Cyber Awareness Best Practices for Businesses

Comerica Bank
RAISE YOUR EXPECTATIONS.

You are ready to move your business forward into the world of Treasury Management solutions through online banking.

Congratulations: the convenient cash management products offered by Comerica Bank will make your banking more efficient and manageable. But with the increased online access comes the risk of your business's information being compromised through cybercrime.

Cybercrimes are not new; cyber-criminals employ various technological and non-technological methods to manipulate or trick you or other victims into divulging your personal or account information. Such techniques may include performing an action such as getting you to open an e-mail attachment, accept a fake friend request on a social networking site, or visit a legitimate, yet compromised, website that installs malware on your computer(s). Modern cybercrime is about money. Cyber criminals are targeting the financial accounts of owners and employees of small and medium sized businesses who are not cyber savvy, resulting in significant business disruption and potential monetary losses.

Don't panic! You want to be sure you are doing everything you can to protect your business online, right? Having protection software is only half of the equation. No single layer of protection is enough; you need a layered security approach, especially when employees are engaging in risky or potentially unsafe behavior online. The best practices developed in this handout are intended to raise your awareness of ways to help protect, detect, and educate business employees on today's online risks.

Much of it is a compilation of information contained in our service User Guides for Comerica Business Connect, in the Consumer Protection Center on Comerica.com, and in articles and messages we've posted on the Comerica Business Connect portal.

Protect

- **Secure your Business's Network of Computers**
  - **Dedicate a Computer –** Minimize the number of, and restrict the function for, computer workstations and laptops that are used for online banking and payments. Better yet, consider using a stand-alone computer that isn't connected to your network to perform your online banking transactions. If a stand-alone is not possible, then ensure that each user of online services uses his/her own device (desktop computer, laptop or mobile) and his/her own password. Do not share computers for accessing financial services. Sharing a computer that has become infected places the login and transaction credentials of all users of that computer at risk of theft and unauthorized use. A workstation used for online banking **should not be** used for general web browsing, e-mailing, and social networking.
  - **Protection Software –** Install and maintain real-time **anti-virus, anti-spyware, firewall,** and **malware** detection and removal software. Use these tools regularly to scan your business network and allow automatic updates for your operating and software systems. Be sure your virus detection software, personal firewalls, adware and spyware-blocking software are up-to-date and all updates and security patches have been installed. Also be sure that every computer that accesses Comerica Business Connect has the Rapport software from Trustee downloaded onto it and the maximum protection settings are selected. Do not ignore warning messages from security software that a potential virus has been detected. Take immediate action.
  - **Firewalls –** Install this hardware to prevent unauthorized access to your network and create a strong password.
  - **Back-up –** Have a contingency plan to recover files on your business computers that were lost due to a catastrophic system/hardware failure. What if there is no preservation of data and everything was erased? Develop a scheduled weekly or daily plan to back-up important business files and secure the back-up disks or external hard drives. Don't forget to test your plan and verify your data will be restored.
  - **Wireless –** Do not use public Internet access points (e.g., Internet cafes, public Wi-Fi hotspots such as airports and government buildings) to access accounts or sensitive business information. If this type of access is needed, employ a Virtual Private Network (VPN) and make sure your transmissions are encrypted.
  - **Mobile –** Be careful using mobile devices and tablets. While convenient, information technology experts say that in many ways, mobile devices are more vulnerable to unwanted access by cyber criminals and data loss that can result in identity theft and access to confidential information and banking accounts.

Online Fraud Protection: Best Practices for Businesses

Comerica Bank
RAISE YOUR EXPECTATIONS.

- **User IDs, Tokens and Passwords –** Do not share your secure User ID and password with anyone, even with a co-worker. Comerica will ask for your User ID when **you** initiate a call, but Comerica will **never** ask for your password.
  - Make sure key employees have a trained backup in the event of an absence, who have their own ID and password available to continue banking business as usual.
  - Don't forget to delete employee IDs and passwords when they leave the business or change responsibilities. Regularly review an active access list and determine any changes to privileges that may be needed.
  - Create strong passwords, not something that is easily guessed. Try using a sentence with punctuation, special characters or a mix of letters and numbers.
  - Change your passwords at least once a month
  - When you sign into a webpage and are given the option to save your password, select **NO.**
- **Dual Control creates safety checks –** Initiate ACH and wire transfer payments under dual control using two separate computers. For example: one person authorizes the creation of the payment file and a second person authorizes the release of the file from a different computer system.
  Note: This helps ensure that one person does not have the access authority to perform both payment functions. Additionally, dual control will ensure that one person cannot give themselves additional authority, or create new user IDs.
- **Block Sites –** Consider enlisting the help of an Internet service to automatically block sites that employees do not need to access for business purposes (i.e., social networking sites, blogs, instant messenger, and free software sites) to reduce the risk of downloading malware or spyware.

Detect

- **Monitor and reconcile your accounts regularly –** Reviewing accounts regularly enhances the ability to quickly detect unauthorized activity. The quicker this activity is detected, the sooner you can take action to prevent or minimize losses.
  Note: If you detect suspicious activity, immediately cease all online activity and disconnect the Ethernet cable and/or any other network connections (including wireless connections) to isolate the system from the network. Immediately call your financial institution to report the suspicious activity.
- **Note any changes in the performance of your computer(s)**
  - Significant loss of speed
  - Computer "locks up" so the user is unable to perform any functions
  - Unexpected rebooting, restarting or the inability to shut down
  - Unexpected request for a one-time password, token, or other information in the middle of an online session

Educate

- **Ask questions –** Treasury Management is here to help. Use the relationship services phone number at **800.852.3649** to speak with a trained product specialist from 9:00 a.m. to 7:00 p.m. ET.
- **Take the TM Connect online tutorials** and view the online **Resources** located on the **home page of TM Connect.** This area contains a wealth of knowledge, especially for new users.
- **Comerica Bank site – www.comerica.com** Customer Protection Center/Prevention Begins with You/Corporate Account Takeover to view a Fraud Advisory for Businesses. This advisory is the product of a joint effort between the US Secret Service, FBI, the Internet Crime Center (IC3) and the Financial Services Information Sharing and Analysis Center (FS-ISAC)
- Be knowledgeable about the online services you use and how they look and work. Call your service provider if you are suspicious about any request you receive for login or personal information that is generally confidential, and if something looks or performs in an unusual way.
- **Continuously educate employees –** Cybercrimes are constantly changing, so software and fraud prevention solutions have to change as well to stay ahead of the game. Determine if you are taking advantage of all the fraud solution options that Comerica offers its business customers. Watch our Fraud Awareness video, Cyber Security 101 at http://www.comerica.com/campaigns/pages/cyber-security-101.aspx
- Stay abreast of current fraud risks publicized on one of our fraud partners' websites. See the Cyber Resource Link box. The online fraud environment changes rapidly so refer to these sites regularly.

- **Be Cyber-street savvy –** Don't view or open attachments or click on links in unsolicited e-mails. **Financial institutions and government agencies do not contact customers by e-mail or phone asking for passwords, credit card numbers, or other sensitive information.** This is also true if you are contacted from an apparent legitimate source (such as the IRS, Better Business Bureau, Federal courts, UPS, etc.)
- **Be wary of pop-up messages** claiming your machine is infected and offering software to scan and fix the problem, as it could actually be malicious software that allows the fraudster to remotely access and control your computer.
- **Report suspicious activity –** Make sure your employees know how and to whom to report suspicious activity within your company and with accounts at your financial institution. Immediately contact your financial institution if you notice unauthorized activity so that the following steps may be taken to:
  - Disable online access to accounts
  - Change online banking passwords
  - Request that the financial institution's agent review all recent transactions and electronic authorizations on the account. If suspicious active transactions are identified, cancel them immediately.
  - Ensure no new changes have occurred on the accounts such as; address changes, added users, or changed PINs.
  - **It is important to note…**
    The above best practices will help you protect yourself, your computer, and your organization – but only if all precautions are followed to prevent unauthorized access to your computer and/or login credentials. Once an unauthorized person has gained access, it may be too late to stop their actions.
    - We have best practices and safe computing reference sources available for you in the Tools and Resources section of Comerica Business Connect, called *Cyber Awareness Best Practices for Businesses*, *7 Practices for Safer Computing* and the film *Cyber Security 101* at http://www.comerica.com/campaigns/pages/cyber-security-101.aspx
    - Notify us immediately if you discover any unauthorized or unusual activity involving your Comerica accounts. Contact Treasury Management Relationship Services at 800.852.3649.

Cyber Resource Links

You should stay informed about current threats by having these resource links saved in your browsers favorites.

Internet Crime Compliant Center (IC3) FBI:
www.ic3.gov

United States Computer Emergency Readiness Team:
www.us-cert.gov

American Bankers Association:
www.aba.com

Department of Homeland Security:
www.dhs.gov

National Consumers League's Fraud Center:
www.fraud.org

National Check Fraud Center:
www.ckfraud.org

Better Business Bureau:
www.bbb.org/data-security/

The Federal Trade Commission is the nation's consumer protection agency:
www.ftc.gov

Federal Bureau of Investigations:
www.fbi.gov/scams-safety

Homeland Security Cyber Security Research and Development Center:
www.cyber.st.dhs.gov

National Cyber Security Alliance:
www.staysafeonline.org

Chamber of Commerce Internet Security Essentials for Businesses:
www.uschamber.com/issues/technology/internet-security-essentials-business