Beton Bauen
SPECIALIST CONTRACTING

DEALING WITH PHISHING EMAIL
GUIDELINES

DEALING WITH PHISHING EMAIL
GUIDELINES

Introduction

How can we protect our business from email phishing scams? This guide explains what to look out for and how you can avoid falling victim.

Scams come in all shapes and sizes, from dodgy emails to fake sites, SMS or Whatsapp, there are lots of attacks and these are growing with frequency.

Phishing attacks are the most common method used to breach organisations today and count for over 80% of successful attacks. All businesses, regardless of their size, will store information that is of value to cybercriminals, such as customer details or payment information.

Sophos tell us that 41% of IT Professionals report phishing attacks on a daily basis, and that 30% of phishing emails are opened by users, so the need for education and prevention when it comes to phishing is as necessary as ever.

What is Phishing?

Email phishing is a method used by cyber-criminals to access valuable information, such as usernames and passwords or account details. Often, the email will direct the recipient to click links and to provide information at the website the links take them to. The emails are often sent at random to thousands of people at a time.

The email claims to come from a reputable company such as your bank or credit card company, social media accounts or logistics companies such as DHL, Parcelforce, etc. The most commonly imitated brands include Apple, Netflix, HMRC and WhatsApp.

How Does It Work?

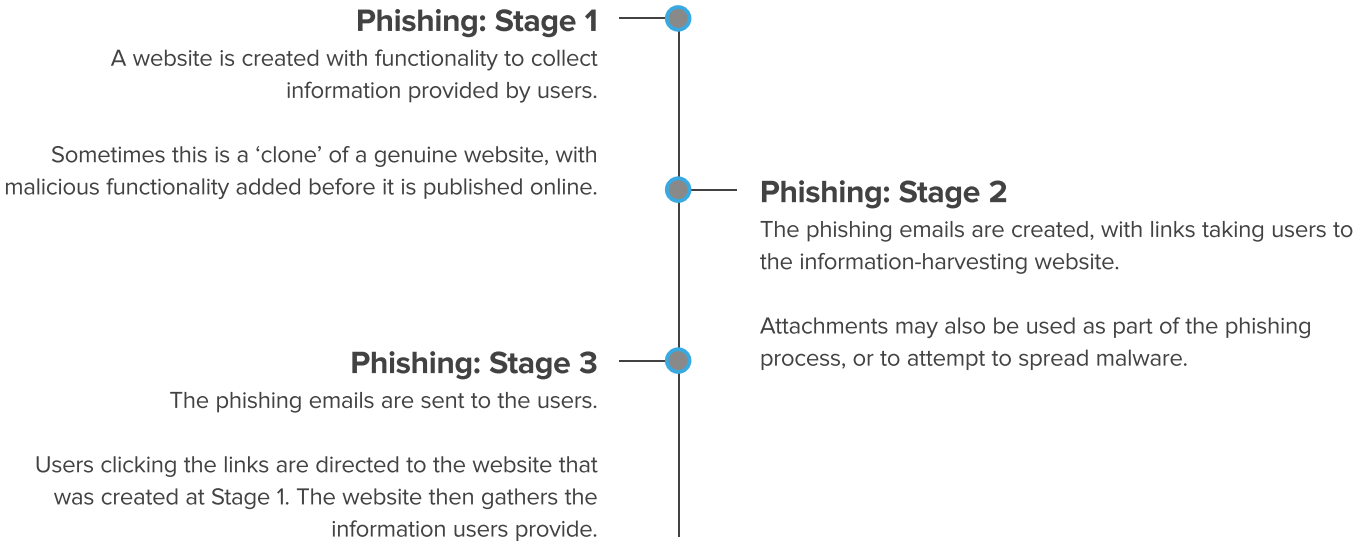
Phishing emails (and websites) are typically designed and stylised to look like a genuine email from a legitimate sender. Phishing is a type of 'social engineering': attempting to manipulate someone into performing actions they otherwise wouldn't. The emails are often designed to try and trick people into panicking and visiting a bogus website, usually by claiming they need to “verify” or “update” your details, or “reactivate” an account. Senders will typically ask users to click a link to a website designed to harvest credentials, or open an attachment – usually malware – that can infect devices.

Sometimes a phishing email doesn’t include a link, but could come in the form of an unexpected invoice, or a request for a statement (outstanding invoices), perhaps threatening legal action if you don’t pay up immediately or alternatively more positive emails with the promise that you are due a tax rebate.

Phishing attacks are an all too common threat and can cause security breaches and data leaks for businesses, no matter how large or small.

DEALING WITH PHISHING EMAIL GUIDELINES

See below to learn more about the three stages of phishing.



However, the scams can be more targeted, too. Spear phishing is where someone acts as a trusted sender, like one of your clients or suppliers, in order to get you to divulge confidential information or transfer funds and invoice fraud is seen with increasing regularity. Whilst this requires more research on their part, you and your employees are far more likely to send such information, or process payments, to someone that you trust.

What's the Point of Phishing?

Obtaining personal data or sensitive information can allow a cyber-criminal to perform further actions more easily than they could do without it. Data collected could provide enough for a cyber-criminal to perform identity theft procedures, and then obtain financial services; or, where passwords have been collected, the attacker may be able to compromise accounts (like email accounts), or even gain full remote access to a computer.

Why is it Called Phishing?

It's generally agreed that the earliest phishing attacks, in the mid-90s, targeted AOL users with attempts by cyber-criminals to steal account details and passwords. This practice was likened to fishing (angling), as the email functioned as a sort of 'bait' or 'lure', and it only needed a few people to 'bite' to make it worthwhile. The 'ph' in phishing replaces the 'f' from fishing in a reference to phreaking, a common hacking style in the late 60s and early 70s involving the manipulation of phones and phone networks.

DEALING WITH PHISHING EMAIL GUIDELINES

Different Types of Phishing

Using phishing simulation, Proofpoint, a US security company, found in their 2019 report that attackers are continuing to focus on people, rather than on trying to defeat technical defences.

An interesting observation in this report is around the awareness and understanding of different age groups. Whilst the 'millennial' generation (as 'digital natives') have been raised on smart devices, a heightened level of user skill doesn't mean a good understanding of cyber security. When asked to answer the question “what is phishing?” 47% of responders in the 18-21 age bracket provided a correct answer, while 58% did in the 22-37 age group, 68% were correct in the 38-53 age group, and 73% in the 54 and above age group.

This cyber-crime can come in different forms - let's look at the most common.

What is Spear Phishing?

Spear phishing is a phishing attack that is directed at a specific individual or organisation. The definition of phishing includes the principle that the attack is based on a mass distribution of emails or messages. Users are not targeted individually, and there may be thousands of recipients.

Spear phishing, however, is a **targeted attack**. The attacker spends more time crafting the email, usually adding details that personalise it in some way (e.g. an attacker that knows, from public information, the place you work and a number of your colleagues, can create a spear phishing attack that uses these details to make it appear more legitimate).

As the distribution of a spear phishing attack is more targeted, it tends to be the case that the request is also specific. A common spear phishing attack requests that an employee performs a payment or transfer of funds of some type, by posing as a senior employee within the organisation. Even tech companies can be victims of spear phishing, as Snapchat found in 2016 when an email claiming to be from the CEO was sent to HR, who then proceeded to provide the information requested.

What is Whaling?

Whaling is a spear phishing attack that is directed at a **senior person within an organisation**, like the Managing Director, Finance Officer or Headteacher. Like spear phishing, whaling is usually a targeted attack, and the attacker typically spends more time preparing the attack than with a generic phishing attack. For this reason, whaling attacks can be difficult to spot.

Also called 'CEO Fraud', in 2017 the FBI stated there had been a 1,300% increase in this attack type since January 2015 in the USA. Troublingly, as these attacks often involve an employee authorising a transaction using their real systems, it is usually not recoverable through the bank once the funds have been transferred, and the use offshore laundering and/or 'money mules' can make it difficult to trace, even for law enforcement agencies.

The best protection from a whaling attack, therefore, is vigilance: wherever possible, verify the authenticity of a request by actually speaking to the person.

DEALING WITH PHISHING EMAIL GUIDELINES

How to Spot Phishing Emails

Unfortunately, phishing emails are getting better (or worse): the attackers are improving the format, style and language to make them more believable. Most don't start “greetings, I have big big time oil deal for you, just share bank details...” anymore.

Fortunately, there are still signs to look for that an email isn't genuine.

Who the Email is Addressed To?

Many phishing emails we've seen use generic address sections (e.g. “Dear customer”) rather than the actual name of the user. This is particularly relevant to phishing emails purporting to be from organisations that you would sign up to personally (e.g. PayPal), as the technology used to insert your name in any emails the genuine organisation would then send is not complicated so, when it's not present, it's a strong sign of fakery.

That's not to say that every email you receive to “Dear customer” is a phishing attempt though! Use this alongside other 'features' in the email to assess its authenticity.

Check Email Address and Domain

Phishing emails that – at first glance – appear to be from a genuine source, but the email address it's been sent from is actually nothing to do with the company it claims to be from. Legitimate organisations sending emails to users will usually do so from a 'domain' (or address) that matches their website (e.g. our email addresses end in **“betonbauen.com”**, and our website is **“https://betonbauen.com”**). You can check by hovering your mouse over the 'sent from' address and looking at the actual address. Sometimes the differences are small (e.g. an additional number or letter added), so look closely.

Also bear in mind that sometimes companies do use alternate domains for different purposes, so this isn't a 100% accurate method of checking.

Check Spelling and Grammar

An oldie but a goodie. Most legitimate organisations will compose their emails properly, with accurate spelling, punctuation and grammar, and a general 'tone and purpose' (see more on this below) that tends to be consistent from email to email.

Despite technological advances and greater sophistication in phishing attacks, it's still common to find spelling and grammatical errors: careful reading of emails often means phishing attacks with these errors can be spotted.

Commonly phishing emails are generated by scammers in countries where English is not the first language and as such grammar, spelling and choice of language may not be correct. The most noticeable forms of errors in written English language can be a use (or lack) of upper and lower case text and/or the use (or lack) of punctuation.

DEALING WITH PHISHING EMAIL
GUIDELINES

Check the Information or Action Being Requested

Generally, genuine organisations will not request sensitive information from users via email. If an email has a link or attachment, and instructions to provide sensitive information in order to achieve something (e.g. a tax refund) or avoid something (e.g. an online account being closed), it's probably phishing.

Genuine organisations will also tend to communicate with users in a consistent way. If their emails don't usually contain links, but all of a sudden one arrives that does, it's a sign that it's phishing or another type of email scam.

This consistency also applies to the organisation's writing style (or 'tone') and the reason they email you (the 'purpose'). Phishing emails often try to make a user action more urgent by stating that if it's not completed within a short period of time there will be consequences.

Take care as well with emails that you don't recognise that want you to reply. Whilst there might not be a link or attachment to be wary of, it can be the case that attackers will send out an initial email in order to identify a smaller list (those who respond to it) to send the actual phishing email to. This plays on the 'commitment and consistency' principle set out previously.

Check Links

Most phishing emails attempt to get users through to a website where sensitive information is entered. Whilst genuine companies do use links in emails, links are so common in phishing emails that it's worth checking them closely.

You can usually check the URL behind a link by hovering your mouse over it. Alternatively, right-click and “Copy link address”, then paste it into a text application (such as Microsoft Word). Often the copied link address will display the actual target, rather than the text you are intended to see. If the URL of the link doesn't match the organisation's legitimate website URL (e.g. **betonbauen.com**) and the domain the email came from (e.g. **someone@betonbauenuk.com**), it's a clear warning sign.

One sign of phishing is repeated use of the same URL (or website address) throughout the email. Sometimes there can be several 'actions' requested or offered in a phishing email, but closer inspection of the links reveals they all take you to the same place.

For example, if the email is suggesting you should log in to change your password, but also to contact the organisation, and to read their webpage explaining what's happened, and all of these links have the same URL, that's a sign of a phishing email.

There are also examples where the entire email is one big link, so clicking anywhere in the email would forward you to the fake website.

DEALING WITH PHISHING EMAIL
GUIDELINES

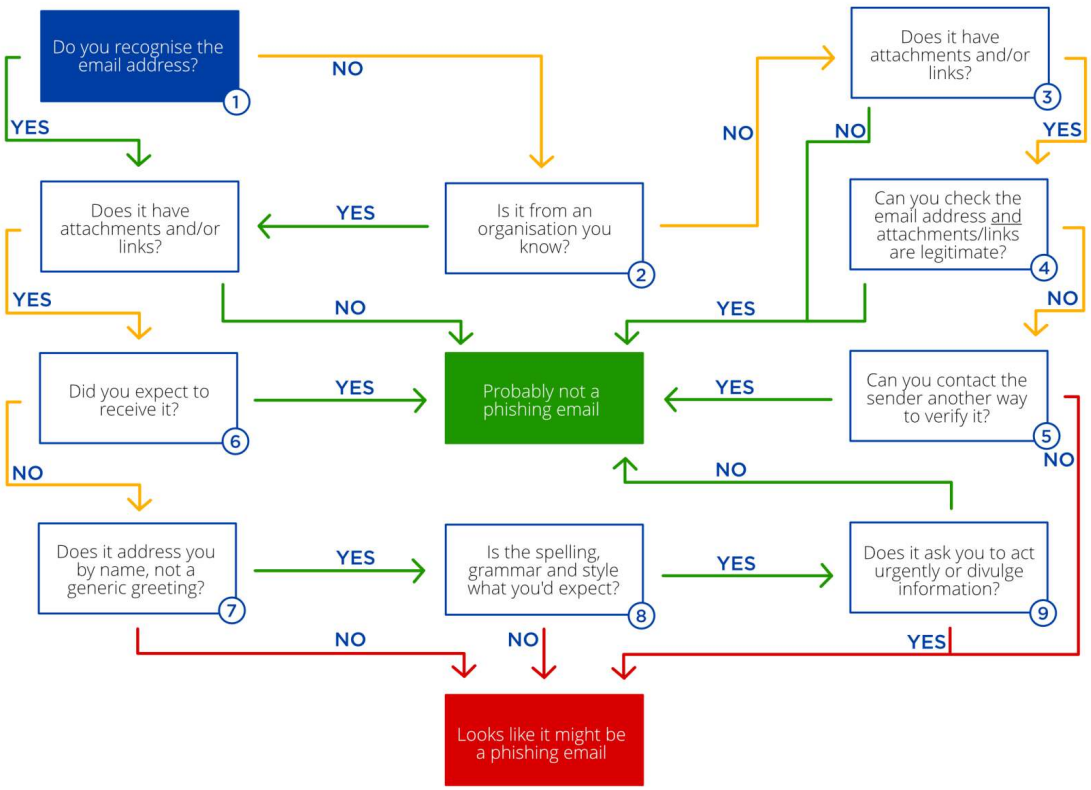
Check Attachments

If an email is unsolicited or unexpected and contains an attachment, it's a sign of phishing or other email-based cyber-crime. Of course, many trustworthy organisations do send attachments to users and customers, so you need to keep in mind those that do, and why they do it (back to the 'tone and purpose' above). Attachments can contain 'malicious payloads' (the parts that cause harm to your computer). Ones to be particularly careful with are:

exe or .msi	A Microsoft Windows executable file
.jar	A Java runtime environment application
.bat or .cmd	A batch file
.js	A JavaScript file
.vb or .vbs	A Visual Basic Script file
.scr	A Windows screensaver file
.psc1	A Microsoft Windows PowerShell script

How do I know if an email is phishing?

As cyber-criminals and their tactics become increasingly sophisticated, it can be difficult to determine whether an email is genuine or not. There remain some tell-tale signs that an email is an attempt at phishing, though. Use the Phishing Flowchart below to help you determine whether an email you have received is genuine or not.



DEALING WITH PHISHING EMAIL
GUIDELINES

How to Avoid Phishing Scams

Sensitive information can often be compromised in an attack, including personal data, bank details and passwords. Staying GDPR compliant means it's important to be aware of how you can protect data.

Unfortunately, you can't stop phishing emails from landing in your inbox, but you can learn how to spot suspicious activity and be prepared to deal with a spam email safely. The most important question to ask yourself is: was I expecting this email? If the answer is no, then think before you click. Be wary of emails that:

- are unsolicited and supposedly come from a reputable organisation, such as a bank or credit card company.
- don't use your proper name, but instead have a vague greeting such as “Dear customer” or “Dear Sir/Madam”.
- request personal information such as username, password or bank details – recognised brands will never do this.
- have addresses which doesn't match the actual website of the organisation – hover over the sender's display name to see what the address actually is.
- use words like 'urgent', 'important' and 'attention' – a popular tactic is to create a sense of urgency or panic.
- are poorly written. Emails from official organisations are usually proofread several times before they are sent and rarely contain typos or grammatical errors. If you see any errors, it's likely that you're being phished.
- ask you to log in through a link - reputable organisations will also never send links to their login pages.

While phishing attacks are now more prevalent than ever, there are plenty of ways you can reduce your organisation's risk and potential exposure to attack.

Technical Phishing Prevention

The different ways technology can help keep you safe from phishing.

Make sure your email system is set up correctly

Whilst technology is only part of the answer to this, it is a part nonetheless. Most email systems either have built-in protections or are compatible with a range of filtering/blocking technology from third party suppliers, that check incoming emails for spam, phishing and malware. This allows the system to then block suspected phishing emails instead of delivering them to the user's mailbox.

Protect devices from malware

Whilst this is generally good security advice - it's critical that all user devices are well protected from malware – it applies specifically to phishing too. Many phishing emails hide malware within them or within the websites to which they attempt to direct the user. In some situations, this malware can do some (or all) of the job of collecting the sensitive information the attackers want. A good endpoint anti-malware solution will provide protection from these issues.

DEALING WITH PHISHING EMAIL
GUIDELINES

Install updates

Install updates and patch software when new updates become available. Ideally, all software across all devices should be set to update automatically.

Protect users from visiting malicious websites

A phishing email will usually encourage a user to visit a malicious website, where the attacker will attempt to obtain sensitive information or deploy malware.

Many content filtering technologies (especially those used in education), will be able to prevent users from accessing these websites, in the same way that they prevent access to websites containing other types of inappropriate content. Like all the other technological measures, it cannot be 100% effective 100% of the time, but it will probably help.

Protect accounts with effective authentication and authorisation

One of the pieces of sensitive information attackers are commonly interested in is the access credentials for systems: the username and password.

Multi factor authentication involves adding at least one more authentication factor to the normal username and password ('something you know') login process, where the additional factors are either 'something you have' (like a one-time password sent in an SMS message) or 'something you are' (like a fingerprint). This can protect user accounts from unauthorised access, even if an attacker does have the username and password.

Some general security controls also apply here, such as ensuring that elevated rights and permissions (e.g. 'administrator' accounts) are only used when needed and that user accounts for staff who no longer work for the organisation are disabled promptly.

Beton Bauen uses Microsoft Office 365 for email. We have now implemented a two-step verification process known as 365 Multi Factor Authentication for each user.

DEALING WITH PHISHING EMAIL GUIDELINES

Human Phishing Prevention

Equip your network's users with the skills to stop phishing.

Training

One of the most important steps is to help users identify phishing emails, and provide mechanisms or processes for reporting them. Whilst many of us think we know what a phishing email looks like, there are many others that might not, so helping users to spot them is a key part of improving security. One aspect that's often missed is what to do with it when you have spotted it, so make sure this is included in training.

Do bear in mind that, even with training, it's generally not possible for users to spot them every time, so the other steps set out below are important too.

Email distribution

Consider recipients of an email. Does somebody in a implementation role (such as a Site Manager) need to included on a mailing list that contains/considers financial data or instructions? Consider that when you Cc or Bcc contacts they may not be authorised to see sensitive data, but at the same time, if their account has been compromised any potential scammer will also have this detail.

Micro-manage your passwords

Using the same or similar passwords across a range of services can make it easy for hackers to access all of your accounts following a single breach. Use a password manager and create strong and varied passwords (using a mixture of letters, numbers and symbols) for each individual account.

Check internal processes

Whilst phishing training is for all staff (as part of security awareness training), there are various processes that should be checked to ensure any weaknesses in certain areas of the operation can be addressed, and there may be additional training for certain teams arising from this. A good place to start is with the normal procedures for parts of the organisation that are commonly a focus of phishing emails: finance operations and IT services. For example:

- What is the process for making normal payments (i.e. to suppliers), and for expediting payments?
- Does everyone involved know how it works, and therefore how to spot unusual requests?
- What is the process for dealing with technical support issues with the various platforms used by the business? Where email is used for this, how can the authenticity be verified?
- Where possible, it's a good idea to document these processes as simply as you can, and then work with everyone to make sure they're followed.

Reconsider information published externally

Particularly for spear phishing and whaling attacks, publicly-available information about an organisation is part of what cyber-criminals use to design more effective phishing emails and deliver them to the correct victims. It is therefore worth considering what visitors to your website do actually need to know, compared to detail that may be more useful to an attacker than to a genuine visitor.

How to Report Phishing Scams

If you're unfortunate enough to have been fooled by a phishing attempt, remember, you're not the only one. All organisations will experience security incidents at some point, so make sure you're in a position to detect them quickly, and to respond to them in a planned way. Follow these simple steps:

Detect incidents early/Report the incident

It's important that you identify what information has been stolen, passed to a third-party or if malware/virus has been installed as soon as possible.

For the Business If an email account has been hacked or an individual has given out sensitive information such as banking details, invoices or credit card data, contact the relevant companies immediately and let them know what has happened. The individual email account password should be reset/changed as soon as possible.

For an Employee Report a possible phishing email and/or hack to your immediately, to a relevant management representative, preferably by telephone. If the email account has been compromised then it is likely a scammer is able to see any correspondence via email at this point.

For Management Most commonly nowadays, a phishing email will try to establish outstanding invoices/debts owing to your business or monies that your business owes creditors. For either the ultimate aim is too change the payment details for the owed party to the scammers' (usually temporary) account. If and when the phishing email / account hack is identified then both parties (the creditor and debtor) should be made aware as soon as possible, thus minimising the financial implications to either business.

Useful Links/Contacts

Action Fraud, the UK's national fraud and cyber-crime reporting centre, provides a central point of contact for information about fraud and cyber-crime and can help report fraud if you or your business has fallen victim.

ACTION FRAUD https://www.actionfraud.police.uk/
NATIONAL CYBER SECURITY CENTRE https://www.ncsc.gov.uk/guidance/phishing