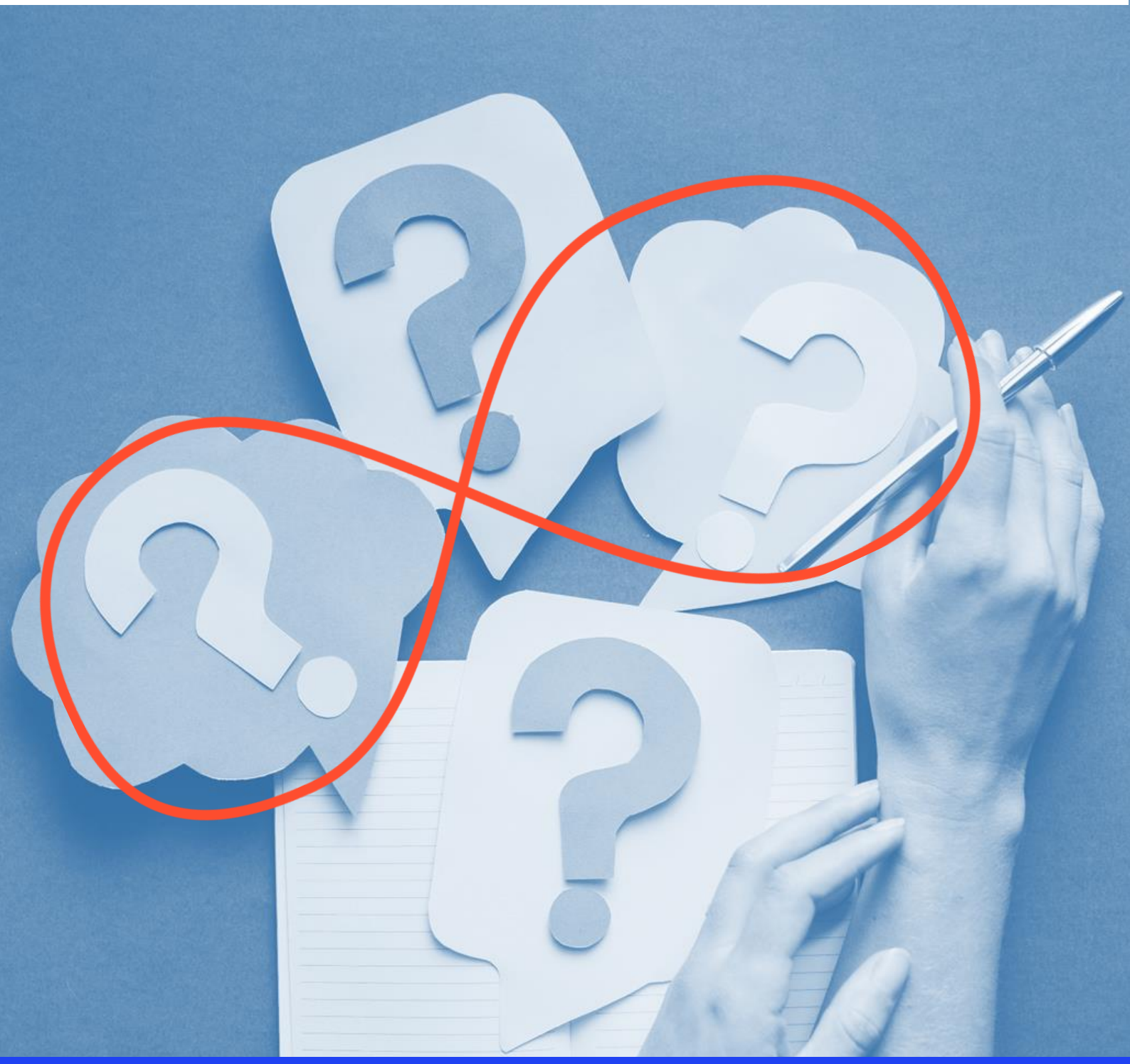
BRANDIT's "How to" Guides



How to stop a domain name being used for phishing purposes?

BRANDIT

How to stop a domain name being used for phishing purposes?

Online business is prevalent these days. Almost every business — local, national or international — has a web presence and domains are a major asset to these companies. However, with cybercrime on the rise, companies in 2021 have experienced increased ransomware attacks, business email compromises (BEC), phishing attacks, supply chain attacks, and online brand and trademark abuse. While domain threats are rising, are companies taking the appropriate level of action to protect themselves and minimise the risk? Companies and other organisations that fall victim to phishing attacks can end up losing millions in revenue as well as irreparable reputational damage. The good news is many of these attacks are preventable with the correct system configuration, employee training, and high-quality cybersecurity tools.

In this "**How to**" guide, we cover the different types of phishing attacks to watch out for and how a multi-layered approach is the best way to keep your organisation protected from cybercriminals.

What is a phishing attack?

No, we are not talking about a fishing trip that ends in disaster! We are of course talking about cyber security breaches. Phishing is one of the main forms of social engineering attacks and is one of the most common security challenges that both individuals and companies face in keeping their information secure. Whether it's getting access to passwords, credit cards, or other sensitive information, cyberhackers are using email, fake websites, social media profiles, phone calls, and any form of communication they can to steal valuable data. Businesses, of course, are a particularly worthwhile target with reports of phishing attacks costing organisations more than €3.21 million every year!

The current pandemic has only increased the threat of malicious activities in the cyber world. In fact, with more of us now working from home and most organisations' infrastructures shifting to the cloud, phishing emails remain rampant! The impact on companies is wide ranging, affecting not only their bottom lines but also major reputational damage due to potential losses in client and customer data.

What are various phishing techniques used by attackers?

Phishing attacks come in all shapes and sizes and often offer irresistible bait. These can include:

- Embedding a link in an email that redirects your employee or customer to a fake website that requests sensitive information.

- Using fake social media profiles and websites impersonating brands.

- Installing a Trojan via a malicious email attachment or ad which will allow the intruder to exploit loopholes and obtain sensitive information.

- Spoofing the sender address in an email to appear as a reputable source and request sensitive information. We've all had that email from an African Prince needing to temporarily transfer money to you and therefore asking for your account details!

- Posing as an employee/manager and send emails asking colleagues to pay an invoice to a reputable firm.

- Attempting to obtain company information over the phone by impersonating a known company vendor or IT department.

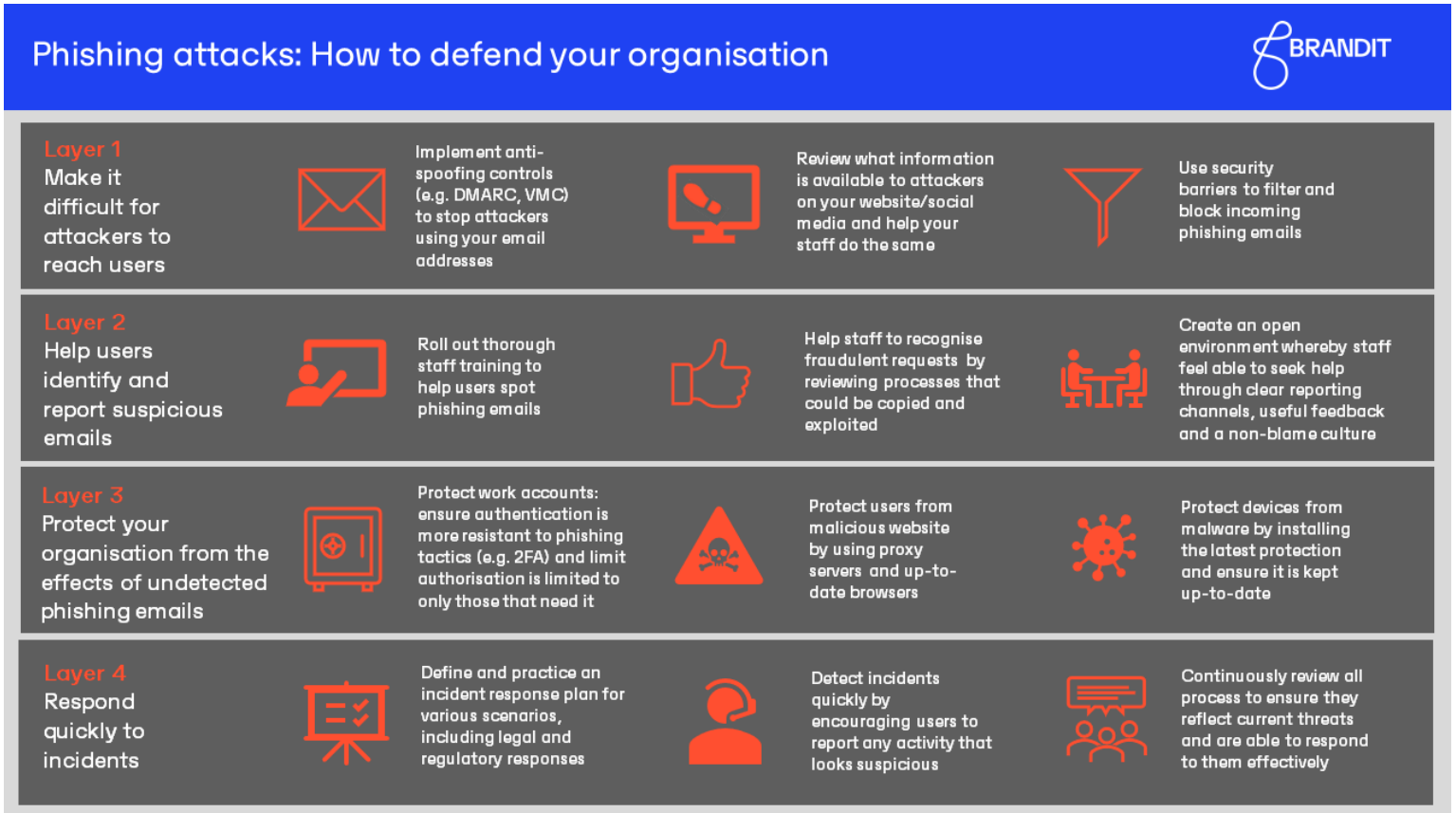
Phishing defences: why you need a multi-layered approach

Typical defences against phishing often rely exclusively on users being able to spot phishing emails. This approach will only have limited success. Instead, companies should widen their defences to include more technical measures. This will improve your resilience against phishing attacks without disrupting the productivity of your users. You'll have multiple opportunities to detect a phishing attack, and then stop it before it causes harm. You also acknowledge that some attacks will get through, as this will help you plan for incidents, and minimise the damage caused.

Our infographic below splits the mitigations into four layers on which you can build your defences:

Some of the suggested mitigations may not be feasible within the context of your organisation. If you can't implement all of them, try to address at least some of the mitigations from within each of the layers.

Summary of multi-layered approach to phishing defences



Our top tips to protect your organisation against domain phishing attacks

In addition to the multi-layered approach outline above, which covers prevention measures against phishing tactics in general, it is also possible to employ further actions to reduce attacks on your domains:

Continuously monitor

Monitor domain names that include your brands, or typos of your brand(s), that are trying to mislead email recipients into believing they are receiving communication from you.

Act fast!

Take immediate action against domain names that have MX record, showing that the domain may be used in an email address.

Put up the barriers

Make sure your company employs effective security barriers, including robust policies, antivirus solutions, web filters, encryption, spam filters, working from home protection etc.

Protect your brand(s)

Protect key brand names as registered trademarks to help you evidence your proprietary rights – this helps to take downs sites and suspend domains.

Collect evidence

Carefully store any evidence (e.g., the original fraud emails, screenshot of phishing websites, phishing messages, etc.) as authorities do not accept takedown requests without concrete proof.

Think outside the box

Research suggests that half of all cyberattacks in the business world now involve supply chains. From accidental or malicious activity by insiders within partner organisations, to external hacks by cybercriminals, make sure you have a clear picture of your supply chain, otherwise it will be very hard to establish any meaningful control over it.

Today, the majority of organisations will experience a domain or other form of spoofing attack.

It's not a matter of "if" but "when" so it pays to have the right protection solutions in place.

You won't reduce the threat level to zero, because there is always the possibility that there will be someone willing to do whatever it takes to break into your organisation. But by doing the basics well, monitoring the web and protecting you IP assets, you're signalling that it's going to take time and effort to break down your cyber walls, and those would-be attackers are better off looking elsewhere for an easier target.

If you need support or guidance with any of the topics covered in this guide, please contact us on one of the below channels:

- Website: brandit.com
- Facebook: @BRANDITGmbH
- Twitter: @BRANDIT
- LinkedIn: BRANDIT.com
- Instagram: @BRANDIT
- YouTube: BRANDIT

BRANDIT

Wiesenstrasse 9, 8008 Zürich, Switzerland Tel: +41 44 5156575 E-Mail: info@brandit.com brandit.com