ARE YOU SECURE? PROTECT YOUR INFORMATION AND YOUR DIGITAL ACCOUNTS

What You Need to Know About Digital Account Security

May 2017

Don't panic!

If you suspect your personal data has been compromised, contact one or all three of the major credit bureaus—Equifax, Experian, and TransUnion—and ask them to put a fraud alert on your file.

Fraud lines:

Equifax
800.525.6285

Experian
888.397.3742

TransUnion
800.680.7289

The world we live in is full of potential threats, particularly when it comes to protecting your personal and financial information. Protecting your financial accounts, and your identity, from unauthorized access will help to reduce your risk of becoming victim to fraud.

Most people are aware that email faces an abundance of threats ranging from hackers, viruses, spam and phishing, to identity theft. A lesser known, but equally dangerous threat, is the threat of account takeovers that result from compromised personal information. Keeping your personal information secure is the first step toward preventing account takeovers and any resulting monetary loss.

KNOW THE BASICS

There are many ways criminals obtain personal information, which can be used to access banking and investment accounts, credit card accounts or medical records. To protect yourself, you need to understand where you may be vulnerable and use appropriate techniques to shield your information.

- **Protect your mobile devices.** According to the Cisco Visual Networking Index, there will be 11.6 billion internet-enabled devices by 2021, exceeding the world's projected population at that time (7.8 billion). There is no doubt that mobile devices are common – and as the capabilities of mobile devices improve, the risk of compromise will presumably increase as well. Like your computers at home, you need the most up-to-date security software, web browser, operating system and apps on your mobile device. Install operating system updates as soon as they become available and use a unique and complex PIN or passcode on your phone at all times. Set an automatic screen lock after a designated amount of time – preferably less than five minutes.

- **Protect your computer.** Malware is malicious software, infecting your computer or mobile device and performing operations you did not authorize and may not be aware of. Malware can take many forms, stealing your personal information, rendering your device unusable, holding your files for "ransom" or copying your

keystrokes to obtain logon information for bank, investment or credit card accounts. You can greatly reduce the risk of malware on your computer by:

  - Using antivirus software
  - Using email services that offer automatic antivirus protection such as AOL, Google or Hotmail
  - Opening email only from trusted sources
  - Only opening attachments you are expecting
  - Always scanning attached files with antivirus software before opening
  - Running regular anti-virus scans

- **Avoid phishing attacks.** Phishing scams are designed to steal personal information. They use doctored and fraudulent email messages to trick recipients into divulging personal information, such as credit card numbers, logon IDs, passwords and social security numbers. Phishing messages often boast real logos and appear to have come from legitimate organizations.
- **Use email wisely.** Email is a great way to keep in touch with family and friends and to use as a business tool. That being said, it's important to note that while you may have great anti-virus software on your computer, your friends and family may not. Be cautious sending sensitive or private information by email. Never send anyone credit card information, your social security number or other private information via unprotected email.
- **Protect your online identity.** It is extremely important to protect your online identity:
  - Use security and privacy settings on websites and apps to manage the information you share and who sees it
  - Avoid sharing your location, which can allow criminals to see where you are
  - Only friend people you actually know in real life and do not divulge confidential information on social media sites
  - Keep track of the "apps" you use and delete apps you do not use

  - Likewise, do not use apps that ask for unnecessary information like social security numbers
  - Before installing an app, check the resource information – if the app asks for permission to access your contacts, your email address or other apps on your device, do not install!

- **Use the account protections that are offered to you.** In addition to using two-factor authentication on all your financial accounts, you can enable secondary controls to protect your email, access to your devices, your mobile accounts and other sensitive information. Many businesses offer extra security in the form of PINs to make changes to your settings and profiles.
- **Know your financial institution.** Establishing a good relationship with your financial institution will help reduce the risk of fraudsters obtaining unauthorized access to your accounts and personal information. An astute relationship manager and an organization with established and effective security policies will recognize and verify transaction requests.

Using common sense and making careful decisions is key to preventing criminals from gaining access to and compromising your accounts. For more information about online and digital account security, visit the Security Center on **northerntrust.com/securitycenter** or speak with your Northern Trust relationship manager.