Reel 'em in

Whether you realised it or not, you have probably already been a target of phishing, a cyber threat involving a hacker disguised as a trustworthy person or company to retrieve personal information from you. Basically, a virtual con artist.

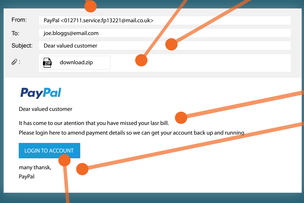
You may be confident that you are unlikely to fall prey to this type of scam, but the severity and realism of these attacks could leave you a little green around the gills. Like most black hats, phishers are reactive criminals. They move with the times and tailor their attacks to current trends whilst taking advantage of our innate human tendencies. It is far easier to trick a human than a computer.

Hook, line and sinker! Could you spot a phishing scam?

Check the sender's email address matches the website address.

Do not download attachments from suspicious emails.

Beware of emails with generic introductions: 'Dear valued customer' etc.



Check for spelling and grammar errors in the suspicious email.

No matter who you think it could be from, always be suspicious of an email that asks for your personal information or login details.

Do not reply directly to a suspicious email. Remember, the phisher is a virtual door to door con artist and can sometimes be very convincing!

Holy Mackerel! 2017 phishing facts

- In a Keepnet Labs phishing simulation to 128 different companies, 48.2% of phishing messages were opened, 31.5% went on to click the malicious attachment or link and 7.9% gave the information and thus enabled the attack to succeed.
- Kaspersky Labs security products blocked 51 million phishing attempts in the first half of 2017 alone.
- Hackers use hacked accounts or 'phish' as currency to trade with one another. If you have been hooked once it is likely that more attempts will be made, especially if the phisher was able to obtain your information.
- Phishing scams capitalise on relevant events, major incidents and global crises.
- Hackers can use web trojans to gather basic information on you whilst you browse the web.

Why 'phishing'

The term was coined in 1996 by a group of hackers who likened their usage of email lures to capture personal data with the sport of angling. 'ph' originates from the phreaking (phone-freaking) hack in the 1970s.

Plenty of phish in the sea

Common phishing scams

Deceptive phishing

Black hats create emails that appear genuine but lure targets to click on malicious links or enter personal information. They often use branding from the company they are impersonating and threaten targets with punishments for non-compliance.

Spear phishing

A personalised attack whereby a hacker learns your personal information from publicly available data to increase the realism of the scam.

Whaling

Essentially the same as spear phishing but targeted at CEOs, directors and other important individuals.

Pharming

Otherwise known as Domain Name System (DNS) based phishing. Hackers configure a website's IP address to take users to a malicious site – even if the user entered the correct URL.

Content spoofing

Hackers replace portions of a site with malicious and misleading content. phishing of this type can appear as an overlay to trap a victim's log in credentials.

Creative phishing scams

Search engine phishing

A hacker creates an appealing but malicious website and employs sophisticated search engine optimisation to make the site rank higher in search results, luring in as many phish as possible.

Typosquatting

Also known as URL hijacking. A hacker creates a malicious website with a URL that closely matches that of a popular web address. The hacker waits for a misspelt URL before reeling in their target.

Angler phishing

A hacker crates a fake Twitter account posing as customer support. The black hat monitors real customer support accounts and responds to customer messages, usually with malicious links.

Dropbox phishing

Hackers have been known to target file sharing services such as Dropbox and Google Docs. The hacker usually displays a fake login page to capture personal credentials.

Something phishy this way comes - scams to look out for in 2018

Security Software phishing

We should expect more phishing attempts in which a black hat is disguised as trusted cybersecurity software. Users rely on their dependable anti-virus software, an ideal means for a hacker to abuse our vulnerability.

Smishing

Otherwise known as SMS phishing. Similar to standard deceptive email phishing but via mobile messaging instead. There has been a recent spike in smishing attacks, so we may continue to see threats of this type in 2018.

eWallet phishing

With the rise in popularity of bitcoin and cryptocurrency, it seems natural that we should expect more phishing attacks that target eWallet users.

Social Media phishing

Social media is a phisher's goldmine. With all that personal data in the public domain, a hacker can with little effort, learn a lot about you. This aside, we should expect to see more specific and targeted attacks on our favourite social media platforms. Whether it be advertising, fake landing pages, fake surveys or games, fake profiles, fake messages from friends; it is all too easy for a phisher to hook innocent social media users.

Don't take the bait

- If you believe you have been a victim of a phishing attempt, report what you know to Action Fraud.
- Regularly check your statements and bills and report anything that seems unusual.
- Ask the sender. If you receive an email from someone you know that seems suspicious, ask them in person. Remember, spear phishing attacks target individuals and can be very subtle and convincing.
- Enabling two factor authentication (2FA) is vital, particularly on file sharing sites like Dropbox which have previously been targeted. 2FA is an extra layer of security, requiring additional information such as a passcode or security question on top of your usual log in data.
- Be wary of surveys and games on social media, many phishing threats are disguised this way.

k3 cloud, hosted and managed services

IT Supply • IT Solutions • Private and Public Cloud

0844 579 0800

Wigan Investment Centre, Wateside Drive, Wigan, WN3 5BA