NORTHWEST
FEDERAL CREDIT UNION

Online Banking Security Best Practices Checklist

Name of Business: _____

Just as you protect your business's physical location from intruders, your business's computers must also be protected. Business computer hacking has quickly gone from a growing threat to becoming a very common activity.
Business members are contractually obligated to maintain security of their computers and must monitor their accounts pro-actively and frequently. The online banking security best practices checklist will help you see were you stand and what measures you need to take to protect your business's computers.

Computer Security

- ❒ Network/Computer firewall installed
- ❒ Dedicated computer for electronic banking (ie, NOT used for email nor web browsing)
- ❒ Automated Operating System updates
- ❒ Commercial anti-virus software (not freeware), with automated updates and regularly scheduled anti-virus scans
- ❒ Automated updates for third party software such as Microsoft Office, Java, Adobe Reader, Adobe Flash, etc.
- ❒ Limited administration rights on the computer
- ❒ Install malware protection
- ❒ Encrypt sensitive data on computer and storage devices.

Administration

- ❒ Designate a person to handle security and is aware of regulatory requirements and guidance documents regarding data security and reviews the Federal Trade Commission's (FTC) guide for protecting personal information
- ❒ Dual Control (ie, one user creates/edits users, another user approves)
- ❒ Administrators and users with "least privilege" - access to the minimal set of accounts and functions to do their jobs

ACH/Wires

- ❒ Dual Control (ie, oner user creates a transaction, another user approves/transmits/rejects)
- ❒ Transaction Limits
- ❒ Daily Limits
- ❒ Email alerts, to multiple users

Daily Operations

- ❒ Daily reporting/reconciliation of transactions and account balances
- ❒ Train all users on security, safe computer usage, and online banking - examples:
  - Change password every 60-90 days
  - Different passwords for each website
  - Passwords of at least 8 characters, with letters, numbers, and special characters
  - Never share passwords with anyone! **NWFCU staff will not ask for passwords**
  - Do not write password on desk notes
  - Don’t click on suspicious email links
  - Don’t select “save my password” options
- ❒ Train all users on social engineering: hackers gathering information via phone calls, etc, to be used in fraud attempts later