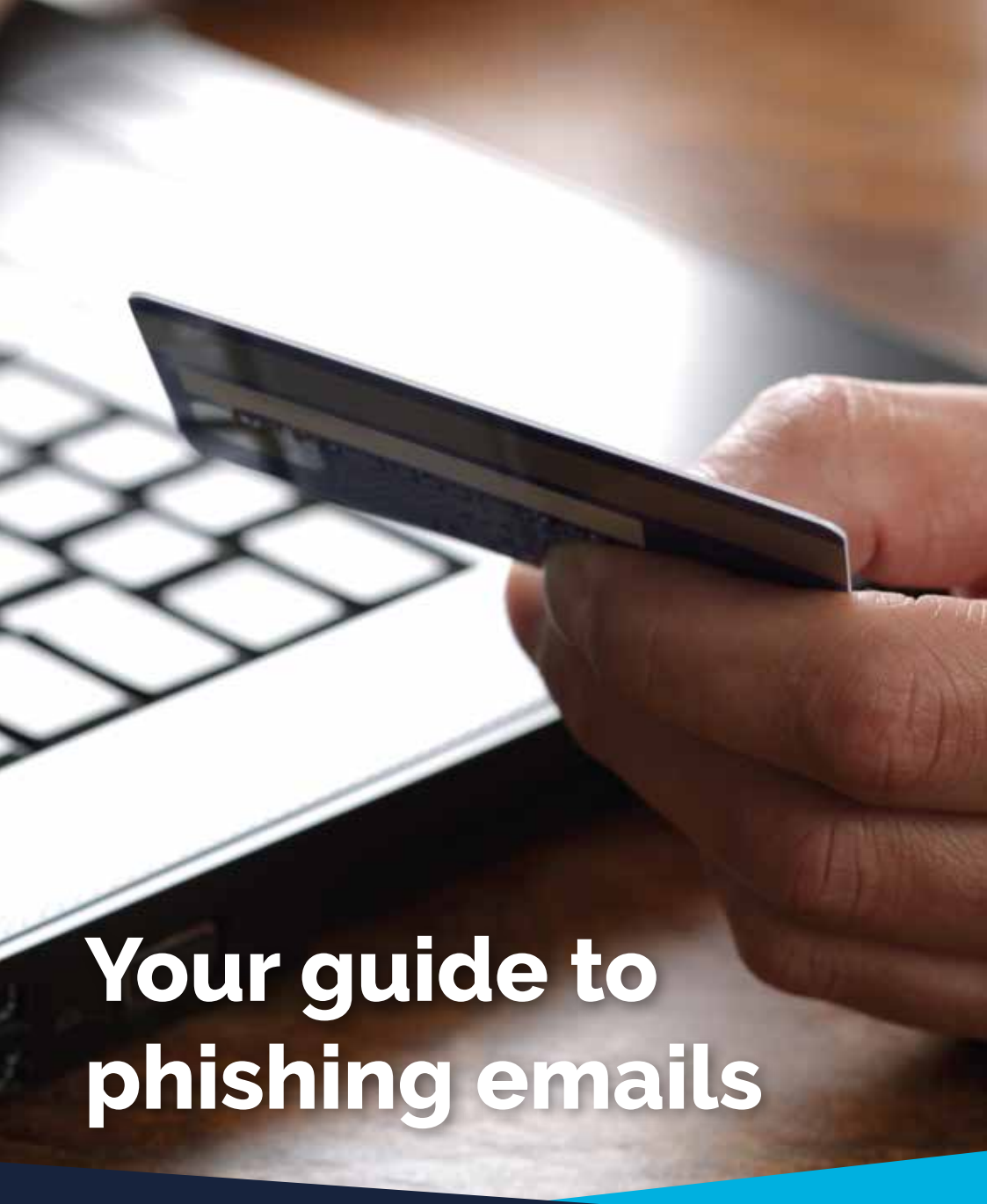


Your guide to phishing emails

Microtrading
Your trusted IT partner

What is phishing?

Phishing is a form of cybercrime whereby important personal information is obtained by deceptive means specifically for malicious purposes.

The first thing to know about phishing emails is that they will typically imitate a familiar and trusted entity, such as your bank, Amazon, PayPal, eBay, HMRC or even your IT administrator. Some have become impressively convincing at this, with sophisticated designs and tactics.

"Emails that seem too good to be true usually are."

A phishing email will try to obtain sensitive information from you – be that login details for an online account or your personal details. Cybercriminals use this information to commit fraud, extortion and identity theft.

Phishing poses a real threat to your business and your staff. This guide will help you to address the issue of phishing emails and reduce the danger they pose.

Why is phishing so common?

Unfortunately, forms of cyberattack such as phishing and malware, are crimes that pay. As a result, the volume and sophistication of these threats continue to grow.

Today, phishing emails are a major problem. People continue to fall victim to phishing scams because they have become adept at duping their audience. However, many of us are far too trusting of brands we recognise, and we interact with emails without hesitation.

What should I be looking out for?

When opening and interacting with emails, users must exercise diligence.

It's not always the same techniques being employed and it's not always the same elements that give the game away either.

Emotion is a big motivator for someone to proceed without caution. Cybercriminals often seek to exploit this, by presenting a scenario that creates worry or joy in the target. They might refer to an issue you're not aware of, an order you haven't made or fictitious moneys that you are due. Adversely, they may take a far subtler approach in the hope of going undetected.

If an email looks suspicious or unusual – even if it appears to come from a known person or organisation – then confirm its authenticity through other means, before interacting with it.

Phishing warning signs:

- Companies you have no connection with, most notably banks with which you have no account.
- Any requests for money or information should be handled vigilantly.
- Government divisions and emergency services, such as the police, don't tend to email.
- Lack of company details in the email's footer, as legitimate senders properly identify themselves.

How do I avoid phishing attacks?

We have broken down the process into some easy-to-follow tips to help you avoid unwittingly giving these cybercriminals what they want.

Tip 1

Is the email asking for personal information?

Emails that ask you for your details, or to log in to an online account, are always worth double checking.

Remember, no bank or financial institution will ask you to share your key personal information via email, or even phone. If you receive an email that requests your PIN or your e-banking password, it is highly unlikely to be genuine.

Tip 2

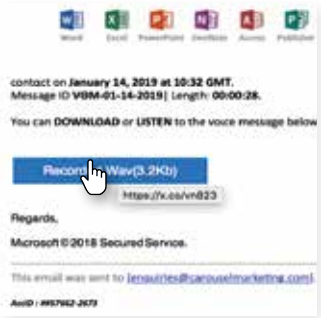
Do the links appear genuine?

Phishing emails nearly always contain a link that you are asked to click on. You should verify if the link is genuine. Here are a few things to look for:

- **Spelling:** Check for misspellings in the link or URL. The changes are often only very slight, so you must be vigilant in checking these.
- **URLs with '@' signs:** If you find a link in an email that includes the '@' sign, steer clear of it even if, at first glance it seems genuine. Browsers ignore URL information that precedes an '@' sign. That means, the URL **www.barclays.co.uk@phishingsite.net** will take you directly to the phishing website and not the Barclays Bank web page.

✓ **www.barclays.co.uk**
✗ **www.barclaysbank.co.uk**
✗ **www.barcleys.co.uk**

- **Disguised URLs:** Sometimes, URLs can be disguised. This means that, while they look genuine, they ultimately redirect you to a fraudulent site. You can recognise the actual URL by hovering your mouse cursor over the link and waiting for the true link address to display. Alternatively, you can right click on the URL and select the 'copy hyperlink' option and paste the hyperlink into a notepad file, but **NEVER EVER** paste the hyperlink directly into your web browser.



Tip 3

Other tell-tale signs

Apart from identifying fake URLs, there are other red flags that may mean an email is fraudulent. Some of these include:

- **The main message is in the form of an image:** This image may click through to a malicious URL.
- **You didn't initiate the action: "You've won the lottery"** – but you hadn't bought a ticket.
- **Attachments from an unknown source:** Never open these, as they may contain viruses that can harm your computer and network.
- **Lack of personalisation:** Trusted emails will tend to include your name "Hi John,".
- **The message seems to urge you to do something immediately:** Scammers often induce a sense of urgency in their emails and threaten you with consequences if you don't respond. For example, your iTunes account will be closed if you don't verify your PIN or password.

How can Microtrading help?

Working with a Managed IT Service Provider (MSP), such as Microtrading, makes identifying malicious emails quicker and easier to do, with experts on hand to assess the situation.

We can also help you to reduce the number of these emails that reach your inbox.

Microtrading specialises in cyber security and won the award for 'Most Outstanding IT Security Solutions Provider' in Birmingham in the TMT Global Excellence Awards 2018.
By beginning with a thorough security audit of your IT infrastructure, we can protect you against a wide range of cyberattacks. Our proactive Managed IT Security Service includes backup and disaster recovery solutions, web protection, managed anti-virus and patch management – all of which play a crucial part in your resilience to cybercrime.

As part of your strategy to combat phishing emails, one of the solutions we would recommend is Microsoft's Advanced Threat Protection (ATP) service, if you are using Microsoft Office 365. This is a real-time protection service that will intercept malicious email and replace unsafe links and attachments, so your business is better protected even if a user is deceived into clicking on a link. It's a low-cost solution that can be easily added and potentially save you from falling victim to a phishing scam and all the serious issues this brings. Microtrading can help you to set up ATP, configure it appropriately for your needs and manage its ongoing monthly billing.

Educating your staff of the threat from phishing emails is one of the best defences. We can provide you and your team with cyber security training and advise on procedures that will maintain awareness and good practice.

Microtrading
Your trusted IT partner

For more information on phishing, cybercrime and how Microtrading can help protect your organisation, call 0121 784 0077 or visit www.microtrading.co.uk