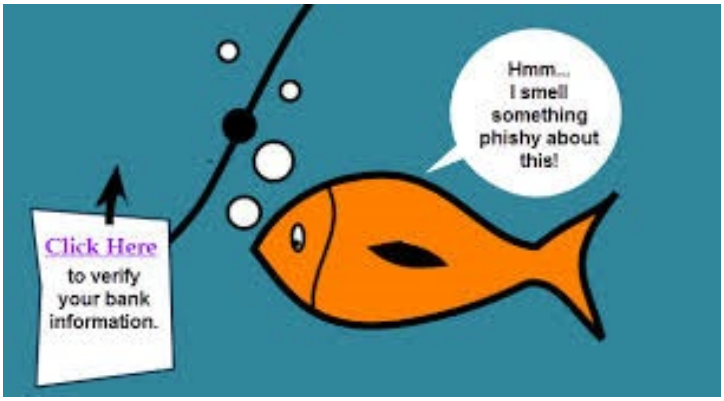
Don’t Fall Prey to Email Phishing Attacks



Please be on high alert for phishing attempts, which often use fake emails or texts that, if responded to, can infect your computer or lead to the theft of logins and personal information.

What is “phishing”?
A type of fraud in which emails pretending to be from reputable companies or from higher executives of the same company **trick victims into providing personal information** like passwords, credit card numbers, corrupt links and malicious downloads.

A PREVENTION CHECKLIST:

- ✓ Check if email header has “External” prefix like - **[External] Whitepaper: Head and heart**
- ✓ When you receive an email, always check that if the sender’s email address looks legitimate. Lack of company details strongly suggest a phish. For example: from: System Admin fakesysAdmin@gmail.com
- ✓ Be alert to emails that are not personalized. Make sure emails address you by name, like – **Dear User**,
- ✓ Hover over links in email messages and on websites to verify a link’s actual destination. Never click on links in unsolicited email messages. Clicking on links in phishing emails can install malware or ransomware.
- ✓ Never respond to unsolicited emails that request personal info and use sensational phrases like “URGENT” or “FINAL NOTICE”. The most popular type of phishing requests the user to update their password.
- ✓ Make sure the web address has https or a padlock icon in the browser window before providing personal information. Secure | https://
- ✓ Remember IT will never ask for your password.

Sincerely,
OCIT – *Your Partner for Success!*