ISSUE
2
March
2023

Security Awareness Bulletin

In this issue

Something very Phishy!

What is phishing?

Phishing is a type of cyber attack where an attacker attempts to trick you into providing sensitive information by posing as a trustworthy entity. This is often done through email, but can also happen through social media, phone calls, or other means of communication.

How can I recognize a phishing email?

Phishing emails often have misspelled words, grammatical errors, and a sense of urgency to prompt you to act quickly. Be suspicious of emails that ask for your personal or financial information. The most common types of phishing emails are ones that claim to be from a reputable company or organization, such as a bank or a government agency, or from an individual in a position of authority, such as a or head of a department, and that ask you to verify your account information or provide your personal information.

How can I protect myself from phishing attacks?

There are several ways you can protect yourself from phishing attacks, including:

- Look for suspicious emails: Be careful of emails that ask for your personal or financial information, or that have misspellings, grammatical errors, or a sense of urgency.
- Be wary of links: Phishing emails may include a link that takes you to a fake website that looks like a legitimate one. Always hover over the link to see the URL. If the URL looks suspicious, it’s best not to click the link.
- Check the sender's email address: Attackers often use fake email addresses that look similar to legitimate ones. Check the sender's email address carefully – not just the sender’s name – to make sure it is from a trusted source.
- Report the email and block the sender. Most email client software includes a feature to mark and report the email as Junk or Spam.
- Keep your software up to date: Software updates often include security patches that can protect you from known vulnerabilities that attackers can exploit. Make sure you keep your operating system, web browser, mail app and other software up to date.
- Use multi-factor authentication: Multi-factor authentication adds an extra layer of security to your accounts by requiring a code in addition to your password.
- Report suspicious activity: If you suspect that you've been the victim of a phishing attack, report it to your IT department immediately.

What else can I do to protect myself from phishing attacks?

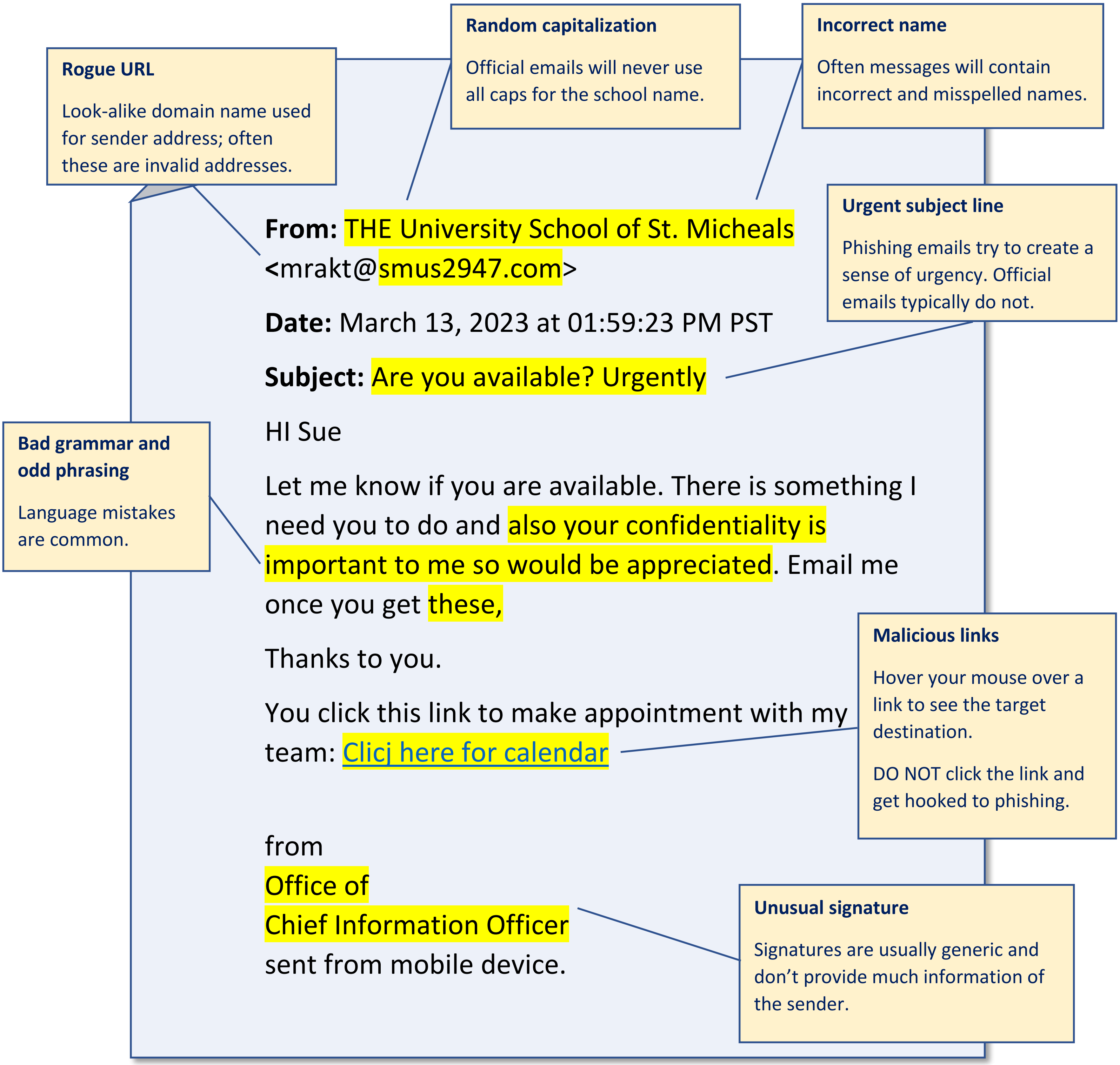
Other best practices to follow include being cautious of unsolicited emails or phone calls from unknown sources, using a spam filter to block phishing emails and other types of spam, regularly backing up your data, and educating yourself and your colleagues on the risks of phishing and how to prevent these types of attacks.

What should I do if I think I've been targeted by a phishing attack at SMUS?

If you suspect that you've been the victim of a phishing attack, report it to IT Security immediately at ITSecurity@smus.ca.

Remember, staying informed and vigilant is key to protecting yourself and our school from cyber attacks.

Anatomy of a Phishing Email



From: THE University School of St. Micheals <mrakt@smus2947.com>

Date: March 13, 2023 at 01:59:23 PM PST

Subject: Are you available? Urgently

HI Sue

Let me know if you are available. There is something I need you to do and also your confidentiality is important to me so would be appreciated. Email me once you get these,

Thanks to you.

You click this link to make appointment with my team: Clicj here for calendar

from
Office of
Chief Information Officer
sent from mobile device.

Rogue URL

Look-alike domain name used for sender address; often these are invalid addresses.

Random capitalization

Official emails will never use all caps for the school name.

Incorrect name

Often messages will contain incorrect and misspelled names.

Urgent subject line

Phishing emails try to create a sense of urgency. Official emails typically do not.

Bad grammar and odd phrasing

Language mistakes are common.

Malicious links

Hover your mouse over a link to see the target destination.

DO NOT click the link and get hooked to phishing.

Unusual signature

Signatures are usually generic and don't provide much information of the sender.