How Commercial Bank & Trust of PA Protects your Business

A fundamental element of safeguarding your confidential information is to provide protection against unauthorized access or use of this information. We maintain physical, electronic and procedural safeguards that comply with federal guidelines to guard your confidential information against unauthorized access or use. Commercial Bank & Trust of PA will continue to enhance and maintain prudent security standards and procedures to protect against unauthorized access or use of your confidential information.

Security Features

Authentication and device identification at login helps safeguard account information and transactions and enables the bank to verify the authenticity of your activity. This helps reduce risk because even if your password is compromised, a potential fraudster still requires additional pieces of information to access the system.

Auto Logoff

Our system automatically logs you out after a period of inactivity.

Password Control and Lockout

We will temporarily disable your account after too many failed attempts to login. Users will then be locked out of the system. Super Users will have to contact the bank to regain access while Delegate Users will have to contact the Super User to regain access.

Secure Socket Layer Encryption

Commercial Bank & Trust of PA utilizes Secure Socket Layer (SSL) technology to protect your data and transmissions over the internet. This technology encrypts or scrambles the information you provide so it's difficult for anyone other than Commercial Bank & Trust of PA to read it. The SSL protocol continuously verifies the identity of each party during the session, encrypting messages to help ensure they remain private and unaltered.

Control Permissions

Control permissions exist within the system where User's access to payment or transfer activities can be restricted or require approval of the Super User prior to completing.

Commercial Bank & Trust of PA

Business Protection Tips

- Conduct a periodic risk assessment of all electronic banking activities and adjust accordingly. Risk assessments should include, at a minimum, occurrence of threats, actual incidents of fraud, changes in company staffing that affect user access and enhancements in security made by the financial institution.
- Institute a standard for classifying all information. Is it confidential, private, unclassified, etc., and a means to identify which employees, or group of employees have access to this information.
- Determine what websites need to be made available to employees in order to conduct business activities. Consider blocking access to file sharing, social media and personal email sites.
- Ascertain who needs access to your banking systems and services and make sure the removal of access to those services is part of your employee exit process.
- Dedicate a computer to be used solely for all online banking activities. If that is not feasible, restrict the use of personal web browsing, emailing and social networking on any computer used for online banking activities.
- Install and update your anti-virus and anti-spyware software frequently.
- Keep your computer's operating system up-to-date.
- Keep your web browser software up to date by installing the most recent version.
- Install a firewall.
- If you do not recognize the sender of an email or have any doubts about the authenticity of an email, do not respond and delete it immediately.
- Do not open the email or click on links or attachments, especially if they tell you the problem is urgent or the attached file ends in ".exe".
- Always use secure passwords. A secure password consists of upper and lower case letters, numbers and special characters.
- Monitor your account activity closely and watch for unusual activity. You can use Commercial Bank & Trust of PA's Online Banking to monitor account balances, 24/7.
- Consider disabling CD, DVD, and USB drives on all computers where these drives are not needed.
- Consider using programs that scan emails for malicious content.
- Do not allow your employees to download unauthorized software or programs.
- Institute a system of dual controls for critical functions so that no single individual is solely authorized to take action without adequate checks and balance.

More business protection tips can be found on the Consumer Financial Protection Bureau (CFPB) at http://www.consumerfinance.gov/ and on the National Cyber Security Alliance's Stay Safe Online Business Center at http://www.staysafeonline.org/cybersecure-business/.

Commercial Bank & Trust of PA

Unauthorized Transactions

While business customers are not entitled to the same regulatory protections as consumers, you should notify the bank as soon as possible if you discover an unauthorized EFT (ATM withdrawals and transfers, POS purchases made with your debit card, online banking payments, and online transfers on your business account. We will use all commercially reasonable means to help you resolve the matter.

Contact Us

Commercial Bank & Trust of PA encourages you to help us protect your information and to keep your information accurate. If you suspect someone has made unauthorized transactions on your Commercial Bank & Trust of PA accounts, or if you believe that any information about you is not accurate, please call us anytime at 1-800-684-2440.

If you send us an email, we may retain the content of the email and your e-mail address in order to respond to questions or concerns that you may have. Since we cannot ensure our response back to you is secure, we will not include confidential or account information such as account numbers in the response.

When we will contact you

From time to time, the bank may contact you unsolicited via phone call or email to inform you of a system issue, inform you about new products and services, or in an effort to continue to build the relationship. At no time will you ever receive a call or email from the bank asking you for your login credentials. If you receive a suspicious phone call or email asking for your authentication credentials you should decline to do so and call us at 1-800-684-2440.