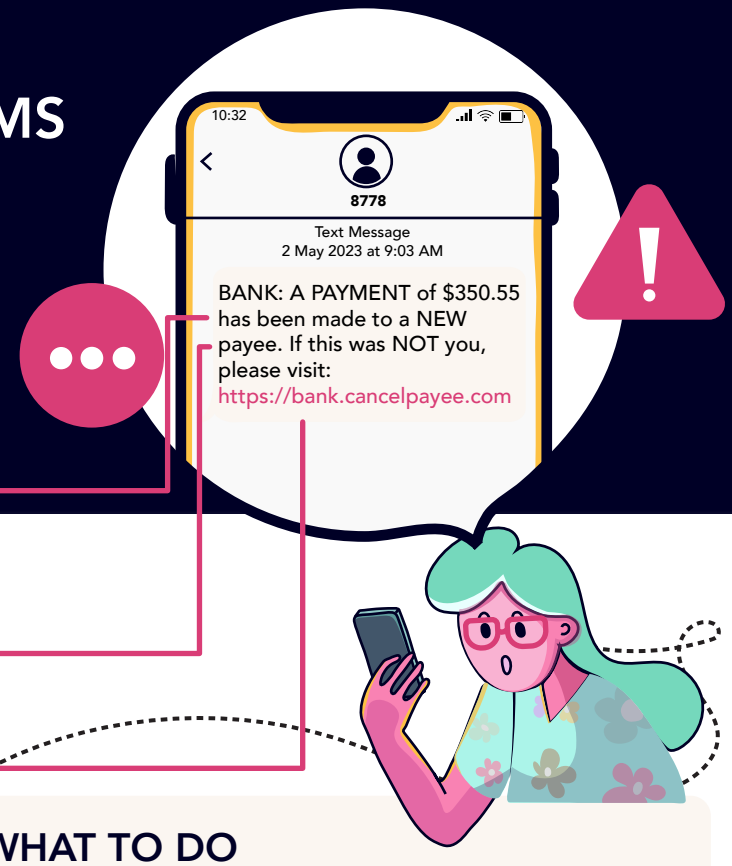
DON'T TEXT & REGRET:
HOW TO AVOID TEXT SCAMS

Text message scams (sometimes called "smishing scams") are ever-changing; however, there are some common themes.



LOOK OUT FOR

- A hook to try and convince you it is an authentic message. For example this could be a message that claims to be from a courier wanting to deliver a parcel or your bank asking you to authorise a payment.
- An urgent call to action. This includes saying your account details or other sensitive information have been exposed.
- A link for you to click. This will usually take you to a separate web page or portal where you will be asked to input personal or financial details, or download/update software on your phone.

WHAT TO DO

- Act with caution if you receive a text message that seems out of the ordinary or from an organisation that would not usually contact you in this way.
- Don't click on any links in the message or download or install any attachments.
- If the message claims to be from an organisation such as a bank or courier company, contact the organisation directly to confirm the communication. And don't use a contact number shown in the text.
- Your bank will not ask you to provide your password or login details over the phone or via text message.

WHERE TO REPORT TO

- If you've received a text scam or have received a suspicious text, please forward the text free-of-charge to 7726. This is a service offered by the Department of Internal Affairs (DIA).
- It will send an automated response asking for the number that sent you the scam text. After replying delete the scam text message and block the number associated with the sender.

Be wary of unexpected texts from people you don't know. If you take action and need help, contact CERT NZ
https://www.cert.govt.nz/individuals/report-an-issue/

certnz

sales@mindshift.kiwi | www.mindshift.kiwi
https://www.linkedin.com/company/mindshiftkiwi/

mindshift
helping people be cyber safe