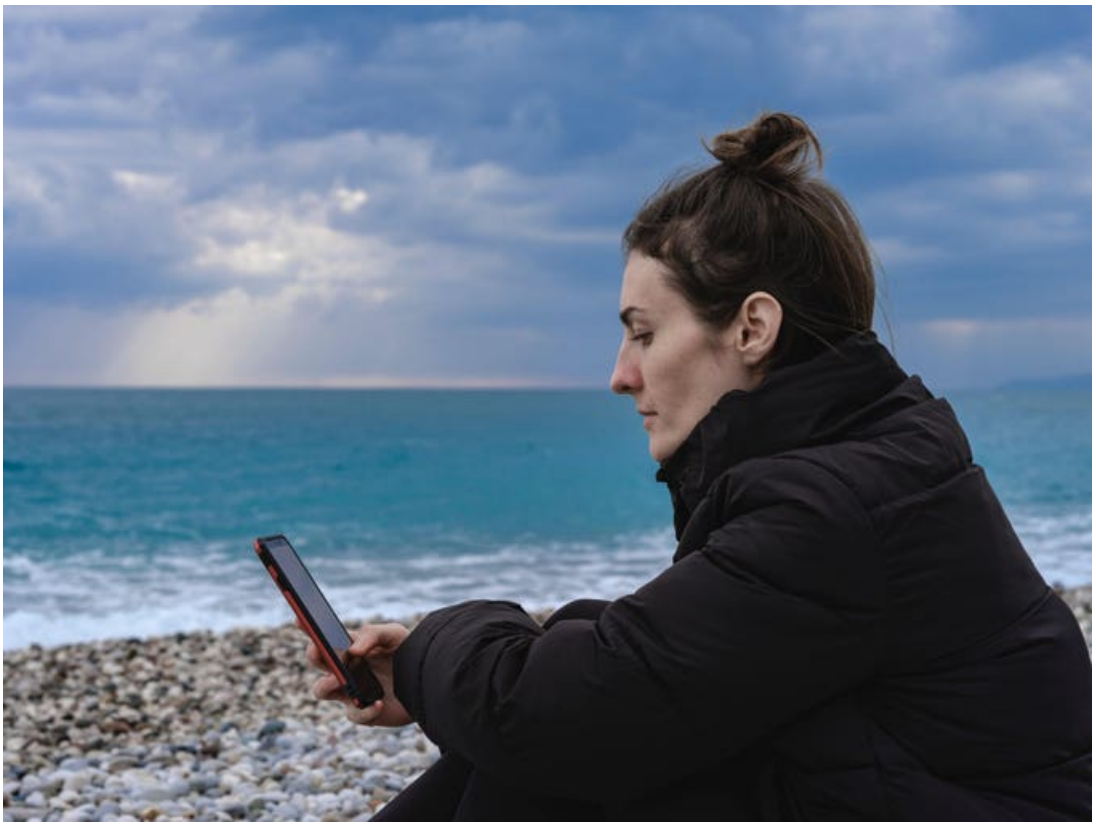
News article

Jul 2024

Data Breaches: How To Protect Yourself From Scams: Forbes Advisor

Scams and hacks seem to be part of life these days.

Craig Archdeacon
Head of Cyber Assurance
Email craig.archdeacon@waterstons.com



After all, we all need to hand over personal information to open a bank account, receive an insurance pay out or get a license to drive a car.

But in the wake of the Optus and Medibank Private breaches the private data of millions of Australians ended up in the hands of hackers and even ended up published online. Right now, it's hard to feel safe, and Australians are contemplating how to better protect their personal data.

Sure, we might not have control over these massive corporate data breaches, but there are steps we can take to protect ourselves from identity theft, phishing and fraud.

How Big Is the Problem?

Scams cost hard working Australians hundreds of millions of dollars each year. They also cause serious emotional harm to victims and their families.

In 2021, Australians made more than 286,600 reports to Scamwatch and reported losses of a staggering $324 million. But as increasingly desperate Australians battle against the rising cost of living and scams become more sophisticated, that figure has grown this year, with reported losses of more than $381 million by the end of August alone.

But Scamwatch reveals that around one-third of people who are scammed never tell anyone, so the true numbers are probably much higher.

Common Scams and Frauds

There has been a surge in scam reports mentioning coronavirus. Scammers are hoping you have let your guard down and are often phishing for personal information, banking or superannuation details.

Scammers may also pretend to have a connection to you, so it's important that you check that a recent text message that sounds odd has actually been sent by who they say it is.

The Optus hack exposed customers' names; date of birth; phone number; email addresses; residential address; and identity documents, such as driver's license, Medicare numbers and passport details.

The hack was so substantial that the government stepped in to minimise the impact for customers, opening an investigation to understand how the breach occurred.

A few weeks later came the Medibank Private breach, whereby hackers accessed the names and addresses, date of birth, Medicare numbers, policy numbers, phone numbers and some claims data.

Scamwatch warns that other common scams include scam text messages about missed calls, voicemails, deliveries and photo uploads. The message asks the receiver to tap on a link to download or access something, which will download malware to your device. The government organisation has been encouraging people to learn ways to identify scams and take the time to check whether an offer or contact is genuine before acting on it.

As scammers develop new ways to catch people out, increasing our vigilance in this way can alert us to the fact that something is a scam.

What To Do if You're Hacked

If you've had your data compromised in some way, then you need to tell all of your banks or credit providers and ask about how you can protect your money.

This could include setting transaction limits on your accounts, enabling multi-factor authentication for online and telephone banking and adding extra security questions,

The company that has had the data breached need to alert authorities, which will make the information public via the media. They also need to let you know what sort of information of yours has been accessed, such as your address, or your driver's license details. Either way, tell your bank and get a new license as soon as it can be arranged.

But prevention is better than cure, so here are 6 steps you can take to minimise the potential that you will be hit by a breach.

1. A Cyber Spring Clean

Set aside some time to go through online accounts and resetting passwords, recommends Ryan OKell, who is the senior cyber security engineer at computer support company, Waterstons.

You can do this by searching your mailbox for verification email services when you first create an account with a company to ensure you actually have access to your account, he says.

"Along the way, keep a list of the web services you've signed up to and catalogue these accounts into a password manager. While it sounds daunting, you'd be surprised how much you can achieve in an hour," he says.

2. Set Up Multi-Factor Authentication (MFA)

If someone has your password but they don't have your mobile phone or authenticator code, they aren't getting in. That being said, some forms of MFA have become obsolete, according to OKell.

"Most organisations wouldn't consider codes received by SMS secure anymore since it isn't hugely complicated to have your mobile number temporarily ported elsewhere.

"The tap notifications aren't great either since there has been a recent uptick in MFA Fatigue attacks where an adversary will push dozens of login attempts so your phone throws dozens of notifications (hoping you'll give in and just hit accept on one of them)," OKell says.

If you're using MFA, look for an authenticator app that generates changing codes, he adds.

3. Set Up a Special Email Address

If you're using Gmail, OKell says that you can technically put whatever you like on your email address when signing up to new services: so long as you put it after a plus sign, then the emails will still come to you.

For example, when opening a new account on dodgywebsite.com, instead of providing your email as john.smith@gmail.com. you could instead enter john.smith+dodgywebsite@gmail.com.

"I'll still receive any emails they send, but this way, if I receive any strange emails or marketing sent to john.smith+dodgywebsite@gmail.com from a third party, then you know where they got my information from," OKell says.

4. Check if you Have Been Hacked

Breaches are far from a new occurrence and in all likelihood, most people are already in a breach and their credentials or information is already out there to some extent, OKell says.

An excellent way to find out if you're in a breach is to pop your E-mail address into haveibeenpwned.com.

This web service is run by an Australian man who collects breach information specifically so people and organisations can see if they are affected for free.

The site will even notify you (again, for free) if your email pops up in a new breach.

5. Get a Unique Password

The majority of people like to just use a combination of "ChildsNameChangingnumberSymbol" but if you're in a couple of breaches, and need to change your email password, it's not a huge jump in logic to see Michael20! and Michael21! and want to give Michael22! a try.

OKell says: "The best and easiest way to deal with this is using a password manager. There are plenty of great ones out there that will generate complicated passwords for you when you're signing up for things and they will even let you know if a password you're using is already in a breach somewhere."

6. Monitor your Credit Rating

Put some monitoring on your credit rating. Sudden changes can indicate financial anomalies related to you, such as new loans or unpaid debts, OKell says.

The financial industry watches payment histories closely and this can usually be one of the first indicators that someone has used your identity to take out a loan or do something nefarious, he says.

"There are a few services out there that offer this for free, but you might want to do a little due diligence on them first to make sure they are legitimate. That being said, some of the other likely indicators can be mail or SMS messages you're expecting from your bank not arriving, so look out for that as a potential sign."

If you are ever suspicious however, never respond to these messages: always find the organisation's contact details yourself on their website.

Thanks for partnering with us on this article, Protect Yourself From Scammers – Forbes Advisor Australia