Cyber Awareness Best Practices for Consumers

SM

Comerica Bank
comerica.com

You are ready to move your banking online. Congratulations: you will be able to conveniently access your financial information, better organize your financial records, and manage banking activity anytime, anywhere. But with the increased online access comes the risk of Internet fraud and cybercrimes.

Cyber criminals use the Internet to defraud consumers in a variety of clever ways. By simply performing an action such as opening an email attachment, accepting a fake friend request on a social networking site, or visiting a compromised, (e.g. infected) website you could be opening yourself and your computer equipment up for cybercrime. Cyber criminals are targeting individuals who are not cyber "savvy," and computers that are not adequately protected.

Don't panic! You want to be sure you are doing everything you can to protect your computer online, right? Having protection software is only half of the equation. Understanding what potentially risky actions you or your family may be engaging in will also give you an added layer of security to help keep your computer free of cybercrimes. The current best practices outlined in this handout are intended to raise consumer awareness of ways you can help protect, detect and learn about today's online risks.

Protect

- **Don't Click the Link –** The threat of cybercrime most often begins with "phishing." Cyber criminals attempt to infect your computer with "malware" which is short for malicious software. Malware includes viruses, spyware and key loggers that get inadvertently loaded on your computer, allowing the criminals to monitor, control and track your online movements, steal your passwords and compromise your accounts. Be extremely cautious when clicking a link unless you know who sent it and what it is. **When in doubt, throw it out!**
  - **Links in email, tweets, posts, and online advertising** can send you to sites that masquerade as your favorite sites or appealing new sites but may automatically download malware without your knowledge.
  - **Opening attachments,** even those that appear to come from a friend or co-worker, can install malware on your computer.
  - **Type a site's URL** directly into your browser; check for indicators that the pages are secure, such as a padlock symbol at the bottom of the page and a URL that begins with "https" instead of "http." Look for clues that would identify the site as fake such as misspellings and incorrect information.
- **Change your Passwords**
  - Create strong passwords, not something that is easily guessed. Try using a sentence with punctuation, special characters or a mix of letters and numbers.
  - Don't use the same password for all your online accounts.
  - Change your passwords at least once a month.
  - When you are signing into a webpage and given the option to save your password, select NO.

- **Session Log-off –** Always **log off** from your online banking session before exiting. Simply clicking "x" or closing a window does not mean you logged off. Shut off your computer or disconnect from the internet when not in use.

- **Arm your Computer with a Security Toolkit –** A security toolkit includes anti-virus and virus detection software, personal firewalls, and adware/spyware blocking software.
  - Update your toolkit frequently:
    - » Install security patches issued by your software vendor (i.e., Norton, Microsoft, etc.)
    - » Update firewall, operating systems, and browser software issued by your vendor (i.e., Black Ice Defender, Windows, Internet Explorer, Safari, etc.)

- **Lock it up –** Do not share your secure User ID and password. Should you have a problem with your Comerica online banking account, Comerica Bank will ask for your User ID when **you** initiate a call, but Comerica will **never** ask for your password.
  - Make sure all authorized family members who access online banking know the assigned User ID, password, and answers to the authentication questions (husbands and wives will share the same access information.) Several wrong attempts will result in automatically locking your access, and you will have to call Comerica's Web Banking department at **1.888.444.9876** to restore access for all users. This procedure is in place for your protection.

- **Face-off with Facebook –** Consider blocking sites that your family (especially children) can't resist using and that may be contributing to your risk of cybercrime. Clicking pop-ups, downloading "free" games or programs, and clicking on information found on social networking sites, blogs, and instant messenger may install 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.
  - If you detect suspicious activity, immediately cease all online activity and disconnect the Ethernet cable and/or wireless connections. Immediately call Comerica Bank at **1.888.444.9876.** Be wary of cybercriminals attempting to re-direct you to non-Comerica phone numbers.

- **Note any changes in the performance of your computer(s)**
  - Significant Loss of speed, malfunction, or repeated error messages
  - Computer locks up so the user is unable to perform any functions
  - Unexpected rebooting, restarting, or the inability to shut down
  - Numerous pop-up ads or ads that display when you're not surfing the web

Cyber Resource Links

Stay informed about current consumer alerts and additional ways to stay safe online by having these online resource links saved in your browser favorites.

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

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

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

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

National Cyber Security Alliance:
www.staysafeonline.org

Comerica Bank Customers – If you've responded to fraudulent e-mails, please contact **Comerica's Identity Theft Resources at 877.881.8955** from 8 a.m. to 8 p.m. ET, Monday-Friday.

For more helpful information, **visit our Consumer Protection Resources Center at www.comerica.com**

Please forward suspicious Comerica e-mails to Comerica Bank at **Fraud@infosecalerts.com**

Educate

- **Ask questions –** If you feel your online account or personal computer has been compromised, contact Comerica Bank at **1.888.444.9876** or send an e-mail to Comerica from your Web Banking home page.

REMEMBER: Comerica Bank will never request personal information such as Social Security numbers, account numbers, PINs, or passwords via e-mail.

- **Comerica Bank site – www.comerica.com** has a Customer Protection Center link located on the home page. We have created our Customer Protection Center as a way to help educate you, the consumer, and to help you avoid becoming a victim of fraud.
- **Be Cyber-street savvy –** Just as you would not share your financial information with a stranger who came knocking at your door, you should not give out personal information online unless you've initiated the transaction. Be wary of communications that implore you to **act immediately,** offer something that **sounds too good to be true,** or ask for **personal information** such as Social Security numbers or account numbers.
- **Be on Cyber Patrol –** Keep your home computer in a central and open location so you can physically monitor your children while they are online. Also remember that young people have many options to connect to the Internet beyond a home computer. Phones, gaming systems, and even TVs have become connected to the Internet. Although these are separate physical systems, malware, viruses, and spyware can be transmitted to your home computer through these devices. Be aware of all the ways and devices your children are using and be sure they know how to use them safely and responsibly. If you have wireless access to the Internet, use the appropriate controls to ensure neighbors or others cannot connect through **your** wireless access point.
  - Consider separate accounts on your computer. Most operating systems (including Windows 7, Vista, Mac OS X, and Unix) allow you to create a different account for each user. Separate accounts can lessen the chance that your child might accidentally access, modify, change settings, and/or delete your files. You can set up certain privileges (the things that can and can't be done) for each account.
- **Lastly… Keep informed –** The online world is ever-changing. New services with great features continually emerge. The Internet has brought the world to your living room, 24/7. While there are endless opportunities with online access, cyber criminals are also working hard thinking up creative ways to compromise your personal information. Keep pace with new ways to stay safe online. Knowledge is power!

Comerica Bank

comerica.com