# Online safety: Online security made easier

Saturday, September 27, 2025

## 0. Some good habits to develop

Using computers, like driving, is inherently risky. There's no way to be 100% safe while doing either activity, but both activities have practices & technologies that can make them safer.


*Figure 1: Satan's Desktop*

*Internal image:*
*"Skull and Crossbones"*
*From* Specimen Book *of Farmer, Little & Company, 1867*
*License: Public Domain*

Here are some common adages to summarize what follows in the rest of the program.[1]

- **You are what you eat**
- **Looks can be deceiving**
- **Never buy a pig in a poke**
- **Loose lips sink ships**
- **A chain is only as strong as its weakest link**

1 I was looking at Kaspersky, "Top 10 Internet Safety Rules & What Not to Do Online" as I developed this list.

-

## 1. You are what you eat

- Only install apps from the official source for your platform
- Look at the ratings and reviews for the app before deciding to install it
- On an **Android**, pay attention to the information about permissions on the app's page in the **Play Store**

| Platform | Source |
|---|---|
| Android | Play Store |
| iOS (iPhone, iPad) | App Store |
| Mac | App Store |
| Windows | Microsoft Store |

*Table 1: Platforms and official app sources*

## 2. Looks can be deceiving

- Phishing
- Too-good-to-be-true
  - Clickbait
  - Phishing
  - Email from strangers saying they want to give you money
- Alarming things
  - Phishing
  - "Relatives" in distress
  - Scareware

## 3. Never buy a pig in a poke

- Know who you're dealing with
- Reputation matters. Look at the ratings and reviews a given site or seller gets.

### Common types of scam

- Job offer scams
- Lottery scams
- Beneficiary scams
- Online dating scams
- Charity fraud scams
- Coronavirus scams
- Repair scams
- Social media scams
- Robocall scams
- Messaging scams
- Online shopping scams

Source: Kaspersky

*Sidebar 1: Common types of scam*

### General tips on scams[2]

- Beware of any requests for your details or money
- Be alert to phishing scams

2 Source: Kaspersky, "Top Online Scams and How to Avoid Internet Scams"

- Don’t respond to phone calls asking for remote access to your computer
- Keep your mobile devices and computers secure
- Use strong passwords
- Review your privacy and security settings on social media
- Avoid streaming content from unknown websites
- Resist the pressure to act immediately
- If it seems too good to be true, then it probably is

### Example: Online shopping scams

- What they might look like (***tl;dr: nowadays they’ll look like the real thing***)
  - Fake site that looks like a real store’s site
  - Social media store
  - Seller on a sales platform like Amazon
- So basically, chances are good that the look and feel of the site won’t give you enough clues. What you can look for will be some of the same things you’d see as red flags whether online or in meatspace:
  - Does this deal sound too good to be true?
  - Does the store accept payment by credit card? If not—especially if they insist on payment by wire, electronic funds transfer, money order, pre-loaded money card—go elsewhere

## 4. Loose lips sink ships

Remember that the *con* in *con artist* is short for *confidence*, and thoroughly innocent facts about you are fodder for con artists.

- Think about what you want in terms of online privacy
  - Keep those thoughts in mind as you use the internet and with any platforms you get into
  - Don’t put anything online that you wouldn’t want your (grandmother|grandkids|boss|nemesis) to see
    - Anything you put on the internet can be there forever
    - Even if you delete accounts & even if no one saved any of your posts, there’s no guarantee that a given post is gone for good

        - This applies to email also
- For any social media you use, align it with your desired level of privacy
    - Look at your privacy settings and adjust them to fit your level of desired privacy
    - Similarly, limit the audience you share posts with
    - You shouldn’t trust any platform to follow your wishes

      Updates will often change policies and require checking that your privacy settings are still what you want them to be
    - A bonus adage: “If it’s free, you’re not the customer, you’re the product.”

| System | Examples | Advantages | Disadvantages |
|---|---|---|---|
| Notebook + pen | | Can’t be hacked online | Unencrypted, so completely open if stolen or lost |
| | | Available even if devices are out of power | Not integrated with your devices |
| Password manager with local storage only | • KeePass2 | Not subject to mass password leaks | Only available on devices with a copy of the database file |
| | | Encrypted | Need to remember a master password |
| Internet-based password manager | • 1Password<br>• Bitwarden<br>• Dashlane<br>• Keeper<br>• LastPass<br>• NordPass<br>• RoboForm | Available anywhere there’s internet | Potential for data breaches (but hackers would then need to break the encryption) |
| | | Encrypted | Need to remember a master password |
| Using a web browser to memorize passwords | • Chrome<br>• Edge<br>• Firefox<br>• Opera<br>• Safari<br>• … | Easy integration with a browser | Potential vulnerability on public computers |
| | | Passwords available on any machine where that browser synchs your browser profile | Requires intervention to keep your password list synched if you use 2 or more browsers |
| | | Doesn’t require any software you’re not already using | Need to remember a master password |

*Table 2: Comparison of various methods for managing passwords*

# 5. A chain is only as strong as its weakest link

## Password management

You should have a system for “remembering” passwords and user names for important accounts, at least. These include:

- Your main email accounts (including any email address you use for password recovery)
- Financial institutions (e.g. banks, credit cards, stock brokerages, etc.)
- Government agencies

## Use strong passwords

### *Characteristics of a strong password*

- The password is unique
  - You use it for only 1 of your accounts
  - Ideally, you’re the only person in the world using it for anything

    This is harder to achieve but go after the rare, obscure, and idiosyncratic. Or let your password manager generate a (pseudo)random string for you.
  - At a minimum, the password has not appeared in lists of hacked passwords

    You can check it at **Have I Been Pwned**, https://haveibeenpwned.com/Passwords. If it’s shown up in even 1 breach, you should regard it as insecure.
- In the technical language of information theory, it has **high entropy**.

  In plain English that means that it’s long and random. Length seems to be more important than randomness, though, and NIST recommends using passwords that are at least **15 characters long**.

# Resources


- Ducklin, Paul, “When VPNs Go Rogue: Understanding the Technology and the Risks,” Solcyber,
  - Part 1, Published May 23, 2024, https://solcyber.com/when-vpns-go-rogue-understanding-the-technology-and-the-risks-part-1-of-2/
  - Part 2, Published May 28, 2024, https://solcyber.com/when-vpns-go-rogue-understanding-the-technology-and-the-risks-part-2-of-2/
- Florida Department of Agriculture and Consumer services, “Online Shopping Scams,” Viewed September 9, 2025, https://www.fdacs.gov/Consumer-Resources/Scams-and-Fraud/Online-Shopping-Scams
- “Great Firewall of China,” *Wikipedia*, https://en.wikipedia.org/wiki/Great_Firewall

- Grauer, Yael, “Which Is Better: Your Browser's Password Manager or a Standalone Service?” Consumer Reports, Published March 19, 2024, Viewed September 18, 2025, https://www.consumerreports.org/electronics-computers/password-managers/browser-password-manager-or-standalone-password-service-a1214951437/
- Have I Been Pwned, “Pwned Passwords,” https://haveibeenpwned.com/Passwords
- Kaspersky, “Top Online Scams and How to Avoid Internet Scams,” Published March 25, 2020, Updated May 8, 2025, https://usa.kaspersky.com/resource-center/threats/top-scams-how-to-avoid-becoming-a-victim
- Kaspersky, “Top 10 Internet Safety Rules & What Not to Do Online,” Published July 30, 2025, Viewed September 4, 2025, https://usa.kaspersky.com/resource-center/preemptive-safety/top-10-internet-safety-rules-and-what-not-to-do-online
- McAfee, “iOS vs Android: A Comprehensive Look at Security,” Published January 17, 2025, Updated May 13, 2025, Viewed September 15, 2025, https://www.mcafee.com/learn/ios-vs-android-security/
- McAfee, “What Is a VPN and Can It Hide My IP Address?” Published February 21, 2025, Modified April 12, 2025, https://www.mcafee.com/learn/what-is-a-vpn-and-can-it-hide-my-ip-address/
- Netflix’s Help Center, https://help.netflix.com/en/node/114701
- NIST, “How Do I Create a Good Password?” Published April 28, 2025, Updated April 29, 2025, https://www.nist.gov/cybersecurity/how-do-i-create-good-password
- Tor, Most Frequently Asked Questions, “Am I Totally Anonymous If I Use Tor?” https://support.torproject.org/#faq_staying-anonymous