NORTHERN TRUST

HOW TO RECOGNIZE PHISHING E-MAILS

PROTECT YOURSELF FROM PHISHING ATTEMPTS

Phishing is a form of cyber fraud that involves sending legitimate-looking e-mail messages to targeted recipients in an attempt to gather personal and financial information. Phishing e-mails may target business and/or personal accounts, and try to: propagate viruses, install malicious code, or steal personally identifiable information such as login credentials, bank account information, social security numbers, or credit card information.

WHAT ARE COMMON SIGNS OF A PHISHING E-MAIL?

- **Incorrect spelling and grammar —** obvious Phishing attempts may contain spelling errors or use words in an improper fashion.

- **Irrelevance —** some Phishing attempts are simply not relevant to your everyday life, such as:

  — the e-mail comes from a bank you have never heard of, yet asks you to verify your account

  — the e-mail claims your order was not delivered, yet you are not expecting any packages

  — the e-mail asks you to download a security patch, yet it is not from your anti-virus or Internet provider.

- **Use of incentives or prizes —** it is common for Phishing attempts to contain offers of money, prizes, or "unclaimed" rebates or property.

- **Phony confirmations —** Phishing e-mails may contain information about purchases, tickets or merchandise that you did not order.

- **Calls to action or threats —** Phishing attempts frequently use key phrases such as "verify your account", "click the link below to gain access to your account", or "if you do not respond within 48 hours, your account will be cancelled/access terminated, etc."

April 2018

Northern Trust will never ask you to provide, update or verify personal or account information via e-mail or an unsecured Internet web site. If you receive such a request, do not provide any information and contact Northern Trust immediately.

- **Misdirected Links —** Phishing e-mails regularly contain links that appear to connect to legitimate websites, yet actually go to different locations if clicked. Hover your mouse over the"link" and look in the lower left corner of your browser window to see the actual destination address. If the link in the corner does not match the link in the text, it may be redirecting you to a malicious web site.

- **Generic Salutations —** In many instances, Phishing e-mails use generic greetings such as "Dear Customer" or "Valued Customer". If it is your bank sending you a message, they will not only know your name and use it in correspondence; they will usually include the last few numbers of your account for verification purposes.

- **Bizarre, unexplained or missing subject lines —** Obvious Phishing attempts may contain strange or abbreviate subject lines or may be missing a subject altogether. Be alert for e-mails that claim to be from a friend or relative but appear suspicious. Your friend's computer may have been infected or their account may have been compromised, and malware may be sending messages to all your friend's contacts. If you receive a suspicious mail from a trusted source, call them to confirm they sent the message.

The Northern Trust Company | Member FDIC

northerntrust.com