

# Phishing



## Phishing - the facts

Phishing is, unfortunately, a far from uncommon activity where a fraudster or crook attempts to part you from your money by gaining access to sufficient details to allow him or her to access your bank account or use your credit card for their benefit.

In short to get their hands on your cash!"

Phishing uses fraudulent e-mails and 'copy cat' websites to try to trick you to reveal sufficient details of your account to allow them to siphon money from it, or to steal your identity.

The starting point is that you receive an e-mail that purports to come from your bank (or other financial organisation) that usually asks you to 'verify' your personal details and helpfully provides a link to allow you to do this.

The link appears genuine **but will not be.**

The reason that is given as to why you are being asked for this information is sometimes "because of an upgrade", or because they want "to pay a tax rebate into your account", or (cleverly) because they think "your account is compromised and they will stop access unless you respond"!

Be aware and read the e-mail carefully - generally the English is bad - both in terms of spelling and grammar. **Don't click the link!**

## The Golden Rules

- **If it's too good to be true – it probably is!**
- **The Bank, the Police will never ask for your pin number**
- **Regularly check your bank and credit card statements (for suspicious activity)**
- **Keep your credit card with you at all times – don't give it to anyone or lose sight of it in a restaurant a hotel or a shop**
- **Don't be fooled because it looks as if it comes from your Bank**

**Credit Cards Bank Details Pin Numbers Names**  
**Addresses Documents Identities Personal Data**  
**Bank Details Pin Numbers Names Addresses Documents**  
**Identities Personal Data Credit Cards Bank Details Pin Numbers**  
**Names Addresses Documents Identities Credit Cards Bank**  
**Details Pin Numbers Account numbers Personal details Data**

## Don't be caught ...

### URGENT !! Messages

One way those 'phishing' try to get you off balance is to use fear to trigger the response they want - which is you providing your details to them!

The e-mail will warn that unless you respond you will lose access to your account, or that they have detected illegal activity on your account and in order to prevent further loss you must verify your information.

To repeat ... **Banks will never ask for your pin number.**

If you are concerned just pick up the 'phone and call your Bank or whoever the e-mail purports to come from, and check. But make sure you decide what number to dial - don't use any on the e-mail or the website - but then you haven't opened the web page have you?

### Other tips

- Don't e-mail personal or financial information
- Exercise caution about opening any attachments or downloading any files from e-mails that you receive.
- Always log out properly and never leave your computer unattended when conducting financial activities
- Always shred your old financial records - in across shredder at least - and keep your cards safe!

### Five Simple Steps

There are five simple steps to prevent being caught by those 'phishing'.

1. Read the e-mail carefully, if the English is poor it almost certainly hasn't come from where it claims to have come from! Don't click without thinking.
2. Pick up the phone to verify.
3. In order to get to the official website TYPE THE URL YOURSELF - don't click!
4. Keep your computer security software up to date.
5. Read your statements to make sure that the money going out of your account tallies with your instructions.

**This is good advice at any time!**



**Don't end up on the hook!**

### More information from the EU ...

This is an issue that is being taken very seriously by the EU, however at the time of writing it does not appear that a phishing guide has so far been produced, however there is more information on phishing at:

- [http://ec.europa.eu/internal\\_market/fpeg/docs/presentation-microsoft\\_en.pdf](http://ec.europa.eu/internal_market/fpeg/docs/presentation-microsoft_en.pdf)
- [http://ec.europa.eu/information\\_society/activities/sip/safety\\_tips/index\\_en.htm](http://ec.europa.eu/information_society/activities/sip/safety_tips/index_en.htm)

Coventry TechnoCentre  
Coventry University Technology Park  
Puma Way  
Coventry  
CV1 2TT

**Europe Direct-Coventry and Warwickshire**  
Phone: +44 (0)24 7623 6377  
Fax: +44 (0)24 7623 6024  
E-mail: [europedirect@cad.coventry.ac.uk](mailto:europedirect@cad.coventry.ac.uk)

The advice in this guide is provided in good faith, and is believed to be accurate at the time of initial publication.

Individuals are advised to carry out their own research, and seek legal advice where appropriate.

Information provided by, or on behalf of, Europe Direct may not be considered as legally binding.