

Your human risk results are in

This assessment uses the same techniques real attackers use to see how your people would respond to an inevitable attack: whether they would click a harmful link, open a malicious file, or hand over their credentials.

The sections below break down what we found, what it means for your organization, and what to do about it.

HUMAN RISK SCORE

Medium risk

549 / 900



A higher score means higher risk.

Domain Scan

D 8

Connected domains

S 2

Connected services

L 860

Lookalike domains

A 147

Connected applications

Connected domains and services

None of these is an immediate risk by itself. But they show a criminal how your business is put together, which makes a highly targeted attack far easier to plan. Domains left dormant for long periods also create an opening for criminals to impersonate your brand.

Lookalike domains

A lookalike is nearly identical to a real domain, with one small change meant to fool the person reading it. Criminals register huge numbers of them every year to impersonate trusted brands and commit fraud.

Connected applications

Criminals are curious about which applications your business uses. With that list, they can exploit known weaknesses in those apps, or imitate them in phishing emails aimed at your 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 meaningful amount of data about your business and employees is available online. If a criminal acquired it, they could use it in social engineering scams or highly targeted phishing attacks. Finding data like this suggests employees are not following sound security habits, such as keeping their work email private and using it only for work.

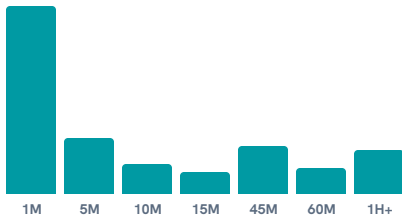
A successful attack could do serious damage to your brand and your reputation, and cause problems for your customers, partners and anyone else connected to your network.

Phishing Campaign

55%

Opened the email

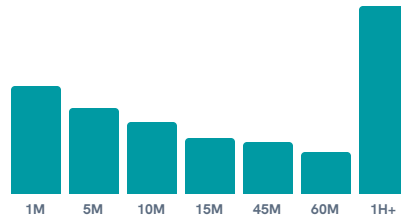
Time until email was opened



44%

Visited the landing page

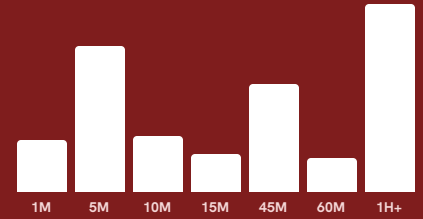
Time until link was clicked



70%

Compromised

Time until user was compromised



Simulated cyber-attack: phishing

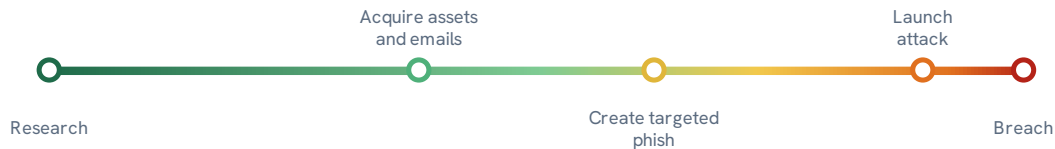
How your employees reacted to the simulated phishing attack shows that an attack like this poses a moderate risk to your business.

A moderate number of employees clicked the link in the simulated email. A criminal could use a similar email to send your people to fake websites that harvest their login credentials, or to infect their devices with malware.

Employees who gave away their credentials on the landing page are open to handing over sensitive information, which leaves your wider network exposed to further intrusion.

Your time to breach is

1 hour 33 minutes



Time to breach is the estimated window between an attacker starting to look for a target and successfully breaching an organization.

The window is based on the data collected while building this report, combined with estimates drawn from industry data.

Summary and conclusions

Based on the findings in this report, the risk your employees represent to the business is medium. A cyber attack aimed at your company has a moderate chance of success.

You can reduce that risk by putting the right processes and technology in place. Criminals will often look first to your people, because employees are a common weak point in any organization's defenses.

A breach could cause serious reputational damage and brand harm, and may carry fines from regulators if the required level of security was not in place to reduce the chance of one.

What you can do to reduce your risk

Your business is at risk of being breached in a cyber attack. To cut the threat of user-related security incidents, sensitive data loss and financial damage, we recommend the secr*iq* human risk program, built on four core elements.

1 Train employees in cyber security best practices

To reduce insider threats and build resilience to an attack that is going to happen sooner or later, your employees' knowledge gaps will be measured and then closed with security awareness training.

Training runs every month as short, engaging lessons designed to make the knowledge stick and change behavior, without disrupting daily work. It covers the core information security habits every employee needs.

2 Put information and data security policies in place

Clear policies and procedures lower your organization's human risk by setting out the standard of expected behavior and showing employees how to meet it.

Key policies are sent to your employees for approval. Their e-signatures are tracked automatically and kept ready for audits, so you can prove your policies are being followed.

3 Run regular phishing simulations

Phishing and social engineering tactics change daily, which raises the chance that your people will hand over sensitive data to a sophisticated attack.

Regular simulated phishing campaigns test how your employees handle new and varied attacks, and give you clear visibility of opens, clicks and compromises. An employee who falls for a simulation is enrolled automatically in a short phishing awareness course to reduce the chance it happens again.

4 Monitor the dark web for exposed credentials

Millions of credentials are exposed in data breaches every year, so your employees have very likely had sensitive data exposed at some point. Criminals use that data to run business email compromise and social engineering attacks.

To lower the chance of these attacks and protect exposed users, secr*iq* scans the dark web and thousands of paste sites on a regular schedule, and alerts you when your data turns up in a breach.

What's your organization's secure IQ?

Get your own free human risk report and see where your people stand.

[secr*iq*.com](https://secr<i>iq</i>.com)

This is a sample report. The organization name and all figures are illustrative and do not describe a real company. Actual reports are generated from each organization's own domain, breach and phishing simulation data.