FACT SHEET

FACT SHEET: Gmail account security

Gmail is a free online email service created by Google. It currently has over 1 billion users and can be used either on a browser or by downloading the application. The user can send, receive, and compose emails to others or themselves. There are also abilities to create and manage calendar dates and tasks.

Preventing Gmail account problems

- Ensure you are using the correct website before logging in.
- Choose a secure password you do not use for other online accounts.
- Set up a second email as a form of recovery in case your primary is compromised or lost.
- Use two factor authentication (2FA) to login and manage changes to your account.
- Log out of Gmail from shared devices.
- Be careful when using Gmail on public computers, such as at libraries.
- If you are prompted to log in to your account by clicking on articles, do not; they may use software that captures your information.
- Regularly check for software and operating system updates on your devices.
- Run a security check to remove any unknown devices from your account.
- Set up alerts to notify you when a new device attempts to log in to your account, or changes are being made to your account.
- Regularly check the forwarding rules of your gmail account to make sure no one is manipulating the emails that you see.
- Visit Google Account Help to find more information on account security.

Additional prevention for business Gmail accounts

- Ensure all business members use two factor authentication (2FA) to login, and choose a third-party authentication app.
- Be aware of who in your business has login details for your account, and remember to update passwords regularly, particularly when staff members leave.
- Never leave devices open or unlocked when unattended.

Setting up 2FA for Gmail

1. Log in to your account
2. Click on the settings tab at the top left of the screen, next to the Gmail logo
3. Click on the "Security" options button. This will take you to "Signing in to Google."
4. Select "2-Step Verification"
5. Click "Get started"
6. You will be required to sign in to your account again as part of the Gmail authentication process
7. Choose your preferred method for additional authentication
8. Follow the on-screen prompts to complete the process.

You can find out more from Google

FACT SHEET

Detecting problems with your Gmail account

You may have a problem with your Gmail account if you experience any of the following:

- ☐ You can no longer login to your account.
- ☐ You receive an alert that your Gmail account has been logged into from a device or location unknown to you.
- ☐ Emails have been sent from your account without your knowledge.
- ☐ You stop receiving emails.
- ☐ Your personal information attached to your account has changed. This may include your name or mobile phone number.
- ☐ Methods for authenticating your account have been removed or added.
- ☐ You receive an influx of emails from users you do not know.
- ☐ Your friends, family or other businesses report receiving strange emails from your account.
- ☐ You see new accounts linked to your Gmail account.
- ☐ A business claims you have not paid an invoice they sent to you, but you are sure that you have (this is an indication that someone may have accessed your account and altered the banking details on the legitimate invoice).
- ☐ Invoices you have sent to your customers have not been paid to you, but into another account (this is an indication that someone has accessed your email account to change your banking details on your legitimate invoices before forwarding them to your clients).

Signs that someone is impersonating your business using a similar email account:

- ☐ Friends, customers or other businesses report they have been receiving unusual emails from a business account with a similar name.
- ☐ Friends, customers or other businesses claim to have sent you emails that you did not receive. These may have instead been sent to a business using a very similar email address to yours.

Responding to Gmail account problems

- Follow the advice from Google Account Help on how to secure a hacked or compromised account.
- Consider the information that may have been contained in your Gmail and any other linked Google accounts. For example, what credentials may have been in your emails, including your inbox and sent items? These could be your own credentials, such as your driver licence or personal information contained in job or rental applications. Or they may be credentials or banking details of your family, friends or customers.
- Contact the issuers of any of these credentials, including Government agencies, banks, superannuation and insurance agencies.
- Review how your Gmail account may have been compromised so you can reduce the chance of it happening again, as well as consider what other types of accounts may be able to be accessed or opened using these details.

For additional support or information, contact IDCARE by submitting a Get Help Form or call 1800 595 150 (Aus) or 0800 121 068 (NZ).