IT Security
PHISHING ATTACKS

St. George's University
Grenada, West Indies

UNIVERSITY
SUPPORT SERVICES

Over 90% of cyberattacks begin with a phishing email. Scammers use email, instant message, or text messages to trick an individual in giving them your personal information. They will make attempts to steal passwords, account numbers, Social Security numbers, credit card numbers, or other identifiable information that will allow them to gain access to your email, bank, or other accounts. These messages often times appear to come from a trusted entity, which tricks the victim to open, click, download, and/or login.

During this pandemic and with companies adjusting to a new norm of work, it is even more important that we all aware of the signs to recognize phishing and work to prevent these threats. As well, what to do should you believe you've fallen subject to a threat. It is each of our responsibility to ensure the security of our student and employee data.

OVER 90% of cyberattacks begin with a phishing email.

WHAT DO PHISHING ATTACKS LOOK LIKE?

Phishing attacks most commonly appear to come from a company or individual you know or trust. As well, they often tell a story to trick you into clicking or opening an attachment. For example, they could include one or many of the following:

- They've noticed **suspicious activity** or log-in attempts
- Claiming there is a **problem with your account** and/or payment information
- Noting you must **confirm some personal information**
- Including a **fake invoice**
- Noting you need to **click a link** to make a payment
- Noting your **eligible for a refund, coupon, or free gifts**

HOW TO IDENTIFY A PHISHING ATTACK

Cyber criminals can make these messages look and feel legitimate. The best approach is pause and evaluate the situation prior to taking any immediate action. There are ways for which one can work to identify a Phishing attack:

- Look for **mismatched URLs** and/or redirects
- Beware of messages conveying **unusual urgency**
- Think before responding to **unauthorized account-related emails**
- Be suspicious of messages **warning of severe consequences** for inaction
- Check for **spelling and grammar mistakes**
- Beware of **minimalism**

Should you believe you have fallen victim to a phishing attack or believe you may have received an email, instant message, or text message that could contain malware and/or a threat, please contact IT Security ITsecurity@sgu.edu