Ministry of Technology, Communication and Innovation

IT Security Unit

SPEAR PHISHING

"Know the impacts behind"

IT Security Awareness **October 2019**

What is Spear Phishing

Spear Phishing is the fraudulent practice of sending emails to specific and well-researched targets while pretending to be a trusted sender, in order to trick targeted individuals to reveal confidential information.

Spear Phishing, unlike normal phishing attacks, is highly targeted. The malicious email is sent to carefully selected persons.

Method Used

Prior to sending the email, the attacker will look for information on the intended victim electronically by:

- browsing information available online
- monitoring the person's online activity
- obtaining personal details of the person via other people

This information will then be used to create a fake email that may appear genuine to the user.

If you suspect you are victim of a Spear Phishing attack, report it to the relevant authorities.

How to spot a Spear Phishing Email

- Unsolicited email coming from **unknown** senders, often requesting for personal information (see illustration on next page).
- Email address containing deceptive domain names, such as go**gg**le.com (fake site) instead of g**oo**gle.com (genuine site), which can mislead the user.
- Contains **suspicious** email attachments (e.g. exe).
- The email is normally **not** signed.
- Spelling/grammatical **errors** in the email.

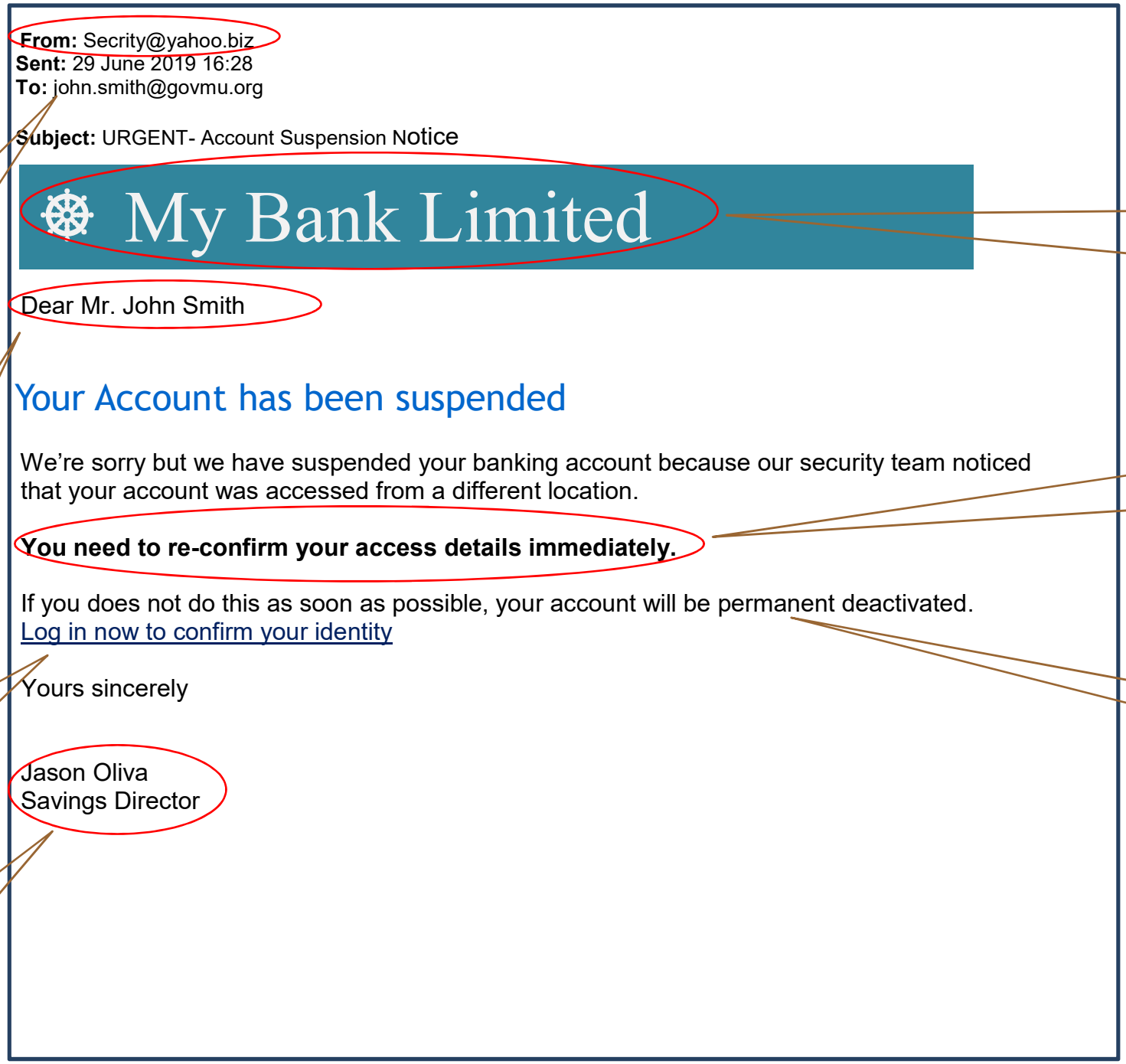
Possible consequences of Spear Phishing Attacks

- Compromise of sensitive information such as credit card details, passwords, which may cause financial losses.
- Using the victim's personal information - such as name, address, identity number - for fraudulent purposes.
- Cause damage to your own reputation.
- Can infect your computer with viruses and spyware.

Some Safeguards against Spear Phishing

- Do **not** click on links in an email to get to any web page, especially if you suspect the message might not be authentic.
- Exercise caution with emails requesting urgent personal and financial information.
- **Avoid** giving out your personal information unless you know whom you are dealing with.
- Secure your password so that only You can access your personal account.

Sample of a Spear Phishing email



From: Secrity@yahoo.biz
Sent: 29 June 2019 16:28
To: john.smith@govmu.org

Subject: URGENT- Account Suspension Notice

My Bank Limited

Dear Mr. John Smith

Your Account has been suspended

We're sorry but we have suspended your banking account because our security team noticed that your account was accessed from a different location.

You need to re-confirm your access details immediately.

If you does not do this as soon as possible, your account will be permanent deactivated.
Log in now to confirm your identity

Yours sincerely

Jason Oliva
Savings Director

Email address from the attacker does **not** seem official

Victim targeted **personally** by using his genuine email address

Specific person targeted

Suspicious links redirecting to a **fake** web address

Name may be from **actual** banker

Name and logo of **actual** bank may be used

Statement urging **immediate** action

Grammatical **errors**