

Basic Digital Safety



Module: Digital Skills
Module code: LCLM4002
Name: Felicia Ficea
ID: 2325311
Group: 2

What is Digital Safety?



How Can We Secure?

Strong Passwords

Two-Factor Authentication (2FA)

Phishing Awareness

Regular Software Updates

Secure Wi-Fi Connections

Data Encryption

Backup Regularly

Privacy Settings Review

Cybersecurity Education

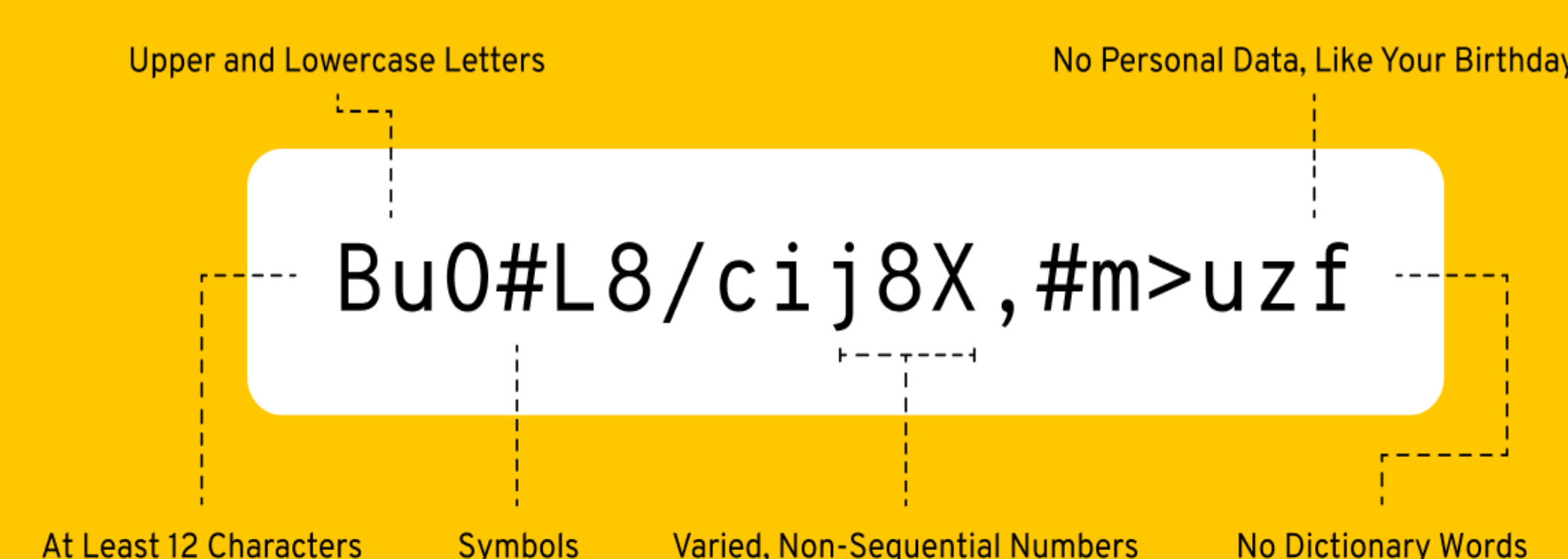
Incident Reporting

1. Strong Passwords

Make your password difficult to guess by using a mix of letters, numbers, and symbols.

Never use a birthdate, a name, or a phrase that anybody can guess.

Rules for a Strong Password



Examples of Weak Passwords

B0u#L

Too Short

spidercat9

Contains Dictionary Words

xcf01234

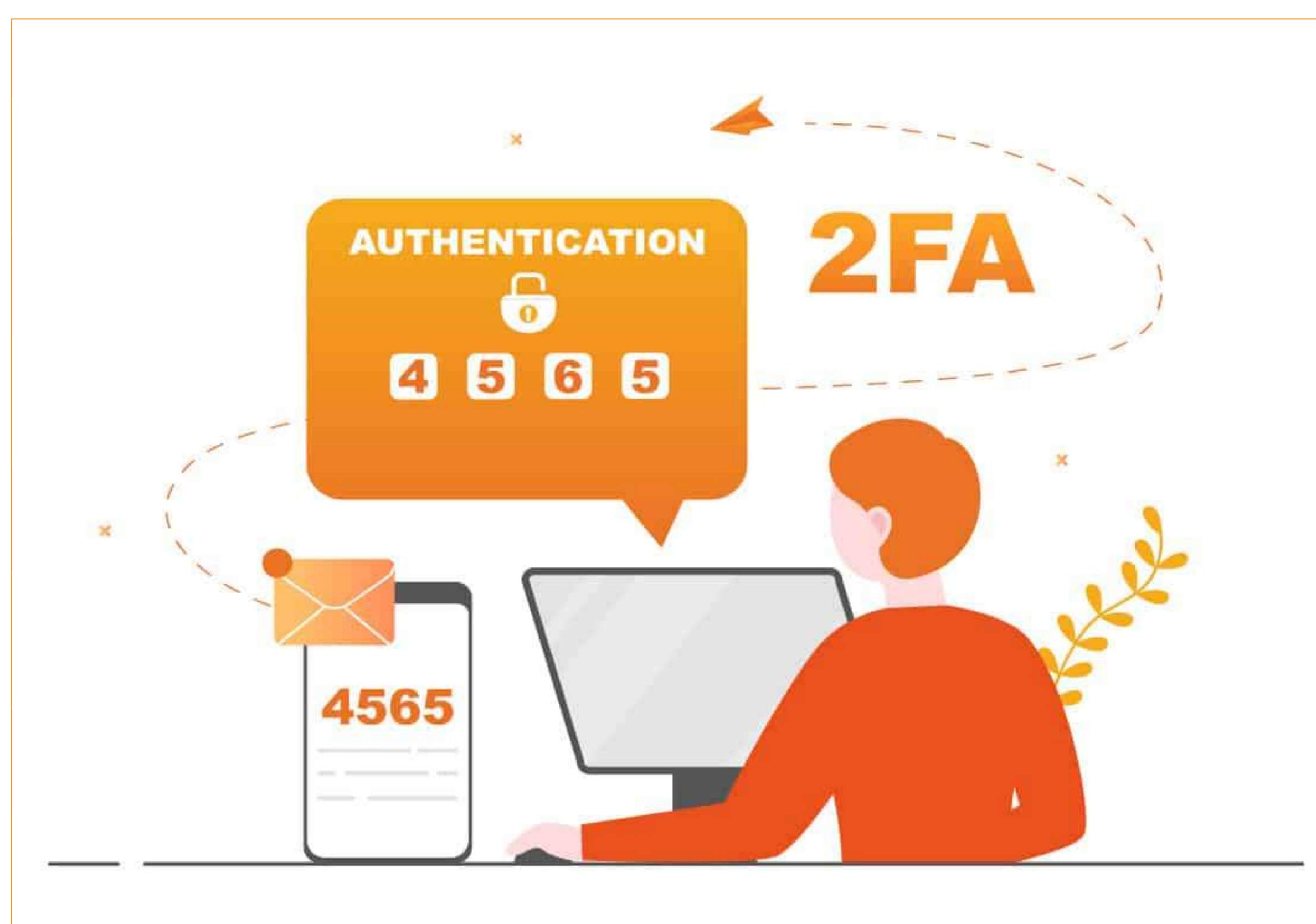
Has Sequential Numbers

A password made of random words may provide an extra layer of protection.

2. Two-Factor Authentication

To further safeguard your accounts, enable two-factor authentication (2FA) wherever it is offered.

Two-factor authentication (2FA) entails using a password and an additional verification method, such a code delivered to your phone.



Even if your password becomes hacked, the danger of unauthorised access is much reduced.

3. Secure Wi-Fi Connections

To prevent unauthorised individuals from intercepting your data, utilise an encrypted Wi-Fi network, ideally one that uses WPA2 or WPA3.

Unless you are utilising a Virtual Private Network (VPN), it is not a good idea to connect to public Wi-Fi networks for sensitive activity.

If you want to keep unwanted people out of your home or business network, you should change the default passwords and activate network encryption.

4. Keep Software Updated

Updating your OS, antivirus, and apps on a regular basis will fix security holes.

To stay safe from the most recent dangers, enable automatic updates whenever you can.

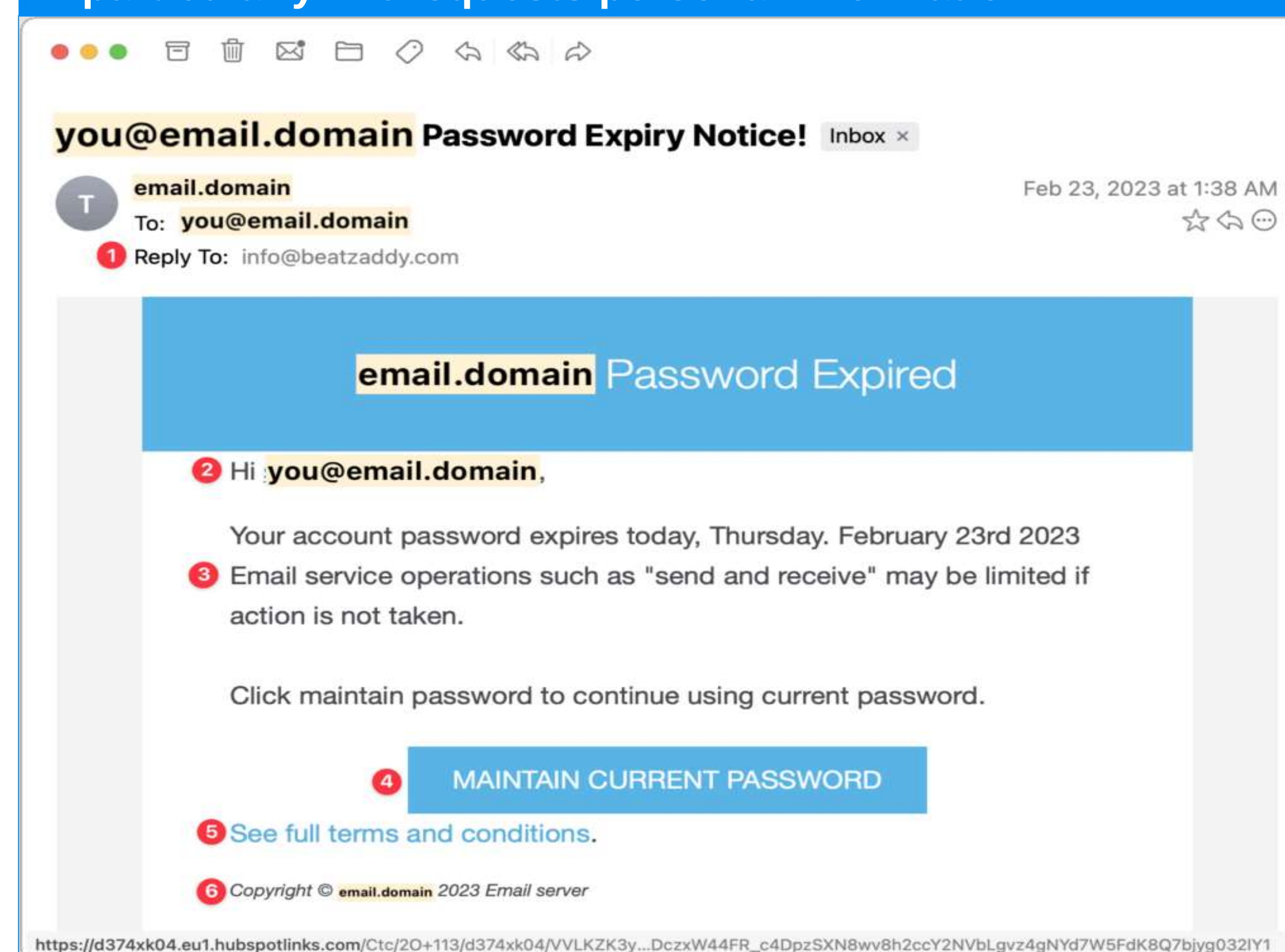


Hackers often target computers running outdated software.

5. Be Wary of Phishing

Always use caution when opening files or clicking on links from unknown senders.

Before responding to an email, be sure it is legitimate, particularly if it requests personal information.

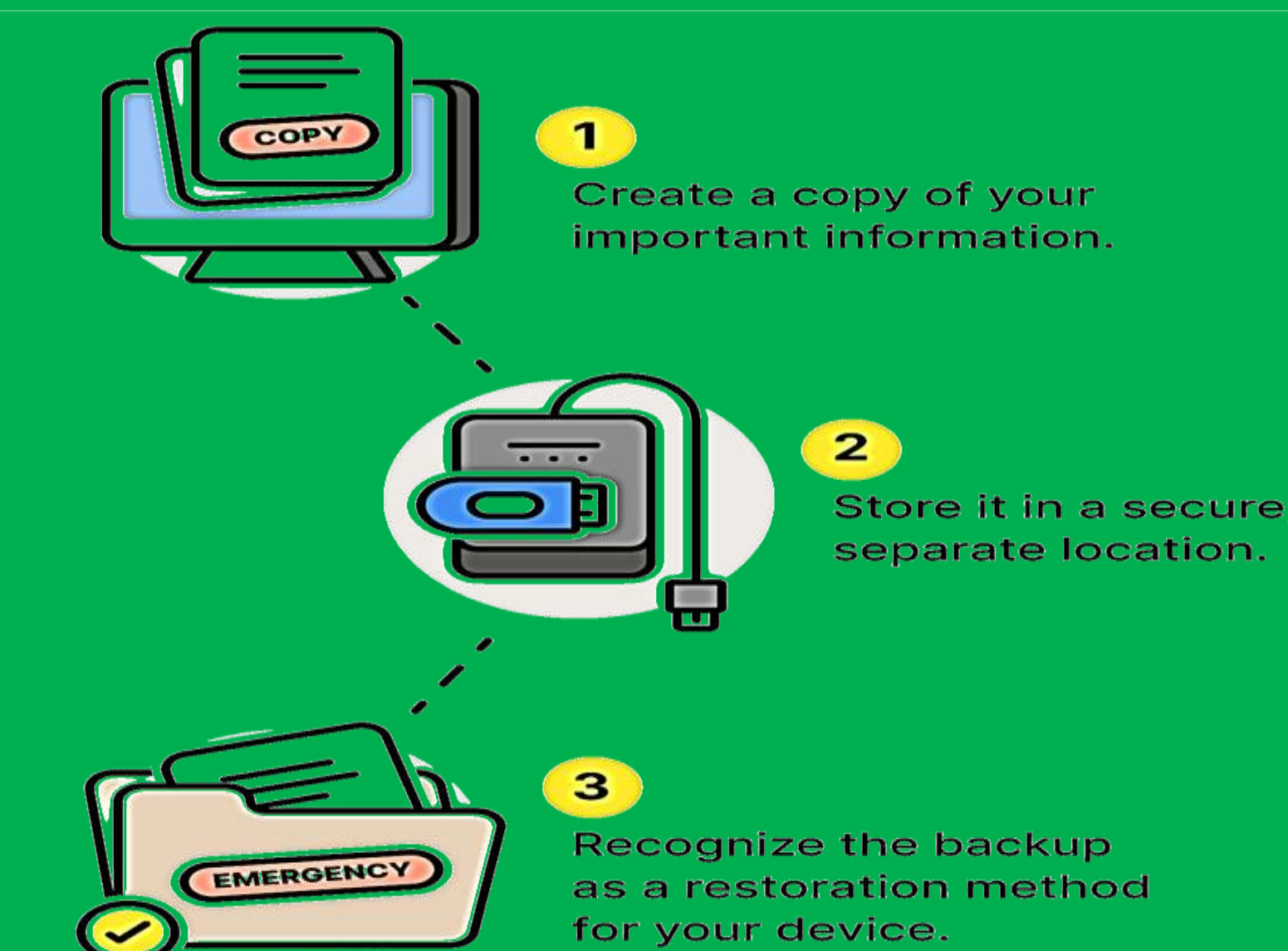


6. Backup Data Regularly

Make a copy of all crucial files and data and save it somewhere safe.

Data restoration is an option in the event that virus or hardware failure occurs.

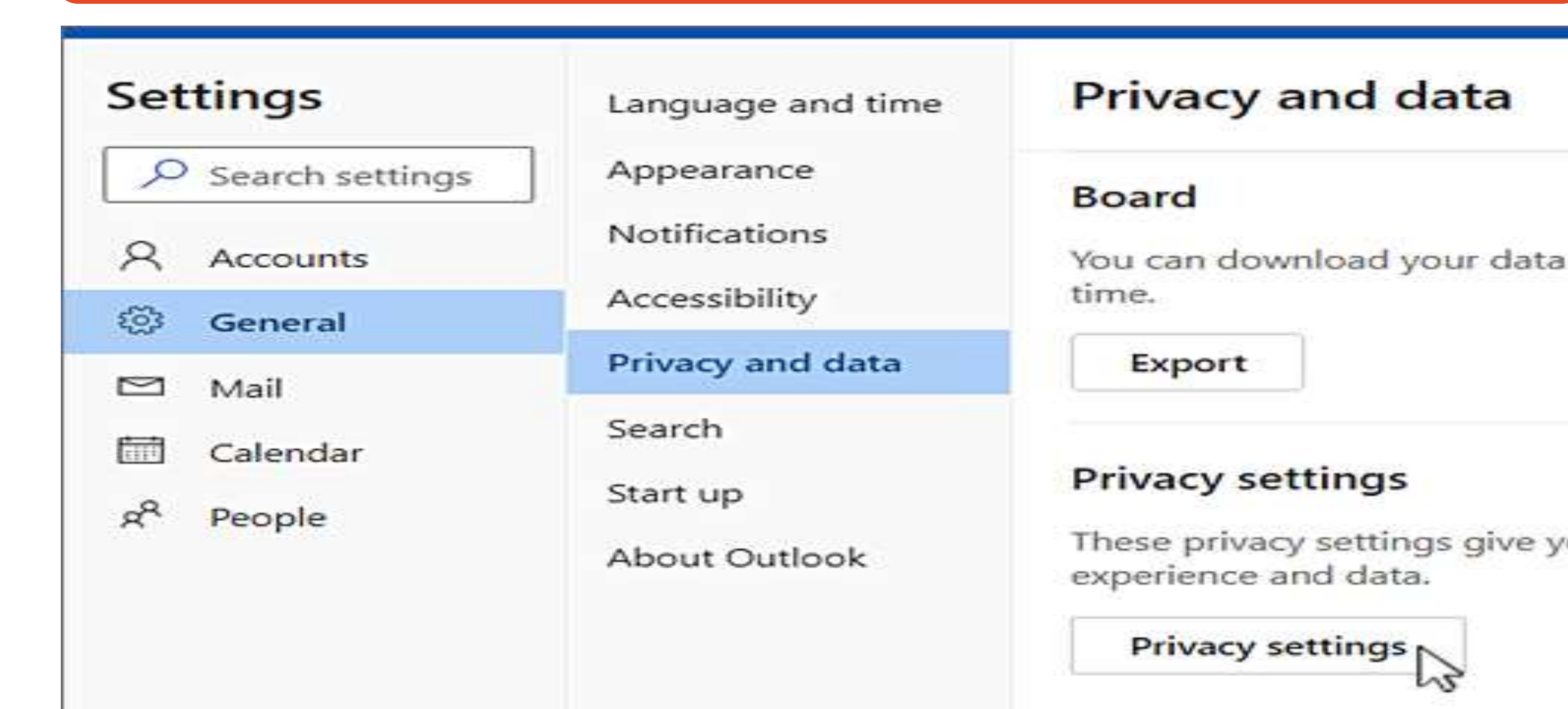
Steps of Data Backup:



7. Privacy Settings

Take a look at your internet accounts' privacy settings and make any necessary adjustments.

Restrict the quantity of private information that is made public



"Stay Safe, Stay Secure"

References

- Finkelhor, D., Walsh, K., Jones, L., Mitchell, K. and Collier, A., 2021. Youth internet safety education: Aligning programs with the evidence base. *Trauma, violence, & abuse*, 22(5), pp.1233-1247.
- Lukasz, T. and Ludvik, E., 2020. Online safety as a new component of digital literacy for young people. *Интеграция образования*, 24(2 (99)), pp.172-184.
- Tomczyk, Ł., 2020. Skills in the area of digital safety as a key component of digital literacy among teachers. *Education and Information Technologies*, 25(1), pp.471-486.
- van der Vlies, R., 2020. Digital strategies in education across OECD countries: Exploring education policies on digital technologies.