CONNECTING CUMBRIA

Keeping Safe: Phishing, Hacking & Scams

What is Phishing?

Phishing is an attempt used by criminals and fraudsters to obtain your personal information and typically happens when you're sent a convincing looking but fraudulent email, although you may be contacted by phone.

If you've got an email address the odds are you've already been phished. Ever received an email about a parcel delivery you never ordered, or asking you to revalidate your account credentials? These are typical phishes which are relatively easy to spot, but the criminals behind them are smart and keep coming up with more plausible scenarios. These emails are often sent to thousands of individuals in the hope that some will be hoodwinked into supplying personal information. This may include user names, email addresses, passwords, bank account, and credit card details.

These phishing attacks will typically encourage victims to enter details on a fake website which often seem to come from a legitimate organisation. Look out for phishing emails that contain:

- Casual or informal wording that's not in the normal style of an email from a legitimate company.
- Familiar language or tone but poor grammar and spelling.
- 'Verify your account' request - banks will never ask you to enter full account details, passwords or PINs onto a website.
- 'There is a secure message waiting for you' - these messages work by putting the emphasis on reading a message - not your actual account. However, the link in the email will still ask for your personal account details.
- 'If you don't respond within 48 hours, your account will be closed' - such messages convey a sense of urgency that can make you respond immediately without thinking. Phishing emails might even claim that your response is required because your account may have been compromised.
- 'Click the link below to gain access to your account' - sophisticated email messages can contain links or forms that you may fill out just as you would do on a legitimate website.
- 'Dear Valued Customer' - phishing emails are usually sent out in bulk and often do not contain your first name or surname

You will get phished - so how do you spot the bait, and what should you do?

Proceed with caution! Emails can come from anywhere, so until you are totally sure an email is genuine…

- DON'T click links or open attachments; these may infect your computer with a virus.
- DON'T reply to the email, or unsubscribe from the emails.
- DON'T ring any phone numbers in the email.

Remember - company logos can easily be forged in an email, making it look more realistic.

Is it a bait? There are some clues you can look out for…

- Is your name missing? Genuine emails from reputable companies personalise their emails with your name
- Are you asked to do something like validate account credentials or re-activate an account?
- Is it requesting personal data or bank details?
- Did the email come out of the blue? Companies don't just contact you asking questions or offering things without you doing something first.
- Has the email been sent to multiple recipients?
- Is it something related to a current news event? Often criminals will use security incidents that have hit the news to plan attacks e.g. a company lost its customers passwords and they need to be reset.
- If it's from someone you know, does it look and sound right?
- Is the grammar right, are there spelling mistakes?

Check for hooks

- Does the sender's address match the organisation that supposedly sent the email?
- Hover over all links to show where they really go
- Contact the sender organisation. But NEVER trust any contact details or links in the email; always use details from the organisation's website

Get away

- Deleting the message is the safest option
- Don't click links saying unsubscribe, this just shows the criminals they've found an active email account

Further protection

- Anti-virus and software updating

Make sure your devices have the latest anti-virus definitions, up-to-date software and patches. This may still protect you if you are a phish victim. Security loop-holes are regularly discovered in software, and lots of scams exploit these vulnerabilities. To run a self-check on your computer, go to the anti-virus software and run a scan.

- Admin-rights

Some malicious software needs administrator privileges to install on your computer. Avoid running your PC with administrator access except when really necessary.

Hacking and Scamming- Tips to keep you more secure

Social Media:

Always update your social media security settings on a PC/laptop. (The features aren't supported on mobiles or tablets.)

Facebook	Linked In
• Make your Facebook page private. • Make your friends list private. • Make your photos private. • Make all your interests and likes private or simply remove. • Make your posts private. • Remove your education information. • Never activate location on social media. • Think before you check yourself in to locations. • Encourage family members to follow same actions. • Manage your friends list. • Never like or befriend unless you are sure of the person or site. • Treat every click or link as suspicious - always check links.	Ask yourself 2 questions • Do you need LinkedIn to do your job? • Are you looking for a new job or contracts? If the answer to both is no, why are you on it? • Remove all interests. • Reduce job title and description to basics. • Remove location information or never be accurate. • Switch off the "viewers of this profile also viewed option" - click on 'me' button then 'settings and privacy' to change your security. • Make sure your profile is set to private with "Edit your public profile and profile viewing options". • Treat every click link or view my profile as suspicious - always check links or confirm people before you accept.

The Internet

• Check to see if a site is HTTPS not just HTTP, although this is no full guarantee of security it will gives some assurance. • Avoid peer-to-peer programs they often are a honey pot for scammers and hackers (if it's too good to be true, it usually is!). • Make sure you run and update your antivirus weekly (minimum). • Make sure your antivirus is installed and running on your mobile phone. • Use and run other programs such as Malwarebytes (free malware detection and removal program). • Avoid signing-up to things and giving out your information. If you have to give it, be inventive.	**Tips to reduce your online footprint** • Clean up your social media footprint and behaviours. • Deactivate any primary accounts or adjust setting to private. • Remove unused old accounts created in past, use google tool deseat.me to help identify and remove old accounts. • Recommended to run self-Google search every 6 to 9 months to check your footprint. • Remove yourself from all search engine results. • For accounts you're unable to close, post fake personal information about yourself. • Consider paying to use data cleansing programs to remove your footprint from the internet, such as: 'delete me' and 'just delete me'.

CONNECTING CUMBRIA

Mobile Phone Security

- Always review Apps before you install them. Apps are often poorly made with security vulnerabilities. And scammers often use free Apps as bait. (If it's free - is it really? What is the app asking for? What are others saying about the App?)
- Install your anti-virus app on your mobile phone and activate it.
- Try to avoid free Wi-Fi. Scammers often use this to access your login details. If using free Wi-Fi, activate your VPN and use a good VPN app such as private internet access.
- Always lock your voice mail messaging with a pin, scammers can spoof your number and access your messages.
- Watch for people shoulder surfing your mobile pin or you logging in on your phone. This sound simple, but often it's the easiest way to obtain peoples login details.

Passwords

Do

- Choose a password with at least 8 characters, and a max of as many as you are allowed.
- Try using 3 random words to create a random phrase: (#use3*wordsand) (always#thinkrandom*). You could use a hobby. If you love football then use 3 words connected to the game such as "striker, boots, goalie".
- Use a random phrase special to you with no spaces and characters added. #1iBoughtmy(blueshoes)@nexton301017. Tell a story and you will remember.
- Using a combination of letters, numbers and characters is good practice. Adding these into your 3 random words or phrase will make it even stronger.
- Changing words to numbers or characters is good such as: star=* / at=@ / and=@nd / For=4 / To=2.
- Have different passwords and change them regularly, don't be in the 70% of people who don't!
- Use a Password Management Tool (e.g. Keepass, TrueKey, LastPass etc.)

Don't

- Don't use your username, actual or business name and avoid using obvious inspirations such as children/partners/pet names/key dates in your life. Passwords can be discovered by social engineering or manual guessing which is why these are considered weak.
- Don't use common dictionary words as the main part of the password such as a month, admin, password, or a numeric sequence such as 12345678.
  (They're in the top 10 most commonly used passwords and would be cracked instantly.)
- Don't use single words (dictionary words on their own). Hackers can use what's called a dictionary attack to try hundreds or even millions of possibilities using words in a dictionary.
- Don't recycle the same password across all your accounts or use a variation on the same password e.g. password1, password2 etc.