



SCAM

TOP TIPS TO PROTECT YOURSELF FROM PHISHING

Phishing emails and SMSs are one of the most common types of cyber-attacks.

Cyber criminals will also try to impersonate trusted contacts (like colleagues, Senior management, and vendors) to trick you into clicking on malicious links or opening attachments containing malware.

Verify First, Zero Trust



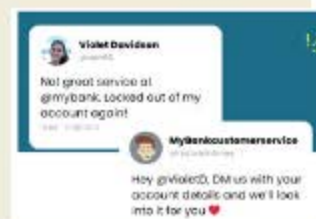
Always verify the identity of customer service accounts before interacting with them on social media.

Check the link to the profile on their official website. Ensure the name matches the official account.

Don't share sensitive info

Never share sensitive information like passwords, logins or credit card numbers over social media messaging.

In the example, it shows that the so called mybank rep is just impersonating the account to get Violet's details.



Inspect the activity



Check their profile page for indications that it is a genuine account; followers, activity, contact information.

Remain Sceptical



Maintain a healthy level of scepticism towards unsolicited messages, even if they appear to come from a known business

Direct contact with the organisation



If possible, always directly contact the company through their official website or customer service phone number.

It might not be convenient, but making that call is the more secure option.

Check URL and Links



Always check the URL of a link before clicking by 'hovering'; fraudulent links often have misspellings or extra characters. Don't trust shortened links'

Report Suspicious Activity



Report any suspicious activity to the social media platform and the impersonated company. The more people call out these impersonators, the less likely they are to do widespread damage.

OUR TEAM



Reach out if you require support or assistance with protecting yourself against phishing attacks.