TransForm
SHARED SERVICE ORGANIZATION
Leading Innovation. Improving Healthcare.

Communiqué

TO: **Hospital Staff**

DATE: 22 June 2020

FROM: Mazen Joukhadar, Vice President, Chief Information, Privacy & Security Officer

RE: **Latest COVID-19 Phishing Campaigns**

Please be advised that we are receiving additional reports and warnings of global COVID-19 security threats. Most recently, over 100 executives with a German multinational associated with a government-led task force procuring PPE, were targeted by a phishing campaign to try and steal their security credentials.

If you receive a suspicious email, text msg, or phone call or if you do receive a COVID-19 e-mail from any external party, do NOT open any attachments or click on any links. Please log a ticket with tech support with the 'subject' of the e-mail and the 'sender' e-mail address (use the TransForm Support Portal or contact the TransForm regional IT/IM service desk at 519-973-4411, extension 7771).

Please delete the concerning e-mail from your mailbox. Please delete the text message from your phone.

As always, please restrict Internet surfing to business and clinical applications and continue to be vigilant when clicking on links or opening attachments from unexpected or suspicious emails addresses.

In most circumstances, a good general principle to follow if an email request seems suspicious or questionable whether you know the sender or not, is TO NOT OPEN attachments, follow web links or respond to the email. If you know the sender, follow up personally, (not responding to the email) before taking action and always follow normal operating procedures. If the sender is unknown, delete the email.

Below are some tips on how to identify fraudulent emails and how to avoid becoming a victim. Also included, is a graphic with some additional tips to protect yourself.

What to look out for:

- Spelling and bad grammar - Cybercriminals are not known for their grammar and spelling. If you notice mistakes in an email, it might be a scam.
- Email Links - Rest your mouse (but don't click) on the link to see if the address matches the link that was typed in the message.
- Threats - Cybercriminals often use threats that your security has been compromised. They may indicate your account will be closed if you do not respond.
- Generic Emails - phishing emails are usually generic, for example Dear First Bank user. If you don't see your name, be suspicious.

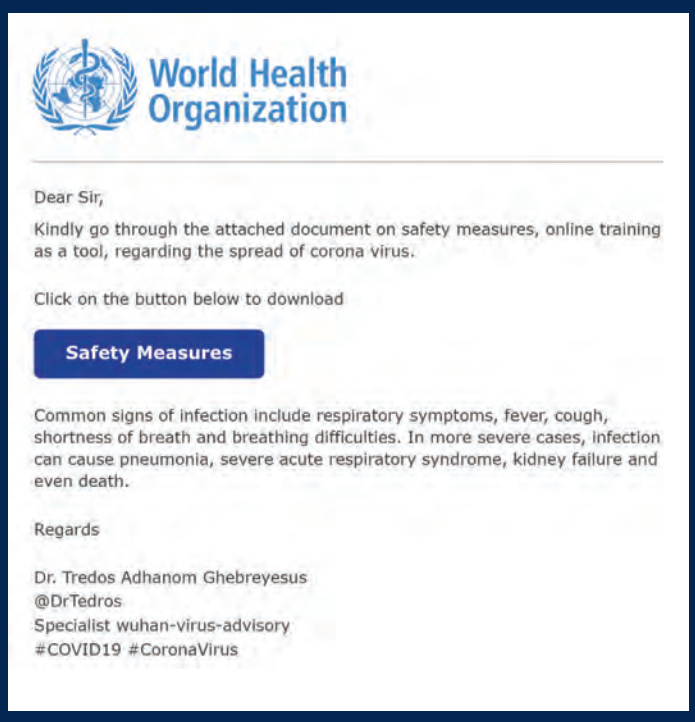
Spoofing popular websites or companies - Scam artists use graphics in email that appear to be connected to legitimate websites but actually take you to phony scam sites or legitimate-looking pop-up windows.

COVID-19 (Coronavirus) Phishing Scams

Attackers are taking advantage of the COVID-19 pandemic by sending phishing emails that look like legitimate awareness training or refunds for event cancellations.

Falling for one of these malicious emails can do real harm to you or your organization.

Scammers will often use scare tactics to trick you into opening a phish.



If you receive an email that mentions COVID-19 or coronavirus:

Don’t immediately interact with the email.

Take your time to evaluate it.

Looks Legitimate:

Verify it with the sender. Don’t reply directly to the email. Use another means of communication.

Looks Suspicious:

Report it to the appropriate team in your organization.

proofpoint®