MS-ISAC

*MS-ISAC Security Primer*

# Online Banking Safety

March 2017, SP2017-1322

Cybercriminals target online bank account credentials, as well as information for credits cards and other payment information with malware, such as keystroke loggers, and social engineering tactics, including phishing emails. The Multi-State Information Sharing and Analysis Center (MS-ISAC) is aware of several cases where cybercriminals accessed and stole or attempted to steal large amounts of money from SLTT government bank accounts. In most cases, it is likely that the targets were victims of an opportunistic compromise. Most frequently these attempts involve the use of unauthorized wire transfers, issued by the cybercriminals while using compromised banking credentials. The MS-ISAC provides the following recommendations to assist SLTT governments in developing online banking best practices and mitigating threats posed by financial fraud.

**TECHNICAL RECOMMENDATIONS:**

- If possible, use a virtual machine on a single computer with a static IP address for all online banking transactions, and register this IP address with the financial institution.
  - Actively monitor the computer for viruses and malware.
  - Limit this computer from conducting any other Internet activity, including email access.
  - If you are unable to dedicate a computer for financial transactions, use a virtual machine.
- Use up-to-date anti-virus, anti-spyware, and anti-adware protection software and deploy a firewall.
- Apply appropriate patches and updates to all computers.
- Enable two-factor authentication for access to all financial accounts.
- Install a spam filter and block phishing emails based on known malicious indicators.
- Setup and use a non-privileged user account on the computer to prevent unauthorized changes to the computer. Use this non-privileged account whenever possible.
- Change default login names and passwords on routers, firewalls, and other network equipment.
- Implement block/black lists and enforce them on the network perimeter.
- Monitor log files, especially proxy server logs, for unauthorized or suspicious Internet connections.
- Whenever possible, do not use a wireless network for financial transactions. If a wireless network must be used, enforce security measures such as enabling encryption and MAC address filtering, changing the service set identifier (SSID) and turning off SSID broadcasting.

**USER RECOMMENDATIONS:**

- Immediately report suspicious financial activity to the information technology and/or security departments.
- If the financial institution offers the ability to enable account alerts and/or restrictions, do so.
- Use a unique, strong, complex password for all financial accounts.
- Never use a link to reach the financial institutions homepage; type the bank's website address into the Internet browser's address bar or use a bookmark.
- Be suspicious of emails and text messages allegedly from the financial institution.
- Do not allow the computer or web browser to save login names or passwords.
- Never access a financial institution from a public computer or from an unprotected mobile device.
- Properly log out of all financial institution websites and close the browser window.

The MS-ISAC is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments. More information about this topic, as well as 24x7 cybersecurity assistance for SLTT governments, is available at 866-787-4722, SOC@cisecurity.org, or https://msisac.cisecurity.org/. The MS-ISAC is interested in your comments - an anonymous feedback survey is available at: https://www.surveymonkey.com/r/MSISACProductEvaluation.