

# How email phishing uses your own data against you







# CONTENTS

**01**

Introduction

**02**

Beware of making information publicly available

**04**

Malicious actors tap dark web data

**05**

Defend against phishing attacks with better security posture


## Introduction

Phishing is one of the most pernicious cyber threats facing small and medium-sized enterprises today. Malicious actors continue to use phishing techniques to exploit poor security hygiene and access sensitive information and business data. A 2019 cyber security study conducted by Carbon Black revealed that phishing attacks were the No. 1 cause of data breaches in Australia, with government agencies, financial services firms and manufacturing companies representing the three sectors most commonly targeted by these threats.

According to the Australian Competition & Consumer Commission, Australians lost more than \$1.5 million as a result of phishing attacks in 2019. It's worth noting that this figure only accounts for reported cases of phishing, so the real cost of phishing is likely significantly higher.

The degree of success with any phishing attack depends on two primary factors: the target's risk awareness and the perceived legitimacy of the malicious actor's communications. Businesses and individuals who adhere to cyber security best practices are far less likely to fall victim to an attack. On the other side, phishing emails are much more effective when they have been tailor-made with the target in mind.

Cyber criminals frequently use personal information to customise their phishing attacks and increase their effectiveness. If businesses aren't careful, their own data could be used against them, leading to a costly data breach.

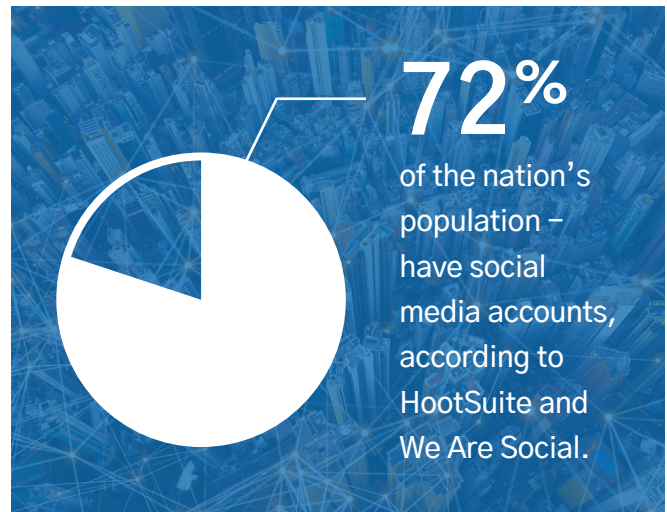


**Australians lost more than \$1.5 million as a result of phishing attacks in 2019.**



## Beware of making information publicly available

Social media platforms offer people a great way to stay in touch with family, friends and acquaintances, but they should be careful about how much information they share on public profiles. Approximately 18 million Australians — 72% of the nation’s population — have social media accounts, according to HootSuite and We Are Social. Those accounts are spread out across several different platforms, including Facebook, Instagram, LinkedIn and Twitter. On average, internet users in Australia have at least six social media accounts.



Those social media platforms provide ample opportunities for malicious actors to gather personal information to fuel their phishing campaigns. Details add credibility to phishing emails, so cyber criminals will take every advantage to incorporate information that applies to specific individuals.

For instance, malicious actors could easily see through a user’s LinkedIn profile who their co-workers and supervisors are, and craft a phishing email that appears to have been sent by one of those individuals. Those communications may reference other people within the organisation or projects that have been mentioned on social media.







**It's important that business leaders stress the risk that social media platforms pose to organisational security.**

This technique, known as spear phishing, is very effective because a surface reading of the email will rarely raise any red flags. The sender is a known acquaintance, the email references specific information that the target assumes is not publicly available and any request made seems reasonable.

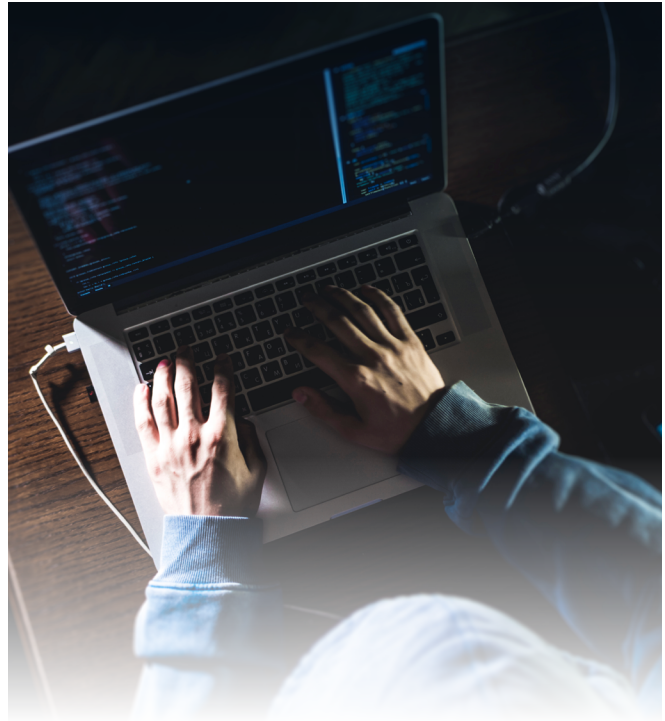
If the reader clicks on a link or downloads an attachment, though, they could be exposing their device, their software and their network to malware. Once the attacker has access to business systems, networks and databases, they can exfiltrate sensitive information and cause untold damage to the organisation.

It's important that business leaders stress the risk that social media platforms pose to organisational security. Even innocuous posts and updates could contain information that could be used to add authenticity to a phishing attack. It's not practical to expect staff members to stay away from social networks, but employees should be made aware that any personal information they share on those platforms is publicly available. Recognising that fact will help staff members view incoming emails — especially those sent from ostensibly legitimate sources — with more scrutiny.

## Malicious actors tap dark web data

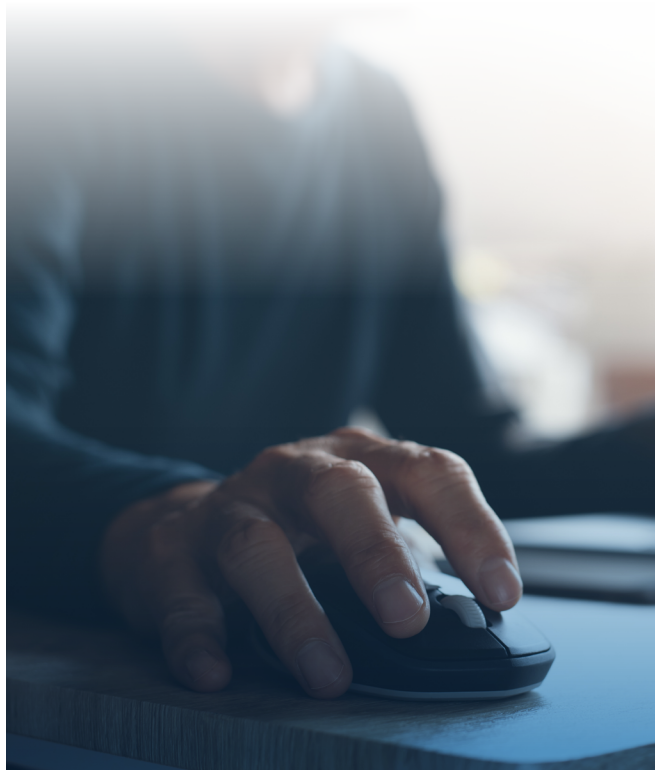
Cyber criminal data collection efforts are not limited to public platforms and sources. The dark web is a treasure trove of valuable information and resources that malicious actors can use to drive their phishing attacks. The average person cannot access the dark web without a dedicated browser client, and many people aren't even aware it exists. The relative anonymity attracts criminal activity, supplying data thieves with phishing kits and personal information pertaining to high-value targets.

Those kits can range from basic templates that capture easily obtainable data and login credentials to more sophisticated packages including fake sites masquerading as popular and trusted payment portals and ecommerce sites.



The dark web's illegal trade also provides a marketplace for cyber criminals to sell and trade personal information, login credentials and other sensitive data. One malicious actor could handle all the legwork gathering all of the details that add colour to a phishing attack — co-workers' names, legitimate email addresses, professional contacts, etc. — and then sell that data to another party. That data thief would then have all the information needed to launch an effective phishing campaign targeted at a specific organisation or person.

Because all of this activity occurs on the dark web, basic security monitoring services are unable to keep tabs on it. More sophisticated solutions, designed with dark web monitoring in mind, offer more visibility into illegal markets and flag any employee or business data that is traded and sold there.





## Defend against phishing attacks with better security posture

With so many avenues available to cyber criminals to enhance and fine-tune their phishing attacks, businesses need to be more diligent than ever about their security posture. Phishing techniques are more sophisticated today and are carefully designed to compromise high-value targets. The red flags aren't quite as obvious as they used to be.

Employees are your first line of defence against phishing attacks, but without proper training and education, they will be nothing more than liabilities. Regular training sessions that teach the latest security best practices, new wrinkles in cyber criminal strategies and tell-tale signs of malicious activity will instil a robust security hygiene within any organisation.

Working with a cyber security partner significantly improves training, prevention and remediation efforts, as they can provide expert advice and support. Biztech's data security professionals can help reshape your company culture and organisational mindset to prioritise threat awareness and risk management.

Combine those educational processes with Biztech's industry-leading email threat analysis solutions to identify malicious activity and actively prevent phishing attacks from exposing sensitive data and accessing business networks and systems.

Today's sophisticated, costly cyber threats require a dedicated, multi-pronged response.

**Partner with Biztech to defend your organisation with the best cyber security solutions available.**

