NORTHERN TRUST

COMPROMISED E-MAIL ACCOUNTS

WHAT YOU SHOULD DO IF YOUR E-MAIL ACCOUNT IS COMPROMISED

April 2018

According to a 2018 Radicati Group study, there will be more than 3.8 billion email users before the start of 2019. Essential for business and personal use, offering fast, affordable and reliable communication, the popularity of e-mail makes it an unavoidable target for cyber criminals.

If you suspect your e-mail account has been compromised, contact your Northern Trust relationship manager immediately to reduce the risk of fraudulent transactions.

HOW TO TELL IF YOUR E-MAIL ACCOUNT HAS BEEN COMPROMISED

The signs of a compromised account are fairly easy to identify. Maybe your friends suddenly start calling you to complain about the "crazy e-mails" you've been sending. Or your in-box is flooded with delivery failure notifications, yet you did not send any e-mail to the addresses listed. Your "sent" folder may be full of messages you don't recognize, or it could be completely empty. Worse still — you try to access your e-mail accounts and you can't — your access is denied.

WHAT ACTIONS SHOULD YOU TAKE IF YOUR E-MAIL ACCOUNT HAS BEEN COMPROMISED?

Compromised e-mail accounts aren't just an inconvenience. There is a direct increase in your risk of becoming a victim of fraud and identity theft if cyber criminals have taken over your account. If your e-mail account has been compromised, don't ignore the signs. Take action immediately.

- **Change your Passwords.** Don't just change the password on your e-mail account. Change the password on any account that can be associated with that e-mail address. Studies have shown that more than 60% of internet users have the same password for multiple accounts. The first thing a hacker will do with your e-mail and password is try the combination on any and all shopping and financial Web sites to see if they can get money from your information.
- **Clean your Computer.** Take your computer to a professional to have it checked for malware and scanned for viruses, keyloggers, and other malicious programs. Do not initiate any online purchases or use your machine to pay bills until you are certain it has been cleaned and is not infected.

- **Update your virus definitions and patch your machine**. Ensure that your operating system and other software have the latest patches and updates installed and keep your virus definitions current.
- **Verify your e-mail settings and content.** Check your e-mail account settings for anomalies such as "auto forwarding" to another address. Review your security questions for accuracy and ensure your encryption preferences are enabled. It's also a good idea to go through your messages to determine what information may have been accessed. Your e-mail has most likely been scanned by an automated program that is designed to pick out information that can be used to gain access to financial accounts. In addition, private information or strategic business plans are at risk. Cyber-extortion is another risk that can result from compromised e-mail accounts.
- **Contact your e-mail provider.** Report the compromise as soon as possible to your e-mail provider.
- **Notify any financial institutions that you do business with via e-mail.** Your e-mail address is likely tied to many of your online activities. If your account is compromised, cyber criminals may ask your bank to send a new user name and password or attempt to initiate transactions claiming to be you. Keep track of every activity tied to your e-mail account, and if the account is compromised, notify your bank, your credit card company and your other online accounts.
- **Create a new e-mail account.** In serious cases, the best option is often to create a new e-mail account. Convenience services, such as automatic forwarding that allows easy transfer of contacts and any new e-mails as well as possible transfers of your archived messages, simplify this change. For maximum security, make sure you use a new password for any new accounts.

WHAT CAN I DO TO REDUCE MY RISK OF GETTING HACKED?

A few common sense precautions can go a long way towards improving the security of your accounts. Start with a strong password — preferably with a minimum of 8 characters, using upper and lower case and including numbers and special characters. Remember to keep your passwords protected at all times; there are numerous commercially available products that will store your passwords in encrypted files on your mobile device or your computer.

- **Learn to avoid Phishing:** Phishing is a form of cyber fraud that involves sending legitimate-looking e-mail messages in an attempt to gather personal and financial information or to propagate viruses, install malicious code, or steal personally identifiable information. Reduce your risk of account takeover by learning to recognize and avoid Phishing e-mails; do not click on links or open attachments within e-mails even when you know who sent them unless you are expecting them and know what they contain.
- **Use two-factor authentication.** Although all accounts are at risk, adding an additional security layer to your account, such as two-factor authentication, can be a worthwhile enhancement to protect your e-mail account even if your

It takes only 10 minutes to crack a lowercase password that is 6 characters long. Adding two extra letters will increase that time to 3 years. One more character and some numbers and symbols — your password now takes 44,530 years to crack. Never underestimate the power of a good password!

password is compromised. For example, Google provides the option of using two- factor authentication to protect Gmail and Google documents from hackers. Other e-mail services, such as Yahoo, also offer a version of two-factor authentication.