RECOMMENDED SECURITY PRACTICES

EMPLOYING GOOD SECURITY PRACTICES

With the increase in remote work, we rely on numerous devices and our ability to connect to the Internet for work and personal reasons. However, cyber threat actors take advantage of our reliance on technology.

Protect yourself by taking stock of all the technology you use, including your mobile and smart devices, computers, and Wi-Fi networks. By knowing what you have, you can prioritize your security efforts and put the right safeguards in place.

GENERAL SECURITY PRACTICES

1. Use unique and complex passphrases or **passwords** and activate multi factor authentication (MFA), if available.
2. Avoid joining unknown, unsecured, or public Wi-Fi networks or use a Virtual Private Network (VPN).
3. Backup data on all devices.
4. Avoid opening files, clicking on links, or calling numbers contained in **unsolicited/suspicious** text messages or emails.
5. Update software, including operating systems and applications.

Top 10 most common passwords of 2023

RANK	PASSWORD	TIME TAKEN TO CRACK	NUMBER OF TIMES USED
1	123456	< 1 Second	4,524,867
2	admin	< 1 Second	4,008,850
3	12345678	< 1 Second	1,371,152
4	123456789	< 1 Second	1,213,047
5	1234	< 1 Second	969,811
6	12345	< 1 Second	728,414
7	password	< 1 Second	710,321
8	123	< 1 Second	528,086
9	Aa123456	< 1 Second	319,725
10	1234567890	< 1 Second	302,709

The NordPass study showed that 86% of cyberattacks use stolen credentials, and online accounts, emails and passwords make up almost 20% of the most commonly sold items on the dark web.

Source: NordPass

PASSWORDS

- Make sure you use strong passwords on all devices or accounts where personal information is stored. They must be difficult to guess. The National Cyber Security Centre (NCSC) recommends using three random words. This includes uppercase, lowercase, numbers and symbols.

- **Different** Email password - Your email address is often used as backup access for forgotten passwords for other accounts. An intruder or criminal may be able to
  - Access private information about you (including your banking details)
  - Post emails and messages pretending to be from you (and use this to trick other people)
  - Reset all your other account passwords (and get access to all your other online accounts)

Strong Password Examples

SunnyBe@chTr1p
F00tb@llT3nnisG0lf

Source: National Cyber Security Centre

VPN

Virtual because no physical cables are involved in the connection process.

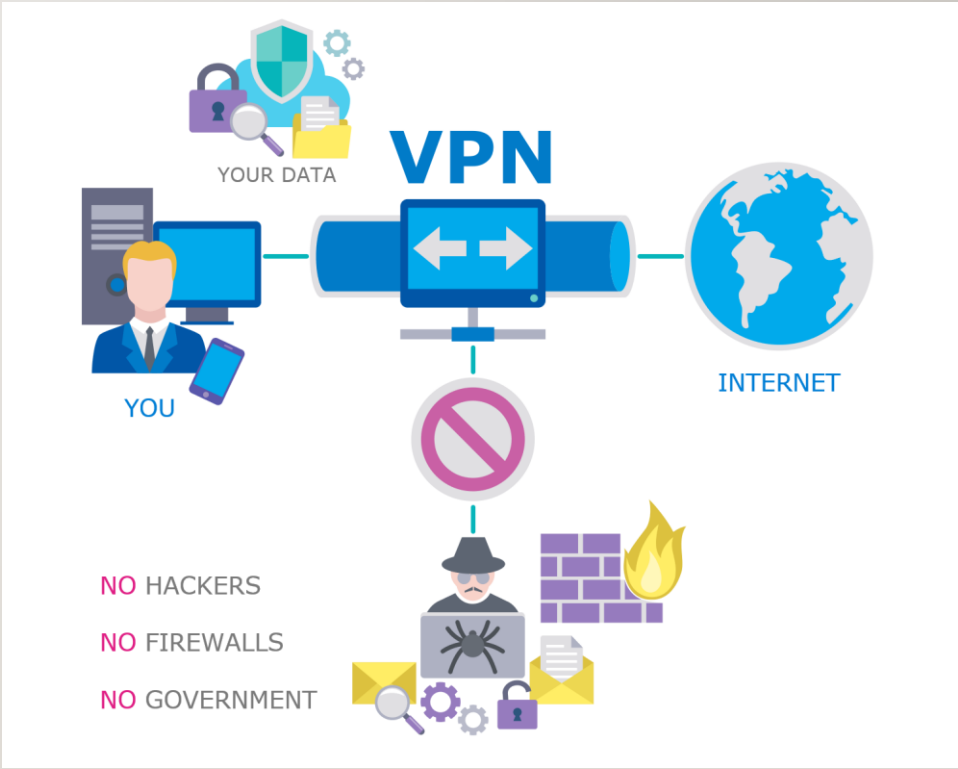
Private because through this connection, no one else can see your data or browsing activity.

Network because multiple devices—your computer and the VPN server—work together to maintain an established link.

A VPN, or **Virtual Private Network**, is a service that creates a secure connection between a device and a remote server over the internet.

VPNs are used to protect a user's online privacy and security by encrypting their data and masking their IP address.

Internet service providers (ISPs) log and track your browsing history through your device's unique IP address. This information could potentially be sold to third-party advertisers, given to the government, or left vulnerable in the face a security compromise.



Source: Microsoft Azure

BACKUPS & SUSPICIOUS EMAILS

- You should back up your data regularly.
- Cloud backups are a popular choice, with many offering a variety of plans depending on the need.
  - Cloud is simple, efficient and can be automatic (phone/tablet terms).
- If using physical devices for storing data, save a copy elsewhere, encrypted and locked away.

- The use of poor grammar, demands for you to act urgently.
- Subject line: Generic or unusual subject line
- Verify the email is original – contact the sender via known method.
  - Banks will not contact you asking for your details (they have them) – this is phishing.
- Is it offering something too good to be true?

MOBILE DEVICE SECURITY

- Connect through a VPN wherever possible.
- Use a PIN or passphrase to protect your device.
- Deactivate features when not in use, such as GPS, Bluetooth, or Wi-Fi.
- Avoid joining unknown, unsecured, or public Wi-Fi networks.
- Delete all information stored on a device prior to discarding it.
- Check privacy policies and user reviews application before downloading to ensure they are reliable.
- Avoid using free password managers that are not part of your operating system or browser.
- Limit the use of “remember me” features on websites and mobile applications – if MFA is not available, type in your username and passphrase or password to log in for important accounts.
- Use encryption features to secure personal or sensitive data and messages.

ANY QUESTIONS?