kyndryl

Three common cyber scams

Email Phishing, Text Smishing, or Phone Call Vishing

What do these have in common?

- Look legitimate and real.
- Attempt to trick or urge you to click a link, download a file or share sensitive information.
- Pretend to be someone you trust (e.g., your bank, the Police, the government, family, friend).
- Aim to steal your passwords and information, cause financial damage to you or your company.

By the time you open the Email, read the Text, or answer the Phone call, the cyber-criminals may have some information on you already. That is why they often sound very convincing and legitimate; but they still need more from you to steal your money or gain full access to your accounts and information.

Avoid getting phished, smished, or vished with three simple steps:

01

Recognize the Warning Signs:

- Sense of urgency and threat using emotionally appealing language.
- Requests to verify or send sensitive information.
- Suspicious hidden URLs.
- Incorrect email addresses.
- Poor grammar or misspellings.

02

Pause & Be Cautious:

- Investigate by hovering over the links. Never click on them. Never call back.
- Pause, are you expecting to be contacted? Even, if the answer is yes, verify and confirm the sender with legitimate sources.
- Do not be scared or bullied into taking action.

03

Report Suspicious Activity:

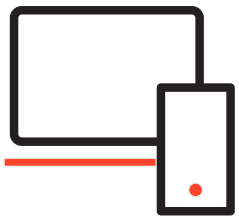
- Report the fraud via country specific official links and phone numbers.
- Hang up the phone and call the legitimate company that is being impersonated or log in via separate legitimate link.
- Ask for help, tell a friend, or loved one.

Examples:

Phishing Emails

are designed to appear to come from a legitimate source, like Netflix customer support, a bank, PayPal, or another recognized organization. The devil is in the detail like the sender's URL, email address, an email attachment link, etc. **Pause and be cautious: don't click.**

Smish



is a fraudulent SMS, social media message that ask the recipient to update their account details, change their password, or tell them their account has been violated. The message includes a link used to steal the victim's personal information or install malware on the mobile device. **Pause and be cautious: don't write back.**

Vish

uses a phone call with a cyber-criminal posing as support agent informing the victim about an apparent suspicious activity on her account in the first stage.

In the second stage the victim is urged to download a file or give away sensitive information threatening that their account will be suspended if they don't respond.

In the final stage the attacker gains full control over the victim's devise. Pause and be cautious: don't click. **Pause and be cautious: don't call back.**

© Copyright Kyndryl, Inc. 2024

Kyndryl is a trademark or registered trademark of Kyndryl, Inc. in the United States and/or other countries. Other product and service names may be trademarks of Kyndryl, Inc. or other companies.

This document is current as of the initial date of publication and may be changed by Kyndryl at any time without notice. Not all offerings are available in every country in which Kyndryl operates. Kyndryl products and services are warranted according to the terms and conditions of the agreements under which they are provided.