Phishing ?

CYBER ESSENTIALS

bsi. ISO/IEC 27001 Information Security Management

Dr Chris Spencer (D.Sc)

Cyber Security Awareness

What is Phishing ?

Phishing is when criminals attempt to trick us into doing 'the wrong thing', such as sharing some sensitive information or clicking a link to a dodgy website.

A Phishing attempt can be made by a text message, social media, or a phone call, but the term 'phishing' is normally used to describe attacks that arrive by email.

Bad actors send phishing emails to millions of people, asking for sensitive information (like bank details) or trying to convince you to click a link to a harmful website. In addition, some phishing emails may contain viruses disguised as harmless attachments, which can be activated when opened.

How to spot a Phish or a Scam

Spotting a phishing email is becoming increasingly difficult, and even the most careful user can be tricked.

Here are five telltale signs that could indicate a phishing attempt.

Dear Colleague ?

Is the email addressed to you by name, or does it refer to you as a 'valued customer', 'friend' or 'colleague'? This can signify that the sender does not really know you and that it could be part of a phishing scam.

Design & Style

Bad actors will try and create official-looking emails by including logos and graphics.

Is the design (and quality) what you'd expect from the sender?

Threat of Urgency !

Does the email contain a veiled threat that asks you to act urgently?

Be suspicious of words like '**send these details within 24 hours**' or '**you have been a victim of crime, click here immediately**'.

Authenticity

Look at the sender's name and email address. Does it sound legitimate, or is it trying to mimic someone you know?

Hover over any web links and look at the address, is it correct?

Validation

Your bank (or any other official source) should never ask you to supply personal information in an email. If you need to check, call them directly.

Use a contact number you know for them, not the phone number in the email.

Too Good to be True !

If it sounds too good to be true, unfortunately it probably is.

It's very unlikely that someone you don't know will have left you money in their will or is going to give you codes to access films for free.

What to do if you've already clicked?

The most important thing to do is not Panic,
and there are several steps you should now take.

- Open your antivirus (AV) software, and **run a FULL scan**, following any advice your AV or Anti-Malware software suggests.
- If you got tricked into providing your password, you should change it immediately (Never use the same password for multiple accounts, if you have in the past change those also)
- If you have lost money, you should report it as a crime to Action Fraud. - https://www.actionfraud.police.uk

Make yourself a harder target.

Information from your website or social media accounts leaves a 'digital footprint' that criminals can exploit.

You can make yourself less likely to be phished by doing the following:

1. Criminals use publicly available information about you to make their phishing emails appear convincing. Review your privacy settings, and think about what you post.
2. Be aware of what your friends, family, and colleagues say about you online, as this can also reveal information that could be used to target you.
3. If you have received an email which you're not quite sure about, forward it to your IT departments phishing or security email address, or you can forward it to the NCSC's Suspicious Email Reporting Service (SERS): report@phishing.gov.uk

Questions ?

Discussion ?

Group Share ?