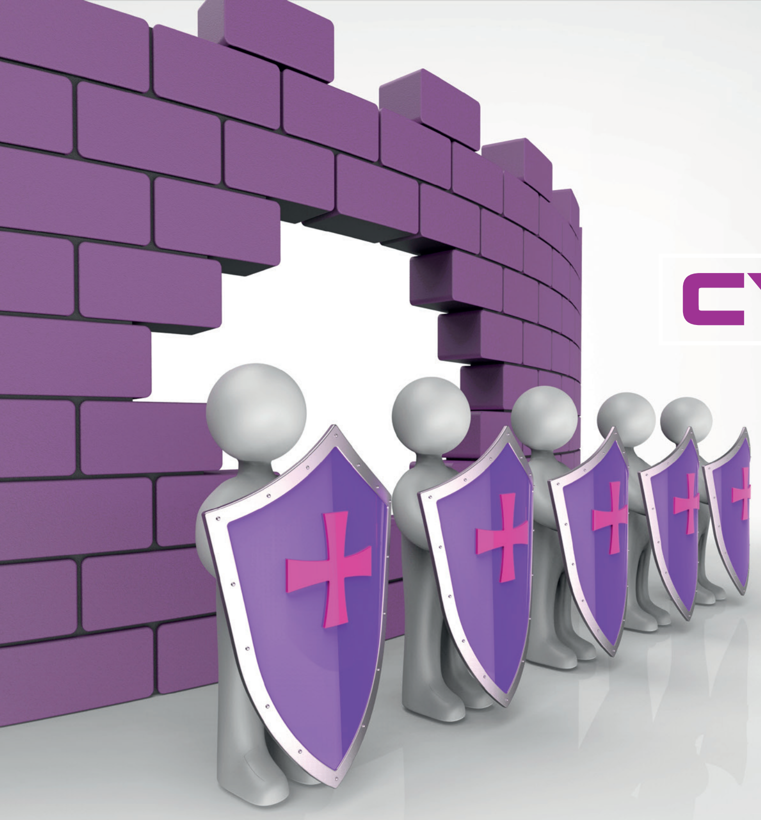

WORKING FROM HOME? BE

CYBER AWARE

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

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.

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

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.

HOW TO SPOT IT

- You have never spoken to the person before
- They called you, you didn’t call them
- Their call demands an urgent response
- Their story is that a process has failed and that their request is routine/no big deal
- They claim to be a colleague or work for company that is important (e.g. the bank, delivery provider, customer, partner)

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

- You have never received messages from this number before
- You don’t recognise the number (if shown)
- It uses the name of a well-known brand (e.g Post Office)
- It contains a link and asks you to use it

EXAMPLES

“CURE FOR COVID-19”

“CHANGE OF BANK REQUEST”

“COVID-19 – DONATE TO HELP THE FIGHT”

“WORLD HEALTH ORGANISATION (WHO)... VIRUS ALERT”

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**
- Bypass mobile device **encryption**
- 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!!

TOP 10 MOST DANGEROUS PASSWORDS

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!

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.

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

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

EXCLUSIVE NETWORKS

Place your company logo here