HOW TO SPOT IT

**Phishing**

**What is it?**
Like fishing but you are the fish. Attackers use emails as bait to get you to click links and open attachments that install damaging malware.

**Remember...**
- Be CERTAIN before you open or click. If you are unsure, ask a member of Group IT to qualify the link.

**Vishing**

**What is it?**
Like phishing, but attackers try to get you to click links, open files or tell them personal information over the phone.

**Remember...**
- Verify any suspicious calls by checking information with a second source.

**Smishing**

**What is it?**
Like phishing, but over SMS.

**Remember...**
- Don't click SMS links! (and don't reply, as sometimes it's to exploit a premium rate service).

**How to spot it**

- It appears urgent
- It looks official (Check email address is right)
- The message begins and/or ends with a generic greeting
- It asks for personal information
- Layout, design and language might not 'feel' right

**Examples**

- Cure for COVID-19
- Change of bank request
- COVID-19 – Donate to help the fight
- World Health Organisation (WHO)... Virus Alert

Protect yourself and your company from the risk of cyber-attack by understanding common threat vectors and how you should respond to them.

You are the human firewall
Phishing and its variants are part of a larger group of social engineering exploits. IT-driven solutions cannot fully protect against social engineering because they encourage humans to do things that are against good cybersecurity policy!

**DO's AND DON'TS**

**Do's**
- Change **passwords** regularly
- Use **strong passcodes** on all mobile devices
- Keep web browsers and **antivirus patched**
- Verify **suspicious incidents** with secondary sources
- Scrutinise all URLs
- Report incidents to the IT team immediately
- Educate yourself and those around you
- Be sceptical and vigilant

**Don'ts**
- Reuse **passwords** or use obvious phrases
- Volunteer **information** to strangers
- Click on unsolicited email attachments and embedded links
- Plug **unknown USB** drives into your computer
- Fear getting in trouble for reporting issues
- Assume you will not be attacked

**THEREFORE, IT IS VERY IMPORTANT TO BE VIGILANT AT ALL TIMES!!**
What to do if you suspect a compromise?

Raise a security incident by emailing your IT support or call an IT support person.

Do not be afraid to report incidents if you made a mistake.

Please do not be afraid to raise the alarm as soon as possible even if you are worried you have done something wrong.

Remember:
- Change passwords regularly
- Don’t use the same password across multiple systems
- Avoid names, places and colours
- The best passwords can’t be found in a dictionary!

TOP 10 MOST DANGEROUS PASSWORDS

1. password
2. hello
3. cat
4. dog
5. asdfg
6. qwerty
7. 12345
8. p@55w0rd
9. H3110
10. P4$$w0rd

Have you been attacked?

Take these steps quickly if:
- You have experienced a social engineering attack
- You believe you may have been infected by malware
- You believe there has potentially been a compromise of confidential information

Steps:
- Stop using your computer/device – turn it off immediately
- Alert your local IT team where applicable
- Forward any suspicious content to a known IT support email address
- Await further instructions

These attacks can happen to anyone.

Exclusive Networks