OneCollab

THE ULTIMATE GUIDE TO **PROTECTING YOUR BUSINESS FROM PHISHING SCAMS**

www.onecollab.co.uk

@onecollablimited
+44 20 8126 8620
info@onecollab.co.uk

Introduction

Email Security Risk Remains High

Welcome to our guide on protecting your business against phishing scams. While companies understand the importance of bolstering cyber security, many may underestimate the prevalence of cybercrime today, particularly when it comes to Phishing.

Throughout this resource, we'll delve into practical strategies for identifying phishing scams, fortifying your business's defences, emphasising the critical role of employee training, and exploring the potential benefits of partnering with a cyber security firm.

Statistics[1]

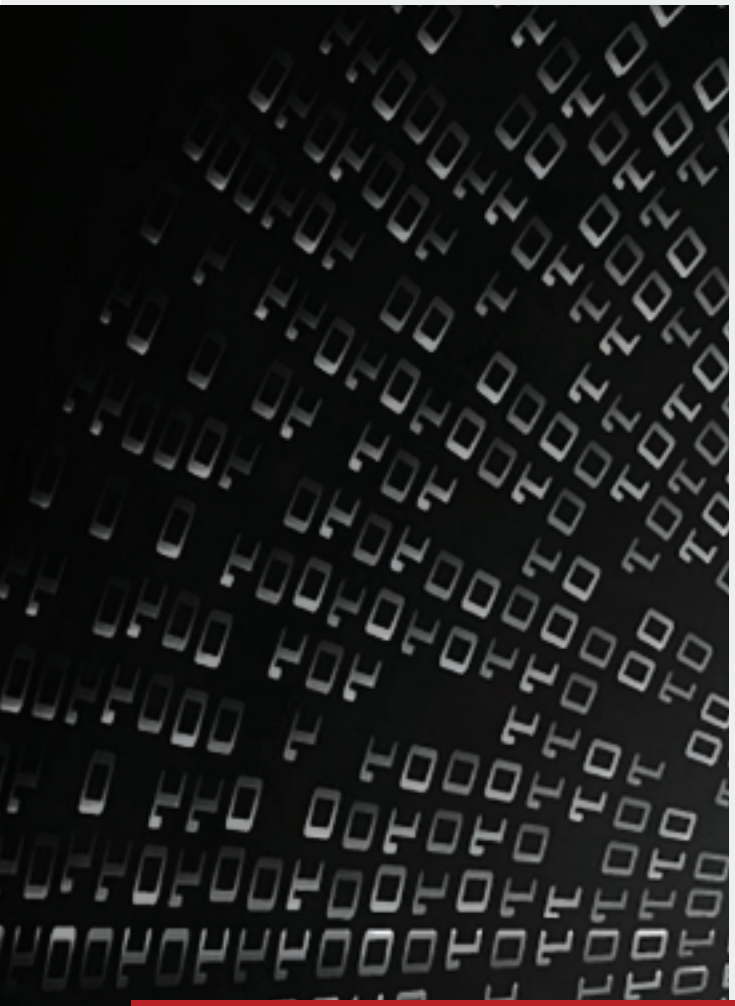
94% of organisations had email security incidents in 2023...

79% of account takeover attacks started with phishing...

95% of cyber security leaders are stressed about email security.

With these statistics in mind, it's clear that vigilance against phishing scams is paramount for safeguarding your business's digital assets and reputation.

[1]egress 2024 Email Security Risk Report



What Is Phishing?

Phishing scams represent a significant form of cybercrime, aimed at deceiving users to obtain sensitive information. Cybercriminals often masquerade as legitimate entities to perpetrate these cyberattacks.

Employees in corporate settings are prime targets, as cybercriminals exploit social engineering tactics to trick them into compromising sensitive data.

This can involve unwittingly downloading malicious files, clicking on infected links, or divulging private information.

Phishing Attack Examples

Levitas Capital Whaling Phishing Attack[2]
In 2020, a whaling attack targeted the co-founder of the Australian hedge fund Levitas Capital. The co-founder received an email containing a counterfeit Zoom link. Upon clicking the link, malware infiltrated the hedge fund's corporate network, resulting in the creation of fake invoices amounting to nearly $8.7 million.

Despite the actual financial losses from the attack being $800,000, it inflicted substantial damage to the hedge fund's reputation. This led to the loss of their largest client and forced them to cease operations.

Google and Facebook Phishing Scam[3]
Between 2013 and 2015, Facebook and Google were duped out of $100 million in a prolonged phishing campaign. Exploiting their common vendor, Quanta, based in Taiwan, the perpetrator sent fake invoices impersonating Quanta, which both companies paid.

After uncovering the scam, legal action was taken in the US. The perpetrator was extradited from Lithuania. Through legal proceedings, Facebook and Google recovered $49.7 million of the stolen $100 million.

[2] News 'Levitas Capital closing after fake Zoom invite sinks $16m super fund investment'
[3] US Attorney Office 'Lithuanian Man Sentenced To 5 Years In Prison For Theft Of Over $120 Million In Fraudulent Business Email Compromise Scheme'

Types of Phishing Attacks

As malicious actors seek to exploit businesses, new types of phishing scams with varying techniques continue to emerge. Let's explore the most common types of phishing attacks.

Whale Phishing

A whale phishing attack occurs when a fraudster impersonates a top executive within a company, aiming to obtain money or sensitive information from another high-level executive within the same company

For instance, a senior executive at your company might contact you regarding a financial crisis that requires your assistance. The fraudster may request login credentials or a wire transfer of funds to purportedly resolve the issue.

Vishing (Voice Phishing)

Vishing is a phishing scam where a malicious actor employs social engineering tactics to coax valuable information out of individuals over the phone.

For example, cybercriminals might impersonate personnel from a financial institution and call unsuspecting victims, soliciting their account information, PINs, or other credentials. They could also pose as vendors, suppliers, or partners to deceive individuals into divulging sensitive information or authorising payment for a counterfeit invoice.

Smishing (Text Phishing)

Smishing involves the use of text messages, appearing to originate from a trusted source, to persuade recipients to provide financial rewards or access to exploitable information.

An instance of smishing could be receiving a text message purportedly from a reputable company, such as a bank, alerting users about unauthorised activity or prompts them to verify account details.

Business Email Compromise (BEC Phishing)

BEC phishing scams primarily target accounting or finance personnel, with hackers aiming to deceive victims into transferring money from corporate accounts to their own.

Criminals begin by compromising financial employees' email accounts and monitoring their activities to understand the organisation's processes and payment procedures. They then send spoof emails impersonating top executives, instructing recipients to transfer funds into designated bank accounts.

Clone Phishing

In a clone phishing attack, scammers attempt to replicate legitimate branded emails previously received by the victim, while embedding a malicious link or attachment. Sometimes, the cloned email may include phrases like "resending" or "sending this again" to deceive the recipient into thinking it is from the original sender.

An example of clone phishing is receiving an email twice, with one originating from a slightly altered email address. For instance, you might receive two identical emails, one from "support@amazon.co.uk" and the other from "supporrt@amazon.co.uk".

HTTPS Phishing

HTTPS phishing involves cybercriminals tricking individuals into disclosing personal information via a malicious website. To lure victims to these sites, phishers conceal malicious links within emails, often disguising them as links to legitimate websites.

For instance, an HTTPS phishing scam might entail receiving an email instructing you to log into LinkedIn to secure your account. Although the email appears to be from LinkedIn support, it is actually a scam. Clicking the link directs you to a fake website designed to steal your login credentials.

Spear Fishing

What is Spear Phishing?

Spear phishing is a targeted cybercrime tactic where attackers impersonate trusted sources to steal sensitive information, potentially leading to identity theft or other malicious activities. Unlike generic phishing, spear phishing focuses on specific individuals.

Spear Phishing vs Phishing What Is The Difference?

While both phishing and spear phishing employ similar tools and tactics across email or SMS platforms to manipulate recipients, spear phishing distinguishes itself with its personalised approach and thorough target research.

Unlike mass phishing campaigns, spear phishing's tailored nature enhances its success rate but restricts its target pool. Typically executed by sophisticated hackers or state-sponsored entities, these attacks aim for specific objectives or target select organisations.

[5]AV-TEST 'Malware Statistics'

How To Spot Phishing Scams

Recognising phishing attempts promptly is crucial for safeguarding your business's reputation and data security. Here are the key indicators of phishing attacks to watch for:

Urgent Action Demands

Attackers exploit urgency to pressure recipients into hasty decisions before scrutinising the email for inconsistencies.

Poor Grammar & Spelling

Phishing Emails often contain grammatical errors and spelling mistakes, unlike professionally crafted communications.

Unusual Greetingss

Formal greetings or unfamiliar phrases inconsistent with usual office communication style should raise suspicion.

Inconsistencies in Links, Addresses & Domains

Hover over links to see where they go. Watch out for familiar names with strange domains or addresses - they might be trying to trick you.

Suspicious Attachments

Most file sharing happens via trusted platforms. Double-check before opening anything unexpected, even from someone you know.

Too Good to Be True

Beware of emails promising rewards or incentives, especially if the sender is unfamiliar or unsolicited.

Unexpected Requests

Be wary of emails from managers or colleagues asking for personal info, even if they seem legit. Especially if they sound urgent!

Requests for Sensitive Information

Be cautious with emails requesting sensitive data from unknown sources. Verify login pages to avoid falling for replicas.

How To Spot Phishing Scams Checklist

Before responding to an unknown or dubious email request, go through this straightforward three-step checklist:

Conduct Research

Before responding to an email or text, verify the legitimacy of the sender's website or phone number.

Ensure you're communicating with a genuine organisation and not falling prey to scammers.

Seek Advice

Consider discussing suspicious requests with a trusted colleague.

Their input could provide valuable insights, especially if they've encountered similar fraudulent messages or notice discrepancies you might overlook.

Verify By Phone

Take the extra step to call the purported sender directly. Use a known, reliable phone number rather than relying on contact details provided in the email or text.

This helps confirm the legitimacy of the request and avoid potential phishing attempts.

How To Protect Against Phishing Attacks

To effectively safeguard your organisation against phishing attacks, it's crucial to implement proactive measures and robust security protocols.

Implement Antivirus

Use Install and maintain antivirus software to block phishing attempts and other malicious content effectively.

Email Authentication

Implement email authentication protocols such as SPF, DKIM, and DMARC to verify email authenticity and prevent spoofing.

Spam Filter

Implement robust spam filters to block suspicious emails from reaching users' inboxes.

Access Controls

Utilise stringent access controls to limit access to sensitive data and systems only to authorised personnel.

Encryption

Encrypt sensitive data, including passwords and personally identifiable information, to prevent unauthorised access in case of a breach.

Web Filtering

Employ web filtering solutions to block access to known malicious websites and proactively assess websites for potential threats.

Multi-Factor Authentication (MFA)

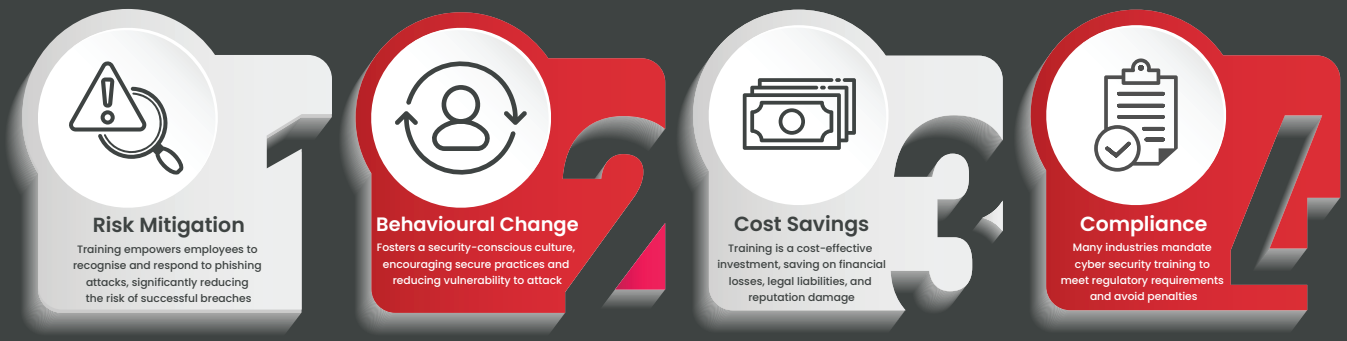
Enforce MFA for added security, requiring multiple forms of identification before accessing accounts or systems.

Regular Updates And Back-Ups

Keep software, operating systems, and security solutions up-to-date to mitigate vulnerabilities, and regularly back up data to ensure quick recovery in case of an attack.

The Importance of Employee Training for Phishing Prevention

In safeguarding against phishing attacks, employee training plays a pivotal role in an organisation's defence strategy. Here's why it's crucial:



Effective Strategies for Employee Training

To effectively combat phishing attacks, organisations should employ these strategies:

Interactive Workshops

Engage employees with real-life examples and simulations to enhance their ability to identify and respond to phishing attempts.

Phishing Simulations

Conduct controlled phishing campaigns internally to assess employee susceptibility and provide targeted training.

Phishing Reporting Systems

Implement simple reporting mechanisms for employees to promptly report suspicious emails, bolstering proactive defence.

Phishing Awareness Resources

Provide accessible resources such as articles and videos to reinforce best practices for identifying and mitigating phishing threats.

Continuous Learning

Ensure training programmes remain up-to-date and adaptable to new threats, keeping employees informed about emerging phishing trends.

Role-Based Training

Tailor training content to specific job roles and responsibilities to address unique phishing c hallenges faced by different departments.

Gamification

Incorporate game-like elements to make training enjoyable and engaging, encouraging vigilant behaviour.

Testing And Assessment

Regularly assess employees' knowledge and awareness of phishing threats to identify areas for additional training.

Responding Effectively To A Phishing Scam

Identifying phishing links can be challenging due to their sophisticated mimicry of official notifications. If an employee falls victim, your company can mitigate the consequences by following these steps:

01

Stay Calm

Avoid panic and assess the email for signs of malicious intent discussed earlier. Determine if data theft, malware installation, or network access has occurred.

02

Contain The Attack

Disconnect the affected device from the internet and all networks to prevent malware spread. Conduct a virus scan, delete detected malware, and reset compromised passwords.

03

Report The Incident

- Notify your company's IT Department, Security Team, or Managed Service Provider (MSP).
- Forward the email to HMRC at phishing@hmrc.gov.uk.
- If the email impersonates a colleague or external contact, inform them to contain the damage.
- Notify affected parties if sensitive data is compromised.
- Mark the email as a phishing attempt in your email client to prevent similar emails from reaching your inbox.

04

Alert Employees

Inform all employees about the phishing attempt, especially if it impersonated someone within the company. Notify customers or vendors if the sender disguised themselves as them to prevent further scams.

Consequences of A Successful Phishing Attack

Phishing, posing as a pervasive threat to businesses, is meticulously orchestrated by cybercriminals to breach defences and compromise data integrity. Beyond the immediate financial losses, the aftermath of a successful attack encompasses profound reputational harm and operational chaos.

In the wake of such incidents, compromised data integrity, erosion of customer trust, productivity declines, and potential legal ramifications cast long shadows, underscoring the paramount importance of implementing robust cybersecurity measures to fortify against such pervasive threats.

It highlights the critical need for proactive strategies, including employee training, robust security protocols, and partnerships with reputable cyber security firms, to effectively mitigate the risks posed by phishing attacks.

Common Consequences

Regulatory Fines
Businesses risking customer data face fines. Breaches of regulations like GDPR, bring hefty penalties, varying by industry and severity.

Direct Financial Loss
Phishing costs encompass staff salaries, breach losses, ransomware payments, and productivity drops, going beyond immediate response expense.

Reputational Damage
Phishing-caused breaches damage reputation and trust. Announcing a breach can harm brand confidence, with lasting effects.

Data Loss
Malicious links can let hackers steal, corrupt, or delete your data.

Business Disruption
Phishing breaches disrupt operations, divert resources, and lower productivity.

Working With A Cyber Security Firm To Protect Against Phishing

Protecting against phishing scams is increasingly challenging, particularly with the rise of sophisticated techniques. Many in-house IT teams lack the expertise and resources to address all potential threats effectively. A reputable cyber security firm can provide invaluable assistance in mitigating cyber threats and defending against phishing scams.

How We Can Help

Expertise

Our specialised expertise and phishing services fill your skills gap and stay ahead of evolving threats and new phishing techniques.

Bespoke Solutions

We offer customised security configurations based on your needs, limiting business data exposure, even if a hacker manages to steal employee credentials.

Recovery Plans

We provide comprehensive backup and recovery plans to minimise the impact of data loss and downtime.

24/7 Monitoring

Our solutions monitor your network activities 24/7 and isolate any attacks to contain damage swiftly.

Regulatory Compliance

We provide regulatory audit support, offering documentation to help you meet compliance requirements & provide assurance to the board.

Employee Training

Our employee training programmes ensure all staff members adhere to your security policy and understand how to prevent phishing scams.

Conclusion

While this advice can help avoid a large proportion of phishing attacks, it's advisable, if possible, to consult a cyber security expert to evaluate your existing security posture and recommend improvements based on the latest threat intelligence. Additionally, consider taking out insurance against cyber-attacks, offering both technical and financial support in the event of an attack.

And if, despite all precautions, your company falls prey to a cyber-attack, it's crucial to report these incidents to the relevant authorities or local cybercrime unit.

Let us enhance your company's cyber security and protect against phishing. Book a consultation today at **info@onecollab.co.uk** for tailored advice based on your company's situation and see how you can minimise vulnerabilities.

OneCollab

Find Out More:
www.onecollab.co.uk

@onecollablimited
+44 20 8126 8620
info@onecollab.co.uk

THE ULTIMATE GUIDE TO
PROTECTING YOUR BUSINESS FROM PHISHING SCAMS