Northfield
SAVINGS BANK

# ONLINE CASH MANAGEMENT BEST PRACTICES

There is no single solution for system security because today's threats come in many different forms and target a wide array of potential weaknesses. Best practices recommend a multi-layered approach to protecting data and systems, frequently referred to as "Defense in Depth." Listed below are a number of basic measures users should implement in order to create a series of protective layers.

| Protective Measure | Description | Purpose |
|---|---|---|
| Firewall | Protect your network from the Internet with a properly configured and monitored firewall. | First line of defense against network attacks from the Internet. |
| Physical Security | Provide physical security for critical network devices, servers, workstations and security tokens. | Prevents tampering, unauthorized access and the physical insertion of key loggers and other hijacking devices. |
| Security Patches | Keep your operating systems current with the latest security updates. Similar steps should be taken to ensure security patches are applied to other software (i.e. Adobe Reader, Java, office suites, Internet browsers, email readers, etc.) | As soon as software vulnerabilities are discovered, hackers begin writing malware to exploit the new vulnerabilities. Staying current on security updates is one of your best defenses. |
| Strong Passwords | A strong password policy should be in place for all users and changed regularly (every 30 days). Encourage pass-phrases or passwords of 8 or more characters that include random characters, special characters, upper and lower case letters and numbers. (Examples: 8rown5hoe, $ummerM0on, 6ot@%53F) | Strong passwords make dictionary attacks and brute force attacks at cracking passwords very difficult. |
| Non-Admin Users | Users should have the lowest level of system privilege to their workstations allowable. Limit the use of administrator equivalent accounts to the task of performing system administration only. | Malware oftentimes relies on the user's security level to install and operate. Not using administrator accounts can limit the risk and damage caused by most malware. |
| Social Engineering Awareness | "Social Engineering" is the art of manipulating people into performing actions or divulging information they would not normally do. It's essentially an attempt at hacking the human element to gain access to information or systems. | By educating staff on the risks of social engineering, you raise awareness and protect yourself from the likelihood of falling victim. Be wary of unsolicited calls posing as bank personnel and making unusual requests or asking confidential information. |
| Virus/Malware Protection | Install a commercial virus/malware protection product and configure to automatically update virus definitions. On-access scanning should be enabled and full scans should be conducted regularly. | This is your last defense of preventing viruses and malware from infecting your computer. |

| Additional Measures for Consideration | |
|---|---|
| Email Access | Because email is a main source of malware and phishing attacks, the PC should not be configured for an email account. If one is necessary, then user training should occur to inform users not to open any emails containing attachments, or from anyone/anywhere that is not required for the eBanking process. |
| Isolated Local Network | Ideally, the eBanking PC should be isolated from any other local area network. Only specific internet access should be allowed as previously stated. If local area network connectivity is required, a firewall should be configured on the PC to only allow access to specific resources such as network printers or internet access proxy servers. |
| Web Browsing | Avoid web browsing on the eBanking PC, especially staying away from social media web sites. Limit Exposure to web sites frequently used to transmit malware. |