) Each issue is packed with the latest insights on protecting yourself, fascinating stories of spies and lies, and no-nonsense advice you can trust. It's like having a cybersecurity strategist in your pocket – don't miss out!



Bring Eric to your organization: Contact@EricO'Neill.net

