PROTECT YOURSELF FROM PHISHING

A guide to recognizing and reporting phishing emails

Phishing emails resemble messages from your bank, social media sites, friends, and maybe even your boss. While they may look legitimate, they will often contain clues that demonstrate their true, malicious nature.

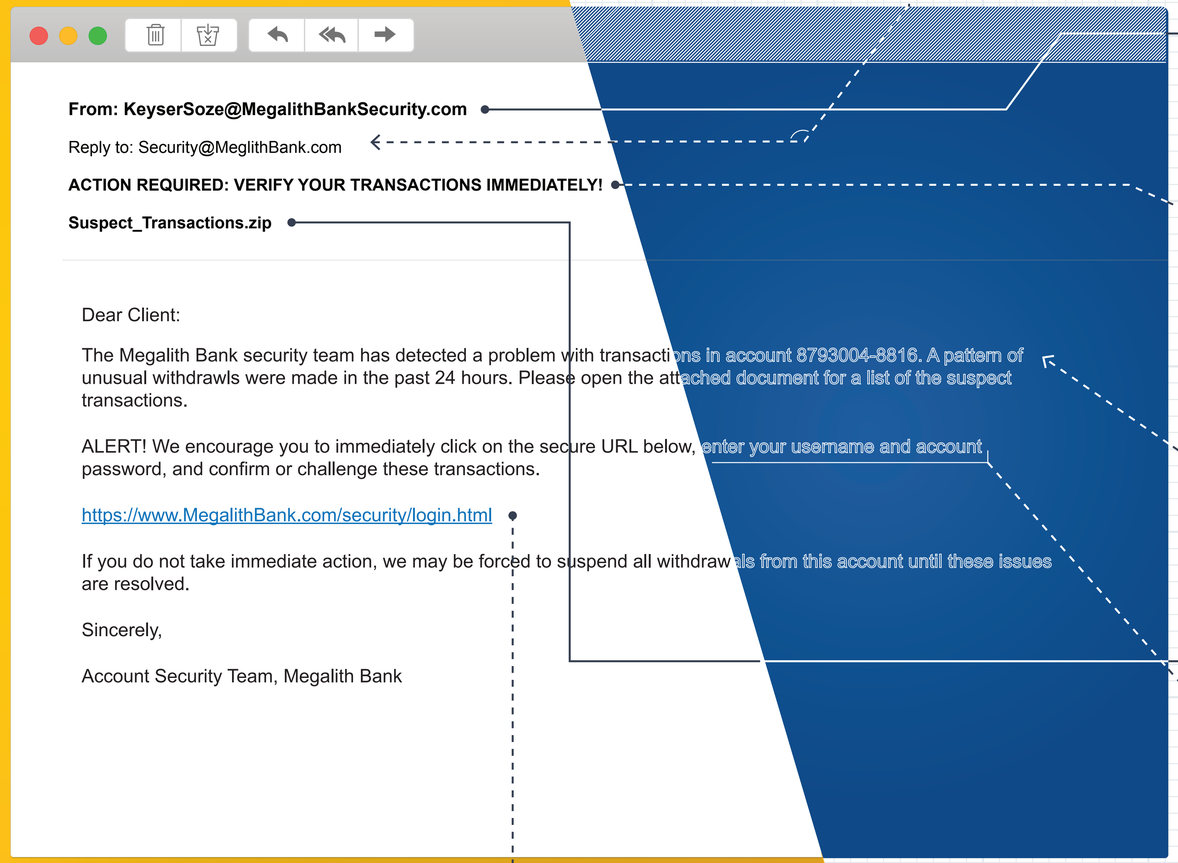
If you receive an email that shows any of these phishing indicators, or just doesn't feel "right," don't hesitate to report it to your IT and security staff. They will be grateful for the chance to stop fraud before it hurts your colleagues or company.

NEVER

- Click on a link, button, or icon in a suspicious email. It might take you to a website that appears to be legitimate but is malicious.
- Open an attachment unless you really know what it is. It may contain malware.
- "Confirm" or "Verify" passwords, account numbers, social security numbers, birth dates, or any other confidential information.

ALWAYS

- Ignore links in suspicious emails. Instead, open your browser, search for the organization (supposedly) sending the email, log in, and see if the information in the email is correct.
- Immediately report emails if they have even one of the clues listed above, or they just don't feel "right."



TOO MANY PHISH IN THE SEA?

Different Reply To and From addresses

WHO WANTS TO KNOW?

A contact name or email address you don't recognize, or a company you don't do business with

IS IT URGENT?

Deadlines, exclamation marks and text in all caps

DO THEY TYPE GOOD?

Awkward wording and spelling errors

DOWNLOAD FOR THE DOWN LOW?

Suspicious or unexpected attachments

WHAT'S YOUR SIGN?

Requests for personal or confidential information (e.g. passwords)

IS IT A TRAP?

A disguised link, or a link that does not match the URL displayed when you hover your mouse over it