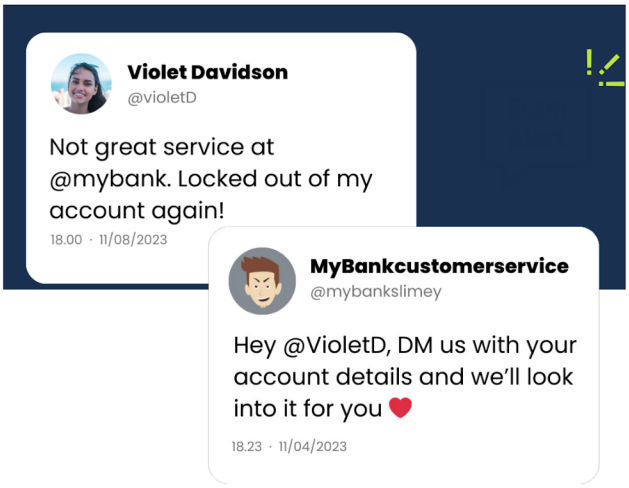
Phriendly Phishing

Top tips to protect yourself from angler phishing

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

Phriendly Phishing

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.

Educate yourself and share knowledge

Stay informed about the latest popular phishing scams to better protect yourself, your friends and your family. Help them learn about protecting themselves from cyber threats with our dedicated friends and family awareness page.

SCAN FOR S.C.A.M.