Your phishing campaign results are in!

This simulation uses real-world phishing techniques to assess how your users would react to an inevitable attack, including whether they would click a harmful link, download a malicious file and/or compromise their credentials.

You can click into the boxes to understand further information about the phishing attack.

Risk Score

Medium Risk

You

549

/900

Domain Scan

8 Connected Domains

2 Connected Services

860 Lookalike Domains

147 Connected Applications

Connected Domains & Services

Although there may not be any immediate risk to connected domains and services themselves, they do help cyber criminals understand how your business is structured. With this information, cyber criminals are free to launch a highly-contextualised attack that has a high chance of success.

Domains that have been left dormant for a period of time also pose a risk, as they create an opportunity for cyber criminals to use lookalike domains to impersonate a brand.

Lookalike Domains

A lookalike is almost identical to an existing domain, but with a slight alteration. They are intended to deceive the target into confusing them with the original domain. This allows cyber criminals to impersonate legitimate brands and conduct fraud, which is why they register hundreds of thousands of look-alike domains each year.

Connected Applications

Cyber criminals are curious about the applications used in your business. With this information, they can exploit any known vulnerabilities in the apps you use to breach your data - or impersonate these apps in highly-targeted phishing attacks against members of staff.

Breach Scan

24%
of your users appear in one or more high risk breaches

45%
of your users appear in one or more medium risk breaches

0%
of your users appear in one or more low risk breaches

Dark Web Scan

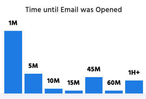
A moderate amount of data about your business and employees is available on the internet. If a cyber criminal were to acquire this information, they could use it in social engineering scams or highly-targeted phishing attacks.

Having data of this nature on the internet shows that employees are not following sound information security practice, such as keeping their work email private and only used in work-related services.

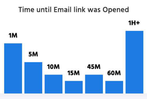
A successful attack could result in significant damage to your brand and the reputation of your business, as well as wreak havoc on your customers, partners and anyone else linked to your business network.

Phishing Campaign

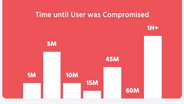
55%
Opened Email



44%
Visited Landing Page



70%
Compromised



Simulated Cyber-Attack - Phishing

Your employees' reactions to the simulated phishing attack shows that an attack of this nature presents a moderate risk to your business.

The link in the simulated phishing email was clicked by a moderate number of employees. A similar email could be used by cyber criminals to direct your employees to fake websites that harvest their log-in credentials, or infect their devices with malware.

Employees that gave away their credentials on the landing page of the simulation are susceptible to handing cyber criminals sensitive information, leaving your whole business network open to further infiltration.

Your Time to Breach is

1 hour 33 minutes

Time to Breach is an estimated window of time between when an attacker starts looking for a target, to when they have successfully breached an organisation.

The window is determined by data we have collected when creating your Risk Report, combined with some estimations based on industry data.

Summary and Conclusions

Based on the report findings, the risk that your employees currently represent to the business is medium. Any cyber attack targeted at your company has a moderate chance of success.

It is possible to reduce risk in your business by deploying new processes and technologies. However, cyber criminals will often look to exploit employees as they are a common weak point in an organisation's defence.

A breach could result in significant reputational impact and brand damage, as well as carry fines from governing bodies if you were found to not have the applicable level of security in place to mitigate the chances of a breach occurring.

What You Can Do to Reduce Your Risk

Your business is at risk of being successfully breached in a cyber attack.

In order to reduce the threat of user-related security incidents, sensitive data loss and financial damage, we strongly propose deploying the following Human Risk Remediation Programme, consisting of **four core elements**:

1. Train employees in cyber security best practices

In order to reduce insider threats, build stronger resilience to an inevitable cyber attack and comply with information security standards, your employees' cyber security knowledge gaps will be evaluated and regular cyber security awareness training will be deployed.

Computer-based training will be conducted and measured every month, in the form of short and engaging courses, designed to maximise knowledge retention and behaviour change without disrupting work efficiency, covering core infosec best practice competencies.

2. Implement information and data security policies

Implementing information and data security policies and procedures will reduce your organisation's human risk by clearly setting the standards of expected behaviour, as well as guidance on how employees can achieve those standards.

Key policies will be implemented and sent to your employees for approval. In order to ensure that your policies are being complied with, employee eSignature approvals will be automatically tracked and accessible for easy auditing.

3. Conduct regular phishing assessments

Phishing and social engineering techniques are evolving daily, increasing the likelihood that your employees will compromise sensitive data in a sophisticated attack.

In order to assess and monitor your employees' susceptibility to new and diverse attacks, regular phishing simulations will be automatically deployed and tracked, giving you full visibility of opens, clicks and compromises. If a user fails a phishing simulation, they will be auto-enrolled onto a short phishing awareness course to mitigate future risk.

4. Monitor the Dark Web for exposed user credentials

With millions of credentials exposed in data breaches every year, it is likely that your employees will at some point have sensitive data compromised on the Dark Web. This data is then used to conduct business email compromise (BEC) and social engineering attacks.

In order to reduce the likelihood of these attacks and to safeguard your exposed users, regular scans will be conducted on the Dark Web and through thousands of paste sites, with your business being alerted when exposed data is detected in a breach.