How to spot a Phish

Phishing is the term given to the activity of tempting you (as one amongst thousands) to give up your personal information. This can include everything from your nick-name to your bank account numbers. The more information that you carelessly or accidentally give away the easier it is for anyone to upscale the value of that information.

Spear Phishing, as the name implies, follows the same principles as general phishing – but is targeted towards one person or one group.

Here are some of the tricks employed to make you give up your precious personal information – and some things to look out for:

1 | Impersonation

As a rule, if your see an email from a known contact you will accept the e-mail and open it. So, to take advantage of this 'habit' the bad guys will create an address that looks familiar – but is different.

e.g. logon@webcasts.com
logon@webcast5.com
John.Knight@Lloyds.com
John.Knight@L1oyds.com

The introduction of other non-European characters can make spotting the difference very difficult. You might find the fake address is hidden under a picture of the address that you recognise.
Take care.

2 | How good is your spelling?

If an e-mail is poorly drafted or contains typos and spelling mistakes – then it is highly likely to be a scam e-mail.

3 | Who is the mail addressed to?

If the mail is not accurately addressed it could well be a phishing mail. It might just be unwanted mail.

e.g. Dear user, Dear Member, Dear “input addressee”
Either way, just delete it.

4 | Does the e-mail ask you for personal information – of any sort?

Don’t be conned: most Cyber Savvy businesses will not ask you for personal data via e-mail (unless encryption facilities are available)
– so don’t give anything away.

5 | Language:

If it doesn’t sound right, it probably isn’t right: ignore it!

6 | Speed is of the essence!

When we are hurried along we are all prone to:
a. make mistakes:
b. miss warning flags that we would notice when not pressurised:
c. make incorrect assumptions for the sake of expediency.

If someone is pushing for an immediate response, they are probably up to no good.
Ignore them if you can.
If you can’t, make them wait.

7 | Who is the e-mail from?

If it's a business one will usually see a detailed 'email signature'. No signature or shabby signature blocks are indicative of a scam in waiting!
Delete the e-mail!

8 | Inspect the integrity of the e-mail.

Does it propose an action 'out of the norm' such as "Please transfer funds quickly"?
Does it suggest a change in receiving bank accounts or business addresses?
Does it demand (or even suggest) that immediate action is required?
Does it direct one to an unknown website: is the website address given current & correct?
If it doesn't feel right or look right – delete the email. (If it is a legitimate e-mail they will re-send it!)

9 | Take care over attachments and redirects to unknown web addresses.

Ignore the invitation unless you are 100% sure that you are 100% safe and will remain that way!

10 | What to do if you think you have a problem: Illegitimi non carborundum

Unplug your computer from the Internet if there is a continuing threat.
Make sure Windows Defender or equivalent is current.
Tell your friends (your e-mail list) that you might have had an issue (Best not to e-mail them!)
If at work – tell your boss or IT dept

Tell your brokers/insurers – Cyber Insurance includes all sorts of useful additional benefits.

BGi.UK
Insurance | Risk Management

www.BGi.uk.com
tel: 01367 246 130 - info@BGi.uk.com
Portwell House, Market Place, Faringdon, Oxon. SN7 7HU