As your business bank of choice, Salem Five is serious about safeguarding your information. We work hard to be certain that our systems are safe, secure and available. As a business owner, you have control over how you manage your account(s), your employees and your transactions with us. Fraud prevention is ultimately easier and less costly when we work as partners in helping your business to be secure and successful.

Security and Fraud Prevention – A common way for businesses to become victims of fraud is when someone who is NOT authorized to perform transactions on behalf of the business obtains credentials that allow the fraudster to log in and complete illegitimate transactions. This is known as "Corporate Account Takeover". It could happen internally (for instance, an employee who illegally creates fraudulent transactions) or externally (a hacker who may plant malware onto your computer and then uses it for fraud). While these are only two examples of security breaches, there are many ways to reduce or eliminate the risk of loss. For example, the most basic safeguards are:

- **Keep your user ID and password private**: Do not be tempted to share your ID's and passwords with anyone.
- **Be unique and change your password**: Create a unique password comprised of upper, lower and numerical characters. Change your password frequently; no less than every 60-90 days.
- **Be different**: Avoid using the same User ID and Password for different online services.
- **Memorize**: Do not write them down or store them on your computer. If you really need to record a password, then use a code system (i.e. transpose letters/numbers) and keep in a secure location.
- **Log Out**: Log out of Online Banking prior to visiting other websites or leaving your computer.
- **Alert Us**: If you notice suspicious or unusual activity in your online banking accounts, please call 800.850.5000

Additionally, there are a multitude of best practices that may be adopted. Each of these enhances the security of your business interactions with us and your customers. For the most part, they fall into two categories; User and Device. Listed below are some considerations that may be useful to you as a business owner:

User Considerations:

- **Training** – Nothing beats training employees to follow safe practices such as those found here. New employee training and follow up training for all employees are keys to success.
- **Dual Control** – Require cash and payment transactions to be handled by two separate people wherever possible.
- **Separation of Duties** – Employees who make payments should not also reconcile accounts.
- **User Limits** – Assign limits to cash and payment transactions.
- **Audit** – Regularly check activity and compare to policies or practices.
- **Reconcilement** – Reconcile accounts as soon as possible.
- **Review** – Statements, cancelled checks, deposit and payment history.
- **Access** – Remove or disable online access for terminated employees.
- **Policies** – Create or amend sound internal policies regarding the safeguarding of information and be certain that policies are communicated and are being followed.
- **Secure** – Secure sensitive information and share only on a "need to know" basis.
- **Restrict** – By policy and practice, restrict users from:
    - Sharing ID's or passwords
    - Clicking on links unknown to them
    - Opening email from unknown sources
    - Installing or removing software unless they are authorized to do so

Device Considerations:

- **Updates** – Keep your device (PC, laptop, tablet, phone, etc.), up to date with system security patches, anti-virus software, etc. Set your security software to scan daily.
- **Firewalls** – Maintain an up-to-date firewall and engage expertise in monitoring activity.
- **Wireless** – If using a wireless corporate network, consider "hiding" it from public view and turn on all appropriate security features. Change the default administrative password immediately upon installation.
- **Data Integrity** – Disable other device access such as USB drives if not needed. Perform reliable backups and test restores regularly.
- **Passwords** – Set parameters requiring strong passwords and frequent changes.
- **Administrative Access** – Only key users should be given administrative access to system connected devices and such access should only be used when necessary.
- **Procedures** – Develop, maintain and train on procedures to be followed when a suspected virus infection or breach occurs.
- **Review** – Regularly review appropriate logs for suspicious activity.
- **Alerts** – To the extent possible, set application alerts to inform you of certain activities. For example, you may wish to be alerted when funds are transferred from an account or when a payment exceeds an established limit.
- **Segregation** – For sophisticated businesses, consider a segregated device to be used solely for transacting business and do not allow web browsing, email, etc. on this machine.

Finally, sound business practices include physical security and vendor management considerations. Best practices for physical security include functioning locks, monitoring and alarm systems, safe data storage (including your backups) and sensitive document shredding. Vendor management practices entail the use of clear contractual language holding vendors to the highest privacy standards, background checks and where appropriate, on-site reviews of vendor facilities.

We take your security as seriously as we do our own. Please do not hesitate to contact us with questions. We're committed to your protection.