EXCLUSIVE NETWORKS

CYBER AWARE

YOU ARE THE HUMAN FIREWALL

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

PHISHING

WHAT IS IT?
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 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 using mobile phones as the attack platform. Smishing is carried out via text message.

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

“COVID-19: DONATE TO HELP THE FIGHT”

“CURE FOR COVID-19”

“CHANGE OF BANK REQUEST”

“WORLD H EALTH ORGANISATION 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

THE 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

THE 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:

- Regularly update passwords
- Use complex passwords
- Don't use a password across multiple systems
- Never reuse passwords
- The best passwords can't be found in a dictionary!

1. 123456
2. 123456789
3. 12345
4. qwerty
5. password
6. 12345678
7. 111111
8. 123123
9. 1234567890
10. 1234567

(source - NordPass: Top 200 most common passwords of the year 2021)

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 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.

EXCLUSIVE NETWORKS

insert company logo here