National Cyber Security Centre
a part of GCHQ

Guidance (/)

Avoiding phishing attacks

Created: 11 Oct 2017
Updated: 11 Oct 2017
Part of: Cyber Security: Small Business Guide(/smallbusiness)

Steps to help you identify the most common phishing attacks.

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 (http://www.bbc.co.uk/news/uk-38332266) for accessing your organisation's information.

Phishing emails are getting harder to spot, and some will still get past even the most observant users. Whatever your business, however big or small it is, you will receive phishing attacks at some point. **This section contains some easy steps to help you identify the most common phishing attacks**, but be aware that there is a limit to what you can expect your users to do(/blog-post/im-gonna-stop-you-little-phishie).

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

You should configure your staff 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. To further reduce the damage that can be done by malware or loss of login details, ensure that your staff don’t browse the web or check emails from an account with **Administrator** privileges. 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.

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.

Tip 2: Think about how you operate

Consider ways that someone might target your organisation, and make sure your staff all understand normal ways of working (especially regarding interaction with other organisations), so that they're better equipped to spot requests that are out of the ordinary.

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

- Do staff 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 you understand your regular business relationships? Scammers will often send phishing emails from large organisations (such as banks) in the hope that some of the email recipients will have a connection to that company. If you get an email from an organisation you don't do business with, treat it with suspicion.
- Think about how you can encourage and support your staff 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.

You might also consider looking at how your outgoing communications appear to suppliers and customers. For example, do you send unsolicited emails asking for money or passwords? Will your emails get mistaken for phishing emails, or leave people vulnerable to an attack that's been designed to look like an email from you? Consider telling your suppliers or customers of what they should look out for (such as '*we will never ask for your password*', or '*our bank details will not change at any point*').

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, 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.

Email filtering services attempt to send phishing emails to spam/junk folders. However, the rules determining this filtering need to be fine-tuned for your organisation's needs. If these rules are too open and suspicious emails are not sent to spam/junk folders, then users will have to manage a large number of emails, adding to their workload and leaving open the possibility of a click. However, if your rules are too strict, some legitimate emails could get lost. You may have to change the rules over time to ensure the best compromise.

Tip 4: Report all attacks

Make sure that your staff 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.

Do **not** 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 single 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 website (http://www.actionfraud.police.uk/report_fraud). Action Fraud is the UK’s national fraud and cyber crime reporting centre.

Tip 5: Check your digital footprint

Attackers use publicly available information about your organisation and staff to make their phishing messages more convincing. This is often gleaned from your website and social media accounts (information known as a 'digital footprint').

- Understand the impact of information shared on your organisation's website and social media pages. What do visitors to your website **need** to know, and what detail is unnecessary (but could be useful for attackers)?
- Be aware of what your partners, contractors and suppliers give away about **your** organisation online.
- Help your staff understand how sharing their personal information can affect them and your organisation. This is **not** about expecting people to remove all traces of themselves from the Internet. Instead support them as they manage their

digital footprint, shaping their profile so that it works for them and the organisation.
- CPNI's Digital Footprint Campaign (https://www.cpni.gov.uk/my-digital-footprint) contains a range of useful materials (including posters and booklets) to help organisations work **with** employees to minimise online security risks.

Further reading

Cyber Security Information Sharing Partnership (CiSP)(/cisp)
Action Fraud (http://www.actionfraud.police.uk)

Topics

Cyber attacks(/topics/cyber-attacks)

Was this guidance helpful?

We need your feedback to improve this content.

Yes No