Checks to determine if your email has been compromised

Intended purpose:

Use this checklist if you suspect your email account has been compromised, this checklist outlines the flags or indicators of a typical breach. If your email account has indeed been compromised action our How To Guide: What to do when your email account has been compromised

- [ ] Your password no longer works

- [ ] Check your sent items for strange emails which you don't recall sending. Bad actors won't always lock you out which means it's a good habit to run through this checklist periodically.

- [ ] If you receive an unexpected password reset email for other accounts it's a sign a bad actor is trying to find out which banks and services you use.

- [ ] Check there is no auto-forwarding or autoreplies set up for your inbox. Bad actors may use these to get copies of emails sent to you or to spam your contacts with phishing emails.

- [ ] Check your email address on the website https://haveibeenpwned.com/ which keeps records of millions of compromised email accounts. If yours appears take the steps outlined in part two of the above listed How To Guide.

- [ ] Many email services offer the ability to check login activity which highlights the IP address and location your account has been accessed. At the bottom we've listed some additional resources which includes where to find this information among the most

common email providers. This only relevant for an external compromise of email account specifically. If it's your device, such as your laptop, that has been compromised and the bad actor is accessing your email account from there, the IP address and location will still indicate your own. This tends to be more relevant to work laptops as an inside job from a bad actor in the IT department of the organisation or a past employee who used that device before you.

- [ ] Sudden or erratic changes to your device/s performance (usually slowed down) is a sign it has been infected with malware or ransomware. As you move through this checklist it's a great time to run an antivirus scan focused on malware, spyware and keyloggers. Also check your Operating System is up to date as well as the programs and apps on every device you access your email account from.

- [ ] Strange messages or posts appear on your social media, some bad actors will use those with a large following to promote a product they have an interest in

- [ ] If you use an email signature – check it doesn't contain any unfamiliar links

- [ ] Check that you are using SSL in your email settings, this is set on as default by most popular providers, however some have the ability to switch it off – it's worth checking you haven't done so accidently in the past. Search your email provider followed by 'SSL settings' to find the appropriate place to check.

If everything listed above checks out it's still worthwhile running your eyes over our How To Guide: What to do when your email account has been compromised to be aware of what you should do if it does happen in the future. Please know sophisticated bad actors *may* find ways to cover their tracks in relation to the above listed flags and indicators. To put your mind

at ease, we would recommend actioning part two of that How To Guide regarding securing your email account.

Additional resources:

From the checklist we've referred to checking settings, here is the path to find where these settings are. 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.

Please note the following setting paths are for the **desktop version** of your email provider (you log in by visiting their website). If you are using an **email client** (eg. you access your Yahoo account using the Apple Mail app), the path to the settings may differ.

Where to find login activity information:

Provider	Path
Gmail	Log into your Gmail account Scroll to the bottom of your inbox Click *Details*
Yahoo	Log into your Yahoo account Click your name in the upper right-hand corner Click *Account Info* Click *Recent Activity*
Outlook	Log into your Outlook account Click your name in the upper right-hand corner Click *Account Settings* You will be prompted for your password Click *Recent Activity*