Beaming

Business guide to: Phishing

What is phishing?

Phishing is when criminals attempt to scam users/employees into carrying out an action (such as clicking a link or downloading a file) that gives access to a device, installs malware or dupes them into giving out confidential information or transferring money.

Businesses are holding more data than ever and also holding more in the cloud and accessing it from lots of locations. This provides greater flexibility and efficiencies, but also adds to the importance of ensuring data is held and transported securely.

Why would someone steal my business data?

Don’t be fooled into thinking that your business’s customer, client or supplier information is “insignificant” or “uninteresting”. Any organisation with customers or financial information is a potential target, and smaller businesses, especially those operating in the supply chain of large organisations, are particularly vulnerable.

The following methods can be used by criminals to gather data from victims:

Email phishing

Emails are sent that will appear to be from valid sources but recipients are tricked in to completing the requested actions such as downloading an attachment, clicking a link or sharing further information.

Social engineering

Attackers leverage information from social media to assist with hooking users in to revealing confidential information or carrying out a specific action.

Vishing

‘Voice – phishing’ where personal or financial information is attempted to be gathered from a phone call.

Smishing

SMS messaging attacks – where a text is sent to try and get users to click a link or share information, this may install malware on to your phone.

Quishing

QR code phishing - where users can be tricked into installing malware on to their devices by scanning an unknown QR code.

Phishing prevention for business leaders

It takes every member of your organisation to help defend against cyber criminals. But there are practices and processes we recommend business leaders take to make it less likely you or your employees will fall victim.

1. Use technology. Spam filtering and anti-malware software should be used as a minimum. These can help to block out suspicious email and scan attachments for threats, whilst a Unified Threat Management device also incorporates firewalls, content filtering, and more.

2. Create Microsoft Exchange or Office 365 transport rules to clearly mark external senders in email subject line. You can add a rule which appends the subject line with '[External]' if a message is sent from outside of the organisation. Though this can be quite intrusive in an email chain it's relatively simple to configure and you'll add a layer of security in spotting external emails purporting to be internal.

3. Operate a policy of 'least privilege' for all staff. By making sure each employee only has the lowest level of user rights to be able to complete their role, there would be reduced impact in the event of an attack.

4. Create safer processes, such as always requiring two forms of authentication or sign-off. For example, you could ensure every request to transfer funds is followed-up verbally or via a web portal.

5. Complete regular staff training and reminders of threats to be aware of, how to spot them and what action to take if they do. Helpful sites to follow to assist with this are the National Cyber Security Centre, Cyber Aware, Action Fraud, and Beaming!

6. Create a culture of transparency around cybercrime. Employees are encouraged to regularly share anything they think could be suspicious and immediately own up, without fear, if they think they have been scammed. Remember if someone is scammed, they are a victim of criminal activity.

Focus on email phishing

The majority of business communications are carried out by email, whilst it is a highly useful tool it is an easy route for cyber criminals. With phishers becoming increasingly sophisticated, it can be hard to spot their emails.

Email users should follow these steps to help prevent becoming a victim to scam emails:

1. Always check the email addresses

Look for deliberate mis-spellings in the email address designed to trick the eye or nonsense addresses full of random characters. When you reply, check where your email is being sent to as scammers can re-direct your messages, giving them the opportunity to continue a conversation without raising alarm

2. Look at how the email is written

There are certainly some clever scammers out there, so this is not a given, but some phishing emails contain poor grammar and spelling that would not pass the proof-reading or normal written style of the legitimate sender or organisation.

3. Don’t automatically click

Be wary about clicking links or opening attachments in emails you hadn’t expected, even if you (think you) know the sender. Store internal documents in a shared location instead of sending them to colleagues via email. When unsure, contact the sender via another means to validate their intent.

4. Use shift+delete

Delete suspicious emails straight away. Use shift+delete to make sure the email bypasses your recycling bin and is permanently deleted.

5. Be extra cautious on mobile devices

It may differ slightly from device to device, so make sure you know how to view the full email address of senders and how to check the full URL of any link you’re directed to.

6. Don’t overshare

Check your digital footprint. Giving away personal informtion will make it much easier for fraudsters to scam you. Think about what you actually need to share. Make social media accounts private and remove any “friends” or “followers” you aren’t certain you know in real life.

7. Being pressured should ring alarm bells

Think twice, especially if you are requested to carry out an action or share sensitive information. If you receive an email that asks you to click a link, download a file, share confidential business information or divulge bank account/credit card details, think before you act, especially if there’s a sense of urgency.

8. Don’t be scared to double check

If a request seems odd then always follow up verbally. You’re demonstrating your commitment to keeping business, customer and supplier data safe so no one should be offended!

Example of a Smishing scam

In many cases, scam text messages purport to be from the recipient's bank and will ask them to click a link or phone a number.

New technology has allowed criminals to infiltrate existing SMS threads, adding a perceived authenticity to their efforts. Hearing that a significant amount of money has been removed from your account may cause panic and with links in an SMS being harder to "inspect" for authenticity, you may click something you wouldn't normally risk.

If you receive a text from your bank giving details of an action you didn't authorise, what should you do?

1. Pause, if a fraudulent transfer has been made already, a ten-minute wait while you verify that this is the case won't make a difference. However, if this is a smishing attempt, rushing to click an "I did not authorise this payment" link may ironically be the thing that allows fraud to be carried out.

2. Check if the message is factual by logging in to your internet banking. Use your authorised banking app or navigate to the bank's website (not by clicking a link in a message!). If you see that no money has left your account you should feel reassured, but you'll still want to follow the next step.

3. Phone the bank. Don't use a number or link provided in the text message. Use your browser bar to navigate to your bank's website and find the phone number there, or look at an old paper statement. When you get through to the bank, they'll ask for the usual details to verify your identity, but you'll know that you're speaking to a legitimate agent because you called them. If there is an alert on your account, the person you speak to will be aware and can guide you through the next steps to be taken.

Beaming

Tips to avoid a Quishing Scam?

QR codes can be quick and easy ways to access webpages and applications on the go and they have become an integral part of daily life. Users often wouldn’t question trusting them, making them susceptible to being misused with cybercriminals initiating malicious campaigns.

If you don’t want to avoid using QR codes altogether there are a couple of things to keep in mind:

1. Do you know the provider? Is this a brand you use frequently and in a familiar place? Is the branding and request consistent with previous occasions. If anything appears different or comes out of the blue, we recommend finding a different method of accessing the content.

2. Check the URL. When you scan over the QR code with your device, the link it is taking you to appears. Always preview the link before clicking and consider, if this matches where you are expecting to be directed to. If you are unsure, don’t follow the QR code link, instead try and access the webpage directly via your browser.

About Beaming

We’re Beaming, a specialist internet service provider (ISP) for businesses. We’ve been helping organisations across the UK with fast, reliable, and secure voice and data connectivity, as well as managed services, since 2004.

From the resilient and secure network we’ve built, to the choice of tailormade products all supplied with expert service, we provide peace of mind that businesses require.

We know that your business is unique, so we take the time to get to know you and your specific needs.

If you’re looking for a reliable ISP for your business, we’d love to chat.

Visit www.beaming.co.uk | Call 0800 0822868 | Email hello@beaming.co.uk | in Beaming Ltd