

## The business owner's guide to **phishing**

Everything you need to know to keep  
your team and data safe

**ILUX**<sup>®</sup>

# About the author



**James Tilbury, CEO, ILUX**

James is a graduate in Computer Science specialising in software engineering. He has worked in various IT-related roles, including a global healthcare manufacturing business supporting the systems and infrastructure.

IT is part of James' DNA. His father was the founder of Tangerine Computer Systems who developed the TAN1648 VDU kit and the Microtan 65, a forefather of home computing in the late 70s.

James has worked around the world, both in a software development role and performing major infrastructure enhancements.


Having identified a need for enterprise-quality IT support and project management for SMEs, James founded ILUX to focus on IT supporting business growth.

First published 2022 by ILUX Limited  
3 Cabot House, Compass Point Business Park, St. Ives; Cambridgeshire. PE28 9WL, UK

Telephone: 0333 311 0109  
Email: [hello@ilux.co.uk](mailto:hello@ilux.co.uk)  
Website: [www.ilux.co.uk](http://www.ilux.co.uk)

Copyright © 2023 ILUX Limited. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the publishers. Opinions expressed in this publication are those of the contributors and not necessarily those of the publishers or editors. We cannot accept responsibility for any errors or omissions.



You've probably heard of phishing and know it's something you want to avoid.

But what exactly is it and how does a phishing attack work?

Many of our clients don't have much experience or know the specifics. The key to keeping your business protected from phishing attacks is to know exactly how they work and the red flags to look out for.

**This guide is here to do just that.**

# What **exactly** is phishing?

It's called 'phishing' because cyber criminals bait unsuspecting victims into 'biting', in the same way you'd lure a fish to a hook with bait.

This virtual bait is usually in the form of an email and once "hooked" the victim's device and potentially their whole network can become infected with malware.

Or the victim is enticed into giving away login credentials which can lead to data and even financial theft.

Phishing isn't just inconvenient. It takes up time, valuable resources and can be expensive to fix if you don't have the right tools in place.

With most things, prevention is better than cure when it comes to phishing attacks.

But be aware phishing doesn't always come in the form of an email. But more on that later.

# Just how prevalent is phishing?

**83%**

83% of organisations reported phishing attacks, up **28%** from 2020

**6bn**

It's expected there will be an additional 6 billion attacks this year

**33%**

A third of phishing emails are opened in error

**60%**

60% of successful phishing attacks result in lost data

**1/99**

1 in every 99 emails is a phishing attack

**90%**

Around 90% of data breaches occur as a result of phishing

# What does a phishing attack look like?

A phishing email will appear in your inbox like any normal email.

It will often look like it has been **sent from a legitimate sender** so you and your staff won't suspect anything is wrong. It appears to be from a legitimate company and gives the impression it is credible.

In some cases the attacker will have researched information about you, such as the services you subscribe to, and the email becomes all the more believable – and therefore riskier. At a glance, the email won't look suspicious, and you may not question the contents.

It is often an urgent request for you to take action and will work in different ways:

- **Ask you to open an attached file, and to confirm details of a recent purchase.** By doing this, your device may become infected with malware. If that device is connected to a network, it's possible that the malware could spread to other devices.
- **Click a link.** This might take you to a fake page (a spoof web page) pretending to be a service you really use. When you login, you have accidentally given your login details to the criminals.

# A phishing attack isn't always an **email**

A phishing attack can take many different forms.



## **Pop-up phishing:**

This is phishing via a pop-up. It may say there's a problem with your device's security and ask you to click a button to download a file, or call a number to get it fixed.



## **Evil twin phishing:**

A fake Wi-Fi network is set up to look like your real one. When you log in, the cyber criminal steals your data.



## **Vishing:**

Like a phishing attack but done over the phone. Someone will call and pretend to be a person or company you know, or a representative of them. They'll ask you to take an action, such as giving them remote access to your device, or visiting a website.



## **Domain spoofing:**

This is where you click a link that looks to be the genuine web address, except it's been faked. Again, once you take action on that site your details have been stolen or you have downloaded malware.

**Spoofing:**

A website that's created to look like the real thing, but isn't. Once you log in, you've given away your credentials (spoofing can be used in conjunction with other forms of phishing attacks too).

**Smishing:**

Like a phishing email, but over SMS straight to your phone.

**Angler phishing:**

Social media posts which are created to encourage people to access an online account or click a link which downloads malware.

**Spear phishing:**

These are sent to specific people who have been researched, so that the information in the email is more relevant and therefore more believable.



**Whaling:**

These phishing emails target people in executive positions within a business, who are likely to have greater access to sensitive areas of the network.

**Clone phishing:**

Copies an email you've already received and adds a message such as 'resending this...' but includes a malware link for you to click.

**Man in the Middle attack:**

A cyber criminal jumps in the middle of an existing email thread and takes over the other side of the conversation. They already have your trust and can ask you to take a specific action.

# Who's at risk?

Sorry to say it, but **everyone in your business and especially you**, as a business owner or director (see whaling, above). It's a real threat you need to take seriously.

This should not be something you can write off in your mind as "it'll never be targeted at us, we're too small or obscure a business."

Cyber criminals use automated tools to target all businesses, of any size, all the time.

Attacks on SME's are often not widely reported but they are being affected every single day.



# How can you stay protected?

As with most types of cybercrime, protection against phishing starts with education.

Everyone in your entire business should have regular cyber security awareness training, and we **really do mean everyone**. If someone is using a device, they need to be aware of the risks and the red flags to look out for.

This may relate to a phishing attempt, or it could relate to one of the other forms of cyber-attack or threats that businesses like yours face every day.

When it comes to phishing attacks, there are a number of warning signs you and your team should be on the lookout for:

- Misspelled words, websites or email addresses
- Oddly named attachments
- Who the email is addressed to
- Poor grammar and punctuation
- An unusual layout to the email

Hover your cursor over the sender's name in your emails, as well as any website addresses. This will show you the actual email address used, or the website you're being directed to.

Don't log in to any of your accounts by following a link in an email. Go directly to the website that you always use and login that way.

Check all emails to make sure they're genuine. Even if they're from close friends or colleagues.

**Don't use the same passwords** across different online accounts. Cyber criminals will often try your credentials on countless other sites once they've stolen them. Using different login details will keep your other accounts protected.

Use a password manager to make sure passwords are long and randomly generated, making them virtually impossible to guess.

Implement multi-factor authentication (MFA) across applications (where you use a second device to prove it's really you logging in).

If you often deal with financial transactions over email, it's a good idea to set up a dedicated email address that invoices should be sent to. If you don't advertise the address, it's far less likely that it will be targeted with phishing emails.

You could also implement codewords with clients or suppliers if an email is regarding payments. If the email doesn't contain the codeword, you know not to process the transaction. Don't email these codewords out, phone your suppliers to tell them about the codeword scheme.

Finally, make sure your policies accurately reflect your stance on financial transactions and the best way to handle them. For instance, you might decide that all transactions must be confirmed over the phone for security reasons.

# Free cyber awareness training and resources

The National Cyber Security Centre offers **free cyber awareness training** for you and your staff. The online course covers four topics:

1. Defending yourself against phishing
2. Creating strong passwords
3. Securing your devices
4. Reporting incidents

## ILUX insights

For practical and easy to use guidance on improving your cyber security, read our blogs

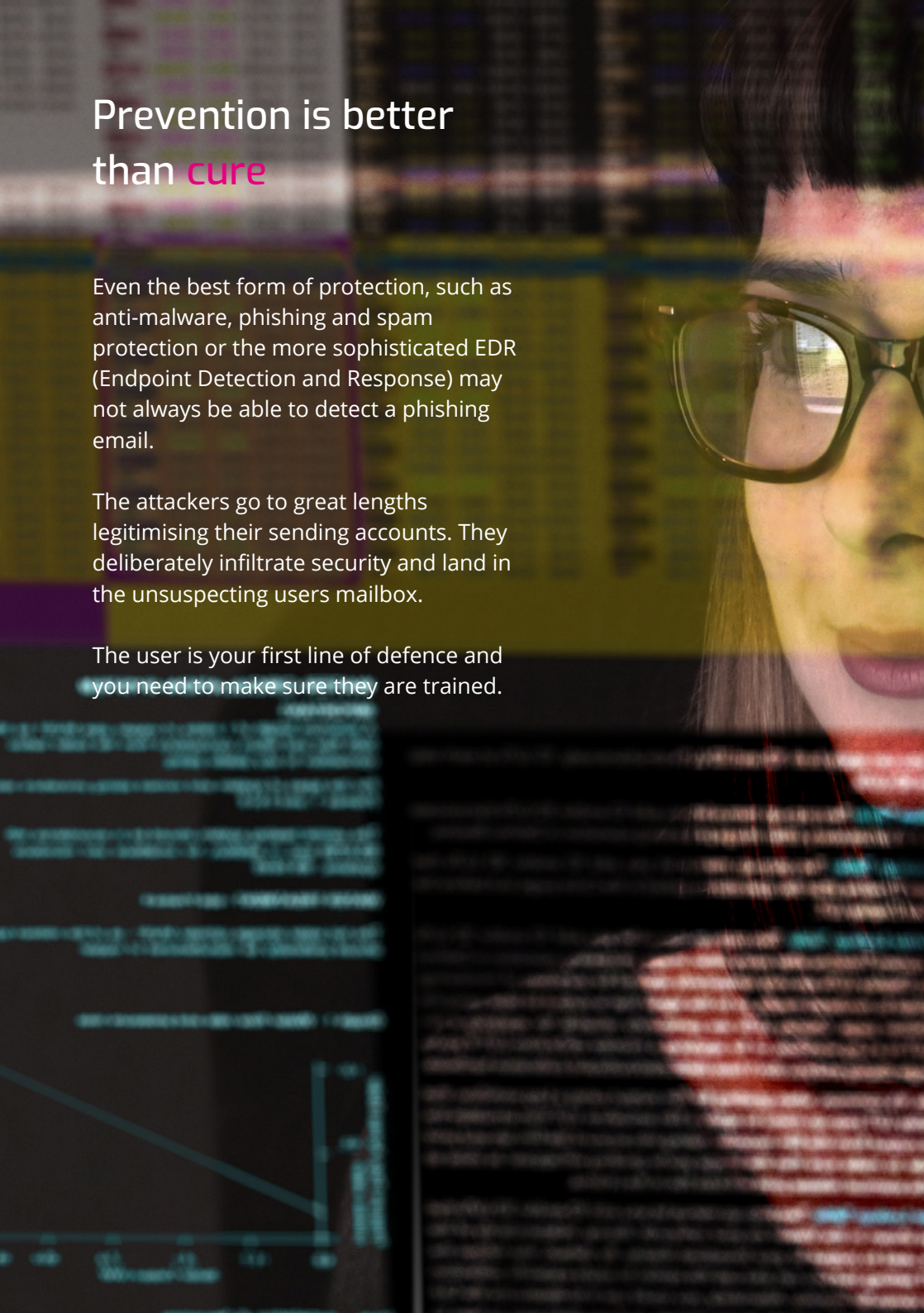


# Prevention is better than **cure**

Even the best form of protection, such as anti-malware, phishing and spam protection or the more sophisticated EDR (Endpoint Detection and Response) may not always be able to detect a phishing email.

The attackers go to great lengths legitimising their sending accounts. They deliberately infiltrate security and land in the unsuspecting users mailbox.

The user is your first line of defence and you need to make sure they are trained.



There's a lot more to phishing than you may have thought. Attacks are evolving all the time, so it's important to take them seriously and protect your business as well as you possibly can.

Help protect your business, **get in touch** today.

The logo for ILUX, featuring the word "ILUX" in a bold, pink, sans-serif font. A registered trademark symbol (®) is located at the top right of the letter "X".

IT that powers success

T: 0333 311 0109

[www.ilux.co.uk](http://www.ilux.co.uk)