Contents

[**1. What is a phishing attack? 3**](#_Toc77183779)

[**2. Reduce access to reduce the effects of an attack 3**](#_Toc77183780)

[**3. Consider ways that someone might target the school 3**](#_Toc77183781)

[**4. Check for signs of phishing 4**](#_Toc77183782)

[**5. Report all attacks 4**](#_Toc77183783)

[**6. Check your digital footprint 5**](#_Toc77183784)

# What is a phishing attack?

A phishing attack is when fake emails are sent to thousands of people by scammers. These messages may ask for sensitive information such as bank details, or contain links to websites which collect information or contain viruses. Scammers are becoming increasingly more sophisticated in the ways they attempt to access your bank account or steal your details to sell on. Phishing emails are getting harder to spot, and [there is a limit to what you can expect staff to do](https://www.ncsc.gov.uk/blog-post/im-gonna-stop-you-little-phishie) to protect your network.

# Reduce access to reduce the effects of an attack

Staff accounts should be configured to provide the *minimum* access required to carry out the role. This means that if staff become the victim of a phishing attack the potential damage is reduced. 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 which 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. If an attacker had unauthorised access to an Administrator account, any damage would be far more outreaching.

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.

# Consider ways that someone might target the school

Make sure staff are aware of normal working practices so that they're better equipped to spot requests which 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 scam is to trick staff into transferring money or information by sending emails that look authentic but do not originate from the supposed sender.

* Do staff know what to do with unusual requests, and know to report them?
* Does the request fit with the role of the supposed sender? Business related requests from teaching staff or finance requests from non admin staff should alert you to potential fraud.
* Consider whether requests made via email should be challenged for validity. Should the requester have their identity verified before action is taken? Having the confidence to ask ‘Is this genuine?’ can be the difference between staying safe or becoming the victim of a costly mishap.
* Do staff understand the school’s regular business relationships? If you get email requests from an organisation you don't recognise, treat them with suspicion.

# Check for signs of phishing

Expecting your staff to identify and delete all phishing emails is an impossible request, but you can advise them to 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 you would expect?
* Is it addressed to you by name, or does it refer to a 'friend', or 'colleague' or a generic ‘bursar’? 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 an urgent request? Be suspicious of phrases such as 'send these details within 24 hours' or 'you have been a victim of crime, click here immediately'.
* Look out for emails that request payment is made to a particular bank account. This is usually for services or goods you don’t recognise. Most business will have been added to your SAP system.
* Look at the sender's name and check the email address carefully. Often the email address looks familiar but has slightly different spellings, or strange extensions.

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. 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. Liaise with your email filtering provider or IT Technician.

# 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 an 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 in the long run.

If you believe that your school 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.

# Check your digital footprint

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

* Understand the impact of information shared on your school’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)?
* Help your staff understand how sharing their personal information can affect them, their reputation and the school. This is **not**about expecting people to remove all traces of themselves from the Internet. Instead, support them shaping their profile so that it works for them and the school.
* [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 you work with staff to minimise online security risks.