PhishNet

The Role of Human Error in Cybersecurity Breaches

In this ebook, we review the current state of cybersecurity threats to Australian businesses and discuss the critical role human error plays in cybersecurity breaches.

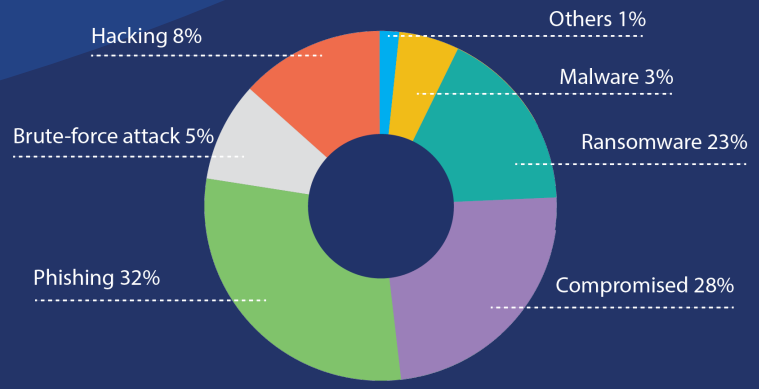
Australian Cybersecurity Breaches at a Glance – Market Overview

According to the Verizon 2022 Data Breach Investigation Report, 82% of data breaches involved a “human element,” including social attacks, user errors, and overall misuse.

> “82% of data breaches involved a human element”

Figures from the Office of the Australian Information Commissioner (OAIC) align with those numbers, with health services and financial companies leading the way in terms of industries with the highest reports of incidents.

The OAIC reported that in the last six months of 2021, 37% of data breaches occurred from “cybersecurity incidents.” The most common sources of cyber incidents included:



While “human error” can include simple and innocent mistakes (such as sending credentials to the wrong person), human error can also act as a gateway for some of the cyber incidents mentioned above.

A Closer Look at the Prevalence of Human Errors

Did you know what the most common password was in 2021?

123456

What about the second most common password?

password, not even with a capital “P.”

These findings from NordPass’s annual study of the top 200 most commonly used passwords reveal that there is a severe lack of fundamental password safety training for the average person.

The Top 3 Common Human Errors Leading to Data Breaches

The first step towards addressing the issue of human error is to be aware of the types of behavior leading to security incidents. The three most common are listed below:

1. Misdelivered Emails

Misdirecting an email with sensitive information is probably the most embarrassing type of data because human error is entirely at fault. According to Verizon's 2021 DBIR report, it is the most common type of error to cause a breach.

2. Simple Passwords

61% of data breaches are caused by compromised user credentials, not through theft, but password cracking methods. Most employees choose passwords as simple as "admin1234" or even just "password."

A password containing a four-letter word followed by a four-digit number could be cracked with brute-force methods in under 1 minute.

3. Password Recycle

Another prevalent password-related error is password reuse. The growing number of data breaches means that most user accounts have already been compromised, and stolen data is usually shared amongst cybercriminals on the dark web. So even a highly complex can easily comprise if it was involved in a previous data breach.

LastPass' 2021 Psychology of Passwords Report estimated that 71% of Australians mostly use the same password variation.

Top Attacks Related to Human Errors

Cybercriminals are experts in finding and exploiting human errors in order to gain sensitive company information. The following are some of the most common human-related attacks that can result in devastating financial losses and reputational damage for the company.

1. Phishing Attempts

Phishing is the most common kind of employee-related crime. With phishing, a person or group are typically contacted via email, phone, or text message. While the context of the conversation differs, the goal is the same: to gain sensitive information such as login credentials, payment/banking details, passwords, and other private data.

This information is used to infiltrate key accounts, resulting in identity theft, financial loss, ransom, and exploitation.

Other common outcomes of phishing include:

Impersonation

Armed with your email credentials, cybercriminals can use your information to impersonate you. When this happens, attackers now have access to your email contacts, which to them is a whole new list of potential victims. Under these circumstances, hackers will send out email blasts, impersonating the victim, and luring information out of others.

Payment Schemes

Sometimes, the point of a phishing attack can simply be to lure victims into payment scams, such as through gift cards, social security, or loan/insurance schemes. These scams can vary in method and monetary value. The end goal, however, is to trick a victim into making payments to the hackers that become impossible to trace.

Skeleton Key

If a hacker gains access to one set of credentials, it can become a domino effect of exploitation. In these cases, hackers may seek to obtain email log-in information as a gateway to more sensitive credentials.

Malware

One of the most common and widely-known effects of cyber attacks is to download malware or ransomware on a victim's device. Malicious files are designed to achieve a variety of destructive outcomes. Some cybercriminals run malware to steal sensitive data for other harvesting purposes. Another method is to freeze or hijack a given network or system, effectively shutting down a company's operations until they can pay up and meet the demands of the cybercriminal.

Selling Data

Data changes hands rapidly on places like the dark web. Sometimes, a cybercriminal might steal your sensitive data just to sell it to someone else. Unfortunately, there is no way of knowing the end goal of this process.

2. Branded Emails

As people become increasingly aware of obvious phishing attempts (such as “too good to be true” offers), cybercriminals are inventing more sophisticated methods for luring people into their scams.

One way hackers are trapping people is by impersonating popular brands that people interact with regularly, either professionally or personally.

Some of the most popular brands who are often impersonated are:

- PayPal
- Google
- Adobe
- Facebook

Methods and Tactics

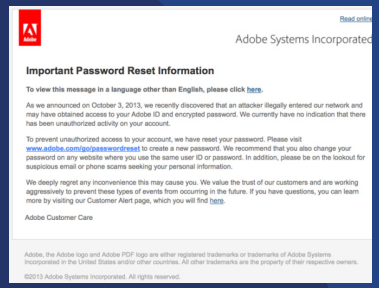
Spam filters do their best to combat malicious links found in phishing attempts. Even common training teaches employees to “hover” over links to preview the destination link. However, hackers are combatting this by using a variation or extension of a domain such as google.com or paypal.com

By using variations of these domains (such as .live that is usually associated with Microsoft), hackers can successfully navigate spam filters and find their way into employee inboxes. Even if an employee takes the extra step to hover, they will likely trust a link that seems so recognisable.

How to Spot a Phishing Attempt

There’s a reason why companies like Google, Adobe, and Microsoft are so often impersonated. These sites allow for user generated content that still contains the brands identifying URL. For example, Adobe and Google drive let users (such as hackers) host their links or attachments to their site. Therefore, even hovering will still see drive. google or adobe.com in some part of the domain.

We recommend to always pay attention to context. Read the whole email - even if it’s from a brand whose emails you receive every day. In most circumstances, if an employee does click a malicious link, the malware will not begin immediately. The attack typically happens after an employee enters their credentials or downloads material. By reading the context of the email and understanding the point of the link from the get go, employees will be better prepared to spot malicious attempts even when they’re disguised under trusted brands.


Adobe Systems Incorporated

Important Password Reset Information

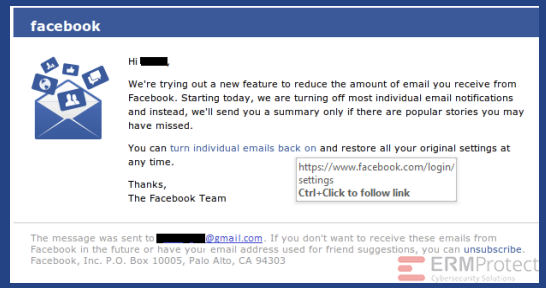
To view this message in a language other than English, please click here.

As we announced on October 3, 2013, we recently discovered that an attacker illegally entered our network and may have obtained access to your Adobe ID and encrypted password. We currently have no indication that there has been unauthorized activity on your account.

To prevent unauthorized access to your account, we have reset your password. Please visit www.adobe.com/go/passwordreset to create a new password. We recommend that you also change your password on any website where you use the same user ID or password. In addition, please be on the lookout for suspicious email or phone scams seeking your personal information.

We deeply regret any inconvenience this may cause you. We value the trust of our customers and are working aggressively to prevent these types of events from occurring in the future. If you have questions, you can learn more by visiting our Customer Alert page, which you will find here.

Adobe Customer Care


facebook

Hi [redacted],

We're trying out a new feature to reduce the amount of email you receive from Facebook. Starting today, we are turning off most individual email notifications and instead, we'll send you a summary only if there are popular stories you may have missed.

You can turn individual emails back on and restore all your original settings at any time.

https://www.facebook.com/login/settings
Ctrl+Click to follow link

Thanks,
The Facebook Team

The message was sent to [redacted]@gmail.com. If you don't want to receive these emails from Facebook in the future or have your email address used for friend suggestions, you can unsubscribe.
Facebook, Inc. P.O. Box 10005, Palo Alto, CA 94303

3. PRETEXTING

Pretexting is a clever form of social engineering in which a cyber criminal attempts to lure information or system access out of a target through a story, or pretext. In most cases, the pretext may come from a seemingly credible source, a friend or coworker, or authority figure to lower the defences of the target. The goal of this pretext is to gain trust and eventually, valuable information. Typically, their story can be considered highly credible, which is why it makes pretexting a difficult tactic to spot.

The following are the most typical scenarios in which pretexting is used.

Scenario 1: Asking for Help

It is normal to receive requests from family, friends, and coworkers on a regular basis. That's why asking for help is often a plausible scenario for pretext phishing attempts.

In this scenario, the cyber criminal may use spoof contact information to appear as a colleague or authority figure, which can quickly lower the guard of the target.

Perhaps an email appears from your CEO asking for help doing a task. This seemingly innocent gesture lures the employee into the trap. If he or she agrees, the attacker may then go on to define the "task" as providing access or information.

Asking for help can come in more direct forms. Some attackers impersonate people in Payroll or HR, asking for help or clarification on payment information or bank account details.

Scenario 2: Requesting Additional Contact Information

Sensitive information, such as payment details and account information, usually needs to be conveyed via phone. In this scenario, cyber criminals attempt to open a pretext to get a target on the phone to convey personal information.

For example, an employee may receive an email (again from a CEO, coworker, or other authority figure) that goes something like this:

Dear x,

Are you available? Can you give me your work or personal number, there's a task I want to discuss with you and it would be easier to talk over the phone.

This seems like a perfectly reasonable request. However, once on the phone, the employee could be walking into a trap, or even a deepfake, where the hacker or even an AI-software is impersonating the person with whom they think they're talking.

Scenario 3: Requests Funds for a Surprise or Event

One of the most unfortunate scenarios is when cyber criminals hide behind the pretext of a good deed or promising social event. Perhaps the hacker tells the victim they are planning a surprise or event for colleagues or business partners. Then, they ask for your "help" or "contribution."

This pretext achieves two purposes. One, it lowers the victim's guard as he or she believes he or she is genuinely doing something good for their team or company. Two, bringing a "surprise" into the mix will naturally encourage the victim to keep quiet about the activity, thereby giving the hacker more time to pull off the phishing attempt.

What Happens if You Respond to a Pretext Phishing Attempt?

If successful in the first step, a hacker likely knows that time is limited, and therefore accelerates the pace of conversation or request. If you do buy into a seemingly reasonable pretext, pay attention to the series of events that happen after, with particular attention to the following considerations:

Pace: is the conversation speeding up past what feels natural for the person or circumstance? Is the correspondent rushing you or putting the pressure on?

Money/Stakes: your alarm bells should go off if there is a significant amount of money involved. When in doubt, take a pause from the conversation and analyze the circumstances.

Sensitive Information: you should NEVER provide sensitive information via email. If you are asked to provide passwords, login information, bank account details, or other sensitive information, it's a good sign to stop and re-analyse the situation.

While there are steps to deescalate the phishing attempt, we believe that prevention is key to stopping phishing attempts. Creating a cyber-aware culture will help employees identify phishing attempts even as hackers use more sophisticated methods.

PhishNet delivers highly effective, engaging, and affordable cybersecurity awareness training to help businesses mitigate the risks of human error data breaches.

Talk to PhishNet today to learn more or check out our free Risk Assessment.

PhishNet

Contact Us

https://phishnet.global

1300 165 046

info@phishnet.global