Someone in your organisation has reported a potential phishing attempt.
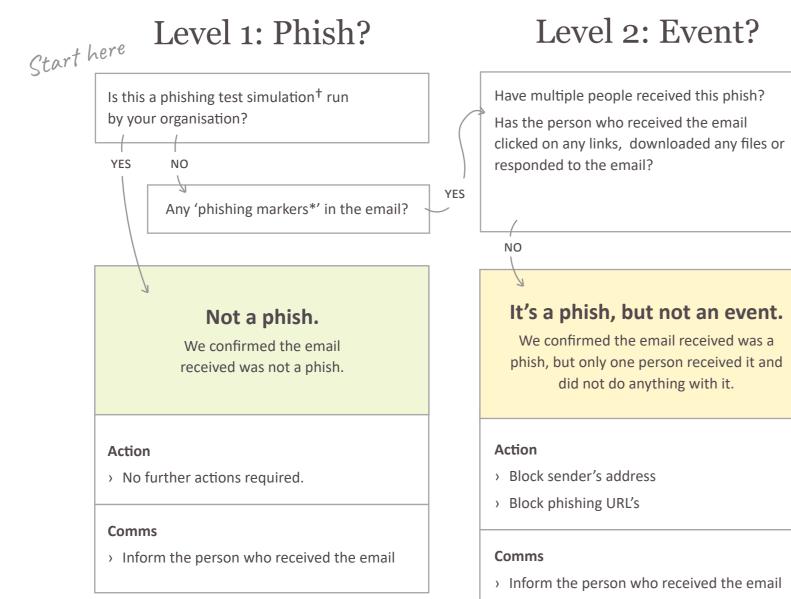
Look at the criticality levels in the flow diagram to determine required actions.

For key tips, resources, and guidance on what to do to prepare for a potential phishing attempt and what to do after an event, check out the corresponding Phishing Response Guidance document: https://www.tec.govt.nz/assets/Forms-templates-and-guides/CSTS/Controls/TEC-phishing-guidance.pdf

Tertiary Education Commission
Te Amorangi Mātauranga Matua

Start here

Level 1: Phish?

Is this a phishing test simulation† run by your organisation?

YES   NO

Any 'phishing markers*' in the email?

YES

Not a phish.
We confirmed the email received was not a phish.

Action
› No further actions required.

Comms
› Inform the person who received the email

*Phishing markers include warning signs like a suspicious domain name, grammar and spelling mistakes, and requests for sensitive information

†A phishing test simulation is used to test how susceptible an organisation is to phishing. The test allows an organisation to create a realistic phishing email attack which is sent to employees so they can learn to identify and report what a fraudulent email looks like.

Level 2: Event?

Have multiple people received this phish?

Has the person who received the email clicked on any links, downloaded any files or responded to the email?

YES

NO

It's a phish, but not an event.
We confirmed the email received was a phish, but only one person received it and did not do anything with it.

Action
› Block sender's address
› Block phishing URL's

Comms
› Inform the person who received the email

Level 3: Breach?

Have any staff interacted with the email? You will need to check email tracking or engagement metrics (if available).

Have any staff clicked on any links or provided sensitive information? You will need to ask all staff that have opened the suspicious email.

Have there been any outbound connections or traffic related to the suspicious links or domains? You will need to review proxy or firewall logs.

YES

NO

It's an event, but not a breach.
We confirmed multiple people received the phish but did not interact with it.

Action
› Block sender's address
› Block phishing URL's
› Purge email from all inboxes

Comms
› Inform the people who received the email
› Tell all staff to be vigilant (in case it is part of a wider attack)

Level 4: Compromised?

Has there been any suspicious activity on the user's account? You will need to review system logs for things that are out of the ordinary, such as logins from unusual locations, unknown IP addresses, or concurrent logins.

Have any new emails been sent from affected users and via email forwarding rules?

Has any malware been found on the user's device, based on a malware scan?

YES

NO

It's a breach, but we are not compromised.
We confirmed people interacted with the phish; meaning we have a breach, but the hacker has not done anything (yet).

Action
› Block sender's address
› Block phishing URL's
› Purge email from all inboxes
› Reset all affected credentials and passwords, and enable multi-factor authentication where possible
› Continue to monitor network traffic for unusual or unauthorised connections or data transfers

Comms
› Inform the people who received the email
› Inform the organisation's leadership team
› Inform affected individuals, customers and suppliers
› Inform the person responsible for IT security

Level 5: Compromised!

What kind of account has been compromised (e.g. user or admin)?
Where and what did the compromised account have access to?

YES

We are compromised.
We confirmed hackers used the breach to compromise our data or systems.

Action
› Block sender's address
› Block phishing URL's
› Purge email from all inboxes
› Reset all affected credentials and passwords, and enable multi-factor authentication where possible
› Continue to monitor network traffic for unusual or unauthorised connections or data transfers
› Scan all systems and devices for signs of malware, unauthorised access, or data exfiltration, using available security tools or antivirus software
› Review system logs, especially authentication logs, for suspicious activities or failed login attempts
› Isolate any compromised systems or devices from the network, to prevent further access or data exfiltration

Comms
› Inform the people who received the email
› Inform the organisation's leadership team
› Inform affected individuals, customers, suppliers
› Inform the person responsible for IT security
› Inform relevant authorities
› Use a crisis comms plan

Activate a 'War Room' and continue to investigate the extent of your situation.

Consider bringing in a cyber security partner for support.