# Don't Open the Gates – Avoiding Banking Trojans

## What is a banking Trojan?

A banking Trojan is malicious software that can steal credentials, such as bank account usernames and passwords, from your computer. Banking Trojans are usually spread through phishing emails. Messages look like they came from a person or organization you trust, but in reality they're sent by cybercriminals to get you to click on a link or open an attachment that will install the malware.

## Why are you at risk?

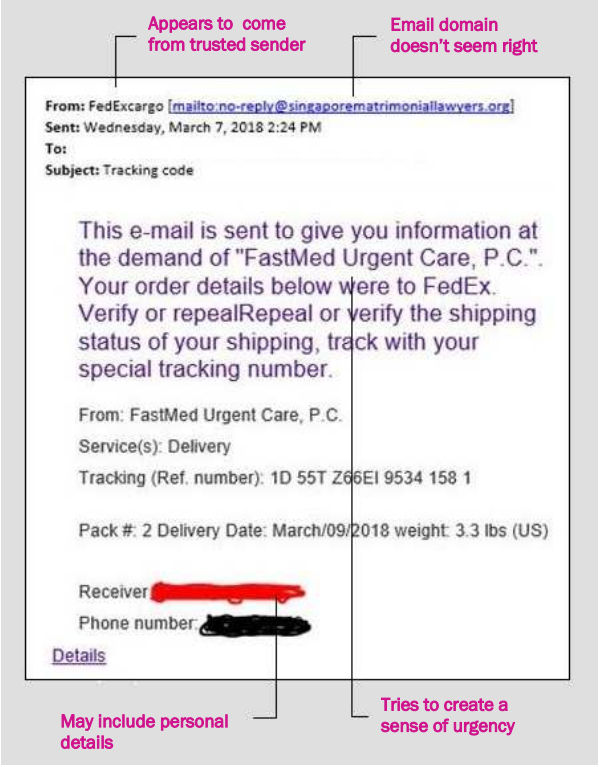
Banking Trojans give cybercriminals an easy way to steal money, and they're using massive spam campaigns to spread them. If one employee falls for a phishing attack, our entire system can potentially be accessed.

## How to spot a phishing email

Cybercriminals have gotten clever in how they design the emails they send out to make them look legitimate. But spear phishing emails often have the following characteristics:

- Made to look like they come from someone you'd trust, for instance, a bank, a tech company, a shipping company, or some other outside organization you would recognize
- Contain an attachment you're not expecting, such as an "invoice" that needs to be reviewed or paid
- Alert you to "account activity" and ask you to log in to review it.
- Try to create a sense of urgency about responding
- Ask you for your username and password, sometimes by replying to the email, but more often by clicking on a link that takes you to a site where you're asked to input the information. **IMPORTANT: Nobody at our organization will ever ask you for your password.**
- Contain email addresses that don't match between the header and the body, are misspelled (like *@gmaill.com*), or have unusual formats (*@company-othersite.com*)
- Have links or e-mail addresses that show a different destination if you hover over them

Here is an example of an actual phishing email:




## What you should do if you get a suspicious email

If you suspect that an email is a phishing email:

- Do not open any links or attachments in the email
- Notify our IT department
- **If you've already opened a link or attachment, disconnect your computer from the internet but do not turn it off, and then immediately call IT**