NORTHERN TRUST

PROTECTING YOUR HOME COMPUTER

SIMPLE STEPS TO PROTECT YOUR HOME COMPUTER AGAINST CYBER CRIME

April 2018

For many of us, these computers and internet connections are the primary tools we use for managing our personal and professional lives. Unfortunately, these computers may also be a target for cyber criminals.

WHAT IS CYBER CRIME?

According to Interpol, Cybercrime is now one of the fastest growing areas of crime. Criminals are attracted to the speed, convenience and anonymity of modern technology, and use computers and the Internet to engage in a diverse range of criminal activities, such as identity theft, internet auction fraud and account takeovers. They may also use other, more technical attacks to deploy viruses, Botnets, malware, keyloggers and spyware to infect or take over your machine.

WHAT CAN BE DONE TO INCREASE THE SECURITY OF YOUR HOME COMPUTER?

Although there are no guarantees, there are simple steps you can take to increase the level of security on your home computers.

- **Start off secure.** The first step to protect your computers is to start with machines without viruses or malware. Buy your computer from a well-known source and avoid used computers if at all possible. If you purchase a used computer, do not trust the pre-installed software. Before you do anything else, reformat the hard drive and reinstall the operating system. If you are unsure how to complete this task, ask someone you trust for help. It does almost no good to try to protect a computer that has already been infected.
- **Keep up your defenses.** It is critical that you keep your computer updated with the most recent versions of your operating system and programs. Cyber criminals are continuously looking for software vulnerabilities they can exploit to their advantage. When computer and software vendors discover vulnerabilities in their systems they issue "fixes" in the form of updates and patches. Even a new computer will already be out-of-date and will require updates as soon as you take it out of the box. Once you've gotten your

The goal of any software claiming to be "anti-virus" or "anti-malware" should first be to prevent the software from entering your system. Second, in the event that the malware does infect your machine, anti- malware should either remove or "clean" your machine, or inform you of the infection so appropriate action may be taken.

machine set up, connect to the Internet and enable the automatic update feature. Scheduling your machine to check for updates once a day will help keep your computer secure.

INSTALL ANTI-VIRUS/ ANTI-MALWARE SOFTWARE

There are literally hundreds of anti-virus applications available, from retailers and from internet service providers (ISPs). Most new machines will come with a free anti-virus software "trial" pre-installed that can be purchased once the trial is over. Make sure that the software solution you choose provides adequate protection, and be aware that many of these programs are only licensed for non-commercial home use and may not be used on computers used commercially or for business.

- **Keep your virus definitions updated.** Just like your operating system, anti-virus software needs to be updated frequently to remain effective. This is usually referred to as updating the "definitions." Because new viruses are being created and distributed all the time, virus software must be current to protect your machine. You can program your anti-virus software to automatically check for new definitions.
- **Run regular scans.** Programming your anti-virus software to run automatic scans is easy and is the method preferred by most users. In addition to an automatic "quick scan," it is a good idea to run a full scan of your machine at least once a week.
- **Backup your data.** Even the best machine may become compromised or suffer a hard drive failure or other disaster. Regular backups to either an external hard-drive or to a secure Cloud service will help you to recover your information should your machine suffer the unthinkable. External hard drives can easily be connected to your computer and programmed to run automatic backups of your photos, documents and home videos.
- **Secure your wireless network.** The popularity of portable computing devices, such as laptop PCs, smart phones and tablets, has increased the number of home users who choose to create a personal wireless network. Wireless networks are established using wireless routers, which can be purchased, or rented from your internet provider. Keeping a strong password on your wireless network and using the strongest available encryption features will help protect your "network," which in turn helps in the protection of your computers and mobile devices.
- **Recognize the Scams.** In most cases, cyber criminals need help from their potential victims to steal information or inject malware or other malicious programs. Phishing e-mails, spoofed Web sites, counterfeit flash drives, or infected CDs or programs are common methods criminals use to gain access to your sensitive information or infect your machine. Constant vigilance will

Many internet service providers offer anti-virus software for free. Check with your provider for available downloads and other services, such as parental controls, that can help to keep your machines safe.

go a long way towards protecting your computer and your information. Keep informed of the most recent scams and tricks by checking reliable resources such as the Federal Trade Commission, the International Cyber Security Protection Alliance (ICSPA) or the Anti-Phishing Working Group. You can also check the "Security Center" on northerntrust.com for useful tips on keeping your accounts and identity secure.

LEGAL, INVESTMENT AND TAX NOTICE: This information is not intended to be and should not be treated as legal advice, investment advice or tax advice and is for informational purposes only. Readers, including professionals, should under no circumstances rely upon this information as a substitute for their own research or for obtaining specific legal or tax advice from their own counsel. All information discussed herein is current only as of the date appearing in this material and is subject to change at any time without notice. This information, including any information regarding specific investment products or strategies, does not take into account the reader's individual needs and circumstances and should not be construed as an offer, solicitation or recommendation to enter into any transaction or to utilize a specific investment product or strategy.

The Northern Trust Company | Member FDIC

northerntrust.com (5/18)