The business owner's COMPLETE GUIDE to phishing

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

It's likely you've heard of phishing and know it's something you want to avoid.

But do you know what it really means and exactly how a phishing attack works?

In our experience, lots of people don't know the specifics. And that's OK. But 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', much in the same way you'd lure a fish to a hook with a big juicy maggot.

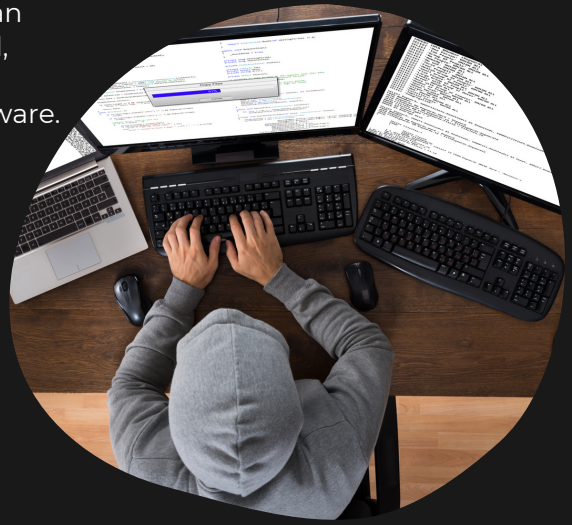
This virtual bait is usually in the form of an email. And when the victim gets hooked, their device and potentially their whole network can become infected with malware.

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

Phishing isn't just inconvenient. You should see how much time, expense and stress has to be invested in fixing the damage.

Understand this: You want to avoid a phishing attack.

Oh, and phishing doesn't always come in the form of an email either. But more on that later.



TO HELP YOU UNDERSTAND JUST HOW PREVALENT PHISHING ATTACKS HAVE BECOME, HERE ARE SOME SCARY STATS...

Last year 83% of organisations reported experiencing phishing attacks - that's up 28% from 2020

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

A third of phishing emails are opened

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

1 in 99 emails is a phishing attack. 25% of these slip through the security filters in your Microsoft 365 inbox

60% of successful phishing attacks result in lost data

52% result in a compromise of login credentials

47% of phishing attacks lead to ransomware, where your data is encrypted and held hostage until you pay a ransom fee

WHAT DOES A PHISHING ATTACK LOOK LIKE?

A phishing email will drop into your inbox like any normal email.

Often it'll look like it's been sent from a legitimate sender so you don't suspect anything is wrong.

This is dangerous when it's pretending to be from a popular company, like Amazon or PayPal.

But in some cases the attacker will have learnt 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. Everything is as it's supposed to be, so it's likely you won't question the contents... especially as it's often an urgent request for you to take action, which can be distracting in itself.

This urgent request will work in different ways: It can ask you to open an attached file, perhaps asking you to confirm details of a recent purchase.

By doing this, your device may become infected with malware. And if that device is connected to a network, it's possible that the malware could spread to other devices.

Another common approach is to ask you to click a link. This might take you to a fake page (known as a spoof web page) pretending to be a service you really use... and when you login, you have accidentally given your login details to the criminals.

BUT A PHISHING ATTACK ISN'T ALWAYS AN EMAIL?

Sadly no. That would make things easier for those of us in defence.

A phishing attack can take many different forms.
These are some of the most common ones...

Pop-up phishing:
Clue's in the name. 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.

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.

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

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).

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

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.

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

Oh, and there are different forms of phishing emails to beware of too...

Spear phishing:
These are sent to specific people who have been researched to some degree, 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.

Ok, you get the idea. Let's stop there.

WHO'S AT RISK?

Sorry to say it, but everyone in your business and especially you, as the boss (See whaling, above). It's a real threat you need to take seriously.

This isn't 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, all the time.

You don't read about small businesses being affected, as those stories don't end up in the news.

DO YOU HAVE EXAMPLES OF WELL-KNOW PHISHING ATTACKS?

Some of the biggest companies in the world have been fooled by phishing scams.

Between 2013 and 2015, Facebook and Google were scammed out of $100 million when cyber criminals carried out an extended phishing campaign.

They took advantage of the fact that both companies used the same Taiwanese vendor, Quanta. They sent a series of invoices pretending to be from Quanta, and both Facebook and Google paid.

When the scam was discovered, it was taken to the US courts. The attacker was arrested and extradited from Lithuania, and Facebook and Google recovered just under half of what was stolen.

In 2014, Sony Pictures became the victim of a phishing attack that wasn't about money. The attackers were believed to have a connection to North Korea, and targeted Sony because of a movie it refused to withdraw that mocked Kim Jong Un.

The cyber criminals used fake emails to steal huge amounts of information from Sony's network. That included email conversations about staff members, scripts, and employees' personal information.

They even gained access to Sony's offices by tricking their way in. Then they impersonated IT staff and installed malware on Sony's systems.

The attack ended up costing Sony around $35 million in IT repairs.

HOW CAN WE 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. Because if someone is using any 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

DO 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.

DO 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.

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

DO implement multi-factor authentication 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.

As you can see, there's a lot more to phishing than you thought. Attacks are evolving all the time, so it's important to take them seriously and protect your business as best you can.

If you want more information, or you need help protecting your business, get in touch.

Book a call with one of our expert technical advisors.

Call: +44 (0)333 202 636

Email: hello@better-it.uk

www.better-it.uk