csb Cambridge
SAVINGS BANK

Protecting Your Information Online— Best Practices:

Security Starts with You.

Strong information security relies on many interconnected elements. The system applications you choose to run within your Network and to access the Internet can affect the security of your data environment. Your company's Security System Administrator plays a critical role in establishing and maintaining the security of your company information assets from threats on the Internet, as well as offline.

Choosing an operating system and security software with the appropriate level of protection will provide the foundation necessary for secure Internet transactions with Cambridge Savings Bank.

In addition to the security inherent in your data system, the administrative security features provided by Cambridge Savings Bank's Business Online Banking allows you to maintain the controls necessary for your daily cash management operations. You have the ability to define authorized user and account restrictions. Your transactions are protected through strong SSL encryption.

Assessing Risk

Different businesses have different levels of risk. Regardless of your company's individual exposure to risk, to avoid reputational and financial risks, the strongest defense includes a powerful offense! Ask your accountant, auditor or legal advisor to assist you in developing a risk assessment program in order to identify specific risk factors for your business.

Pay particular attention to:

- Assets within your organization that are critical to operations or have value to others, including customer records, intellectual property information, system access information, and other sensitive data.

- Potential weaknesses in your business operation. Knowing how you may be vulnerable is the first step to protecting yourself.

Information Security

Cambridge Savings Bank's Business Online Banking application is designed to work with your strong information security practices, to protect data residing on information sources and databases.

To safeguard your data, we recommend that you:

- Develop Information Security policies and procedures that establish guidelines for employees to follow.
- Install Anti-Virus and Anti-Spyware detection software applications, and obtain and install security patches regularly. Establish rules for automatic sweeps of your network to mitigate risks to destructive worms or computer viruses, phishing, pharming and hidden programs to trap keystrokes, User ID and passwords.
- Do not combine "read" and "maintenance" access to single individuals. It is best to segregate these duties.
- Establish efficient PC System Reports that document each user's computer activity.
- Require dual authentication (User ID and passwords).

- Establish strong password “rules” and guidelines - 10 alpha/numeric & special characters is a good rule of thumb (i.e. R{ds0xR#1!= Red Sox are #1!).
- Force password changes every 45-60 days.
- Prohibit the sharing or writing down of User IDs and passwords.
- Require employees to lock terminals when leaving their terminal or workstation.
- Enable screensaver options to force lock of employee PCs after 3 minutes.
- Create and incorporate a Change Management Program (grant, modify, and deny access levels based on job responsibilities, promotion, and termination).
- Specify a maximum of three login attempts. Establishing limitations will prevent unauthorized persons from trying to guess passwords.
- Use fraud detection systems such as *Positive Pay,* an automated fraud detection and reconsolidation tool for businesses that offers secure website access to manage the daily reconciliation of business accounts on a daily, weekly, or monthly basis.

Preventing Fraud

Understanding that fraud can happen in any business will enable you to incorporate security safeguards to reduce your risk. If you become a victim of fraud, you have certain rights and responsibilities. Here are recommendations and resources for what to do and who to contact as soon as you discover something that appears fraudulent.

- **Check or Debit Card Fraud**: If you are a victim of check fraud, call Cambridge Savings Bank’s Customer Contact Center immediately at **888.418.5626**.
- **Credit Card Fraud**: If you are a victim of credit card fraud, call Cardmember Services at the number located on the back of your card.
- **Scams**: If you suspect that something you receive in the mail or a phone call you receive may be a scam artist trying to target you for information, notify your state district attorney and the Better Business Bureau.

Additional resources to protect your business:

U.S. Small Business Administration
800-u-ask-sba (800.827.5722)
www.sba.gov

Federal Trade Commission
202.382.4357
www.ftc.gov

Yellow Pages Publishers Association
800.841.0639
www.yppa.org

U.S. Postal Inspection Service
www.usps.gov/websites/depart/inspect

Better Business Bureau
www.bbb.org

Massachusetts District Attorneys Offices
http://www.mass.gov/mdaa/district-attorneys/offices/