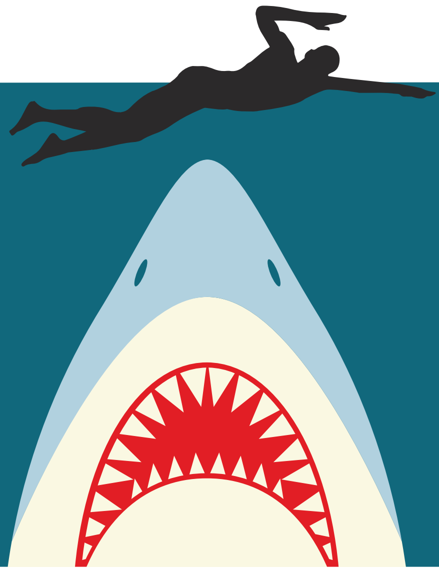
eitas

# Information Technology

# SURVIVING A PHISHING ATTACK



## WHAT IS A PHISHING ATTACK?

Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution or person to lure individuals into providing sensitive data such as personally identifiable information, personal health information, banking and credit card details, and passwords. The information is then used to access important accounts and can result in identity theft and financial loss.

## YES, YOU CAN SURVIVE A PHISHING ATTACK

### WATCH THE EMAIL SUBJECT AND TONE

- Be on your guard to any messages that induce a sense of fear or urgency. Is the tone of the email typical of your boss?
- Be wary of emails about financial transactions (shopping, banking, trading, shipping and invoices) that you are unaware about even if they come from a person or brand you know.
- Be careful of communication from a person or brand that you weren’t expecting.

### ASSESS SENDER INFORMATION CAREFULLY

- Watch for misspelt or different names for known people and unusual email addresses.
- Always distrust sender you don’t know.
- Watch for different sender patterns of behavior. Are emails coming to you from people you know but the email address is different than what they normally use?

### EXAMINE ALL LINKS

- Hackers use a combination of good and bad links within each message. Hover on any link and check the tooltip before you click. Be a detective when determining if links are legit.
- Be careful of shortened or numeric links. Instead of clicking links in an email, open a web browser and type in the link the email intends to take you to.

### BE CAREFUL WITH ATTACHMENTS

- Don’t open executable type attachments. These include files with the following extensions: exe, com, bat, cmd, pif, sh, scr, sct, sys, js and html.
- Be careful with Microsoft Office or PDF attachments. Only open these if you trust the sender.

If you are still concerned about an email, please contact the person directly by giving him/her a phone call or talking in person. If you still have concerns, please contact Information Technology at it@eitas.org.