Northern Trust

IS YOUR EMAIL SECURE? PROTECT YOURSELF FROM EMAIL BASED FRAUD SCHEMES

What Every User Needs to Know about Email Security

The world we live in is full of potential threats, particularly when it comes to protecting your personal and financial information. One of the biggest risks in the area of cyber security is email. Email is incredibly simple and incredibly important. This simplicity is what allows email work so well; however, it is also what makes it very insecure in its natural form.

Email faces threats ranging from hackers, viruses, spam and phishing to identity theft and “man in the middle” attacks. The fact is; keeping email as secure as possible should be a priority for all users to help reduce the risk of compromised accounts and financial fraud. If your email is NOT encrypted it is easy to copy, easy to intercept, and easy to alter. Unprotected, it’s simply an efficient and effective way for cyber criminals to compromise your financial information and steal your money.

START WITH THE BASICS

Email compromise remains the most dangerous threat facing users of electronic mail. That being said, there are a variety of lesser threats that can be addressed first, to help reduce the risk that your email will get “hacked” or compromised.

- **Prevent virus outbreaks and spam.** You can greatly reduce the risk of computer viruses by using antivirus software. Likewise, using only email services that offer automatic antivirus protection (such as AOL, Google, Hotmail, and Yahoo), opening email only from trusted sources and only opening attachments you're expecting will reduce the risk of contracting Malware on your computer. Always scan attached files with antivirus software before opening. You can also reduce the amount of spam you receive by being cautious where you post your email address. Avoid publishing your email address on Web sites or submitting it to every site or organization that requests it.
- **Avoid phishing attacks.** Phishing scams are designed to steal personal information. They often use doctored and fraudulent email messages to trick recipients into divulging personal information, such as credit card numbers, account credentials and social security numbers. While online banking and e-commerce Web sites are generally safe, you should always be careful about divulging personal and corporate information over the Internet. Phishing messages often contain real logos and appear to have come from the actual organization, but that doesn’t make them more legitimate.
- **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 on your computer, your friends and family may not. Be cautious about who you send confidential information to over unprotected email. Never send your credit card information, Social Security number, or other private information via unprotected email to anyone.

SECURE YOUR EMAIL, PROTECT YOURSELF

There are a few key elements of email security that every user can implement to minimize the risk of account compromise and email fraud.

- **Embrace encryption.** Using encryption for communications with your financial institutions and wherever else you are conducting business will help protect your personal information from attackers. Encryption protects email in transit, and can protect the information within your computer if used properly.
- **Separate your email accounts.** Keep several active email accounts that can be used for different reasons. This can include an account for friends and family, an account for business and financial information, and an account for "throwaway" messages such as newsletters, advertisements from merchants you do business with, sales flyers, etc. This will reduce the chances that Spam and Phishing emails will infiltrate your important accounts, and won't cause a problem for you if the "throwaway" account gets hacked or suspended.
- **Become a Password expert.** Use a strong, complex password at all times, change it frequently, and do not use the same password for multiple accounts. Do not save your email account passwords in your mail programs or web browsers. Consider using a Password "Vault" program to save your passwords in an encrypted file.
- **Use "Secure Communication" methods.** Whenever possible, utilize the Secure Communications feature offered by your financial institution and communicate using the encrypted portal. The easiest way to keep your financial information secure is to avoid using email for business or financial purposes completely.
- **Know Your Financial Institution.** Establishing a good relationship with your financial institution will help to reduce the risk that compromised email accounts will be used to conduct financial fraud. An astute Relationship Manager, and an organization with established and effective security policies, will recognize and verify transaction requests BEFORE sending money out of your accounts. Avoid email for any transaction requests to avoid the very real threat of a cyber-criminal using your accounts to steal your own money.

Email, for all its great features, is not suitable for all types of business. At the end of the day, email security comes down to common sense and careful decisions. For more information on email security, visit the Security Center on www.northerntrust.com/securitycenter or talk with your Northern Trust relationship manager.

DON'T PANIC

If you suspect hackers may have got hold of your personal data, contact one or all of the three major credit bureaus—Equifax, Experian, and TransUnion—and ask them to put a fraud alert on your file. The fraud line for Equifax is 800.525.6285; for Experian is 888.397.3742, and for TransUnion is 800.680.7289.