Pop-Up Group - How to avoid Being Fooled by Scams

Criminals try many ways to trick you into giving away your personal or financial information via the internet. They can then gain access to your accounts and steal your money.

Some Basic Questions to ask yourself

When you receive a dubious communication, try asking yourself:	Scam (Y/N)?
Is this unexpected? Out of the blue?	
Is it too good to be true? [like a windfall]	
Is it using scary or threatening language ?	
Does it insist I act immediately?	
Does it avoid calling you by name? (eg Dear Valued Customer)	
Does it insist on my passing on or "Sharing" the message?	
Is the spelling, phrasing and general style unusual? (overly familiar perhaps)	
Are they asking for payment in advance before any work, competition entry etc?	
Does it give me reasonable time to think about it?	
It is expressed in a calm and reasonable manner?	
Can I **phone them and ask** if it's genuine? Use a **number you already have**!	

More subtle clues

Does a message call you by name rather a lot?	
Is the "From" address mis-spelled? Do the name and address conflict? *	

* Checking an email's "From" address

The "From" **name** may look right, "Nationwide", "HMRC" or a friend's name, but examine the ***email address*** *too* - given inside **<**angle brackets like these**>** and containing the @ sign.

The *address* usually appears next to the *name*, but sometimes you have to dig deeper, eg

a) choose "details"
b) or choose down-arrow at the end of the name
c) or or hover the pointer over the name or right-click or long-tap on the name

Time for some Examples ...

We will look at some on the screen. Which of those questions will expose the scams?

Precautions you can take or yourself

1. Use strong passwords that are different for each email, computer, shop account ...
2. Change important passwords often
3. Keep the operating system and security software up to date
4. If you receive a message you don't trust, delete it
5. If you are suspicious but don't want to ignore it, then
   - If you recognise whom it appears to come from, phone them and ask!
   - If it is phone call you are suspicious of, check it from a different phone
6. Follow any advice given by your bank, the police etc
7. Opt out of the "open register" of the electoral roll - contact the City Council
8. Make your landline number ex-directory?
9. Install an Antivirus app? (Avast, AVG, Kaspersky, Malwarebytes, Norton, ...)
10. Check you have a Firewall (usually on the router)

Protect your friends and other people

- Delete unnecessary entries in your address book or contacts
- Send group emails using BCC (blind copy)

Web sites can be Fake or Spoofs - Look out for:

- Unusual or odd looking screens
- Unexpected requests when banking, such as asking your security information in full?
- Your anti-virus app may helpfully warn you about a potentially fake site when you try to open it. **Do not ignore the warning.**
- Look above the page at the **web address** - does that look unusual or odd?
- Are you being asked for more security or personal information than usual?

References

- **Get Safe Online** - www.getsafeonline.org/- choose Protecting your computer
- **Age UK** - www.ageuk.org.uk - search for **staying safe online** or choose Menu then ... > Information and Advice > Work & Learning > Staying Safe Online
- The **Which?** Magazine (subscription needed!) - which.co.uk.
- **Janet Elizabeth** > **Be Safe** - janetelizabeth.org.uk - choose **computer help** then **Be Safe** there are my favourite links at the end,
- **Ask Leo** - askleo.com - search for Best Antivirus and ignore adverts "AD" (adverts)!
- Have any of my passwords been hacked (pwned)? - haveibeenpwned.com

Why does it matter?

Opening an email does no harm, but following a scammer's instructions can do damage.

- A harmless looking **phone number** could be a very expensive one
- Using **saved passwords** and web history, they could spend your money at online shops
- If you give criminals access to your computer and files, they could lock your files and demand a **ransom**.
- Blackmail
- Through your address book they can **scam your friends** and family
- Using away your payment card or bank details they can clean out your account
- They may sign in and **impersonate you** as you on social networking sites like Facebook
- Access to your data could even let them **impersonate you in real life**