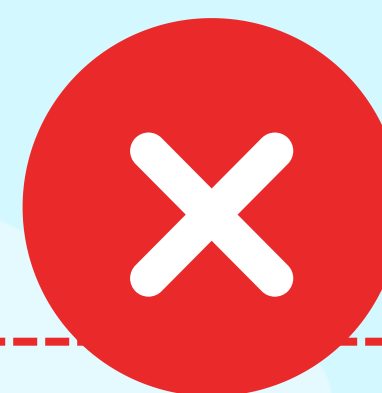# Do's & Don'ts
Phishing

✓

DO use separate email accounts for things like work and personal.

DO be careful about opening attachments, even from trusted senders

DO check for the sender's mail address before you provide personal information

DO install antivirus and update your browsers regularly

DO call the sender to confirm if the email is legitimate or not

✗

DON'T respond to phone calls asking for bank details. It might be vishing (voice phishing).

DON'T send passwords or any sensitive information over email.

Don't reply to, click on links/url or open attachments such as ZIP files and .exe files in emails from unknown sources

DON'T click on "verify your account" or "login" links in unknown email

DON'T SAVE usernames and passwords in browsers.