# Beware Fake Emails

This article contains guidance on how to recognise suspicious emails, things you should not do in response and some action you can take.

## Recognising Suspicious Emails

It will look like it has been sent from a valid source, such as: someone you know and trust, your bank or building society, a solicitor, a delivery company, a retail company, a charity, a government department, a lottery or similar. This is not a complete list.

- It may contain a vague request that will cause you to want to find out more, such as "Apologies for bothering you. Could you please do a quick favour for me?".
- It may simply ask you to click a link, it may imply that the link will be something important, interesting, humorous, etc, or it may not offer any explanation for the link.
- It may suggest that you have won a large amount of money in a lottery or other competition, and they need your bank details so they can transfer the winnings into your account.
- It may claim that your bank or building society has been hacked and they need your details so they can transfer your money into a secure account.
- They may claim to be a solicitor acting as executors for a deceased person who has left some money to you, and they need your details etc.
- They may claim to be a delivery company with a package for you and they need you to agree a delivery time.
- They may attach a file that they tell you is your invoice.
- They may claim to be a charity asking for donations.
- They may claim to be a government department, and apparently you're entitled to some benefit, and they need your details etc.
- If they have already hacked someone you know, they may claim to be that person who has gone abroad on holiday, suffered some kind of calamity and is in desperate need for some money.

- They may claim to be the company that issued your credit card and your card needs to be replaced with a new one so they will send someone round to collect your current card but they need you to tell them your pin number.
- They may claim to have detected a virus on your computer and you need to install their anti-virus software to remove that virus, and they demand payment for their software. However if you fall for that and install their software it will turn out to be a virus that will really infect your computer.
- If you receive an email asking you to authenticate or verify your email address, and you have not made any arrangement with our webmaster to issue an email address to you, then you should treat it as suspicious, and you should not reply to it, don't click any link in the email, and don't open any attachment it may have.

Possibly many other ruses that try to get you to reply, click a link or open an attachment.

They are looking for proof that your email address is active and that you read and reply to emails, and if they get a response from you they will put your email address on their list of confirmed addresses for further targeting, so if you don't respond to them in any way they will not get that proof.

They are trying to get you to divulge your security information which they can use to steal your money and/or your identity.

An attachment or a link to a website may open up an opportunity for them to install a virus onto your computer.

## Things You Should Not Do

- Never reply to a suspicious email. Any reply to a suspicious email will go to the cyber criminals instead of the apparent sender of the email.
- Never click any link in a suspicious email.
- Never open any attachment in a suspicious email.

## Some Action You Can Take

If your email app includes a button or link for "show full header" or "show original", click that and it will display a load of technical gobble-de-gook, which includes information that professional fraud investigators can use to determine where the email actually came from, so they can track down the cyber criminals and take legal action against them. If the technical stuff opens in a new tab, you will need to select, copy and paste it into what you send to:

report@phishing.gov.uk

For more information, see The National Cyber Security Centre:

https://www.ncsc.gov.uk/collection/phishing-scams/report-scam-email

Please note... You should not report a crime to the NCSC in this way. If you think you may have been a victim of fraud or cyber crime, and live in England, Wales or Northern Ireland, you should report this to Action Fraud at www.actionfraud.police.uk or by calling 0300 123 2040.

If you know the apparent sender of the email and you know how to contact them without replying to the email, you should try to let them know that their email or computer has been hacked, and they should scan their computer, change their passwords and cancel their hacked email account and start a new one with a different password.

If you have done any of the things in the "Things you should not do" section above, you should assume that the cyber criminals now know your email address and they are likely to target you in some way, so you also need to take precautions to avoid being a victim.

## Other Precautions

As a precaution before you receive a suspicious email, make yourself familiar with what your email app always displays near the top of the screen before displaying what the sender sent to you, so you will know any links provided by the email app, such as "show original" or "show full header", and try these out so you will know what they do.

This how it looks in gmail:

Reply | Reply to all | Forward | Print | Delete | Show original

When you click "Show original", the technical stuff opens in a new tab, you can select and copy this info to include in your report to report@phishing.gov.uk; simply close the tab to return to the normal email.

In Outlook, you need to click the "More actions" button, it is three horizontal dots to the right of the reply and forward buttons. A pop-up menu appears, from which you choose "View" and then "View message source". The technical stuff then appears in a new pop-up window, you can select and copy this before closing the window.

Other email apps will have similar methods, so find out what your app does.

Make regular back-ups of your data to an external hard drive or other separate storage device.  It's also worth keeping a copy of software setup files that you used to install software, along with any authentication codes that prove you're a valid user of the software.

Do not keep your back-up drive connected to your computer while also connected to the internet; someone I know used to have both connected at the same time and a virus got onto their system and infected both the main computer and their back-up device as well as their cloud back-up, so they lost all their data.

Always follow this procedure:

1. disconnect from the internet,
2. scan your computer for any virus and deal with any that the scan finds,
3. connect your back-up device,
4. scan your back-up device to make sure it is clean,
5. perform your back-up,
6. disconnect your back-up device,
7. reconnect back onto the internet.

If cyber criminals destroy your data or steal it and demand a ransom, you can re-install your operating system and recover your data from your back-up device.  Also change all your passwords and email address.  Then you can use your saved software setup files to re-install your additional software.

Always have a good internet security package running on your computer, install updates when they're available, and run regular scans of your computer.

Install Windows (or Apple or Google) updates as they are often to improve your computer's security.