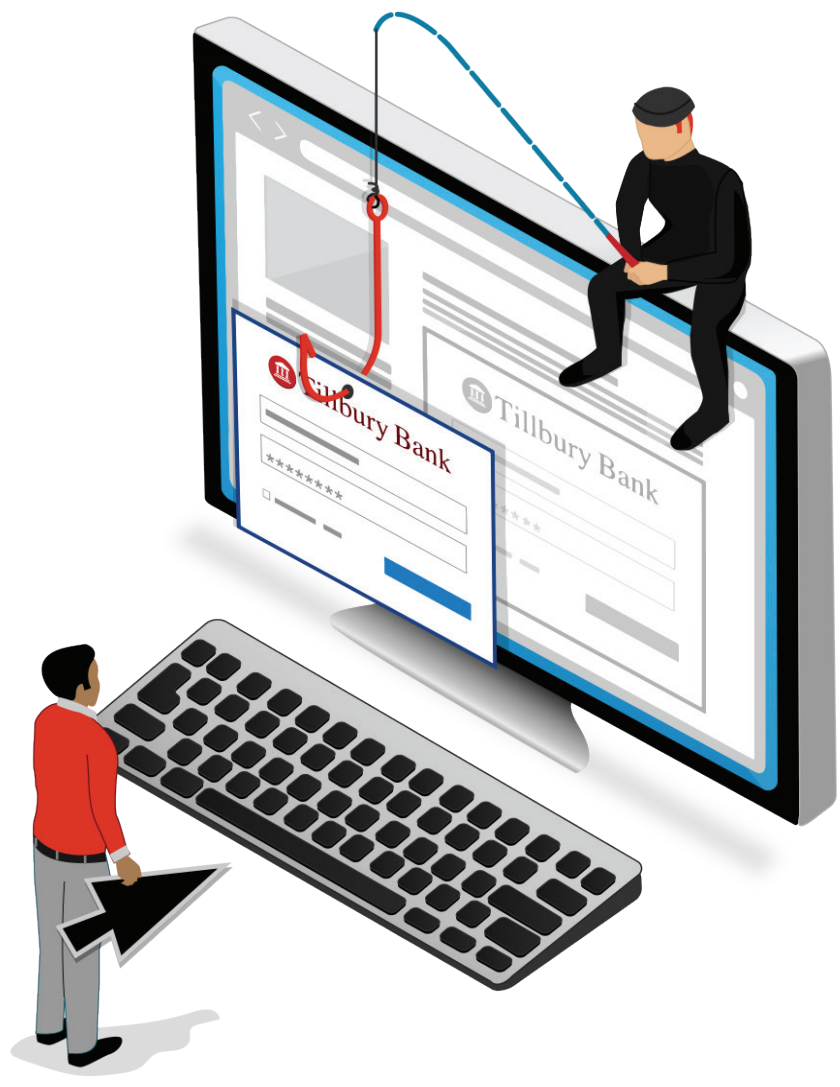
AttackSpotlight

Scammers Mimic Real Banking Emails

Scammers Mimic Real Banking Emails

Do you work with a bank as part of your job or to manage your personal finances? If so, be on alert. Scammers are crafting emails designed to look legitimate and evoke fear about a potential issue with your money or account. They want to make you act without thinking. Some of these phishing emails contain a link. Others contain an attachment with a link inside. Clicking on either link will send you to an authentic-looking (but fake) login page that steals your banking credentials. Once scammers have your credentials, they can pose as you and engage in malicious activities.



They might try to:

Request transactions

Transfer money out of your (or your company's) account

Use your account to trick others into approving transactions

Reuse your password to access other accounts

What do I look for?

There are multiple variations of this phish. Here is one example that use several tactics common for scammers. Here is one example that shows several common tactics used by scammers.

ACH

CH **Citibank Business**
Monday, March 11, 2019 at 11:36 AM (1)
Show Details

Dear, (2)
You scheduled a payment of $2,888.03 for your account ending in Regular Personal Checking 6521.

Click here to see transaction details (3)

You scheduled a payment of $2,888.03 for your account ending in Regular Personal Checking 6521.
Following is the detail:

Batch Name:
Batch Type: CCD
Payment Type: Receive a Payment
Offset Account: Personal Checking 5521
Effective Date: 03/11/2019

Total Credits (QTY)
$2,888.03 (1)

Total Debits (QTY)
$2,888.03 (4)

Credit Holds (Qty)
$0.00 (0)

Debit Holds (Qty)
$0.00 (0)

This is a secure message from Citibank Business

Questions about banking, mortgage, and investment Services? Click here
Small business customer service chat available 24 hours a day - 7 days a week

---

1 Examine the Sender

The sender's address includes the name 'Citi' to fool you.

But look closer: The email is really from securebankingservices.com, not CitiBank.

Don't be fooled by domains that include brand names or words like "secure".

2 Consider Content in Context

Is this expected? Be careful with unexpected transaction descriptions or requests, even when they look legitimate.

Scammers often research you or your organizationto get details to use in the lure.

3 Examine the Link

While the URL uses a secure connection (https://), this doesn't mean the site is legitimate.

This link is malicious and redirects you to the following site: securebankingservices.com

How do I protect myself?

If you receive an email that asks you to make a transaction, or scares you by making it look like a transaction has been requested:

- Be extra suspicious of emails asking you to wire or transfer money.
- Be wary of unusual emails that are sent from corporate executives, especially if the requests are urgent or secret.
- Confirm requests for money transfers and account information with the sender. Don't reply directly to the email. Use another means of communication.

proofpoint
Security Awareness Training