Cayman Islands Government

Clicked, Paid or Shared Information? What to Do Next

If you have clicked a suspicious link, made a payment or shared personal or banking information, act promptly. Taking action can help reduce further harm.

What you should do next depends on what happened. Stop communicating with the suspicious person or account, and use official websites, apps or independently verified contact details to get help. Do not use links or contact details supplied in the suspicious message.

If you made a payment or shared banking information

If available, use your online or mobile banking platform to temporarily block or freeze your card to help prevent further unauthorised transactions.

Contact your financial institution immediately. Use the contact details in your banking app, on your card or on its official website. Explain what happened, including any payment you made or banking, card or security information you provided. Ask what steps are available to protect your account and whether the payment can be stopped or recovered. Recovery is not guaranteed.

Follow the financial institution's instructions and report suspected fraud to RCIPS. Do not send further money, even if someone claims another payment is needed to release funds or recover your losses.

If you shared a password, login information or verification code

Change the affected password immediately through the genuine website or app. If you use the same password on other accounts, change it on those accounts too.

Where available:

- Sign out of other sessions or devices.
- Check that your recovery email address and telephone number have not been changed.
- Enable multi-factor authentication, which adds another security check when you sign in.
- Review recent activity for changes or transactions you do not recognise.
- If you shared a one-time verification code, contact the account provider promptly through its official support channel. Changing a password alone may not resolve every risk.
- If you cannot access the account, use the provider's official account recovery process.

If someone is using your account to contact others, warn your contacts through another trusted channel.

If you shared other personal information

Make a note of what you provided, such as your address, date of birth or a copy of an identity document.

Contact the relevant organisation or document issuer using independently verified details and ask what protective steps are appropriate. Be alert to further messages or calls that use those details to appear convincing.

If you suspect identity misuse or another crime, report it to RCIPS.

If you clicked a suspicious link

Close the page and do not enter information, download files or follow further instructions.

Clicking a link does not automatically mean your account or device has been compromised. However, if you entered information or made a payment, follow the relevant steps above.

If you downloaded or opened a suspicious file, installed software or gave someone access to your device, seek technical help promptly. Run a full scan using your device's security software where available.

If a work account or device is involved, contact your organisation's IT or security team immediately.

If you shared false or misleading content

If you discover that information you shared was false or misleading, correct or remove your post and let the people you sent it to know. Share a reliable source explaining the correct information where available.

If you cannot verify the claim, say that clearly and stop sharing it as fact. Unverified information is not automatically false.

If you find suspected Government impersonation

If an account, website, message or advertisement claims to come from Government or uses a Government official's name or image, check independently before interacting.

Type gov.ky into your browser or contact the relevant Government entity using details published on its official website.

If you suspect impersonation or fraud, keep any evidence you already have and report it to RCIPS. You can also report the account, post or advertisement through the platform's reporting tools.

Keep relevant information

Where possible, retain:

- Messages, emails and correspondence.
- Screenshots of suspicious content.
- Website addresses, account names and contact details used.
- Dates and approximate times.
- Payment or transaction records.
- Details of the information you provided or actions you took.

Do not delay contacting your bank or securing an account while collecting evidence. Do not reopen suspicious links or continue communicating solely to gather more information.

Cayman Islands Government

Report suspected criminal activity

Report suspected scams, fraud or other criminal activity to RCIPS through an independently verified official contact route or your local police station. Call 9-1-1 in an emergency.

Visit GOV.KY/report-a-scam for guidance on reporting suspected scam posts and adverts.

For more guidance on checking information, visit GOV.KY/cybersafe.

Cyber Safe provides public information and guidance. It is not an incident-reporting or investigation service. Contact your financial institution, account provider, IT team or RCIPS as appropriate to what happened.