THE ULTIMATE GUIDE TO PHISHING

Don't let your staff take the bait!

MetaCompliance®

In today's increasingly digital world, so much of what we do, whether it's for business or pleasure, is carried out online. This increase in online activity has resulted in a massive explosion in cybercrime.

Cybercrime has become a powerful tool for criminals looking to steal our personal data and extort money. The speed, anonymity and convenience of the internet has enabled criminals to launch highly **targeted attacks** with very little effort.

According to a recent report from cybersecurity firm **Norton**, cybercriminals stole a total of £130bn from consumers in 2018, including £4.6bn from British internet users.

The most successful and dangerous of all the cyber attacks is **phishing.** Research has found that 91% of all cyber attacks start with a phishing email.

Phishing continues to be the most common form of cyber attack due its simplicity, effectiveness and high return on investment. It has evolved from its early days of tricking people with scams of Nigerian prince's and requests for emergency medical treatment.

The phishing attacks taking place today are sophisticated, targeted and increasingly difficult to spot.

MetaCompliance®

What is Phishing?

Phishing is a type of **online scam** where criminals send out fraudulent email messages that appear to come from a legitimate source. The email is designed to trick the recipient into entering confidential information (ex: account numbers, passwords, pin, birthday) into a fake website by clicking on a link.

The email will include a link or attachment which once clicked, will steal sensitive information or infect a computer with **malware**. Cybercriminals can then use this information to commit identity fraud or they may sell it on to another criminal third party.

Traditionally, phishing attacks were launched through massive spam campaigns that would have indiscriminately targeted large groups of people. The aim was to **trick** as many people as possible into clicking a link or downloading a malicious attachment.

There would always have been a proportion of people that clicked on the link; however, as the general public has become more knowledgeable about phishing, attackers have become more sophisticated in their approach.

The staggering number of emails sent every day around the world means that it's an obvious attack method for cybercriminals. Radicati Group have estimated that 3.7 billion people send around 269 billion emails every single day.

Researchers at Symantec suggest that almost one in every 2,000 of these emails is a phishing email, which means around 135 million phishing attacks are attempted every day.

Types of Phishing Attack

Phishing attacks come in many different forms but the common thread running through them all is their exploitation of human behaviour. The following examples are the most common forms of attack used.

Spear Phishing

Spear phishing is a more targeted attempt to steal sensitive information and typically focuses on a specific individual or organisation. These types of attack use personal information that is specific to the individual in order to appear legitimate.

Cybercriminals will often turn to social media and company websites to methodically research their victims. Once they have a better understanding of their target, they will start to send personalised emails which include links that once clicked, will infect a computer with malware.

Vishing

Vishing refers to phishing scams that take place over the phone. It has the most human interaction of all the phishing attacks but follows the same pattern of deception. The fraudsters will often create a sense of urgency to convince a victim to divulge sensitive information.

The call will often be made through a spoofed ID, so it looks like it's coming from a trustworthy source. A typical scenario will involve the scammer posing as a bank employee to flag up suspicious behaviour on an account. Once they have gained the victim's trust, they will ask for personal information such as login details, passwords and pin. The details can then be used to empty bank accounts or commit identity fraud.

Whaling

What distinguishes this category of phishing from others is the high-level choice of target. A whaling attack is an attempt to steal sensitive information and is often targeted at senior management.

Whaling emails are a lot more sophisticated than your run of the mill phishing emails and much harder to spot. The emails will often contain personalised information about the target or organisation, and the language will be more corporate in tone. A lot more effort and thought will go into the crafting of these emails due to the high level of return for the attackers.

Smishing

Smishing is a type of phishing which uses SMS messages as opposed to emails to target victims. It is another effective way to trick individuals into divulging personal information such as account details, credit card details or usernames and passwords.

This method involves the fraudster sending a text message to an individual's phone number and usually includes a call to action that requires an immediate response.

Clone Phishing

Clone Phishing is where a legitimate and previously delivered email is used to create an identical email with malicious content. The cloned email will appear to come from the original sender but will be an updated version that contains malicious links or attachments.

How Phishing can Damage Your Business

Attacks against businesses have almost doubled in the last five years and the damage from a phishing attack can be devastating. Over the years, businesses have lost billions as a result of phishing attacks. Microsoft estimates that the potential cost of cybercrime to the global community is a staggering 500 billion and a data breach will cost the average company about 3.8 million.

Despite having the strongest security and defence technologies in place, cybercriminals will often exploit the weakest link in a company's defences which is often its employees. Just one human error can result in a massive loss of sensitive data.

Research from Cisco found that 22% of breached organisations lost customers in the immediate aftermath of an attack, demonstrating just how seriously consumers take the security of their data.

MetaCompliance®

A successful phishing attack can result in:

Identity Theft

Theft of Sensitive Data

Theft of Client Information

Loss of Usernames and Passwords

Loss of Intellectual Property

Theft of Funds From Business and Client Accounts

Reputational Damage

Unauthorised Transactions

Credit Card Fraud

Installation of Malware and Ransomware

Access to Systems to launch Future Attacks

Data Sold on to Criminal Third Parties

Top Tips:

to Spot Phishing Attacks

1. A mismatched URL

One of the first things to check in a suspicious email is the validity of a URL. If you hover your mouse over the link without clicking on it, you should see the full hyperlinked address appear.

Despite seeming perfectly legitimate, if the URL does not match the address displayed, it's an indication that the message is fraudulent and likely to be a phishing email.

2. The email requests personal information

A reputable company will never send out an email to customers asking for **personal information** such as an account number, password, pin or security questions. If you receive an email requesting this information, it is likely to be a phishing email and should immediately be deleted.

3. Poor spelling and grammar

Cybercriminals are not renowned for their top-quality spelling and grammar. Whenever legitimate companies send out emails to customers, they are often proofed by copywriters to ensure the spelling and grammar is correct.

If you spot any **spelling mistakes** or **poor grammar** within an email, it's unlikely to have come from an official organisation and could indicate the presence of a phishing email.

Top Tips:

to Spot Phishing Attacks

4. The use of threating or urgent language

A common phishing tactic is to promote a sense of fear or urgency to pressurise someone into **clicking on a link**. Cybercriminals will often use threats that your security has been compromised and that urgent action is required to remedy the situation.

Be cautious of subject lines that claim your account has had an “unauthorised login attempt” or your “account has been suspended”. If you are unsure if the request is legitimate, contact the company directly via their official website or official telephone number.

5. Unexpected correspondence

If you receive an email informing you that you have won a competition you did not enter, or a request that you click on a link to receive a prize, it’s highly likely to be a **phishing** email. If an offer seems too good to be true, it usually is!

MetaCompliance®

How to protect yourself against Phishing Attacks

Identifying a phishing email has become a lot harder than it used to be as criminals have honed their skills and become more sophisticated in their attack methods.

The phishing emails that we receive in our inbox are increasingly well written, personalised, contain the logos and language of brands we know and trust and are crafted in such a way that it is difficult to distinguish between an official email and a dodgy email drafted by a scammer.

McAfee estimates that **97%** of people around the world are unable to identify a sophisticated phishing email so cybercriminals are still successfully tricking people into giving away personal information or downloading malware. Thankfully, there are some steps you can take to avoid being phished.

1. Never click on suspicious links

The most common type of phishing scam involves tricking people into opening emails or clicking on a link which may appear to come from a legitimate business or reputable source.

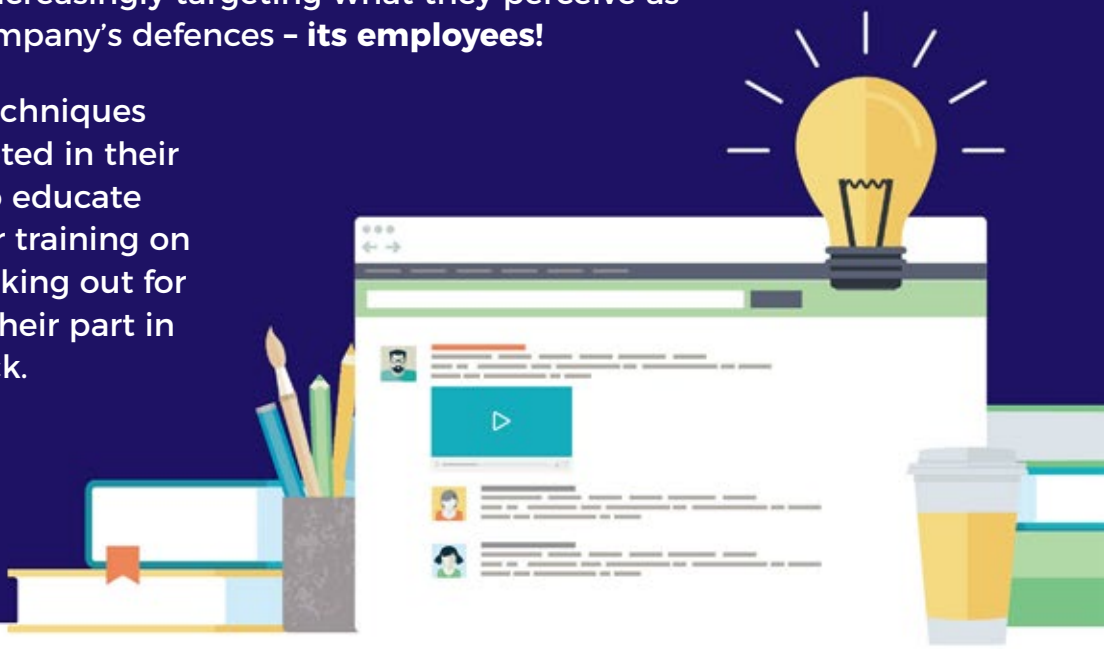
By creating a sense of urgency, users are tricked into clicking on a link or opening an accompanying attachment. The link may direct you to a fake website where you are prompted to enter your personal details or take you to a website that directly infects your computer with ransomware.

2. Educate Staff

Companies may have the strongest security defence systems in place, but it offers little protection if cybercriminals are able to bypass these traditional technological defences and get straight to an employee to trick them into divulging sensitive information.

Over **90%** of all successful cyber attacks are a result of information unknowingly provided by employees. As networks become harder to breach, hackers are increasingly targeting what they perceive as the weakest link in a company's defences – **its employees!**

As hackers hone their techniques and become more targeted in their attacks, it's important to educate staff and provide regular training on what they should be looking out for and how they can play their part in preventing a cyber attack.



3. Be careful what you post online

The internet and social media has transformed how we communicate with each other on a day to day basis; however, this **culture of sharing** has provided cybercriminals with an easy way to profile potential victims ensuring their phishing attempts are more targeted and harder to spot.

Hackers are turning to social media sites to access personal information such as age, job title, email address, location and social activity. Access to this personal data provides hackers with enough info to launch a highly targeted and personalised phishing attack.

To reduce your chance of falling for a phishing email, think more carefully about what you post online, take advantage of enhanced privacy options, restrict access to anyone you don't know, and create strong passwords for all your social media accounts.

4. Verify the security of a site

Before entering any information into a website, you should always check that a site is safe and secure. The first step is to hover your mouse over the URL and check the validity of the web address. You should look for a padlock symbol in the address bar and check that the URL begins with a 'https://' or 'shttp://'.

The 'S' indicates the web address has been encrypted and secured with an SSL certificate. Without HTTPS, any data passed on the site is insecure and could be intercepted by criminal third parties.

However, this system is not totally foolproof, and within the last year, there has been a notable increase in the number of phishing sites using SSL certificates. Users are advised to be extra cautious and look for further evidence that the site is secure.

5. Update anti-virus software

Anti-virus software is the first line of defence in detecting threats on your computer and blocking unauthorised users from gaining access.

It is also vital to ensure that your software is regularly updated to ensure hackers are unable to gain access to your computer through vulnerabilities in older and outdated programs.

MetaPhish™

MetaPhish has been specifically designed to protect businesses from phishing and ransomware attacks and provides the first line of defence in combatting cybercrime.

If you would like more information on how MetaCompliance can help to protect and educate your staff, please visit our website.

MetaCompliance®

E info@metacompliance.com
W www.metacompliance.com

MetaCompliance®