FRAUD AWARENESS

How to tell if an email is fraudulent

There are a number of areas you can check to help determine if an email you've received is legitimate or not. Start by looking out for spelling mistakes and poor grammar. Another red flag is a threatening email that fakes a sense of urgency or makes threats to trick you into action.

Do you know who the email is from, and can you verify the sender?

It's important to remember that login credentials can be stolen and used by attackers to send malicious emails from known, trusted accounts.

ALWAYS check the 'from' email address, and be aware that this can be faked. Scammers will also copy brand logos and email formatting to make an email appear legitimate.

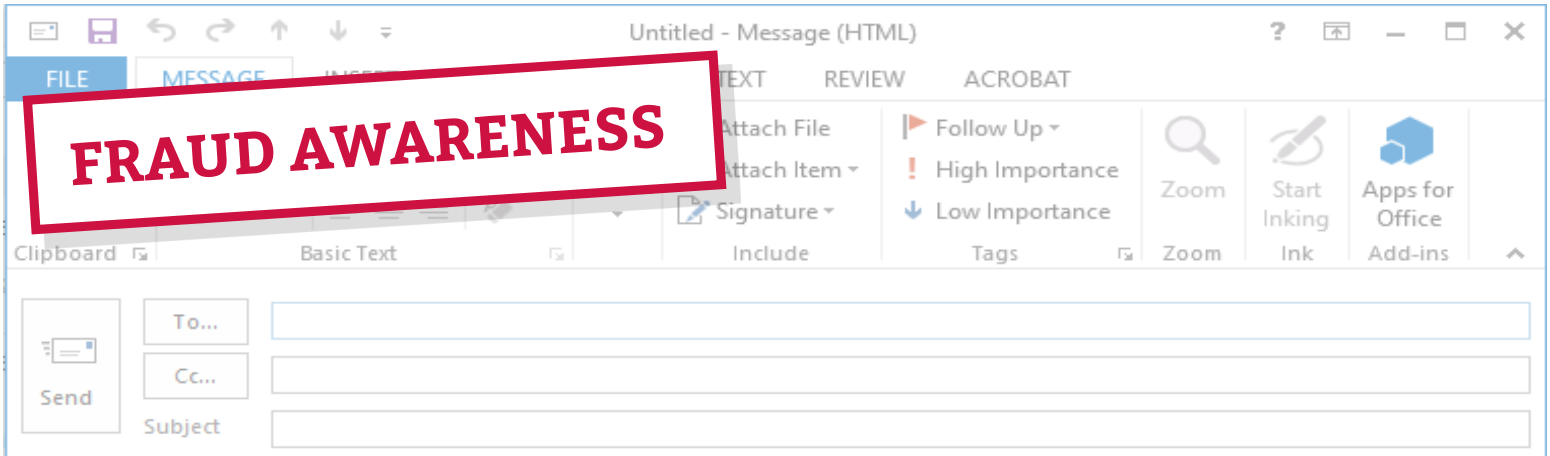
Does the email contain a link, attachment or ask for sensitive information?

Scammers may try to trick you into clicking links or opening attachments. Before you click any links or open attachments you must check if they are legitimate. You can do this by hovering over the link if you're on your computer, or 'tap and hold' on mobile devices to review the link before accessing it.

Remember that links can be disguised to appear as legitimate and often contain the imitated business name as part of the link. Before you click a link, download a file, respond with sensitive data or complete a wire transfer, you must be 100% confident the sender is who they say they are and that the request is legitimate.

Heritage Bank

People first.



FRAUD AWARENESS

What should you do if you think an email is fraudulent?

- Don't click on any links or attachments
- If the email is from an organisation you know, check with them directly before acting on the e-mail
- Call a known phone number (not from the email) and ask about the message
- Check for a trusted website by searching for it online or typing the URL into your browser.
- Report the email in an appropriate manner to the organisation which is the subject of the phishing scam, if applicable
- Block the sender and delete the email

Remember: While Heritage may send information or confirm receipt of items by email, we will never ask for you to disclose your bank account details or personal information over email.

Other Acts by Scammers

- Be wary of spam emails, chain letters and persons purporting to be representatives of Government Departments, financial institutions or other businesses.
- Do not give your name, bank account details (including internet banking login details and/or one time passwords sent in text messages from your bank), copies of your drivers licence, passport, birth certificate or any other personal details or documents to anyone other than for legitimate purposes.
- If someone contacts you asking for personal information, check carefully that they are legitimate.
- Be suspicious of any correspondence from overseas asking you to forward large sums of money or advising that you have won a prize.
- If someone blocks access to your computer or personal files, and then asks for a payment to remove that block, report the incident to the Police.
- Keep up to date with the types of scams in circulation, so you can identify them if needed

---

The following are official Australian Web sites with more information about fraud:

Australian Government "Scamwatch"
www.scamwatch.gov.au/

Australian Government's "Stay Smart Online" Web site and email Alert Service
www.staysmartonline.gov.au/

Heritage Bank
People first.