# About PHISHING

Like many cyber-attacks, phishing targets many people at the same time, but what is unique to phishing is that the attacker seeks to trick or con their victims into revealing sensitive information. This may take the form of an email, where the cyber-criminal pretends to be someone that you know or trust such as your bank, your work, your PayPal account, Microsoft, the inland revenue or even the police.

Because you might believe it is a legitimate message from someone you know, you are more likely to give the cyber-criminal sensitive data such as your bank details, credit card information or passwords. In an email, there will often be a link that you are asked to click on to address an urgent problem. Often the fake email will contain a link or an attachment containing malware.

### ****WHAT IS SPAM?****

Other than a questionable meat in a can that became a staple of wartime Britain, spam is an unsolicited message sent in bulk from a sender or a company. Just under half of all emails sent are thought to be spam, and in some estimates that could add up to around 107 billion spam emails sent out each a day globally. Most spam messages are irritating advertisements, but some spam messages are harmful and contain phishing or malware.

Never click on a link in an email, social media message or text unless you are 100% sure it is safe and you have expected to receive it. By clicking a malicious link, you could inadvertently instigate a download of malware or ransomware to your computer or your entire home or work network. Malware and ransomware are software designed to do harm.

### ****HOW TO IDENTITY PHISHING EMAILS****

Unfortunately, phishing emails in recent times have become very convincing. There are some ways to check your email without opening it at all.

**Email subject**
The subject of the email is usually something to alert you and cause anxiety. A common one in 2020 is “are you from (insert your town)?” or “You are in DANGER!!!!”

They seem to be very informal, and often have a rather non-uniform structure. Always examine and review your email subjects before opening them.

**Email sender**

The sender of the email usually tries to make the address convincing e.g. sam@microsoft.info.cc. Firstly, most corporations use .com as an address or if based in the UK it is .co.uk or .gov.uk. If the subject or the sender is suspicious, do not open it.

**Email content**

If you hover above the email with your mouse, a box appears with what is in the email dialogue, it will probably be text that is geared to scare the reader with some alarming news that requires urgent action. Phishing emails rarely use your name, instead addressing you as valued customer or such like. These are all clues that this is a scam email.

Microsoft Outlook allows users to preview every email message in the application window before opening them. Do not click hyperlinks sent in email messages unless you trust the sender 100% and you were expecting this message.

### ****TYPES OF PHISHING ATTACKS****

Phishing is one of the most common and frustrating threats we face on the Internet. Most of us know what it is, and how it works, but we still get caught out. The scam, which involves criminals sending messages that masquerade as legitimate sources, targets millions of organisations every day. The messages direct recipients to a bogus website link that may capture personal information or contain a malicious attachment. It is commonly thought that phishing occurs only in emails, but it is now being modified to other platforms such as SMS, social media and phone calling. Anyone could fall victim to one of these scams.

#### **SPEAR PHISHING**

Whilst phishing is based on deploying a phish on a large indiscriminate group, a spear phish is based on targeting a specific person in an organisation or an individual. These messages are usually carefully constructed with aspects of the individual’s personal and work life to goad a response. This is a targeted attack and the phisher will spend a lot more time to procure the information.

The aim of these attacks is knowledge, usually as a way to get ransomware or a virus into the system. These can be very convincing, so stay on alert! If, in the workplace, you receive an unorthodox email from a colleague, contact them with their office number or go and talk to them to check it is legitimate. New members of staff can be especially susceptible to spear phishing attacks which is why cyber security training needs to start on day one.

#### **WHALE PHISHING**

Whale phishing is like spear phishing but even more targeted, taking aim at the senior executives of organisations. It has exactly the same intentions but a very specific vector. Head of HR is a common target for whale phishing. Techniques used in whale phishing are much more subtle than any other phishing attack. Tricks like fake links and malicious URLs aren’t very effective in this instance, as criminals attempt to imitate senior staff members. Scam involving fraudulent tax returns are a common way of whaling. Tax forms contain considerable amount of personal information: names, addresses, bank account information and social security numbers.

#### **VISHING & SMISHING**

Vishing and Smishing make use of telephones to replace emails as the method of communication. Smishing involves criminals sending text messages and Vishing involves telephone conversations. A common vishing scam involves a criminal posing as a fraud investigator telling the victim their bank account has been breached. Another commonly used vishing scam involves posing as compensation claim company asking about their recent car accidents.

In both cases, the aim is to get debit/credit card information from potential victims. These attacks are usually aimed to retrieve information for more organised groups, and any information that can be procured will help target you in a more sophisticated attack.

To prevent this, only answer calls that you are expecting or from recognised callers. If you accidentally answer the phone to someone you don’t know who is asking about your life or accounts, just hang up and block the number. Smishing is very similar to vishing, but done in SMS text message format. They will have links or messages to try and incite a response but do not answer these. Do not click the links, just delete them immediately.

#### **ANGLER PHISHING**

Social media is a relatively new attack vector which offers many ways for criminals to trick people. Angler phishing can involve a criminal masquerading as a customer service account or a legitimate business on social media, hoping to reach dissatisfied customers, and luring their victims into handing over access to their personal data or account credentials.

### ****AWARENESS IS YOUR BEST LINE OF DEFENCE****

If you receive an email, a text message or phone call from someone who says they are your bank or any other institution, always be suspicious. A legitimate company will never phone or email you and ask you for your passwords or bank details. If you are in doubt, delete the message and go to the company’s website and find their phone number. Call them to check that they have been in touch with you.

There are no technical controls that you can put in place to address phishing. This is very much a people’s problem and the attacks are conmen. These conmen take advantage of busy and stressed human beings who are likely to make a mistake of giving information away. They deliberately put pressure on the victim by creating some kind of urgency, telling you that your bank account is in danger, you have a huge fine or that your PayPal account has been frozen, and then they use that emotional disturbance to enable you to make a poor and rushed decision.

These kind of attacks are also known as ‘social engineering’ which means that attackers manipulate people instead of technology, the way to protect users from phishing attacks is education and awareness.