Social Engineering Red Flags

Cybercriminals have upped their game. Have you?

Look out for these red flags so you don't fall for cybercriminals' tricks.

Email Phishing

Email Phishing is still the most common attack cybercriminals use to deceive people.

Before reacting always remember to check:

- ☑ The subject line
- ☑ To, From, and Reply to lines
- ☑ Time and Date lines
- ☑ Links and attachments
- ☑ Urgency to action

QR Codes

QR code scams are on the rise and unfortunately here to stay. These codes can be linked to malicious websites and download spyware on your devices.

Be sure to:

- ☑ Avoid scanning codes without knowledge of their origin.

Red flags are everywhere. You just need to know how to spot them. Remember to stop, look, and think before taking any action!

Ransomware

Cybercriminals will attach ransomware, a type of malware, to links and attachments found in emails that will lock users out of their own system if clicked on.

Remember:

- ☑ **Don't pay that ransom!** Paying the ransom does not guarantee you will receive your data back.
- ☑ Always double-check any links or attachments found in emails.

Social Media

Oversharing on social media has made cybercriminal's attacks more effective since the attacks can be more tailored to potential victims.

Be wary of:

- ☑ Profiles with model-like photos
- ☑ Profiles with few connections
- ☑ Generic profile information
- ☑ Direct messages posing as government officials or copyright violations

KnowBe4