


THE ULTIMATE GUIDE TO PHISHING

Don't let you staff take the bait!

Download the eBook 



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 2017, including £4.6bn from British internet users.

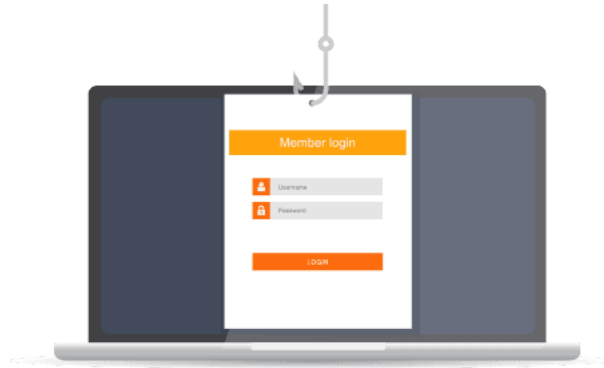
The most successful and dangerous of all the cyber-attacks is phishing. Research has found that 91% of all cyber attacks start with a phishing email.

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.

What is Phishing?

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 2017, 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.



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 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 Attacks

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.

The cybercriminals will often turn to social media and company websites to research their victims. Once they have a better understanding of their target, they will start to send personalised emails which include links which 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 cybercriminals.





Smishing

Smishing is a type of phishing which uses SMS messages as opposed to emails to target individuals. It is another effective way of cybercriminals tricking 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 to a business can be devastating. Over the years, businesses have lost billions as a result of phishing attacks. Microsoft estimates that the potential cost of cyber-crime 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.

A successful phishing attack can result in:



Identity Theft



Theft of Sensitive Data



Theft of Client Information



Loss of Usernames and Password



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 so to Criminal Third Parties

It is vital that businesses take steps to ensure they are doing all they can to educate staff on the dangers of a phishing attack. Training employees in how to effectively recognise a phishing attempt is key in mitigating the risk to an organisation.

For further information on how you can protect your business from phishing attacks, click here (<https://www.metacompliance.com/blog/phishing-attacks-5-ways-to-protect-your-business/>).

For further information

on how you can protect your business from phishing attacks

 [Download Now](#)

Top Tips to Spot Phishing Attacks

Identifying a phishing email has become a lot harder than it used to be as the 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 globe are unable to identify a sophisticated phishing email so the cyber criminals are still successfully tricking people into giving away personal information or downloading malware. Despite the increasing sophistication and convincing nature of these emails, there are still some giveaway signs that may alert us to the presence of a phishing email.



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 is 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.

- 🔗 What is a Ransomware email? 5 (https://www.metacompliance.com/blog/what-is-a-ransomware-email-5-tips-for-how-to-detect-one/)
- 🔗 How to spot a phishing scam (https://www.metacompliance.com/blog/how-to-spot-a-phishing-scam/)

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 is unlikely to have come from an official organisation and could indicate the presence of a phishing email.

- 🔗 Characteristics of a phishing attack (https://www.metacompliance.com/blog/the-art-of-the-phish/)

4. The use of threatening or urgent language

A common phishing tactic is to promote a sense of fear or urgency to rush someone into

clicking on a link. Cyber criminals 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!

How to protect yourself against Phishing Attacks



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.

Legitimate businesses will never send emails requesting you click on a link to enter or update personal data.

🔗 Simulated Phishing Tests for Employees (<https://www.metacompliance.com/blog/phishing-test-for-employees-why-its-important/>)



2. Educate Staff

Companies may have the strongest security defence systems in place, but it offers little protection if cyber-criminals 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.

Don't let your staff take the bait!

MetaPhish has been specifically designed to protect businesses from phishing and ransomware attacks and provides the first line of defence in combatting cyber-crime. If you would like more information on how this can be used to protect and educate your staff.

Phishing & Ransomware



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 cyber criminals 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 the 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.

Read our guide to protecting yourself from hackers

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.

Protecting Yourself from Hackers



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 best way to do this is to look at the URL of a website. If it begins with a "https" instead of "http" it means the site has been secured using an SSL Certificate (S stands for secure). SSL Certificates ensure that all your data is secure as it is passed from your browser to the website's server. There should also be a small padlock icon near the address bar which also indicates the site is secure.



5. Install 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 programmes.

- 🔗 Protecting your from Phishing Attacks (<https://www.metacompliance.com/blog/10-ways-to-protect-yourself-against-phishing-attacks/>)

Products

- › Phishing(<https://www.metacompliance.com/products/phishing-and-ransomware/>)
- › eLearning(<https://www.metacompliance.com/products/elearning-cyber-security-and-privacy/>)
- › Privacy(<https://www.metacompliance.com/products/privacy-management/>)
- › Awareness Management (<https://www.metacompliance.com/products/security-awareness-training/>)
- › Policy Management (<https://www.metacompliance.com/products/policy-management-software/>)

Latest News

- › Blog(<https://www.metacompliance.com/blog/>)
- › Webinars(<https://www.metacompliance.com/webinars/>)
- › Company News(<https://www.metacompliance.com/company/news/>)

Resources

- › Knowledge Base(<https://support.metacompliance.com/>)
- › Dummies Guide to GDPR(<https://www.metacompliance.com/resources/gdpr-for-dummies/>)
- › Free Awareness Assets (<https://www.metacompliance.com/resources/cyber-awareness-posters/>)
- › Blog(<https://www.metacompliance.com/blog/>)
- › Case Studies(<https://www.metacompliance.com/resources/case-studies/>)

About

- › Contact(<https://www.metacompliance.com/company/contact/>)
- › Our Philosophy(<https://www.metacompliance.com/company/our-philosophy/>)
- › Careers(<https://www.metacompliance.com/careers/>)
- › Partners(<https://www.metacompliance.com/company/partners/>)



(<https://www.metacompliance.com/erdf/>)



HM Government
G-Cloud 11
Supplier

(<https://www.digitalmarketplace.service.gov.uk/g-cloud/search?q=metacompliance&lot=cloud-software>)

Gartner | Peer Insights

Software Ratings and
Reviews from
IT Professionals ★★★★★

([https://www.gartner.com/reviews/market/security-awareness-computer-based-training/vendor/metacompliance?](https://www.gartner.com/reviews/market/security-awareness-computer-based-training/vendor/metacompliance?utm_source=metacompliance&utm_medium=referral&utm_campaign=widget&utm_content=YTQxZGYzOTItOTJiOS00YWVjLWVmYWUtMDQ2ODM0)

[utm_source=metacompliance&utm_medium=referral&utm_campaign=widget&utm_content=YTQxZGYzOTItOTJiOS00YWVjLWVmYWUtMDQ2ODM0](https://www.gartner.com/reviews/market/security-awareness-computer-based-training/vendor/metacompliance?utm_source=metacompliance&utm_medium=referral&utm_campaign=widget&utm_content=YTQxZGYzOTItOTJiOS00YWVjLWVmYWUtMDQ2ODM0)



Phishing

eLearning

GDPR

Awareness

Policy

ransomware and Phishing create daily havoc for both consumer and organisations. These are clever scams that rely on human weakness and individual error to obtain money or influence. Only by embedding simulated phishing scenarios as a key aspect of your cybersecurity awareness program can an organisation hope to prepare its staff to avoid the worst excesses of these threats.

MetaPhish (<https://www.metacompliance.com/products/phishing-and-ransomware/>) is a module of our cloud based Integrated User Awareness Management solution that delivers high quality, multilingual training (<https://www.metacompliance.com/security-awareness-training-localisation/>) experiences should the user click on the simulated phishing email. The system comes prepopulated with relevant and high quality content and provides extensive reporting to allow remediation of identified problem areas.

MetaCompliance® © 2021 All Rights Reserved.



Cyber Security Terminology(<https://www.metacompliance.com/cyber-security-terminology/>) Privacy Policy(<https://www.metacompliance.com/company/privacy-policy/>)
Cookie Policy(<https://www.metacompliance.com/company/cookie-policy/>) Copyright(<https://www.metacompliance.com/company/copyright/>)

English

e) td ia
/) n
 c
 e)