8 OF THE MOST UNEXPECTED WAYS CYBERCRIMINALS CAN TARGET YOUR BUSINESS & HOW TO PREVENT THEM

Lanrex | technology that means business

02 8875 0800 | 02 8875 0888 | info@lanrex.com.au | lanrex.com.au

CONTENTS

Since June of last year, Australia has been on high alert for cyber attacks after the Australian Cyber Security Centre (ACSC) announced the most coordinated state-based cyber attacks on targeted institutions. The scale of these attacks have highlighted the need for Australian to step up its cyber defences with a **$1.7 billion cybersecurity strategy** funded by the Federal government.

Over the years, Australian organisations of all sizes have been increasingly targeted by malicious attacks that are continuously evolving and growing more sophisticated every time. The Australian government reports that cyber security incidents have cost businesses by up to **$29 billion per year**.

Given rising attacks, how can organisations stay up to date in their cyber security response?

In this ebook, we'll explore eight unexpected ways cybercriminals can affect your business and what you can do to prevent them.

01

URL PHISHING

A URL is simply explained as your Web Address. The URL tells others the location of a web resource on a computer network and how to access it.

URL phishing is a type of attack where cybercriminals contact you using a disguised email to direct victims to a misleading website. On this website they ask for sensitive information such as usernames, passwords, or banking details.

What is the impact?

32%	of breaches involve phishing
4%	of recipients in any given phishing campaign click on the malicious link.
57%	of organisations have URL protection measures in place
$58M	Reported losses from phishing reached $58 million in 2019

02

SPEAR PHISHING

Spear phishing is a highly personalised form of email phishing that aims to steal sensitive information such as login credentials or financial details which is then used to commit fraud, identity theft, and other crimes. Cybercriminals research their targets and create carefully designed messages, often impersonating a trusted colleague, website, or business.

Traditionally, hackers focused on malware attacks, but in recent years they have shifted their efforts to ransomware and targeted phishing attacks with the goal of capturing user credentials.

What is the impact?

43%	of organisations said they had been victims of a spear-phishing attack in the past 12 months
2019	In 2019, phishing was the most commonly used method for scamming with 25,168 cases. 513 of those reported led to financial losses at **AU$1.5 million**.
23%	Only 23% of organisations said they have dedicated spear-phishing protection in place

03

LATERAL PHISHING

In lateral phishing, recently hijacked accounts are used by cybercriminals to send phishing emails to unsuspecting recipients in their contacts list. This can include family and company contacts and can even spread externally outside organisations. These attacks can have a high success rate because they come from a legitimate email account and appear to be from a trusted colleague or partner.

What is the impact?

1 in 7 organisations has experienced a lateral phishing attack

55% More than 55% of these attacks target recipients with some work or personal connection to the hijacked account

11% of these attacks successfully manage to compromise additional accounts, leading to even more lateral phishing attacks

04

BUSINESS EMAIL COMPROMISE

Business Email Compromise (BEC) attacks typically impersonate an employee in the organisation in an effort to defraud the company, its employees, customers, or partners in giving out confidential finance information. These targets are then tricked into doing wire transfers or disclosing sensitive information. These often use social-engineering tactics and compromised accounts, and they often include no attachments or links.

What is the impact?

7% Makes up 7% of spear-phishing attacks

$1.7B Caused more than $1.7 billion in losses in 2019 alone

800% Payroll scams are growing more than 800% recently

05

CONVERSATION HACKING

In conversation hijacking or an impersonation scam, cybercriminals integrate themselves into existing business conversations or initiate new conversations based on information they've gathered from compromised email accounts to steal money or personal information.

Conversation hijacking can be part of an account-takeover attack. Attackers spend time reading through emails and monitoring the compromised account to understand business operations and learn about deals in progress, payment procedures, and other details.

Cybercriminals rarely use the compromised accounts to send a conversation hijacking attack, though. Instead, attackers use email-domain impersonation.

What is the impact?

400% increase in domain-impersonation attacks to facilitate conversation hijacking recently

- Attacks are low volume, but effective, personalised, hard-to-detect and costly

$400K Shark Tank's Barbara Corcoran lost nearly $400,000 due to a phishing scam

06

ACCOUNT TAKEOVER

Account takeover or an account compromise is a form of identity theft and fraud where cybercriminals use brand impersonation, social engineering, and phishing to steal login credentials and access email accounts.

Once the account is compromised, hackers monitor and track activity to learn how the company does business, the email signatures they use, and the way financial transactions are handled. This helps them launch successful attacks, including harvesting additional login credentials for other accounts.

What is the impact?

29% of organisations had their Microsoft Office 365 accounts compromised by hackers in one month

1.5M More than 1.5 million malicious and spam emails were sent from the hacked Office 365 accounts in that 30-day period.

07

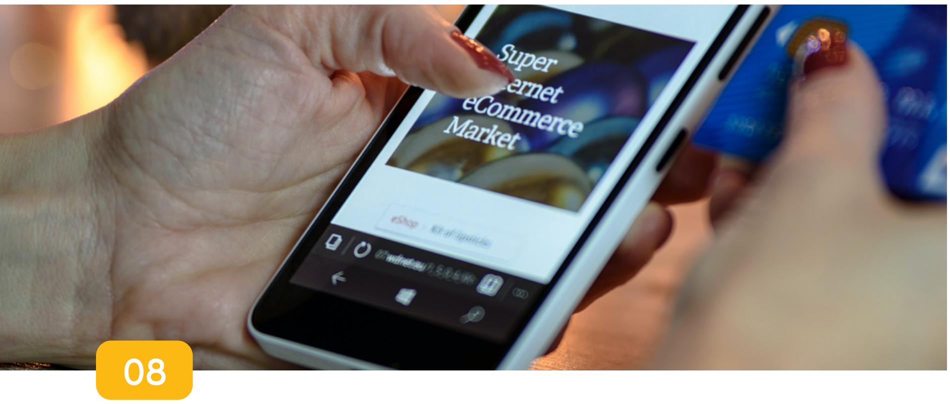
DOMAIN IMPERSONATION

Domain impersonation is often used by hackers as part of a conversation-hijacking attack. Attackers attempt to impersonate a domain by using techniques such as typosquatting, replacing one or more letters in a legitimate email domain with a similar letter or adding a hard-to-notice letter to the legitimate email domain. In preparation for the attack, cybercriminals register or buy the impersonating domain.

Domain impersonation is a very high-impact attack. It can be easy to miss the subtle differences between the legitimate email domain and the impersonated email domain. For example, an attacker may try to impersonate a website using a very similar URL.

What is the impact?

400% An analysis of about 500,000 monthly email attacks shows a 400% increase in domain-impersonation attacks used for conversation hijacking



08

BRAND IMPERSONATION

Brand impersonation is designed to impersonate a company or a brand to trick their victims into responding and disclosing personal or otherwise sensitive information.

A common type of brand impersonation is service impersonation, which is a type of attack designed to impersonate a well-known company or commonly used business application to steal personally identifiable information, such as credit card and Tax Identification Numbers. Emails are typically well-designed as an entry point to harvest credentials and carry out account takeover.

What is the impact?

47% Service impersonation is used in 47% of all spear phishing attacks

- Microsoft is the most impersonated brand in spear-phishing attacks

30K There are almost 30,000 spoofing attacks each day

77% of the Fortune 500 companies do not have Domain-based Message Authentication, Reporting & Conformance (DMARC) policies set up

THE STEPS TO SAFEGUARD YOUR BUSINESS

The evolving tech landscape means the scale of cyber threats is ever increasing. Businesses must take all these actionable insights and deploy a cyber security strategy that can mitigate risk and counter new threats that only grow more sophisticated every day.

Here are some key steps to help you get started.

01 Perform a full Security Assessment to establish a baseline and address existing vulnerabilities.

02 Secure your email, this is where most attacks originate from.

03 Apply security policies on your network e.g limit screen timeouts and user access.

04 Train your users, often! Run simulation testing to ensure they are not becoming complacent.

05 Implement Web Gateway Security, which detects cloud-based web and email threats and blocks them before they reach your team.

06 Encrypt files on your devices, including those being emailed and those on mobile devices.

07 Utilise Dark Web research to know in real-time what passwords and accounts of yours have been posted up for sale.

08 Supercharge protection with Security Incident & Event Management. This provides valuable defence against advanced threats and meeting compliance requirements.

09 Utilise Advanced Endpoint detection and response. This technology replaces outdated anti-virus solutions to protect your computers from malware, viruses, and cyber attacks.

STRENGTHENING YOUR IT DEFENCE WITH LANREX

2020 has seen many Australian organisations impacted by cyber security breaches and malicious attacks with **61% of data breaches made in the first half of the year** according to the Office of the Australian Information Commissioner (OAIC). Many of these breaches happened unnoticed with organisations unable to respond in time.

With businesses having to shift to remote ways of working throughout the COVID-19 outbreak, it's high time for organisations to review the impact of their changed business practices to their overall privacy and boost their cyber security strategy this year and beyond.

A managed service provider like Lanrex can strengthen your **cyber security strategy**, so you can easily identify risks to your business and build an effective response that fits the needs of the current times. Our team of IT professionals can ensure your business data stays protected, so you can minimise downtime and prevent security breaches that can easily damage your reputation and lead to costly remediation.

Don't leave it all to chance. Any vulnerability is too high a risk to ignore.

Explore **Lanrex's cyber security solutions** today, and we can further discuss how to tailor it according to your business's needs.

Lanrex | technology that means business

IF YOU ARE WONDERING HOW A TECHNOLOGY PARTNERSHIP WITH LANREX COULD WORK FOR YOUR BUSINESS,

GET IN TOUCH

Phone: 1300 526 739
Email: info@lanrex.com.au
Address:
Level 2
13-15 Lyonpark Road
North Ryde NSW 2113
Australia