# THE DIGITAL FOOTPRINT & CYBER DEFENCE TOOLKIT

- Online scams are the most common fraud on earth
- Most scam victims are aged 45+
- Online scams are more popular since the pandemic as more people shop online
- Most high value scams use information scraping to build up a picture of the target, the more information that's available the easier it is to exploit

# THE DIGITAL FOOTPRINT

- It's very easy to increase your footprint and hard to reduce it
- It's a collection of information, not just one thing
- There are people actively trying to find and exploit information about you

# THE THREE THINGS TO REMEMBER ABOUT YOUR **DIGITAL FOOTPRINT**

# TYPES OF CYBER ATTACK

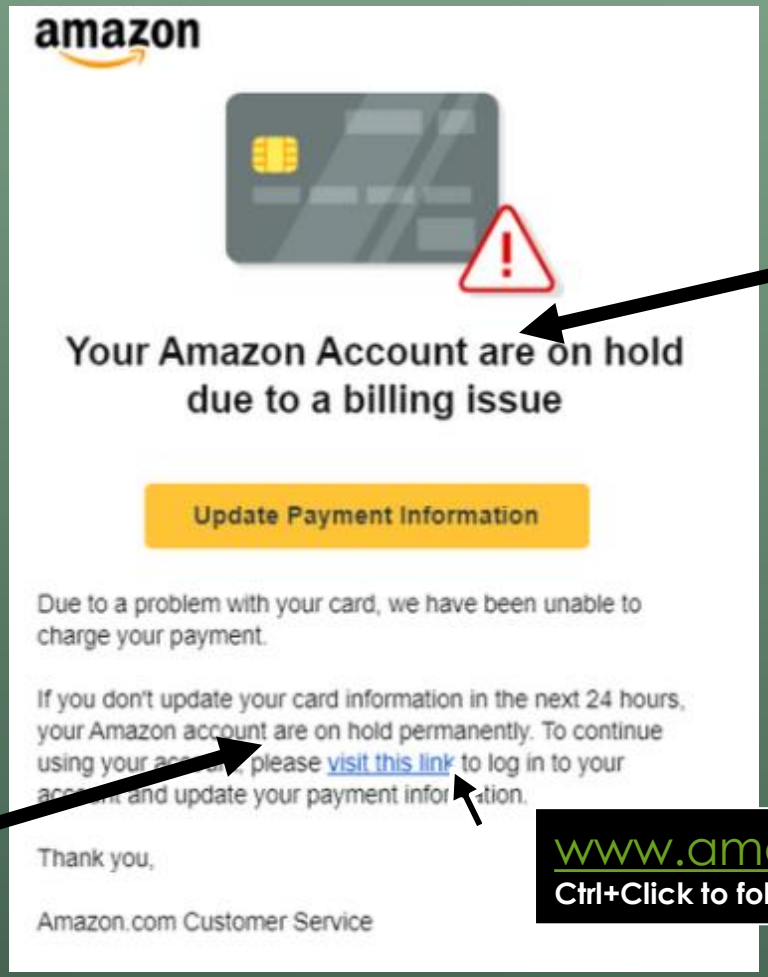
# PHISHING – THE NUMBER 1 ATTACK

# THREAT PHISHING

Who is the sender?

The grammar isn't right

The link seems strange



# LURE PHISHING

Did I Even Enter?

Too good to be true?

Check the links

Who is it from?

Credit cards offer more protection


# IT'S THE BANK CALLING ☺ (VISHING)


Call them back on a known number

Don't give them any personal information

# SHOULDER SURFING

Be observant

Am I on a public network?

Am I being watched?

Am I doing something private?

# WEBSITES

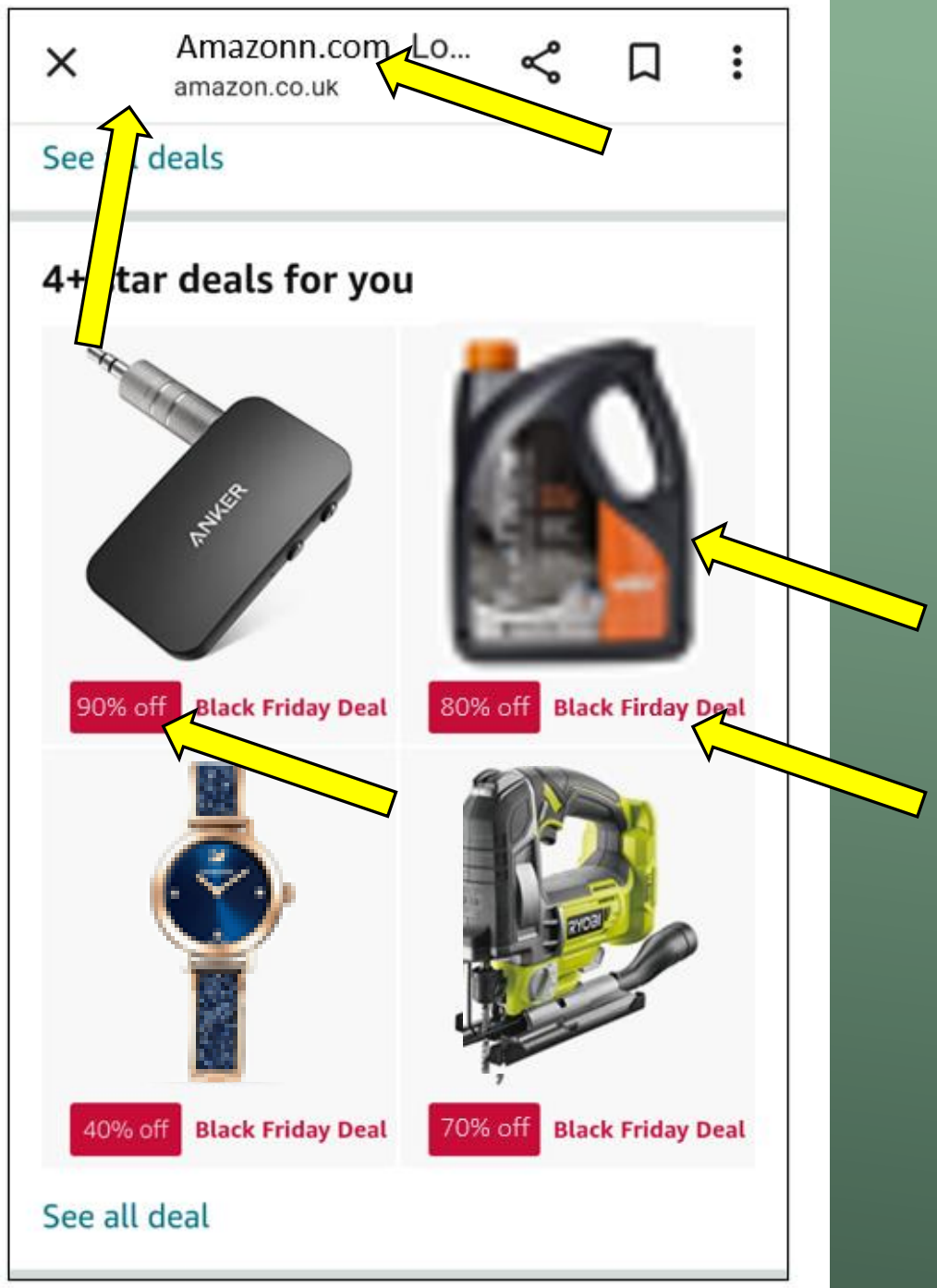
Not padlocked

Address looks wrong

Poor quality images

Spelling/grammar

Deals look too good to be true



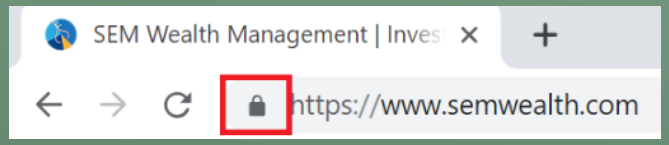
# BUILDING YOUR CYBER DEFENCE TOOLKIT

# GENERAL

- Use multi factor authentication
- Use antivirus software
- Keep your software up to date
- Configure your privacy settings – need to know
- Apply caution when using public networks

# ONLINE SHOPPING

- Is the website secure (look for the padlock)




- Use a credit card rather than a debit card (Chargeback protection)
- Use a dedicated holding bank account

# SOCIAL MEDIA

- Configure your privacy settings and who can see your content
- Think about how your posts build a portfolio of information
- Don’t accept friend requests from people you don’t know

# EMAIL

- Use different email addresses for different purposes
- Use anonymised email addresses
- Don’t sign in to your email on a public network
- Configure your email privacy settings
- Phishing emails. Think about the email and who it’s from, could it be too good to be true?

# PASSWORDS

- Make them strong (Case/numbers/use the £ symbol)
- Only save passwords on trusted devices
- Don’t let others see them you entering a password, especially on your phone
- Don’t share them or leave them lying around
- Change them often and don’t make them all the same

# FINAL THOUGHTS

- Don’t be afraid, the INTERNET IS AMAZING if you tread carefully
- Consider your DIGITAL FOOTPRINT
- Build up your CYBER DEFENCE TOOLKIT
- If you are ever in doubt, don’t click that link!!!