Checklist: What to do if you think you've been hacked

Cyberattacks are a growing and expensive trend that threatens both individuals and businesses, with the global cost of cybercrime expected to top $US6 trillion by 2021. And for Australians, our risk of cyberattacks is increasing year-on-year.

So what happens if you think you've been hacked? Read on for a step-by-step checklist to securing your accounts.

What are the different types of hacks?

There are far too many types of hacks to list here, which should give you an indication of how prevalent they are and how easy it is to get swindled by them!

Some of the most common hacks that target everyday people include phishing, malware and ransomware, identity theft, remote-access scams, and cookie theft.

How do I know if I've been hacked?

Unfortunately, there are many different ways you can be cyberattacked, but here are a few different signs that you've probably been hacked:

- Your internet searches are redirected to unfamiliar webpages.
- You get spammed with pop-ups frequently—even with an ad blocker.
- You receive a specific ransomware message asking for money.
- Your passwords aren't working.
- Software has been installed on your system without your consent.
- You see lots of fake antivirus messages and ads.

- You're missing money from your bank account.
- Personal or confidential business data about you has been leaked.

So, what next? Here's what you need to do if you think you've been hacked—check them off as you go!

Step 1: Reset all your passwords

Immediately change all your passwords on any accounts you think might have been affected. If you use the same password across several accounts, make sure they're unique from now on.

Regularly changing your passwords is also a good habit to get into. System permitting, make sure you use a mix of letters, numbers and characters, and use upper and lowercase to make them more secure. If you're worried about forgetting all your passwords, a helpful tool like a password manager can make life easier.

Step 2: Contact your bank or financial provider

Most of the time, hackers want either your data or your money—so if you think you've been hacked and your online banking credentials have been compromised, call your bank immediately. They'll be able to tell you if there have been any recent transactions and also put a hold on your account.

If money has been stolen, follow where it leads. There may be transactional information that includes items being shipped to an unfamiliar address, or some of your accounts may have been changed to one-click purchases. Lock them down and, if necessary, share that information with your bank and the police.

Step 3: Scan your computer system and remove any devious programs

Use your antivirus software to do a full sweep of your computer. It should flag any malicious activity and automatically remove software that shouldn't be there. However, it's worth doing your own search for programs that have been recently installed. After all, with nearly a billion malware programs out there, even the best antivirus software can miss things.

Step 4: Recover your accounts

If a hacker has already changed your passwords and you can no longer access your accounts, you'll need a way to recover them. The good news is that most services have comprehensive account-recovery options—you'll just need to answer some security personal questions like "What's your mother's maiden name?" or "What's the first street you lived on?" You would have given answers to these questions at the time your account was set up, so hopefully you remember the answers you gave!

Here's how to do it for your Facebook, Twitter, Apple and Google accounts. For any other service, simply do a search for "[service name] account recovery".

Step 5: Let friends and family know

You'd be surprised just how convincing some hackers can be when taking over your accounts, and in many cases, they'll use phishing tactics to pose as you while getting your friends and family to click on malicious links.

As soon as you think you've been hacked, let your friends and family know and tell them not to click on anything you might have sent them, from emails to instant messages and even SMS.

Step 6: If it's a serious hack, back up your data and reinstall your OS

In the worst cases, there may be too many backdoors into your system to fix yourself. And unless you want to pay a cyber professional to do a complete audit of your system, it may be in your best interests to just perform a 'hard reset'.

First, make sure you transfer any important data to an external hard drive or to the cloud before resetting your operating system (OS). Then it's time to do a complete system purge, wiping your hard drives clean and then reinstalling Windows, iOS, Linux or whichever OS you use.

There's a good chance that most of us will get hacked at least once in our lives, but that doesn't mean you can't mitigate the damage and better prepare yourself for the future. These steps will help you take back control and protect your computer system going forward.

You don't need to get hacked to think about other ways to protect yourself. Whether it's protecting your car, home and contents, pet, or even your own life, income and business, Choosi can help you compare various types of insurance. Start comparing now by clicking on any of the links below:


Life Insurance


Funeral Insurance


Pet Insurance


Business Insurance


Car Insurance


Home & Contents Insurance