



## Online Banking – Protecting Your Business

At Central Valley Community Bank we take your banking security seriously, so we want to share some online banking guidance. Small businesses are frequently targeted by fraudsters because they often have fewer resources to protect their information.

### To Better Protect Your Business We Support the Following Guidelines:

1. Use a computer that has industry standard operating systems such as Windows, Mac OS, etc. Avoid open source, or shareware systems that are not maintained.
2. Keep your computer operating system patched regularly with manufacturer patches to update security for the operating system.
3. Install an industry standard anti-virus software and make sure it is updated regularly.
4. Install and maintain an industry standard email spam filter and malware filter (often included in anti-virus products as a package).
5. Maintain a separate computer for banking and business applications and avoid surfing the Internet or installing game software on the dedicated PC.
6. Install an industry standard firewall between your Internet modem and your home network or PC. If using wireless in your home, make sure to take appropriate measures to maintain security.
7. Use complex formats for passwords on all PC and network equipment. For example, use 8-12 characters, a mix of lower and upper case letters, numbers, and special characters. Do not spell words or names, and do not use dates.
8. Keep all application software updated with the latest releases.
9. Avoid opening any email that is not recognized as valid. When in doubt, delete.
10. Keep security settings at recommended levels.
11. Monitor and reconcile bank accounts daily to recognize fraudulent activity quickly and report unusual transaction activity.
12. NEVER share your password with anyone.
13. Turn off your modem when not using your computer for Internet activity. Reducing the time that your modem is actively broadcasting limits a hacker's opportunity to successfully gain control of it. They can't hack what they can't see. Do the same for wireless access in your home. Only use wireless when necessary. If others in the home are using wireless to surf the web, disconnect the cable to the business computer.

Note: This list is not intended to be exhaustive, or reflect any particular industry standard at this time. Customers using the Internet to conduct online financial transactions do so at their own risk and must recognize that the Internet is inherently vulnerable to unauthorized access and attacks. The Bank disclaims any liability associated with such unauthorized access or attacks and does not make any representations, implied or direct, that the listed precautions will prevent or otherwise protect against the same.