Phishing Emails

Your complete guide to understanding the threat posed to your business

www.usecure.io

usecure

Table of Contents

INTRODUCTION

The Threat of Phishing Emails

Why your business is vulnerable

Phishing is the #1 cyber threat

Phishing is the most common starting point of cyber breaches.

Almost every employee deals with emails day-in day-out. Since all it takes is for a criminal to have access to an email inbox to carry out a scam, email provides a convenient access point to intrude company networks.

Why you need this guide

This guide is for business owners, IT professionals, line managers and other stakeholders and decision makers who want to understand the risk posed by phishing emails to their business.

In order for your business to stay safe, protect its reputation and save valuable time and money, it is essential that phishing emails are understood and addressed throughout the company. This guide will introduce you to the forms that phishing emails take, why they succeed, and how your company can stay safe.

What is phishing?

All you need to know about the most dangerous cyber attack

Phishing is the use of deceptive emails to obtain sensitive information. Some of these are generic scams sent out by cyber criminals to as many recipients as they can reach. For example, the advance-fee scam involves an email from a supposedly wealthy person in a perilous situation, often in a volatile country. They ask the recipient to kindly forward some money to help them out of trouble, with the promise that it will be returned manyfold once the sender has 'regained access to their funds'.

Other phishing emails are more specific to the recipient. This is called spear phishing. In a spear phishing attack, the cyber criminal will do research into the recipient to find information that will make the scam more likely to succeed, such as names of vendors and business associates who the scammer could attempt to impersonate.

Phishing emails are used to...

- **Obtain sensitive information** such as trade secrets
- **Obtain personal information** like bank account numbers and street addresses
- **Infect your device** with malware through malicious attachments
- **Lead you to bogus websites**
- **Dupe you into making payments** to fake bank accounts
- **Get you to pay fake invoices**

Who sends out phishing emails?

Phishing emails are sent out by cyber criminals posing as legitimate persons or businesses, such as banks or online file sharing services.

Anyone with access to an email account can create a phishing email, which is part of the reason why phishing has become such a worldwide epidemic in recent years.

What makes a phishing attack successful?

Here's how cyber criminals succeed

Cyber criminals have a number of tricks up their sleeve that they deploy to make for highly-successful phishing scams. While a phishing email could take endless different forms, there are a few main elements that almost all successful phishing scams will contain.

Carrot or Stick

An offer too good to refuse - or a threat - is likely to grab a recipient's attention.

Familiarity

Familiar domains, brand names and even names of colleagues are used to make scams appear safe.

Authority

Phishers often pose as banks or senior managers as authoritative senders grab the attention of users.

Urgency

Phishing emails claim to be urgent so users are less likely to think twice before clicking and acting on them.

Timing

Cyber criminals time their emails carefully - for example for Friday afternoon when users are more carefree.

Lack of awareness

Employees that aren't enrolled on phishing training or testing programmes are far more likely to fall for scams.

The stages of a phishing attack

Successful scams happen in three steps

There is more to each phishing scam than just an email. To understand how phishing attacks work and how they can be counteracted, it is important to know how they are constructed before they are sent out to their targets.

From when a cyber criminal first plans an attack to when a user exposes their credentials there are three distinct stages in which the phishing attack takes place.

Information (Bait)

First, the cyber criminal gathers the necessary information to perform the attack. This could be as simple as finding an email used by a bank and copying it off, or as complicated as penetrating into a company network through a series of fake messages, calls and impersonations.

Promise (Hook)

In the second stage of a phishing attack, the criminal will come up with a ‘hook’ that will catch the attention of the victim. For example, this could be a message that warns the recipient that their bank account has had unusual activity - or an email from the company’s CEO asking for urgent help with making a payment.

Attack (Catch)

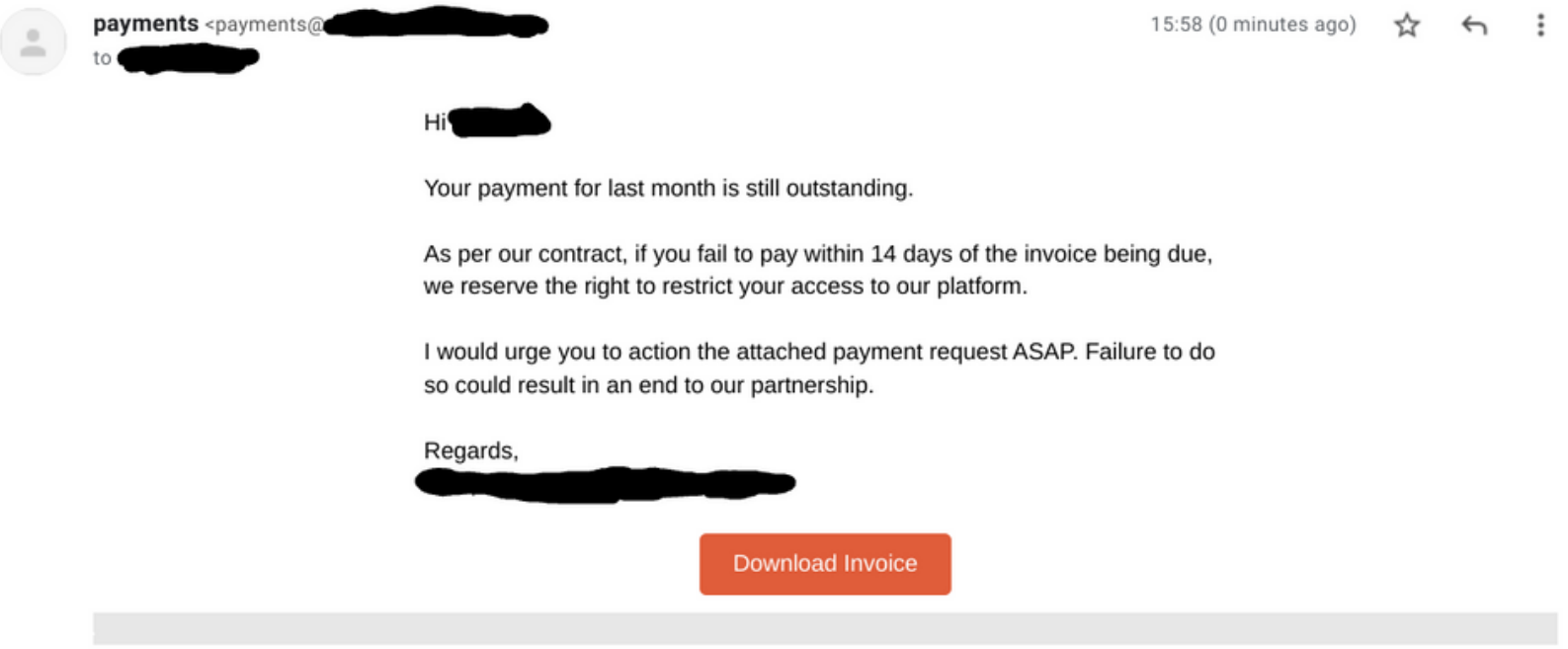
The third stage is where the phishing email is actually sent out, and the cyber criminal awaits the victim’s response. Spam filters and the users’ knowledge of and ability to identify suspicious emails will be tested here.

What does a phishing email look like?

Here's one of the most common emails

Phishing emails can take on a huge number of different forms. However, some scams are far more popular than others, and often scams follow a few common trends.

This is an example of a phishing email that contains a fake invoice. These types of scams are extremely common in businesses of all types and sizes, since employees that handle payments every day are easy targets for a scam. The cyber criminal that sent this email is likely to have done research into the tools that the company uses - which is often easily done through social media such as LinkedIn - and sent a fake 'invoice' from one of the partners of the company. If the recipient had paid the invoice, the money would have been lost to the cyber criminal's account.



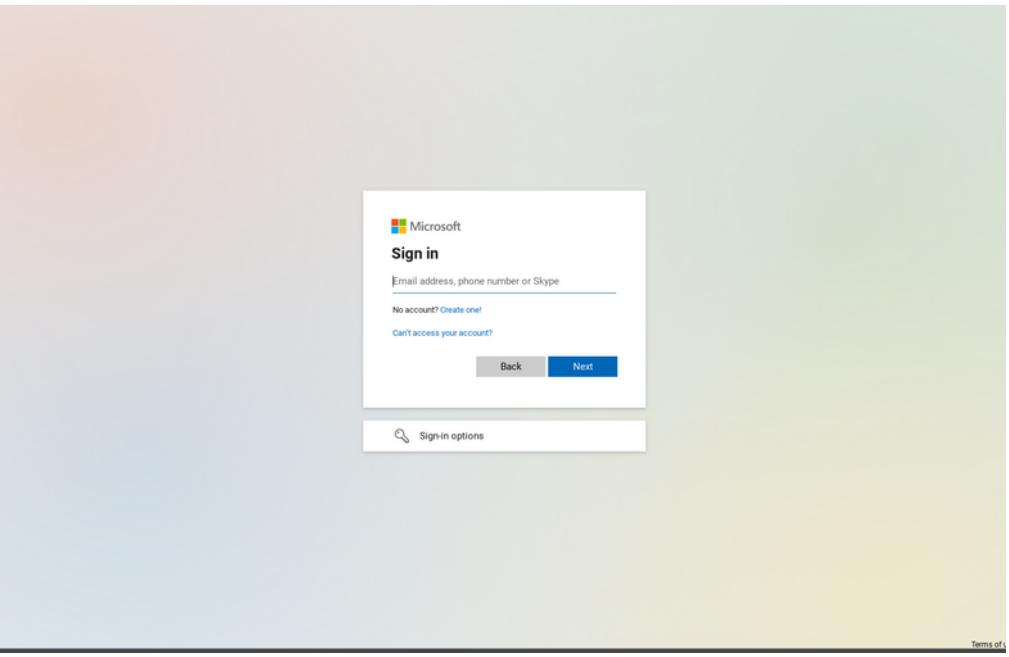
Website spoofing

The fake sites used to harvest credentials

Website spoofing is when a cyber criminal creates a website that looks identical to a real website page - usually a log-in page - in an attempt to harvest user credentials or other information.

An example of website spoofing

One of the most common website spoofs are for log-in pages to popular online services, such as Microsoft 365. A user may receive an email that claims to link them to a business resource, which leads them to what looks like a M365 log-in page. When the user enters their details, however, these fall right into the hands of the cyber criminal who created the page.



What happens when a user enters their details?

When a user enters their details, these will be sent directly to the cyber criminal. However, the user will likely not be aware that this has happened. Most spoofing pages are set up to redirect the user to the real log-in page after, so the user will likely think a temporary glitch has happened and re-enter their log-in details. They will then log in to the real service, completely unaware that their details were picked up by a cyber criminal in the middle.

What are the different types of phishing?

These are the most common scams

New phishing scams are created every single day, but the majority of scams fall into one - or more - of the main types. Here's what the common different types of phishing are, and what they involve.

Spear phishing

Spear phishing emails are targeted at a specific group of people, such as employees of a specific company, and use information about them to make the scam more likely to succeed.

Whaling

Whaling attacks specifically target high-value targets such as CEOs and investors, called 'whales' due to their potential to access large funds and valuable information.

Smishing

Smishing, also known as SMS phishing, includes all phishing scams that take place over SMS and text-based messaging services.

CEO Fraud

These types of scams involve a cyber criminal impersonating the CEO of a company and sending out messages to employees, often asking them to make an urgent payment or hand over sensitive information.

Business Email Compromise

In a BEC attack, a cyber criminal infiltrates messages sent between business partners, such as a vendor and customer. These scams often involve the sending out of fake invoices to steal money.

Vishing

Vishing, aka voice-based phishing, includes all phishing attacks that take place over telephone calls or other voice-based communications.

Pretexting

Pretexting is the use of a made-up story to make a phishing scam more likely to succeed. This often involves the cyber criminal posing as a person in trouble who asks for 'help' from the target of the scam.

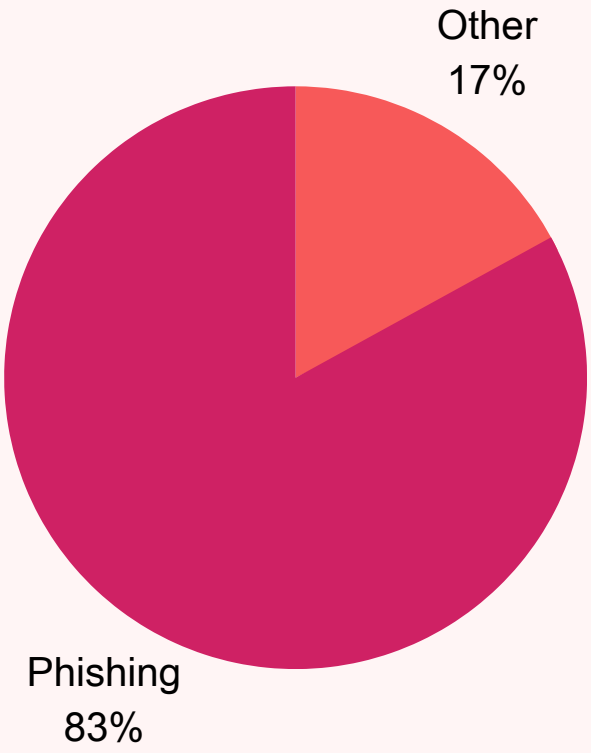
Angler phishing

This type of scam involves a cyber criminal posing as a well-known brand on social media, and replying to public messages of people complaining about their experiences with the brand, in an attempt to harvest private information.

Phishing in numbers

Phishing is the #1 cause of data breaches in businesses

Source: UK GOV, 2021



Key numbers

39%

Proportion of businesses that identified cyber breaches (Source: UK GOV, 2021)

$4,6m

The average cost of a breach caused by a phishing email (Source: IBM, 2021)

14%

Proportion of businesses that train staff on cyber security measures (Source: UK GOV, 2021)

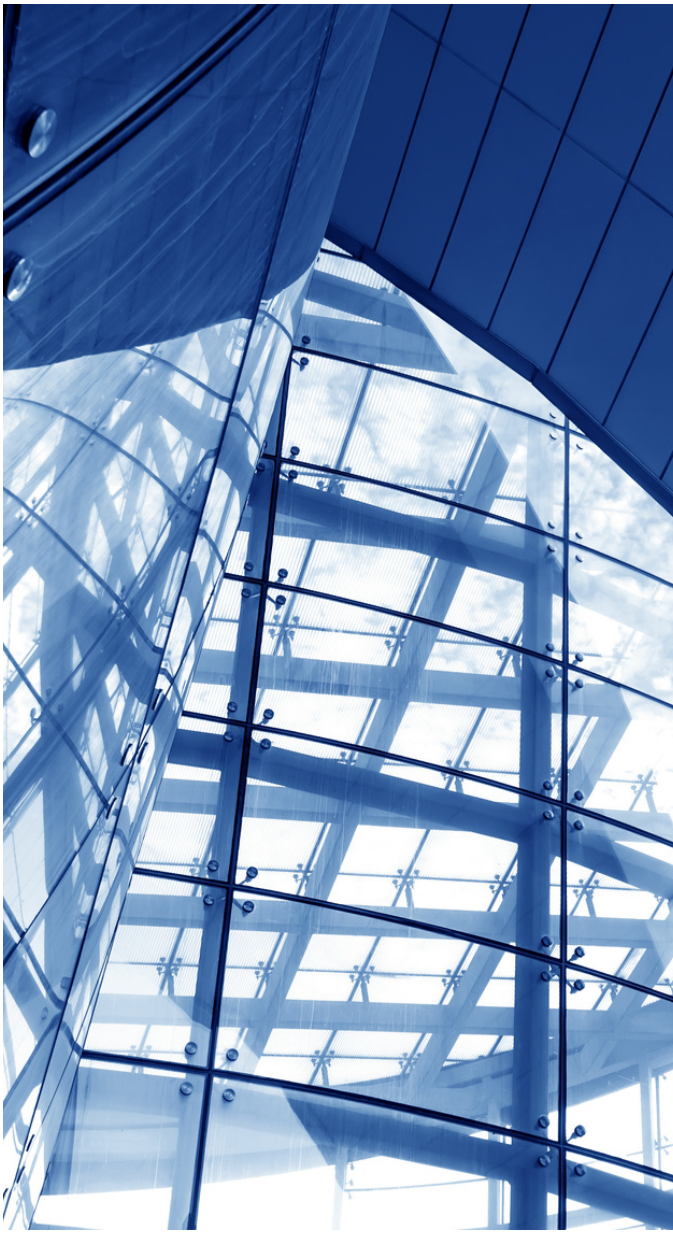
How can you protect your business from phishing?

Take the essential steps to stay safe

While there's almost no chance of stopping phishing emails from hitting your company's inboxes, you can significantly reduce the chances of a successful breach by taking the proper precautions.

The first step in reducing the risk posed by phishing emails is taking the proper technical measures. This means instituting a spam filter to block emails that come from suspicious sources or contain suspicious content, and enabling security messages for users such as banners that warn users when an email comes from outside the company.

However, no technical measure can stop all phishing emails. The second step to stopping the threat of phishing is too often overlooked, but is just as important. This involves addressing the human factor: training employees to understand the threat posed by phishing, identify the signs of phishing, and to take the proper precautions when they send or receive information over email.



What is anti-phishing software?

Anti-phishing software is software that is designed to stop phishing emails from landing in users' inboxes. This includes tools such as spam filters and AI-powered email scanners.

How to stop employees falling for phishing attacks

While anti-phishing software is necessary for any business, it is not enough to stop employees from falling for phishing emails. No software can stop every scam from finding their way to user inboxes.

Training users on email security as well as identifying and correctly dealing with phishing emails is essential to secure your business against phishing and related cyber threats. It's important that users are aware of common signs of phishing, such as look-alike domains and unusual requests, and that they take caution when receiving unexpected attachments or payment requests.

Testing user response to phishing emails helps you understand the risk posed by phishing to your business. A phishing simulator lets you send realistic phishing emails to your end users and gauge their response. In addition to letting you assess the risk level, phishing simulations are also a great way for your users to learn and put their skills to practise, and often provide a better and a more retention-focused way to learn than a training course would be able to provide by itself.

Read next

Phishing Simulations 101

Why, how, and when to run them

Click here to read

usecure

Questions?
Contact us.

www.usecure.io