**Behavioural & Technical Security Controls**

**Behavioural**

1. **If you didn’t request it, don’t trust** **it**
2. **Never download and run a file from a source you don’t 100% trust**
3. **Never enter sensitive information** after following a link or pop-up
4. **Validate the link** by making sure it hasn’t been manipulated e.g., hidden URLs or IDN homograph attacks
5. **Minimise personal information disclosure**
6. **Validate the sender –** contact the sender to confirm its legitimacy
   1. Can even enter the phishing attempt into google and most known scams will match and appear in a search
7. **Validate the attachment –** Virus total, can forward an email to them and they can check it for viruses – will only show known viruses
8. **BUY A PAPER SHREDDER** for offline applications

URLvoid.com

* A website database of all websites that have been reported as malicious or not
* Can enter a link sent to you into this website to see if it has been reported before

Whois.com

* Database to identify what a website is and who’s behind it
* Like typing in a company name into the gov website
* Can find the IP of the server hosting the domain
* Can then do a reverse IP search and see what other domains the server is hosting to identify any dodgy activity

**Technical Controls**

1. **Use an email provider with security** controls to mitigate spam, phishing, malware etc.
   1. Some email clients automatically scan emails for malicious activity
   2. Compromises privacy but increases security
2. **Set up Alerts** – for logins etc.
3. **Change email viewer to be text instead of HTML**
4. Use **safe browsing mode**
5. **Isolation and Compartmentalisation**
6. Using a **VM**
7. **Application white-listing**
8. **Sandboxes**
9. **Opening attachments online** (Google Docs and Etherpad)
10. **Using OpenPGP signatures** to validate sender
11. Use **anti-virus and endpoint protection**
12. **Host files and provide links** instead of attaching to email
13. **Use Live operating** **systems**
14. **Application and Execution** **controls**