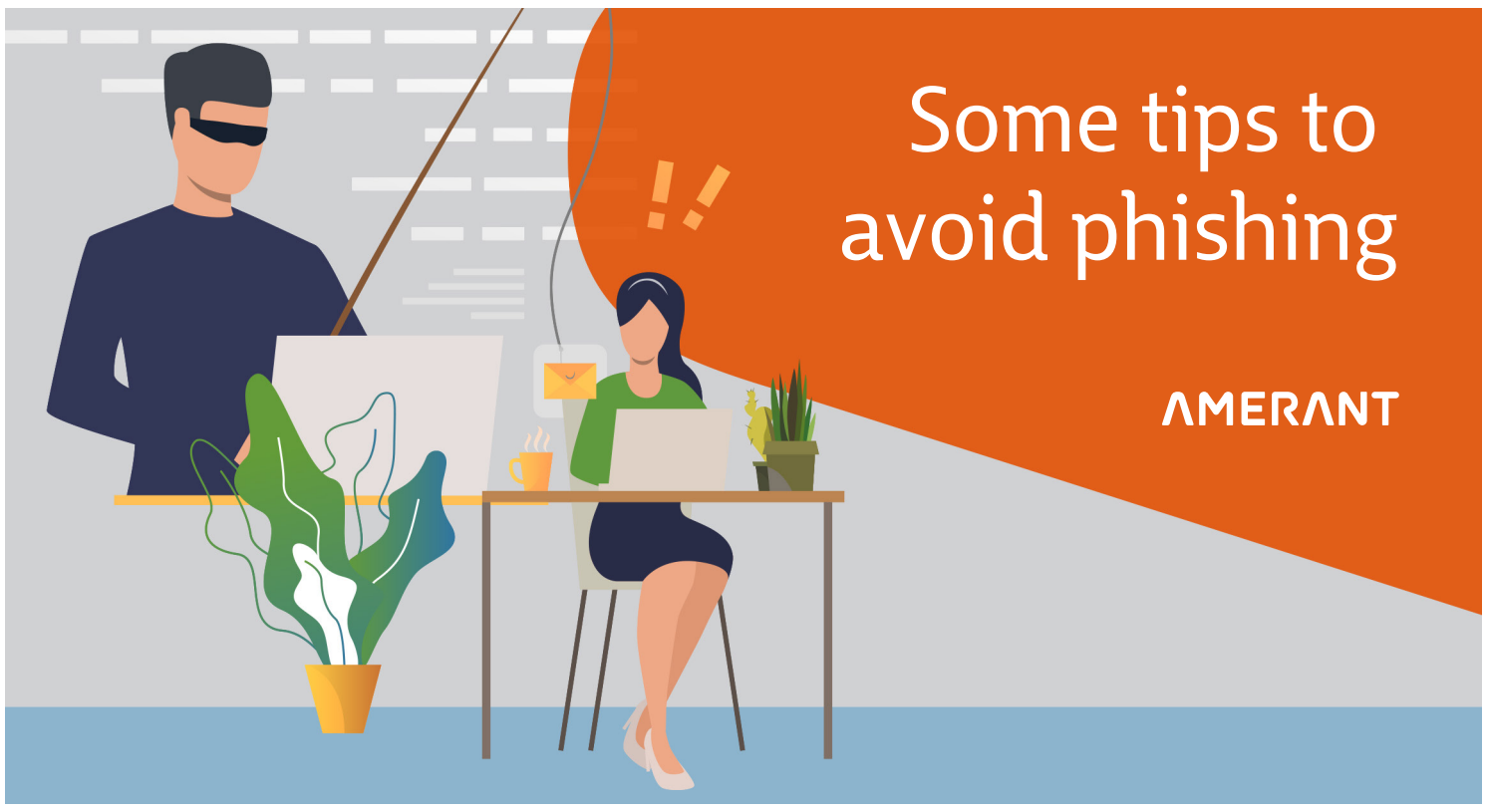

We strive to provide you with the tools and resources you need to keep your account information secure. We believe that the best defense against any fraud attempt is an educated you.

What is Phishing?

Emails, calls, or texts by fraudsters pretending to be a trusted person/business to get sensitive information like account details and passwords.

What to watch for:

- Unsolicited messages requesting to reply back with personal information
- Messages with links to unfamiliar or unusual domains
- Misspellings in a sender's email address and domain names
- Messages with a sense of urgency/necessity

Example of a phishing email:

From: **WESTPAC BANK** **<yeri@promo-msk.com>**
Subject: Account Verification Required

Dear customer,

Westpac has recently detected suspicious activity from your account. In order to ensure your account has not been compromised, **please verify your account details** through the following link:

Verify your information

Failure to do so within 48 hours will result in your account being locked.

Kind regards,
Westpack Bank Security Team

To learn more about phishing, please visit the Security Center on our website and click on "Phishing Attacks."

Helping you keep your personal information secure is our commitment. If an email or text message appears suspicious, do not click on any links, and contact us immediately at our Call Center.