Phishing attacks: defending your organisation

How to defend your organisation from email phishing attacks.

Introduction

This guidance suggests mitigations to improve your organisation's resilience against phishing attacks, whilst minimising disruption to user productivity. The defences suggested in this guidance are also useful against other types of cyber attack, and will help your organisation become more resilient overall.

This guidance is aimed at technology, operations or security staff responsible for designing and implementing defences for medium to large organisations. This includes staff responsible for phishing training.

> **Note:**
> Staff within smaller organisations will also find this guidance useful, but should refer to the NCSC's Cyber Action Toolkit beforehand.

What is phishing?

Phishing is when attackers send scam emails (or text messages) that contain links to malicious websites. The websites may contain malware (such as ransomware) which can sabotage systems and organisations. Or they might be designed to trick users into revealing sensitive information (such as passwords), or transferring money.

Phishing emails can hit an organisation of any size and type. You might get caught up in a mass campaign (where emails are sent indiscriminately to millions of inboxes), or it could be the first step in a targeted attack against your

company, or a specific employee. In these targeted campaigns, the attacker uses information about your employees or company to make their messages even more persuasive and realistic. This is usually referred to as **spear phishing**.

The mitigations described in this guidance are mostly focused on preventing the impact of phishing attacks within your organisation, but if you implement these measures, you will be helping to protect the whole of the UK. Setting up DMARC, for example, stops phishers from spoofing **your** domain (that is, making their emails look like they come from your organisation). There are numerous benefits in doing this:

1. Your own company's genuine emails are more likely to reach the recipients' inboxes, rather than getting filtered out as spam.
2. From a reputational aspect, no organisation wants their name becoming synonymous with scams and fraud.
3. The more organisations set up DMARC, the harder it is for the phishers to succeed.

Why you need a multi-layered approach

Phishing mitigations often place too much emphasis on users being able to spot phishing emails. As we explain below, this approach risks wasting both time and money without improving security. Instead, you should widen your defences to include technical measures, with user education being just one aspect of your approach. A layered approach means you'll have multiple opportunities to detect a phishing attack, and then stop it before it causes harm. Some phishing attacks will always get through, so you should plan for incidents which means you can minimise the damage they cause.

The mitigations below require a combination of **technological**, **process**, and **people-based** approaches. They *all* must be considered for your defences to be really effective. More specifically, the guidance splits the mitigations into four layers on which you can build your defences:

1. Make it difficult for attackers to reach your users
2. Help users identify and report suspected phishing messages
3. Protect your organisation from the effects of undetected phishing emails
4. Respond quickly to incidents

If you can't implement all of the mitigations, try to address at least some of the mitigations **from within each of the layers**.

The problems with phishing simulations

No training package, including phishing simulations, can teach users to spot *every* phishing attempt. Asking users to examine, in depth, every email they receive will not leave enough hours in the day for work tasks. It's an unrealistic and counter-productive goal because responding to emails and clicking links is an integral part of work.

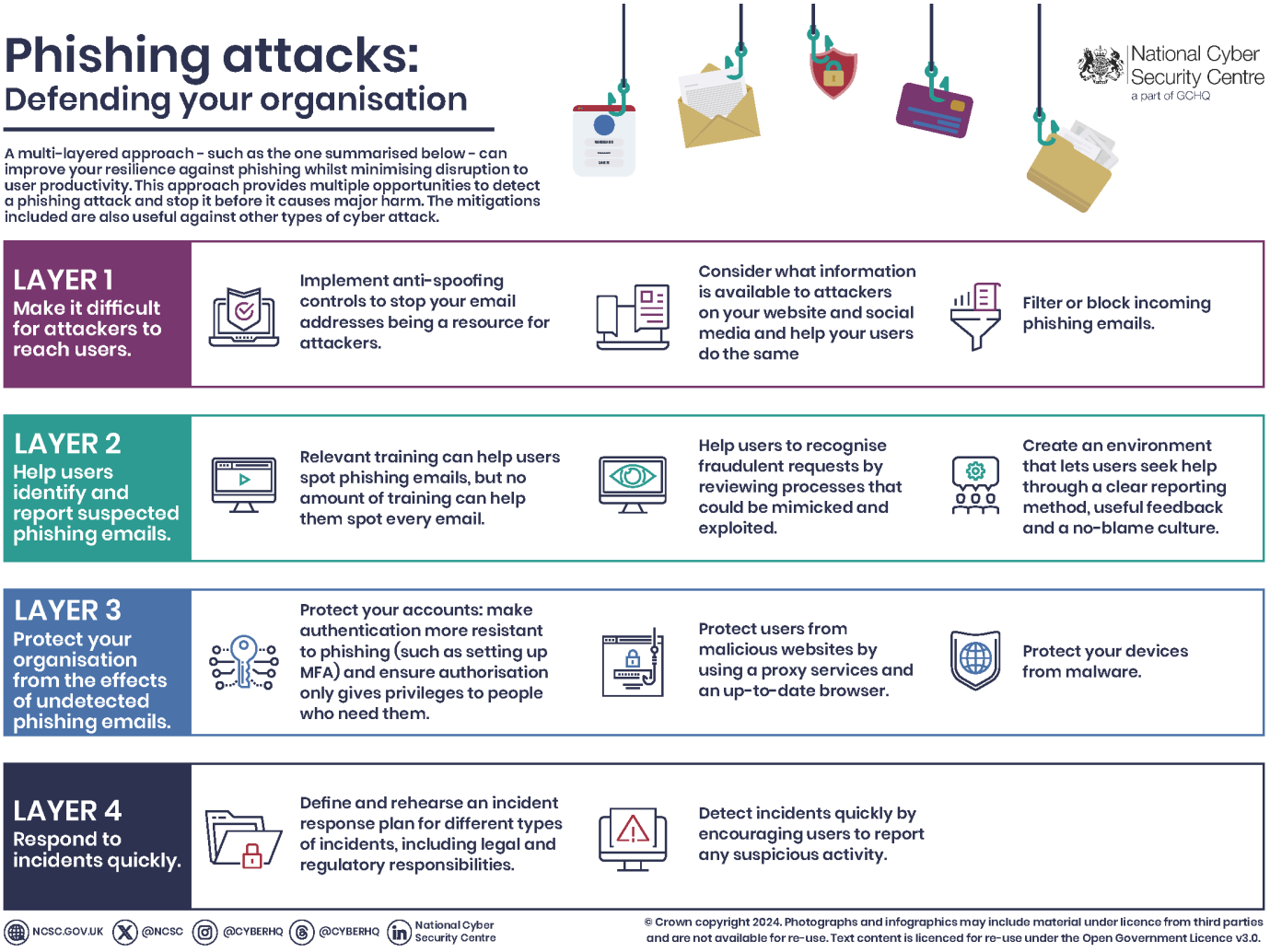
Phishing simulations can also create legal risk. Since no one can be expected to spot all phishing emails, punishing people for clicking on emails you've sent starts to resemble entrapment. For this reason, you should always check with your HR department before undertaking any phishing simulations (the NPSA has a set of free resources to help you design training.)

More practically, blaming users for clicking on links doesn't work. People click for a range of reasons. These could be personality traits or situational (for example, if a person is busy and stressed). Threatening someone with punishment doesn't change these factors.

Phishing simulations also erode trust between employees and security. Employees who are afraid for their jobs will not report mistakes. Employees should instead create a positive cyber security culture so employees feel comfortable reporting phishing incidents, and in this sense, they can be a valuable early warning system.

So why are phishing simulations so popular? One reason is that they allegedly provide clear, quantitative metrics that demonstrate how progress (in an area

you care about) is being made. However, metrics express an organisation's values, and if you appear to value the absence of reports of problems, you incentivise people to keep quiet about issues. You should consider how you can formulate your security metrics to also include successes. For example, as well as measuring how many people clicked on a phishing email, focus on how many people reported it.



Infographic: Summary of layered defences (download available below)

Four layers of mitigation

+ Show all

Layer 1: Make it difficult for attackers to reach your users Show

/

Layer 2: Help users identify and report suspected phishing emails Show

Layer 3: Protect your organisation from the effects of 'successful' phishing emails Show

Layer 4: Respond quickly to incidents Hide

All organisations will experience security incidents at some point, so make sure you're in a position to detect them quickly, and to respond to them in a planned way.

Detect incidents quickly
Knowing about an incident sooner rather than later allows you to limit the harm it can cause.

How do I do this?

- Ensure users know in advance how they can report incidents. Bear in mind that they may be unable to access normal means of communication if their device is compromised.
- Use a security logging system to pick up on incidents your users are not aware of. To collect this information, you can use monitoring tools built into your off-the-shelf services (such as cloud email security panels), build an in-house team, or outsource to a managed security monitoring service.
- Smaller organisations that may lack dedicated logging resources may wish to try CISA's Logging Made Easy open source project, which provides a practical way to set up basic end-to-end Windows monitoring of your IT estate.
- Once a monitoring capability has been set up, it needs to be kept up to date to ensure it remains effective.

Have an incident response plan
Once an incident is discovered, you need to know what to do to prevent any further harm as soon as possible.

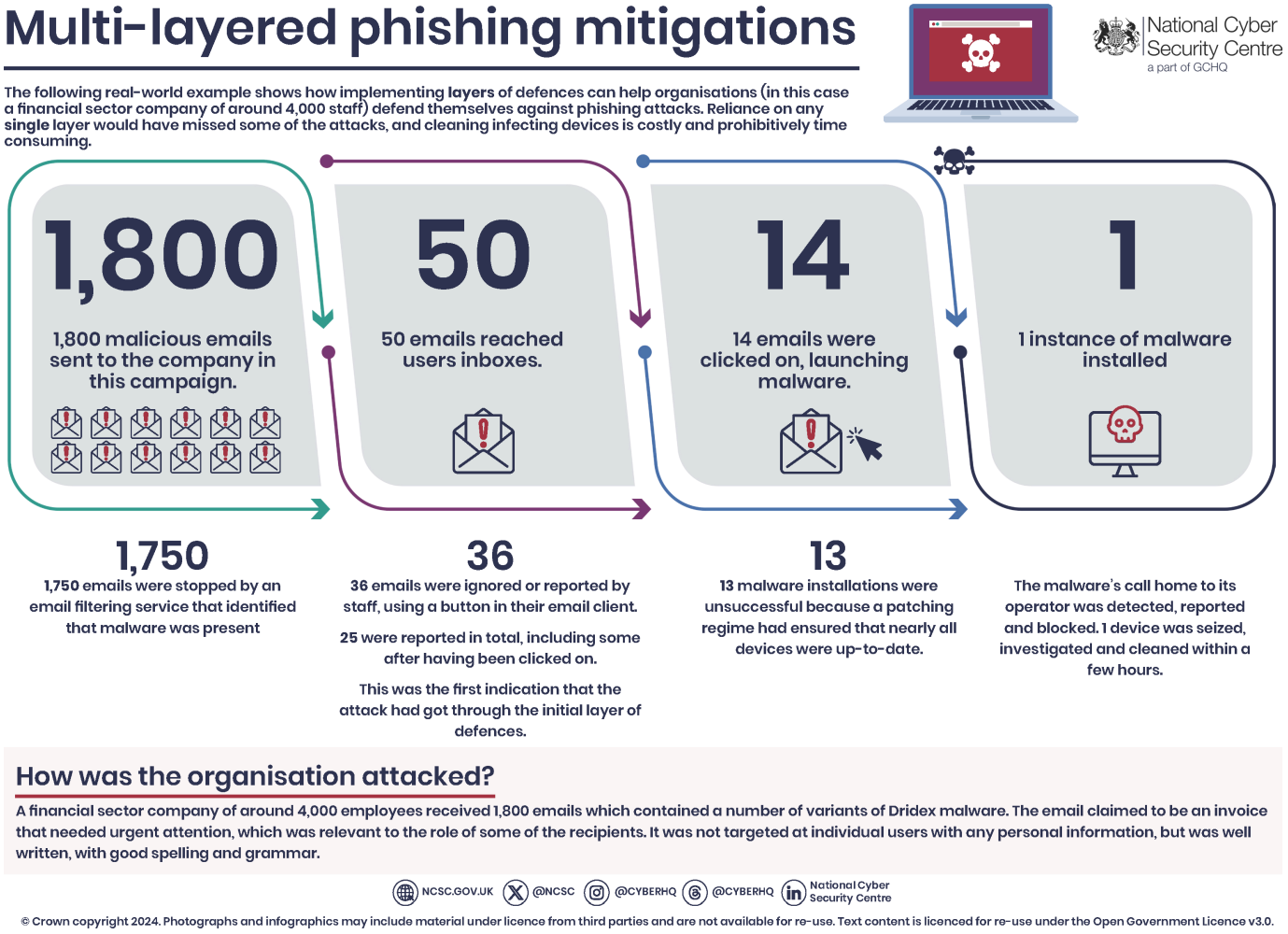
How do I do this?

- Ensure that your organisation knows what to do in the case of different types of incidents. For example, how will you force a password reset if the password is compromised? Who is responsible for removing malware from a device, and how will they do it? For more information, refer to the NCSC's Incident Management guidance.
- Incident response plans should be practised before an incident occurs. The best way to do this is through exercising. If you're new to this, the NCSC has created Exercise In A Box, a free online tool which helps you to find out how resilient you are to cyber attacks, and lets you practise in a safe environment.

Case study: example of multi-layered phishing mitigations

The following real-world example illustrates how a company in the financial sector used effective **layered** mitigations to defend against phishing attacks. Reliance on any single layer would have missed some of the attacks, and resulted in a costly and time consuming clean-up operation.

The company, which has around 4,000 employees, received 1,800 emails containing a number of variants of Dridex malware. The email claimed to be an invoice that needed urgent attention, which was relevant to the role of some of the recipients. It was not targeted at individual users with any personal information, but was well written, with good spelling and grammar.



Infographic: Multi-layered phishing mitigations (download available below)

Summary of the phishing attack:

- **1,800** emails were sent to the organisation by this campaign
    - **1,750** were stopped by an email filtering service that identified that malware was present.
- This left **50** emails that reached user inboxes.
    - Of these, **36** were either ignored by users, or reported using a button in their email client. 25 were reported in total, including some post click; this was the first indication that the attack had got through the initial layer of defences.
- This left **14** emails that were clicked-on, which launched the malware.

    - **13** instances of the malware failed to launch as intended due to devices being up-to-date.
- **1** instance of malware was installed.
- The malware's call home to its operator was detected, reported and blocked.
- 1 device was seized, investigated and cleaned in a few hours.

PUBLISHED

5 February 2018

REVIEWED

13 February 2024

VERSION

2.0

WRITTEN FOR

Small & medium sized organisations

Large organisations

Public sector

Cyber security professionals