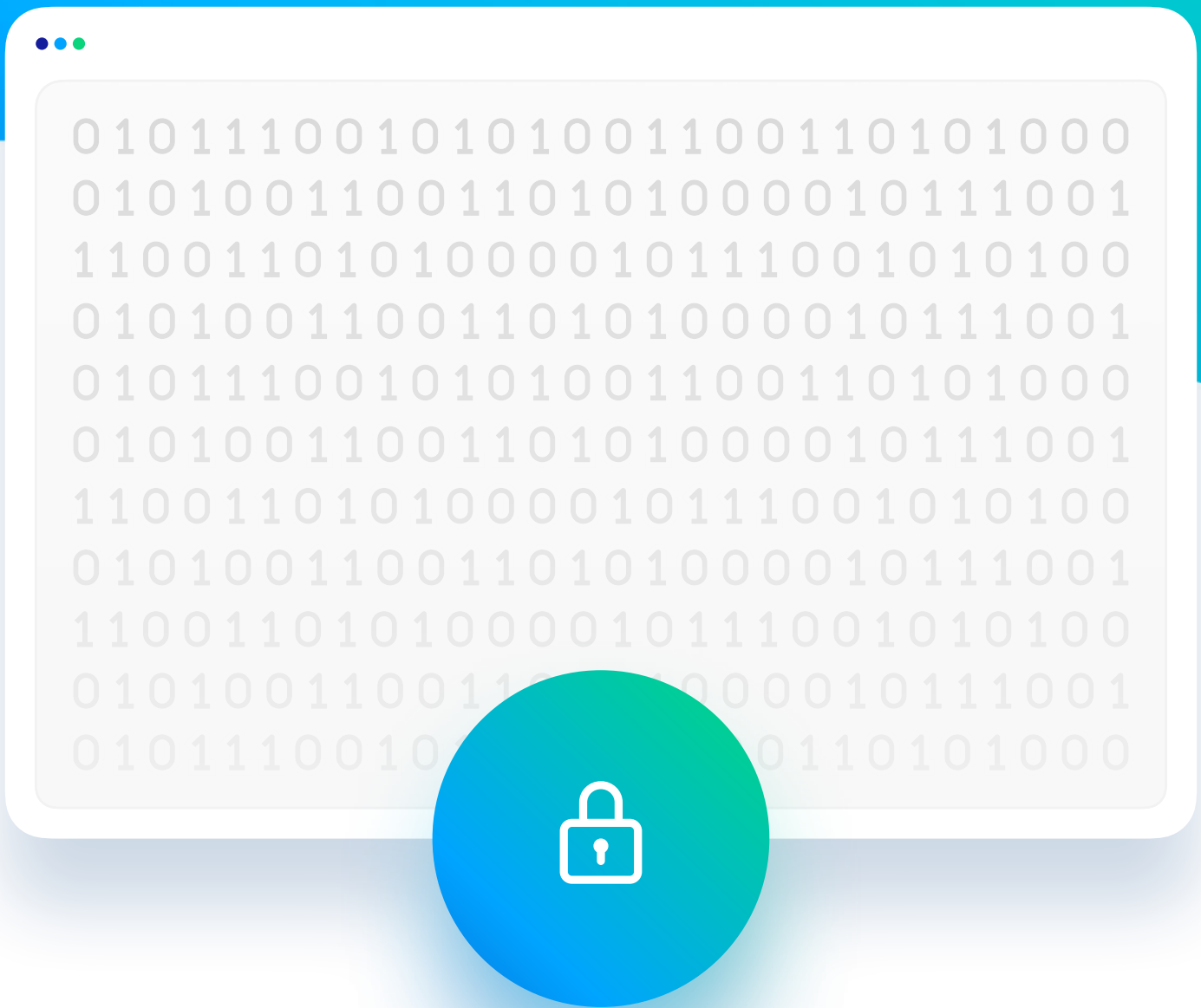
BACKUPVAULT

Phishing attacks

What are they and how can you protect your business against them?



In recent years, phishing has become increasingly frequent.

The rise in attacks signifies an influx of money in cybercrime. This means cybercriminals have been successful and so have the time and resources to make phishing attacks more complex, convincing, and difficult to detect.

With so many potential threats out there, it's absolutely essential that you're familiar with the key elements of phishing scams and that your business has an effective data protection strategy to protect against and cope in the event of an attack.

So, let's examine what exactly phishing is and how to develop a secure line of defence against it for your business.

What is phishing?

Phishing is a form of cybercrime in which attackers try to gain access to the valuable data of online users by deceiving victims into clicking on fraudulent and malicious links.

Most commonly, phishing attacks occur via email or text messages, imitating legitimate websites and sources, sometimes to uncanny levels of success.

If you are targeted by phishing, criminals may, unfortunately, unlock sensitive data such as bank details, credit card data, and other personal login credentials.

A staggering

90%

of all cybercrime starts with a phishing attack.

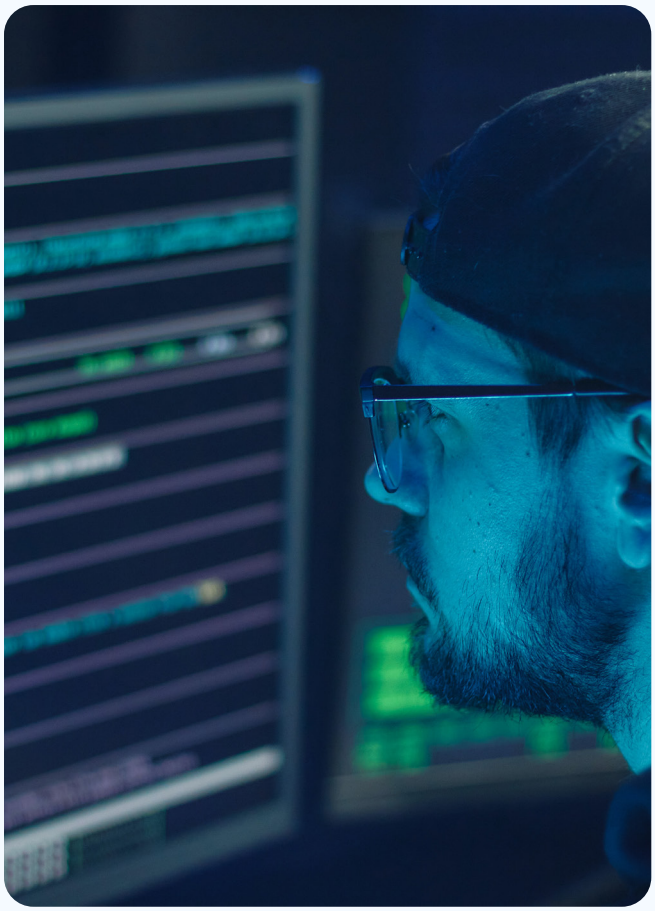
Phishing and the threat to your business

Due to the size and scale of business data, the potential reward is much greater for criminals when they target an organisation over an individual, putting your company at even higher risk.

Phishing attacks exploit businesses by stealing their data, installing malware on their systems, and disrupting their ability to function.

As a result, 60% of small businesses targeted by a cyber attack go under within the first six months.

And with only 1 in 5 companies training their employees on how to recognise and respond to phishing tactics, it's becoming easier for cybercriminals to successfully hack into valuable business data in the first place.



Understanding the types of phishing attacks and common signs will empower your staff to make wise decisions when met with a potential attack.

Common types of phishing attacks:

- Fraudulent text messages and phone calls
- Deceptive emails
- Social engineering and deception
- Links to fake websites

Signs to look out for:

- Questionable sender or reply to address
- Unusual contact from a high-up in an organisation
- Urgent requests or threats
- An offer that appears too good to be true
- Requesting login details and personal information
- Spelling and grammatical errors

How do I protect my business from phishing attacks?

It's vital to protect your business from cybercriminals to avoid the detrimental effects of an attack, while also taking away the opportunity for them to commit dangerous online crimes successfully.

The effects of phishing attacks should not be overlooked or underestimated.

What are the potential impacts of phishing on your business?

Loss of critical data

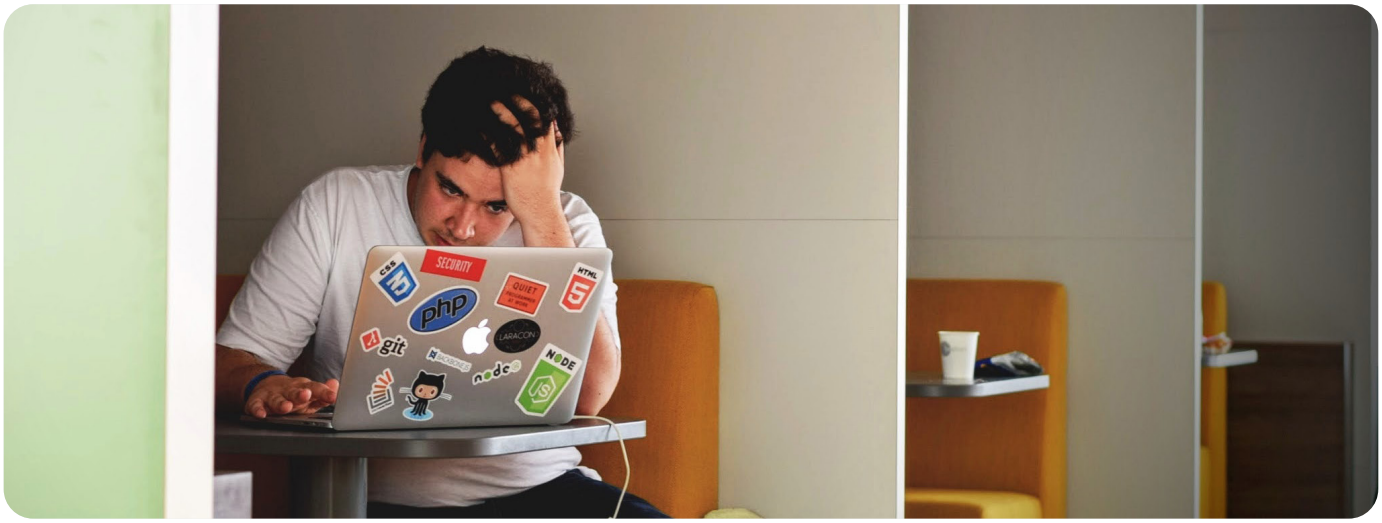
Halting of operations

Legal ramifications

Damage to brand image and reputation

Financial loss through extended downtime, loss of sales, and possible ransom payments

Wasted time and resources on data recovery efforts



Falling victim to a phishing attack can leave your business vulnerable in many ways, no matter what size. Even highly established global organisations have fallen for and suffered the effects of phishing. Most notably, both Facebook and Google lost more than an accumulated $100 million to a series of phishing emails between 2013 and 2015. So, in an increasingly risky space, how do you make sure your business is safe from cybercriminals targeting your industry?

Integrating a comprehensive cybersecurity strategy into your business is essential for safeguarding against phishing.

Necessary steps to protect your business.

While there are a worrying 3.4 billion phishing emails attempts made daily, there are many powerful systems you can put in place to protect your business and avoid succumbing to cyber attacks.

01

Implementation of security measures

The best way to avoid the effects of an attack is to prevent them from happening in the first place. There are plenty of security measures you can have in place to deter cyber attacks. Consider incorporating firewalls, antivirus software, malware detection, and spam filters into your systems.

02

Employee education

Equip your staff with the knowledge to recognise and respond to phishing scams with cybersecurity awareness programs and training. They'll learn about phishing risks and best practices so they can act as an extra line of defence for your business.

03

Multi-factor authentication

If cybercriminals gain access to some of your login credentials, it doesn't have to mean they can access your data. Incorporating a multi-factor authentication and login system means they cannot get past the additional layers unless a member approves it of staff.

04

Security audits and vulnerability assessments

With phishing scams becoming more common and sophisticated, you must respond appropriately to the advancements. Maintain regular assessments of your security systems to ensure they are up to date and to highlight any potential vulnerabilities.

05

Establishing an incident response plan

While it's essential to work hard to prevent phishing, it's also important to be prepared in the unfortunate case of an attack. Develop an incident response plan for your team to give your business the best chance of minimising damages and downtime.

06

Securely backing up all the data

If an attack is successful, you must have all of your critical data securely backed up. Your data should undergo regular immutable backups, meaning they cannot be changed by ransomware, and a physically separate location for extra protection.

07

Developing a disaster recovery plan

Having your data hacked doesn't always have to mean the worst. Ensure your business is ready to respond with a lightning-fast data recovery system. A proper disaster recovery plan can reclaim data in its untouched form in just a matter of clicks.

What should you do if your business has become a victim of phishing?

If your business suffers a phishing attack, you must act immediately. You and your team must have a strategic response ready to go, and everyone must be trained and understand their role in the process before it happens.

Vital steps to take after phishing:

Notify relevant parties, such as IT personnel and management

Isolate affected systems and disconnecting from the network to prevent further data corruption

Conduct a thorough investigation to determine the extent of the breach

The best way to achieve peace of mind surrounding phishing and cybersecurity is to invest in a professional backup and data protection solution, so you can let the experts worry about protecting your most valuable assets.

BackupVault: A trusted solution for data protection

Trusted by professionals worldwide, BackupVault provides consistent, reliable, GDPR, ISO and SOC2 compliant data protection solutions to SMBs, large enterprises, and government organisations. Our highly effective solutions ensure that your company doesn't lose any data in the event of an attack, allowing you to regain access to your information instantly.

We can help secure your data and educate users to prevent phishing scams with:

Effective Security Awareness Training for the whole team

Regular, scheduled immutable backups

Expert remote management and reporting

Native ransomware protection and active malware detection

It couldn't be simpler to start keeping your valuable data safe from phishing attacks and malicious software.

Our friendly team can help remotely setup the software for you. Daily secure cloud backups and security scans are performed automatically. Whatever size business you're operating, we provide scalable solutions to grow with your business.

Ready to take the stress out of the threat of phishing?

Contact us or start your no-nonsense 14-day free trial today to start protecting your critical data from phishing attacks with BackupVault, plus a Security Awareness Training platform for employees. Check out our full suite of powerful data protection solutions.

Free trial

Security awareness training

BACKUPVAULT

backup@backupvault.co.uk

020 3397 5159

Wilson House, Lorne Park Road
Bournemouth, Dorset, BH1 1JN