NORTHERN TRUST

PROTECTING YOUR BUSINESS COMPUTERS

IMPORTANT STEPS TO PROTECT YOUR BUSINESS AGAINST CYBER CRIME

Computer security for the small to medium-sized business doesn't have to be complex or overly expensive. The foundation is built on strong governance that includes policies, standards, procedures and commitment from executive management. Also essential is a comprehensive analysis of the most critical information that needs protecting. From there, a multi-layered approach is recommended. Using desktop security products such as anti-malware/anti-virus, anti-spam and firewalls, combined with more advanced services such as network intrusion detection, security tokens, and disk encryption, in particular for mobile devices such as laptops, can help reduce the risk of unauthorized access and cyber-crime.

WHY SHOULD YOUR BUSINESS BE CONCERNED ABOUT COMPUTER SECURITY?

Protecting client information is both required by current privacy laws and considered a good business practice. Today's clients expect organizations to have controls in place to secure their personal information. Historically, businesses have always been a target of cyber criminals and many hackers will try to exploit business web sites that have old and unsecured coding or run on older web servers and operating systems.

Here are some steps that your organization can take to help protect against common security threats.

- **Keep your computers up to date.** It is critical that computers are consistently updated with the most recent versions of the applicable 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 brand new computers require

April 2018

At Northern Trust, we're committed to protecting your privacy and financial wellbeing, so much so that privacy and security are principle tenets of the design and operation of Northern Trust Passport, our online technology platform.

To protect your information, Northern Trust regularly evaluates and updates its security technologies and maintains physical, electronic and procedural safeguards that meet and exceed federal standards.

updates as soon as they are taken out of the box. Updates should be performed as soon as computers are installed and automatic updates should be enabled either independently per system or through the development of a corporate update system. Scheduling machines to check for updates once a day will help keep your system secure.

- **Install anti-virus/anti-malware software.** There are a number of anti-virus applications available from retailers and internet service providers (ISPs). The software you choose should be evaluated to ensure that it will provide adequate protection based on factors such as whether your company uses a firewall. Applications available for personal computers may not be appropriate for a business.
- **Keep the "definitions" updated.** Anti-virus/anti-malware software needs to be updated frequently to remain effective, which is often referred to as updating the "definitions." Unfortunately, because hackers are creating and distributing new malware on a regular basis, anti-malware software must be current to protect machines properly and can usually be programmed to automatically check for new definitions. ■
- **Run regular scans.** Programming anti-virus software to run automatic scans on a regular basis is the preferred method for most users. One easy step is to have the software run an automatic "quick scan" with a full scan scheduled at least once a week. ■
- **Backup all data.** Because hackers are consistently attempting to cause damage through enhanced methods, even the most up-to-date software protection may not be enough and a computer may become compromised, suffer a hard drive failure or other malfunction. It is highly recommended that you perform regular backups should a computer suffer the unthinkable. Backups of critical data should be stored in multiple secure locations including storing three secure copies; one copy on a local redundant hard drive, one copy backed up locally to a secondary device and one copy stored remotely. ■
- **Secure wireless networks.** The popularity of portable computing devices, such as laptop PCs, smartphones and tablets, has increased the number of businesses who have chosen to create and use internal wireless networks. Wireless networks should always use a strong password and the strongest available encryption features. This will help protect the network and, in turn, help in the protection of the computers and mobile devices using the network.

Constant vigilance will go a long way towards protecting your business. Keep informed of the most recent scams and tricks by checking reliable resources such as the Federal Trade Commission, International Cyber Security Protection Alliance (ICSPA) or Anti-Phishing Working Group. You also can check the Security Center on the Northern Trust web site for useful tips on keeping your system 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)