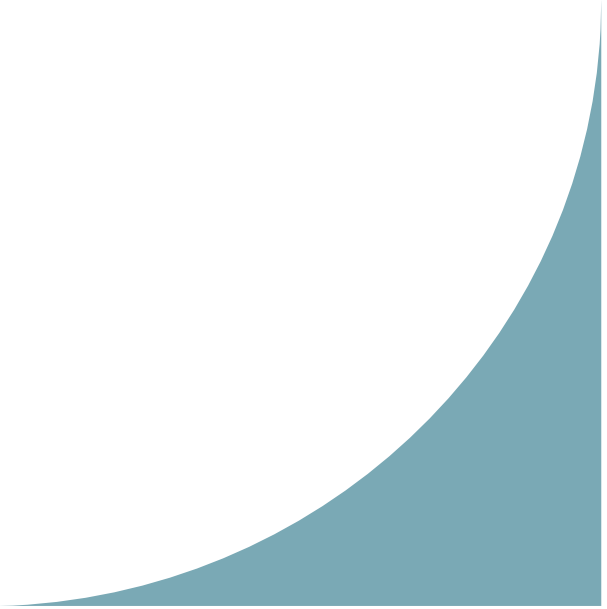
Security update...

Agenda

- Use a separate Administrator Account
- Use “Two Factor Authentication”
- Suspicious emails?
- Look out for “risky” URLs
- Topics for future meetings



Before we start…

- Last Tuesday was “patch Tuesday” so you are all updated, right…?
- You are all using a password manager now, right…?
- You are switching to Passkeys whenever you can, right…?
- If the answer to any of the above is not “Yes” then take a look at November 2024’s slides again ASAP and watch the videos from December 2024
  - Hacking passwords
  - Good passwords
  - What are Passkeys?

Use a separate Administrator Account

- By default, your login account on Windows usually has Administrator privileges
  - That means that not only **you** can do anything but also that any "malware" you may have downloaded can **also** do anything (!) and you won't know it is happening…
- You can get an extra level of protection if you create a dedicated, local, Administrator account and make your own account just a "Standard" account
  - You can still do anything you want **BUT** you will be prompted for your Administrator account password when you try to do something that your Standard account does not have the required privilege to do
- Do these in the order shown:

How to create local administrator account on Windows 11 - Pureinfotech

How to Change Administrator to Standard User and Vice Versa in Windows 11? – WebNots

Use “Two Factor Authentication” (2FA)

- Usually something you know (e.g. password) and something you have (e.g. they send you a code)
- You should turn on 2FA wherever you can
- Turn on 2-step verification (2SV) - NCSC.GOV.UK

Suspicious emails?

- Look at the email address that sent the email

  That is usually a giveaway,

  e.g. an email appearing to be from a company you know has a funny gmail.com address

Look out for “risky” URLs

- Use WHOIS Search, Domain Name, Website, and IP Tools - Who.is to find out more
- Can see who owns it, when it was created, etc…

Topics for future meetings

- VPNs