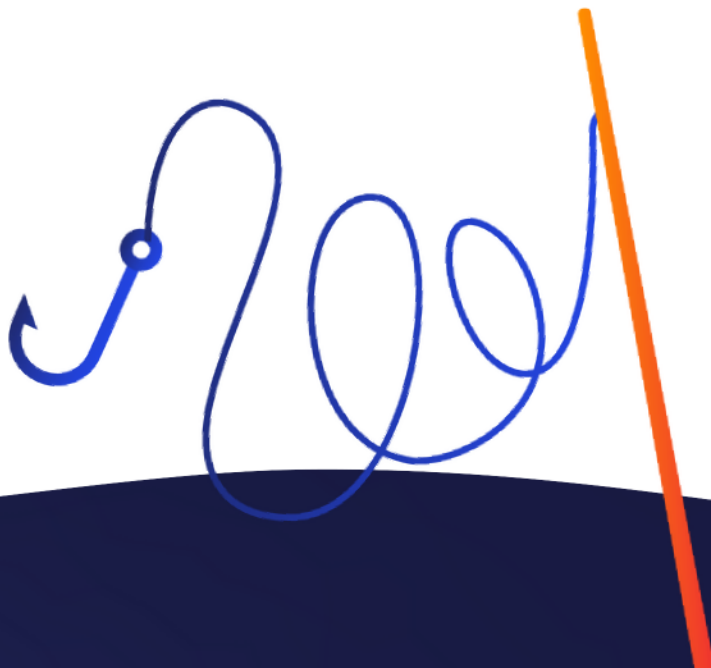
censornet.

The ultimate guide to phishing prevention.

A detailed look into phishing prevention; from the latest trends and types of attack through to identifying phishing and what organisations should be doing to mitigate risk.

Contents.



Introduction.

“Cyber security is a **top priority** for many organisations.”

The UK government’s 2023 **Cyber Security Breaches Survey** reports that 91% of mid-sized organisations and 96% of large organisations consider cyber security a high priority.

Organisations are increasingly recognising the need to broaden cyber awareness in order to mitigate risk, with as many as 49% seeking external information or guidance over the last 12 months on the cyber threats their organisation might face.

There are many ways organisations can approach cyber security: risk management, cyber insurance, deployment of technical controls, and organisation-wide awareness training, just to name a few.

But it’s a combination of measures that are reported to be most effective.

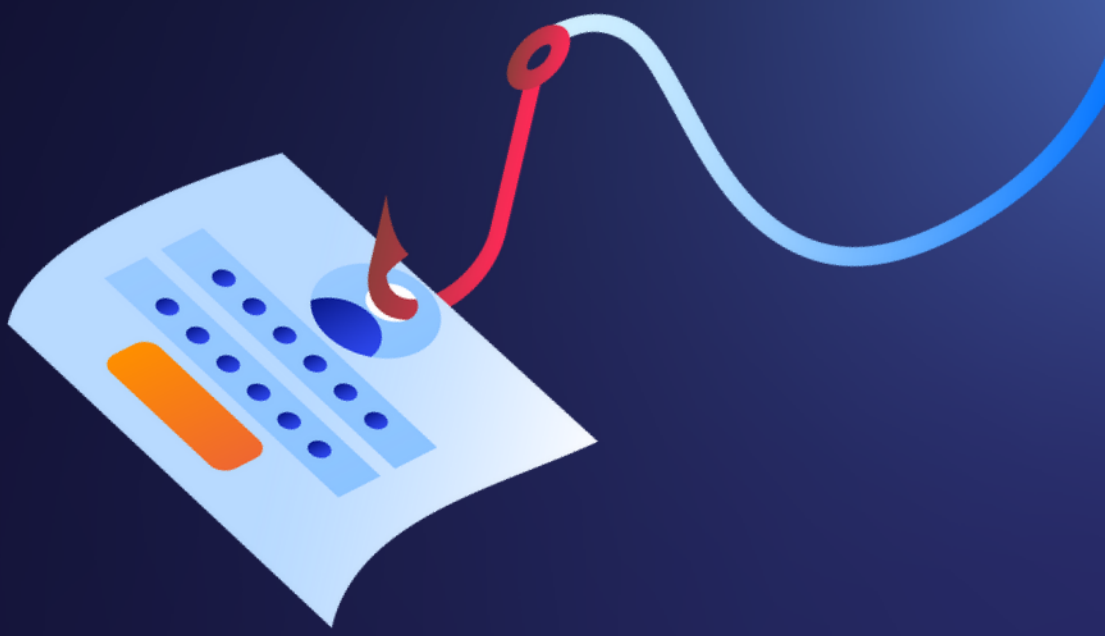
“Phishing attacks **are by far the biggest** threat to organisations.”

Firewalls, internet gateways and malware protection are all critical pieces of technology to protect your organisation from phishing attacks.

But stand alone, **they’re not enough**.

Cyber criminals and their methods of attack are becoming more sophisticated, regularly getting past such measures.

In addition to these technical solutions—to protect your people from phishing—the National Cyber Security Centre (NCSC) and other governing bodies strongly recommend regular awareness training for all employees, to educate them on everything from spotting phishing, through to how to report a potential attack.



Thoughts from our CEO.

It shouldn't be news to anyone reading this guide that phishing emails top the leaderboard when it comes to methods used by cyber criminals.

The UK government's 2023 Cyber Security Breaches Survey reports that 79% of all attacks in the last 12 months originated from an employee clicking a phishing link.

And this is reflected in our data. Recent analysis shows that in the last 12 months, over 88K untrained employees were susceptible to a simulated phishing email sent out via this very platform by their employer. These are huge numbers.

I'd like to stress here that our phishing simulations are not designed to 'catch' people out. They are an important benchmarking exercise for organisations, and they are delivered as part of the overall learning journey. Following each of our phishing simulations we redirect employees to educational landing pages that show them what to look out for next time.

Ed Macnair,
CEO

We find this way of working builds buy-in, and helps organisations quickly achieve a positive cyber awareness culture.

Your people are being targeted everyday by increasingly sophisticated phishing attacks, and without the correct awareness training, the risk to your organisation is insurmountable.

So, it begs the question (or questions), how susceptible are your people? Do your people know how to spot the latest phishing threats? And what is your organisation doing to help, and proactively mitigate risk?

Top phishing simulation trends.

Untrained users are 8.8 times more likely to click on a phishing simulation than those receiving regular training.

8.8x

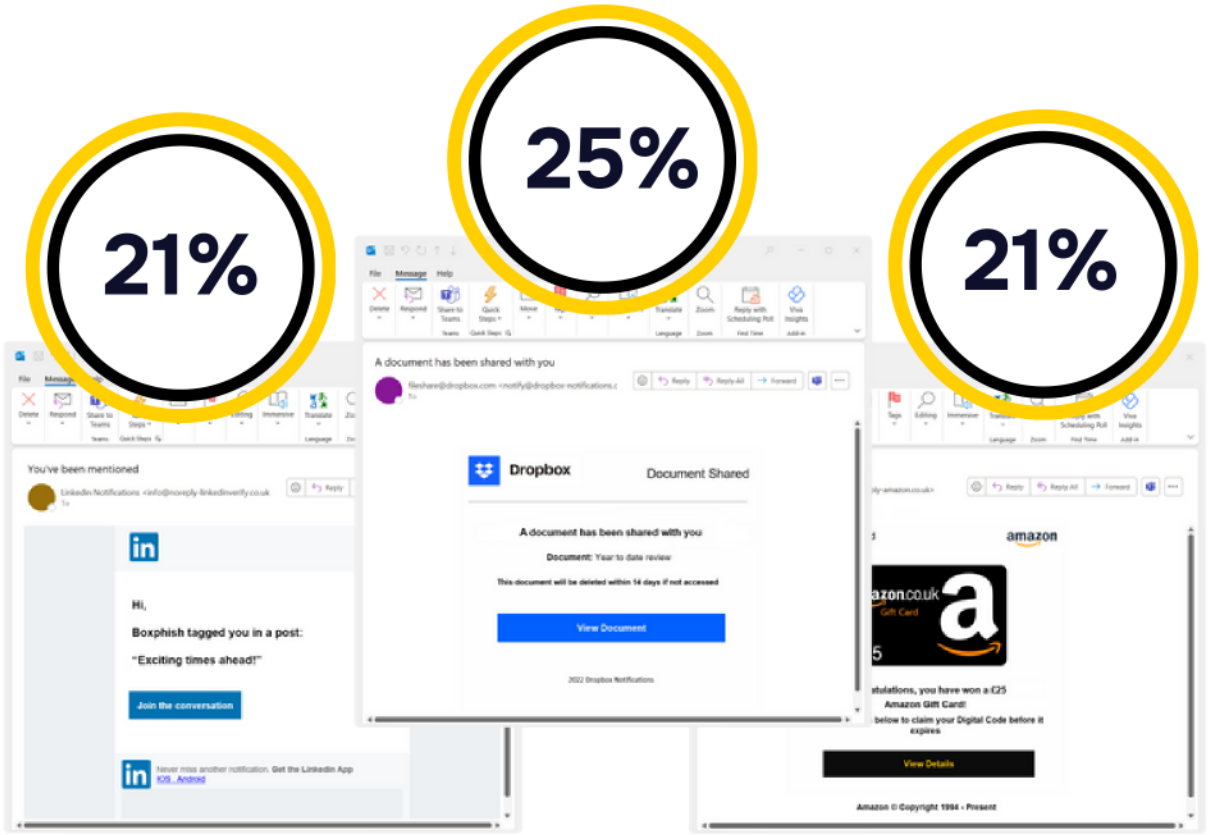
We compared the average susceptibly of new users (users that are yet to be enrolled onto a learning journey but have been sent a phishing simulation), and those that have been receiving regular training, and the numbers are remarkably different.

New users have an average susceptibility rate of 22%, whilst those receiving on-going training have an average susceptibility rate of just 2.5%, highlighting the positive impact of regular training.

Trends continued.

Our most clicked phishing simulations mimic that of reputable brands and contain familiar types of email communication. They also include a level of urgency or ‘fear of missing out’. These are common—and effective—tactics used by cyber criminals.

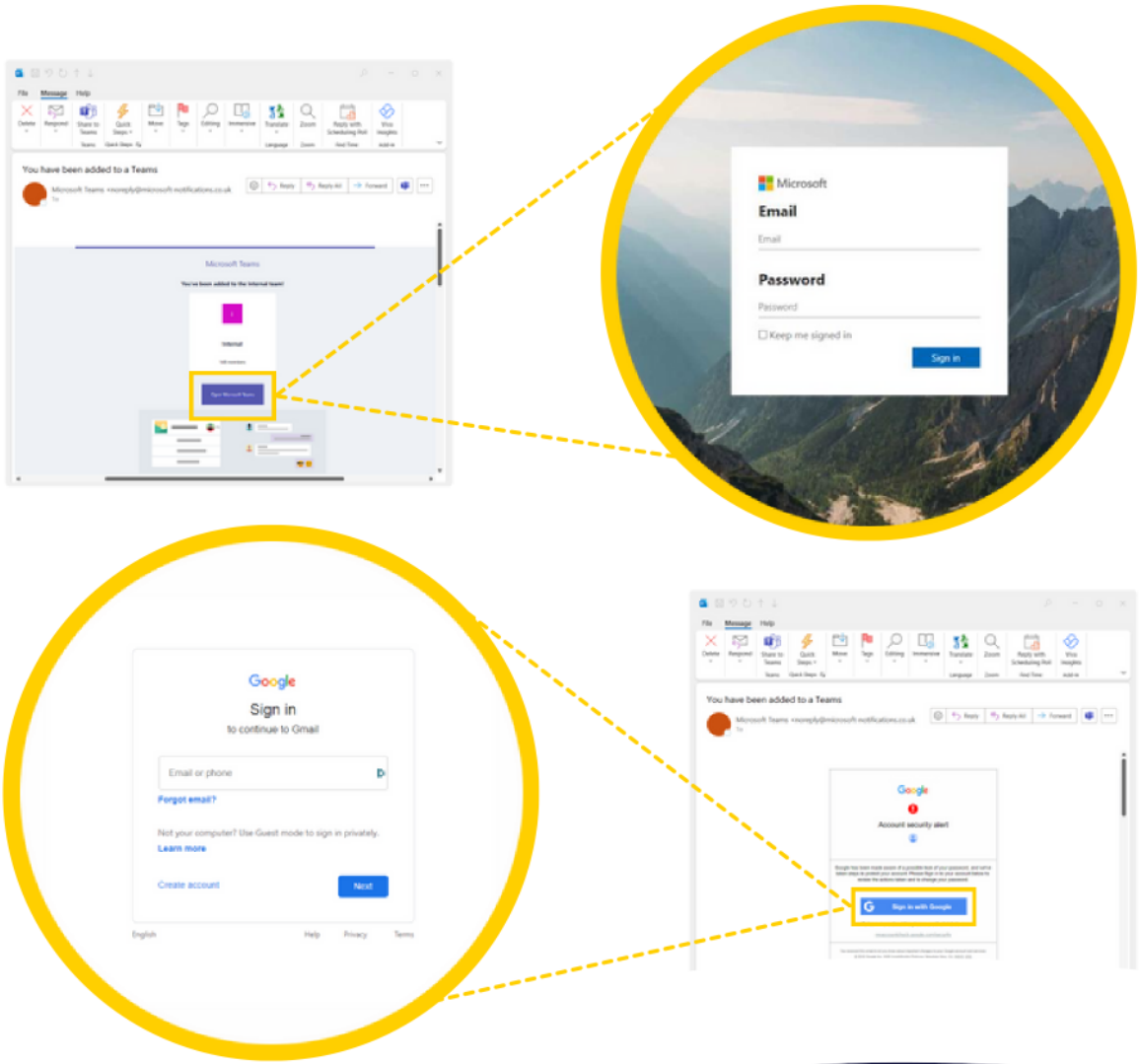
25% of all users that received our ‘Dropbox document share’ phishing simulation, clicked it. This was closely followed by our ‘LinkedIn you’ve been tagged in a post’ simulation and our ‘Amazon redeem a gift card’ simulation; both receiving click through rates of 21%.



Trends continued.

Phishing simulations mimicking business applications such as Microsoft and Google also have a high click through rate, averaging **17%**.

The credibility of these business applications and the tone of the phishing email i.e., implying urgency or playing on a user's emotions, significantly increases the chances a user will enter credentials into a fake landing page following clicking a phishing simulationlink.



The types of phishing to look out for.

Phishing comes in many shapes and sizes. Most of us are aware of email phishing, spear phishing and maybe even SMS phishing. But what about social engineering, domain spoofing, vishing, evil twin phishing and angler phishing? The list goes on...

In order to keep your people safe, an understanding of the different types of phishing is crucial.

Most phishing attacks are sent via email. Cyber criminals often register for a fake domain that closely mimics a real organisation.

They then send thousands of generic emails trying to trick people into giving aware sensitive information.

Spear phishing is a form of email phishing. The difference? It's more sophisticated. Cyber criminals typically have a victim in mind.

They source information prior to the attack – perhaps your name, job title or address and send a highly personalised email with the aim of catching you out.

CEO fraud or executive impersonation, is another type of email phishing. This time, the cyber criminal is aiming to impersonate someone senior within an organisation.

Cyber criminals often apply urgency to these emails, asking for things such as bank transfers.

Smishing, also known as SMS phishing, acts in the same way as any email-based phishing attempt. But this time, email is replaced with an SMS message. Cyber criminals often try to mimic leading high-street banks and ask you to verify a fake bank transfer or to confirm your bank details.

With an evil twin attack, cyber criminals will set up a fake Wi-Fi network that looks real or mimics that of a legitimate nearby network.

If you select the evil twin Wi-Fi and enter your details to 'connect', the cyber criminal will capture your information.

Vishing, also known as voice phishing or phone phishing, is a type of attack whereby a cyber criminal uses a phone call or voice message to trick you into divulging sensitive information or performing an action that can harm you, or your organisation.

Social engineering is a type of phishing attack that deliberately targets your emotions.

It uses psychological manipulation to trick you into making security mistakes or giving away sensitive information. These attacks often take place over several weeks.

Domain spoofing, also known as DNS spoofing, is a type of attack whereby a cyber criminal imitates the domain of a legitimate organisation—either via email or a fake website—with the aim of luring you into entering sensitive information.

Whaling attacks target senior managers or executives of an organisation—typically someone with access to a lot of sensitive information.

These attacks aim to trick you into giving away incredibly valuable information.

Angler phishing is where a cyber criminal will create a fake social media account and pretend to be either another social media user or perhaps a customer service employee.

Using their disguise, the cyber criminal tries to convince you to give away information or install malware.

The impact of phishing.

Individuals and organisations alike are regularly bombarded with fraudulent emails and messages.

With rapid technological change continuing and cyber criminals always adapting their techniques, it is becoming even harder for people to spot the genuine from the fraudulent.

Financial impact

Phishing attacks can lead to significant financial losses. Whether that's through fraudulent use of personal data, holding an organisation ransom or persuading people to pay fake invoices or bills.

Financial impact

Phishing attacks can seriously disrupt an organisation's day to day operations. Once a cyber criminal has found their way into your network, they can install malware, which could cause significant system downtime.

Reputational damage

Successful phishing attacks can have a huge impact on an organisation's reputation. People quickly lose confidence in the organisation's ability to keep their information safe and often jump ship to a competitor following a reported attack.

Phycological impact

And don't forget the phycological impact for employees. Cyber attacks increase scrutiny, workload and pressure on your workforce.

Tips to spot the next phishing attack.

Although there are many different types of phishing attack, the methods of identifying them can be generalised.

We recommend that employees follow these six steps when they receive an unexpected email.

Always check the email domain

Legitimate organisations will never contact you from a publicly accessible domain such as ‘gmail.com’ or ‘hotmail.com’. Always check the senders email domain.

Never share sensitive data

Legitimate organisations will also never ask you to share sensitive information like login details or personal data over email. If you’re unsure, call them directly.

Watch out for domain spoofing

Email addresses may appear genuine at first glance but often include spelling errors such as ‘Amazom.com’. Check domains thoroughly.

Hover before you click

Before clicking a link in an email, use your mouse to hover over the link. This will reveal the true URL destination. If it looks suspicious, do not click it. Report it.

Beware of urgency

Take caution when receiving urgent requests from ‘co-workers’, even if the email address looks correct. This may be a case of account takeover. Always pick up the phone to verify the email is legitimate.

Always verify attachments

Organisations rarely send documents like invoices as email attachments. If you’re unsure, always pick up the phone to ensure that the attachment has come from the right source and is not malicious.

How organisations can mitigate risk.

There are several ways organisations can begin to protect themselves from phishing attacks, but no single solution offers complete protection.

“Adopt a **multi-layered approach for effective risk** mitigation.”

As we’ve previously discussed in this guide, a combination of technical measures alongside regular employee awareness training proves most effective. This will broaden defences and improve organisation-wide resilience to phishing attacks.

The **National Cyber Security Centre** recommend dividing your approach into four areas:

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

How organisations can mitigate risk.

1

Make it difficult for attackers to reach employees

- Implementation of anti-spoofing controls will prevent your email addresses being a resource for attackers.
- Consider what information is publicly available on your website or social media profiles and help your employees do the same.
- Rollout technology to filter or block potential phishing emails.

2

Help employees identify and report suspected phishing emails

- Ensure your employees get regular training to help them spot the latest attacks.
- Help employees recognise fraudulent activity by reviewing processes that could be mimicked.
- Create a cyber aware environment that encourages employees to seek help via clear reporting methods, feedback, and a no-blame culture.

How organisations can mitigate risk.

3

Protect your organisation from the effects of undetected phishing emails

- Protect your accounts with security features such as two-factor authentication and strict privilege management.
- Protect employees from accessing malicious websites with up-to-date browsers and proxy servers.
- Protect workplace devices from malware.

4

Respond quickly to incidents

- Define and rehearse an incident response plan for different types of incidents including legal and regulatory responsibilities.
- Encourage employees to report suspicious activity so that incidents can be detected quickly and efficiently.

How organisations can mitigate risk.

A multi-layered approach such as this will give your organisation multiple opportunities to detect a phishing attack, and then stop it before it causes harm.

You also acknowledge that some attacks will get through. This acknowledgement will help you plan for incidents and minimise the damage caused to your organisation.

Phishing attacks are becoming more sophisticated. Although technical controls are crucial, your employees are often your first line of defence. To protect your organisation, it's important to raise organisation wide awareness and build a positive cyber security culture that empowers your employees to spot, and report suspected phishing attacks.

Autonomous Integrated Cloud Security

E. EMAIL

Secure your entire organisation from known, unknown & emerging email security threats - including email fraud.

S. SAT

Defend your organisation against cybercriminals by strengthening your engaging and stimulating automated training.

W. WEB

Protect users from webborne malware, offensive or inappropriate content & improve productivity.

C. CASB

Discover, analyze, secure & manage user interaction with cloud applications - inline & using APIs.

M. MFA

Reduce impact of large scale data breaches by protecting user accounts with more than just passwords.

ID. IDaaS

Control user access with complete identity-threat protection. Automatically authenticate users using rich contextual data.

Our Platform

Our cloud security platform integrates email, web, and cloud application security, seamlessly with identity management and advanced data loss prevention to activate the Autonomous Security Engine (ASE).

This takes you beyond alert driven security and into real-time automated attack prevention.

Advanced DLP

Prevent sensitive data getting into the wrong hands.

Enterprise-grade DLP across email, web and cloud applications for the ultimate real-time protection.

Autonomous Security Engine

Prevent attacks before they enter the kill chain.

Enable traditionally silo'd products to share and react to security events and state data whilst leveraging world class threat intelligence.

Matrix House, Basing View,
Basingstoke, RG21 4FF, UK
Phone: +44 (0) 845 230 9590

Park Allé 350D, 2605 Brondby,
Denmark
Phone: +45 61 80 10 13

700 Lavaca Street Suite 1400-
PMB#100122 Austin, TX 78701
Phone: +1 (877) 302-3323

censornet.