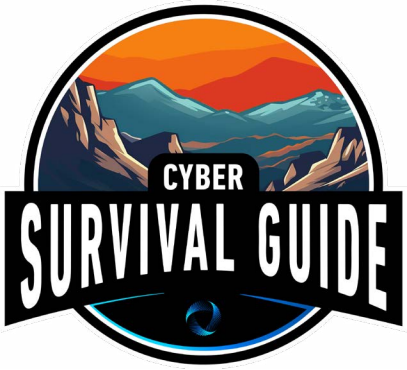

2024 CYBER SURVIVAL GUIDE

Stay Safe Online by Being Prepared

As with most things, preventing a cyberattack is easier than dealing with the fallout in many cases. By practicing some good cyber hygiene behaviors, you can stay on the trail headed to amazing internet experiences!

- Lock down your login with strong passwords, a password manager, and multi-factor authentication
- Back up your data regularly to the cloud or an external drive (or both!)
- Antivirus software is worth it
- Update your software regularly (turning on automatic updates is easiest!)
- Avoid the phishing bait

Most of the unfortunate events described in this guide are caused by phishing attacks, which is when a cybercriminal sends you an email, message, social media post, or text that includes a malicious download or link.

If the hacker can trick you into clicking, you risk downloading a virus, losing control of an account, or becoming held hostage by ransomware.

With the rise of generative artificial intelligence, phishing messages now have better grammar and can even be personalized. Whenever you receive any sort of digital communication, take a few seconds to understand if the message is trying to get you to act before you think about the request too much.

Current technologies allow cybercriminals to spoof real businesses and other organizations in email addresses or caller IDs. Even if the sender seems real, scrutinize the message. If you have doubts, contact the person, company, or organization in a different way, like through a phone number found on their official website.

Here are some common signs of a phishing message:

- Does it contain an offer that's too good to be true?
- Does it include language that's urgent, alarming, or threatening?
- Is the greeting ambiguous or generic?
- Does it include requests to send personal information?
- Does it stress an urgency to click on unfamiliar hyperlinks or attachments?
- Is it a strange or abrupt business request?
- Does the sender's e-mail address match the company it's coming from? Look for little misspellings like pa**v**pal.com or a**n**azon.com.

If you think you clicked on a malicious link in a phishing email:

- Don't download any attachments or files
- If you are at work, alert your IT or security teams
- If using a personal account, report the incident to the platform
- Don't call any phone numbers or download "antivirus" software that appear in popup windows
- Run a scan on your computer for malware and viruses
- Consider credit and dark web monitoring to catch fraud attempts