# How to stay safe online:
# Tricks to avoid, tips to know

When we leave our homes, we lock our doors and  set the alarm. We roll up our windows and take our keys when we park our cars. When we meet a stranger, we're not likely to share our ATM PIN.

When we use the Internet, we should also take some basic security measures to protect our personal and financial security.

Whether you're a student starting to navigate the digital world, a working adult managing financial transactions online, or a senior communicating with friends and family on social media, these basic precautions will help protect you from cyber threats.

This guide outlines some security basics and provides practical tips for a safe online experience. It will help you fully enjoy the benefits of the internet with peace of mind.

# Key concepts

When it comes to online security, make sure you're familiar with the following terms and concepts.

## Glossary

**Authentication:**

The method you use to prove that you are who you say you are, such as a password, fingerprint or two-factor authentication (2FA), which might ask for a code from your phone as an extra step.

**Authorization:**

Once your identity is confirmed, this determines what you can do or see on a system, like allowing you to view but not edit specific files.

**Encryption:**

This secures your data by scrambling it so only the intended parties can read it when it's sent over the internet or saved online.

**Hacking:**

Attempting to gain access to computer information through illicit means.

**Firewalls:**

Special filters that help block unauthorized files and users from reaching computers and networks. They filter out suspicious traffic and prevent outsiders from accessing private data.

**Malware and viruses:**

Malware is any software intentionally designed to cause damage to a computer, server or network. A virus is a type of malware that can copy itself and spread to other devices. Both can harm your system, steal, scramble or delete your data. Anti-virus/malware software protects your devices.

**Ransomware:**

A specific type of malware that blocks access to a computer system and attempts to extort its user by requesting payment in order to restore access.

**Social engineering:**

Any scam that tricks users into revealing secret information such as passwords or bank account numbers.

**Virtual Private Networks (VPNs):**

VPNs let you create a secure connection over the internet. They hide your IP address, encrypt your data before sending it and help protect your online identity. You can purchase VPN services from several providers, including NordVPN, Surfshark, Private Internet Access and ExpressVPN among others.

PASSWORDS:

# DO's and DON'Ts

## DO

- ✓ **Use strong passwords:** Good passwords are hard to guess. Long passwords and those that include a mix of at least 12 upper- and lowercase letters, numbers and symbols are considered strong.
- ✓ **Keep each account unique:** Use a different password for every account.
- ✓ **Use a password manager:** Like a keychain, a password manager helps you keep all your passwords in one place, so you don't have to remember them. Better yet, let it create and store complex passwords for you. There are several password managers in the market such as 1Password, NordPass, RoboForm and Keeper.
- ✓ **Change often:** Change your passwords regularly.
- ✓ **Enable two-factor authentication:** Add an extra layer of security to your accounts so if ever your password is compromised cyber criminals will have a harder time accessing your accounts and you can more easily regain control.

## DON'T

- ✗ **Don't be obvious:** Avoid easy guesses like "password," family member names or birthdates.
- ✗ **Don't reuse passwords:** One breach shouldn't open all doors.
- ✗ **Don't write passwords down:** Especially not where others can find them.
- ✗ **Don't share passwords:** Keep it private. Don't share with anyone.

**10 commonly used passwords** (Psst. These are too easy to guess):

1. 123456789
2. password
3. admin
4. abc123
5. 111111
6. sunshine
7. qwerty
8. iloveyou
9. FirstLast1
10. root

**80% of breaches are caused by passwords being lost, stolen or broken** through a "brute force attack," in which computers try many common word combinations and frequently used passwords until a match is found.

HOW TO AVOID

## Phishing expeditions

Phishing is a type of online fraud where criminals try to trick you into giving them your personal information, such as passwords, bank account numbers or credit card details using social engineering. They do this by sending you fake emails, text messages or websites that look like they come from legitimate organizations such as your bank, your employer or a government agency. If you click on a link or open an attachment in these messages, you may download malware that can harm your computer or steal your data. Here are some tips to avoid phishing scams:

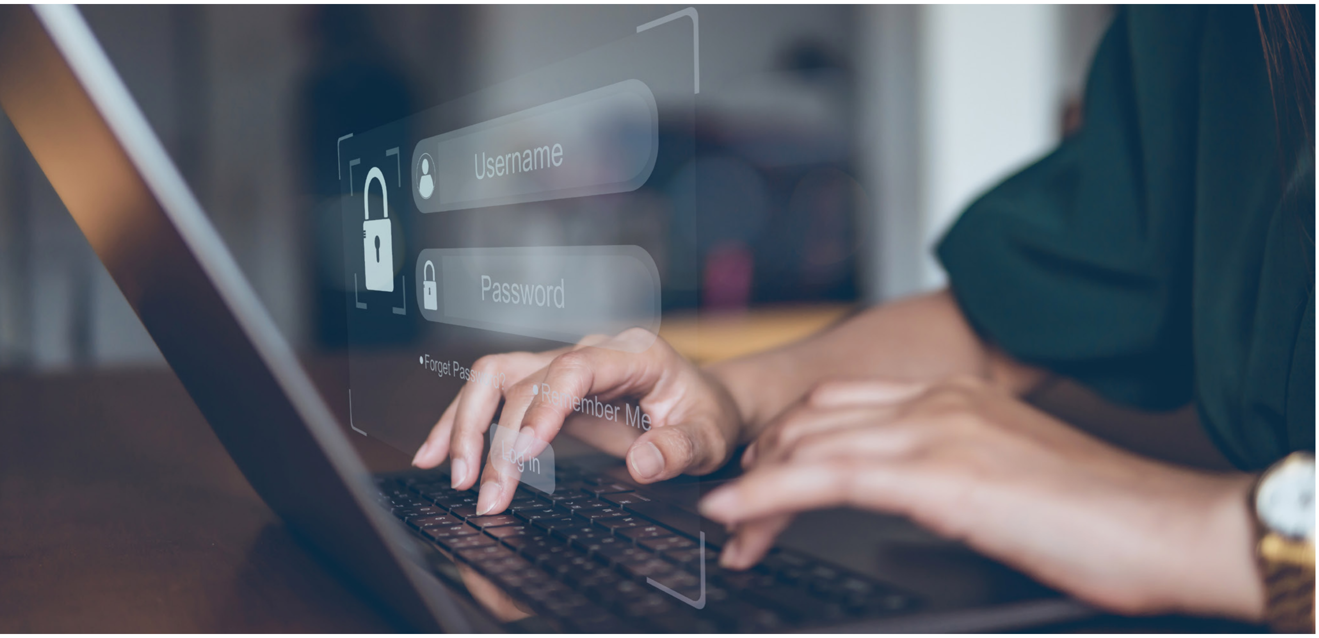
**Check the sender:** Always look at the sender's email address and compare it with the official website of the organization they claim to represent. If the email address does not match, or if it contains random letters or numbers, it is likely a phishing attempt.

**Verify the content:** Look for spelling and grammar mistakes, vague or urgent language, or requests for personal or financial information. These are all signs of phishing. Do not reply to these messages or click on any links or attachments. If you are not sure if a message is legitimate, contact the organization directly using a different channel, such as phone or web browser.

**Use security software:** Install and update antivirus and anti-malware software on your computer and mobile devices. These programs can help detect and block malicious websites and downloads. You should also use a firewall and encrypt your wireless network to prevent unauthorized access.

**Don't let them pressure you:** Bad actors use a false sense of urgency to get you to make a mistake. Threats of closing your account, being locked out or receiving a fine can get you off your game.

**Report:** If you receive a phishing email, don't just delete it. Most email platforms have an option to report it as phishing. You can also forward it to spam@uce.gov, which is a service of the Federal Trade Commission (FTC). By reporting phishing, you can help protect yourself and others from online fraud.



STAY SMART & STAY SECURE

# 9 ways to keep your digital life safe

1. **Update regularly:** Keep your software, apps and operating system current. Updates often include security patches that protect against new threats.
2. **Be wary of links and attachments:** Don't click on links or download attachments from unknown sources or suspicious emails. They could lead to dangerous websites or contain malware.
3. **Use secure networks:** Avoid using public Wi-Fi for sensitive transactions like banking or shopping. If you must use public Wi-Fi, always use a VPN to secure your connection.
4. **Back up your data:** Regularly back up important files to an external or cloud storage. This protects your data in case of a cyberattack (or hardware failure).
5. **Enable privacy settings:** Adjust the privacy settings on your social media and other online accounts to limit the personal information you share publicly. Avoid posting things as "public" unless you want the whole world (including criminals) to see.
6. **Secure your devices:** Use strong passwords, touch ID or face ID to lock your devices. This prevents unauthorized access if your device is lost or stolen.
7. **Never enable macros:** If a dialog window requests to change something on your computer or asks you to click "yes" to enable macros, be very suspicious.
8. **Be skeptical:** Treat unsolicited phone calls, emails and messages with suspicion, especially if they ask for personal information or money. If it sounds too good to be true, it usually is.
9. **Stay informed:** Keep up on the latest online scams and learn to recognize fraud signs. The FTC website offers a trove of resources: **https://consumer.ftc.gov/identity-theft-and-online-security**

## About Brightspeed

Launched in 2022, Brightspeed is building a future where more communities can benefit from a more connected life. We believe where you choose to call home shouldn't limit your options — and we're building the infrastructure to provide millions of homes with fast, reliable internet. So wherever you're streaming, gaming or working, you'll enjoy an uninterrupted experience. **Learn more at www.brightspeed.com**.

In collaboration with
ciena