Bank Your Bank of Choice
Owen County State Bank

Online Banking Recommendations
To Prevent Account Compromise

Cyber-thieves can sometimes gain control of a business bank account by stealing the valid online banking credentials of the business through the use of malware. Malware is malicious software (such as a keylogger) that can infect a computer and often spread across the entire business internal network.

To help avoid **Malware** corrupted systems, and to help prevent an account takeover through online banking, Federal guidelines suggest you start with a Dedicated Computer, then Monitor Access Closely.

1. Use a Dedicated Machine
Computers are relatively inexpensive; use a separate dedicated machine for all of your online financial transactions.

2. Turn off Computer When Not in Use
As trivial as this sounds, shut the machine down when it is not in use; this can limit your exposure - many of the modern worms/trojans exploit vulnerabilities in the Windows Operating System, and contrary to popular belief do not require the user to have taken any actions such as opening emails or visiting malicious websites.

3. Monitor Traffic
Implement firewall/proxy instrumentation on both your ingress and egress points, monitoring and logging all traffic to/from your machine to ensure unauthorized access is denied no matter from what point it is initiated. The machine should be used for financial transactions only; all non-business essential network traffic (such as email or internet surfing) should be denied to/from this machine.

4. Regulate Changes
Implement a change management process for any work that is to be done on machines performing financial transactions (this should include any changes to proxy or firewall settings that could impact these machines). Changes must require multiple party approvals. Convenience is not an acceptable reason to open access.

5. Think Virtual
Virtualized environments are another option employees can leverage; the solution can work for multiple employees or employees who travel and who need to perform financial functions on the road. Again, computers are relatively cheap; use a netbook or comparable alternative dedicated exclusively to financial transactions.

Home Office: 201 W. Morgan St., PO Box 151, Spencer, Indiana 47460
Telephone: (812) 829-4811 Toll-Free: (888) 275-6272 Facsimile: (812) 829-3295
Gosport: (812) 879-4218 **Bloomington:** Kings Crossing (812) 935-4811, South Walnut (812) 935-0406
Website: http://www.ocsbank.com **email:** webmaster@ocsbank.com

Online Banking Security Guidelines
For Business And Corporate Customers

These tips and others are available from **www.staysafeonline.org** sponsored by the National Cyber Security Alliance and **www.onguardonline.gov** maintained by the Federal Trade Commission. For more information regarding cyber security, visit the US Computer Emergency Readiness Team at **www.us-cert.gov**.

- Check your account balances and activity on a daily basis. This will lead to early detection of problems and help prevent additional losses if an account intrusion has occurred. Use online banking alerts for account balance triggers.
- Initiate financial transactions (ACH origination, etc) under dual control, with a transaction originator and a separate transaction authorizer.
- Employ best practices to secure computer systems in your workplace.
- Carry out online banking activities from a stand-alone, hardened and completely locked down computer system from which e-mail and Web browsing are not possible. (See “Recommendations to prevent account compromise”.)
- Be suspicious of e-mails purporting to be from a financial institution, government department or other agency requesting account information, account verification or banking access credentials such as usernames, passwords, card numbers, PIN codes and similar information. Opening file attachments or clicking on web links in suspicious emails could expose the system to malicious code (Malware) that could hijack your computer. If an email asks you to click an embedded link to log into an Online Banking site, be skeptical. Use the saved link for that site from your favorites list instead.
- Create a strong password with at least 10 characters that include a combination of mixed case letters, numbers and special characters.
- Prohibit the use of “shared” usernames and passwords for online banking systems.
- Use a different password for each website that is accessed.
- Change the password several times each year.
- Never share username and password information for Online Services with third-party providers.
- Limit administrative rights on users’ workstations to help prevent the inadvertent downloading of malware or other viruses.
- Install a security software suite that includes antivirus, anti-spyware, malware and adware detection, from a reputable vendor. Keep the software up-to-date through an automatic update feature and configure it to perform recurring, automated complete system scans routinely.
- Install commercial, actively managed firewall software on all computer systems. Free software may not provide protection against the latest threats compared with an industry standard product. A firewall limits the potential for unauthorized access to a network and computers.
- Routinely install all new software and hardware patches or use the automatic update feature when available. Ensure that all your software, including your operating system and application software such as Microsoft Office, Adobe Flash, Apple QuickTime, Adobe Acrobat, etc., are updated as well and not just the computer’s operating system.
- Implement block/black lists and enforce them on the network perimeter.
- Always verify use of a secure session (“https” not “http” in the website’s address) in the browser for all online banking.
- Avoid using automatic login features that save usernames and passwords for online banking.
- Never leave a computer unattended while using any online banking or investing service.
- Never access bank, brokerage or other financial services information at Internet cafes, public libraries, etc. Unauthorized software may have been installed to trap account number and sign on information leaving the customer vulnerable to possible fraud.
- Stay in touch with other businesses to share information regarding suspected fraud activity.
- Report any suspicious transactions to OCSB immediately, particularly ACH or wire transfers. There is a limited recovery window for these transactions and immediate escalation may prevent further loss by the customer.