LAYER 8

Avoiding phishing attacks

5 tips share with your team. . .

In a typical phishing attack, scammers send fake emails to thousands of people, asking for sensitive information (such as bank details), or containing links to bad websites. They might try to trick you into sending money, steal your details to sell on, or they may have political or ideological motives for accessing your organisation's information.

Phishing emails are getting harder to spot, and some will still get past even the most observant of us. Whatever your business, however big or small it is, you will receive phishing attacks at some point. Here are some easy steps to help you identify the most common phishing attacks,

Tip 1: Configure accounts to reduce the impact of successful attacks

- Configure your employees' accounts in advance using the principle of 'least privilege'. This means giving staff the lowest level of user rights required to perform their jobs, so if they are the victim of a phishing attack, the potential damage is reduced.
- An Administrator account is a user account that allows you to make changes that will affect other users. Administrators can change security settings, install software and hardware, and access all files on the computer. So an attacker having unauthorised access to an Administrator account can be far more damaging than accessing a standard user account.
- Therefore to reduce the damage that can be done by malicious software, ensure your people don't browse the web or check emails from an account with Administrator privileges.
- Use two factor authentication (2FA) on your important accounts such as email. This means that even if an attacker knows your passwords, they still won't be able to access that account.
- If your IT is run by an external provider. Ask them to set this up for you.

Tip 2: Think about how you operate

- Consider ways someone might target your organisation, tricks include sending an invoice for a service you haven't used, so when the attachment is opened, malware is automatically installed (without your knowledge) on your computer.
- Another is to trick people into transferring money or information by sending emails that look authentic. Think about your usual practices and how you can help make these tricks less likely to succeed.

  For example:
  - Do people know what to do with unusual requests, and where to get help?
  - Ask yourself whether someone impersonating an important individual (a customer or manager) via email should be challenged (or have their identity verified another way) before action is taken.
  - Do people understand your regular business relationships? Scammers will send phishing emails from large organisations in the hope that some of the recipients will have a connection to that company.
- Think about how you can encourage and support people to question suspicious or just unusual requests, even if they appear to be from important individuals. Having the confidence to ask 'is this genuine?' can be the difference between staying safe, or a costly mishap.

Tip 3: Check for the obvious signs of phishing

Expecting your staff to identify and delete all phishing emails is an impossible request and would have a massive detrimental effect on business productivity. However, many phishing emails still fit the mould of a traditional attack, so look for the following warning signs:

- Many phishing scams originate overseas and often the spelling, grammar and punctuation are poor. Others will try and create official looking emails by including logos and graphics. Is the design (and quality) what would you'd expect from a large organisation?
- Is it addressed to you by name, or does it refer to 'valued customer', or 'friend', or 'colleague'? This can be a sign that the sender does not actually know you, and that it is part of a phishing scam.
- Does the email contain a veiled threat that asks you to act urgently? Be suspicious of words like 'send these details within 24 hours' or 'you have been a victim of crime, click here immediately'.
- Look out for emails that appear to come from a high-ranking person within your organisation (CEO, MD, Finance Manager), requesting a payment is made to a particular bank account. Look at the sender's name. Does it sound legitimate, or is it trying to mimic someone you know?
- If it sounds too good to be true, it probably is. It's most unlikely that someone will want to give you money, or give you access to some secret part of the Internet.

Tip 4: Report all attacks

- Make sure that your team are encouraged to ask for help if they think that they might have been a victim of phishing, especially if they've not raised it before. It’s important to take steps to scan for malware and change passwords as soon as possible if you suspect a successful attack has occurred.
- Don't punish staff if they get caught out. It discourages people from reporting in future, and can make them so fearful that they spend excessive time and energy scrutinising every email they receive. Both these things cause more harm to your business in the long run.
- If you believe that your organisation has been the victim of online fraud, scams or extortion, you should report this through the Action Fraud. Action Fraud is the UK’s national fraud and cyber crime reporting centre.

Tip 5: Keep up to date with attackers

Attackers are always trying different methods of attack, even when tools like automatic email protection have prevented previous attempts. So it's worth keeping on top of the techniques used by attackers, to try and stay one step ahead. Consider signing up for the free Action Fraud Alert to receive direct, verified, accurate information about scams and fraud in your area by email, recorded voice and text message.

At Layer 8 we send out a monthly newsletter packed full of advice. If you'd like to sign-up send us an email saying 'add me to your newsletter' at enquiries@layer8ltd.co.uk

https://layer8ltd.co.uk