What to do if your email account has been compromised

Intended purpose:

If you have completed our Checklist: Checks to determine if your email has been compromised or are certain it has, use this How To Guide to minimise the damage and take back control of your email account (if possible). Time is of the essence to minimise the damage a bad actor can do.

Part One: Focus on regaining control and minimising the damage

1. It's possible bad actors used malware on your device to gain access to your account. Run an antivirus scan ensuring it checks for spyware and keyloggers in particular. Check your operating system, programs and apps are up to date on all devices you accessed your email account from. **It is important to do this early before you start logging into other accounts or changing passwords. The continued presence of malware can undermine the effectiveness of the next steps, you must be sure you're working with a clean and secure device.**

2. Instigate the email provider's password recovery process and change your password straight away. If this doesn't work the bad actor has likely rerouted the recovery information so contact customer service by phone immediately. See additional resources below for the contact information for common email providers.

3. Inform your close friends, family and business contacts by phone or another email account as they may be subjected to phishing emails from your compromised email account. We've written a message to

save you time simply copy and paste it from the additional resources section below. Ask for help here as it can be time consuming – your spouse or friend can make phone calls and send emails from their account while you continue through these steps.

4. Contact your bank and put a temporary freeze on any account or credit card with high available funds / credit or which you use to make online purchases. Be wary you may receive phone calls *claiming* to be your bank or other account asking for more identifying information. During this period, it's worth heightening your suspicions for incoming calls – reputable banks and companies won't ask for identifying or sensitive information over the phone.

5. Your email is commonly used to secure other online accounts (shopping sites, social media etc) so the bad actor has access to the 'forgot my password' function. Make sure you can log in to accounts that use the compromised email address as the username and change the email address to a secondary one. Change the password of every other online account which shares the same password as your compromised email account. This will be quite time consuming.

If you cannot regain access to your account within a few hours, it's worth considering cutting your loses and setting up a new account. Consider those we've listed in our recommendation of email providers and revisit point 2 of this checklist once you've set a new one up. Inform your contacts of your new email address and tell them to block your compromised email address.

Part two: After you have regained control of your email account – secure it

1. Once you regain access to your account consider our articles on setting strong passwords or a Password Manager

2. Enable 2FA.

3. Tighten your spam filter settings and ensure you have ticked the box to use SSL in your email settings.

4. Change your security questions – give false answers to the questions. The most common answers to 'what is your favourite food?' are 'pizza' and 'chocolate' so make yours 'calculator' or something just as unrelated.

5. Consider using a VPN from now on to encrypt your online traffic and protect your private information.

6. Consider upgrading your cybersecurity starting with your antivirus program - modern features include real time account monitoring and cloud-based threat updates. Usually operating a subscription model offering full support to you in the event of a compromise or threat at the highest payment tier.

7. Think about the sensitivity of information you send via email and consider changing email providers to a provider with stronger security options, using an encrypted file-sharing service with expiration time for access to the file, or protecting files themselves with passwords.

8. Read our article about phishing to be informed how those threats work as they are usually sent via email.

9. Report the hack to your email provider. This is more of a public service as, depending on how your account was compromised, the provider may be able to stop other users from falling prey to future threats.

Additional resources:

Below is information referred to within the How To Guide. We've used the three most prominently used email providers (rather than those we recommend) which, depending on the research, are used by between 70.1% to 85% of the US population. If you use a different email provider, the path is likely to be similar or you may need to search online for your specific provider's instructions.

Contact customer support information (Part 1, Step 2):

User Beware: Email providers don't really want to hear from you by phone and would prefer you went through their chat bots for support when you can't access email. They do a great job burying their phone numbers from being found online - the below phone numbers have been verified *at the time of posting* however they may be changed by the provider. It is very important to know that there are many fake phone numbers, basically phishing scams, posing as a customer support numbers. Be careful.

Provider	Path
Gmail	1-855-836-1987
Yahoo	800-305-7664
Outlook	800-892-5234 or https://www.microsoft.com/en-us/worldwide.aspx

Basic message to contacts (Part 1, Step 3):
As you are working to regain access to your account time is typically of the essence so to save you typing a message to everyone, we've put together the following basic message. Send via alternate email or text to your family, friends, and workplace (if relevant). Edit as desired.

Hi everyone,
It looks like my email has been hacked. Please don't open any emails that come from me or click any links that may appear on my social media or that you get from me through any other platform for the time being. I'm working through it now; I will contact you again when I have resolved this and secured my account or opened a new one. If you need to contact me, please call me on my mobile number if it's urgent. For non-urgent matters please don't contact me so I can focus on resolving this without interruption for the next few hours.

The last line is there as your closest friends and family will likely call you offering assistance. You may get multiple text messages back – don't feel obliged to reply to them, the last line should signal that you're busy right now.