SUNRISE BANKS

Security Awareness Partnership

How to Protect Your Business

Sunrise Banks’ top priority is to ensure the security and confidentiality of customer information. The bank implements various processes and technologies that all have the goal of protecting customer information, but accessing banking services via the Internet presents a certain amount of risk which requires a security partnership between Sunrise Banks and its customers.

Below is a list of security tips to help you safeguard your business data.

- **MONITOR EMPLOYEE ACTIVITY** — Limit administrative control on bank accounts and services, segregate duties, and review payment activities daily.
- **UNDERSTAND YOUR INSURANCE** — Meet with your insurance agent to see if any cyber liability coverage is in place or can be acquired. Understand limitations and exclusions.
- **MONITOR YOUR ACCOUNTS REGULARLY** — Look for suspicious transactions and report any such activity to the bank or your credit card company immediately.
- **IMPLEMENT GOOD COMPUTER ANDSYSTEM CONTROLS** —
  - Enable automatic updating for operating systems and applications.
  - Ensure that Anti-virus/Anti-malware software is automatically updating every day.
  - Employ email spam filtering service.
  - Configure email client software so that it does NOT automatically open or display embedded graphics or pictures in email messages.
  - Consider using dedicated cellular MIFI cards for “wireless” internet access if banking must be done from laptops or portable devices.
  - Turn on system auditing and retain log files— consider hiring a consultant to ensure this is occurring properly.
- **DESIGNATE COMPUTERS** — Strongly consider the use of stand-alone PC(s) for banking activities that are NOT used for internet browsing, email, or any other functions.
- **TEST YOUR SYSTEMS** — Consider having Firewall, Wireless, Server and Workstation systems tested to ensure they are configured to operate securely.
- **FOLLOW GOOD PASSWORD PRACTICES** — DO NOT use the same password for banking that you use anywhere else. Make your banking password complex and as long as the system will support and you can remember.
- **PHYSICAL SECURITY OF NON-PUBLIC CONSUMER INFORMATION (NPI) —**
  - Restrict access to NPI to authorized employees who have undergone background checks.
  - Prohibit or control the use of removable media.
  - Use only secure delivery methods when transmitting NPI.
  - Paper documents of NPI are stored in a locked environment.
- **THINGS TO AVOID —**
  - DO NOT perform banking activities from home or on personally owned PCs.
  - DO NOT perform banking activities from public use PCs or kiosks.
  - DO NOT open attachments or links from unsolicited or unexpected email messages claiming “there is a problem with your account” or “there is a problem with your payment”.
  - DO NOT provide information proving who you are (i.e. password, SSN, account numbers) to unsolicited callers or unsolicited email.
- **SIGN-UP TO RECEIVE ESTATEMENTS —** By receiving your statements electronically you reduce the potential for your account information to be compromised by mail fraud.

SUNRISE BANKS

Best Practices

- **BEST PRACTICE TIPS FOR SUNRISE BANKS TREASURY MANAGEMENT PRODUCTS —**
  - Consider implementing use of Dual Control for outgoing ACH files and Wire transfers.
  - Set individual user limits appropriate for the Treasury Management product based on your business need.
  - Notify Sunrise Banks when employees leave your company, so digital access is removed.
  - Banking information obtained for ACH files, Wires and from scanned checks via EZ Deposit are considered non-public information (Ex – Routing & Account Numbers) and should be stored in a secure location.
  - Never leave a computer unattended while using any Treasury Management product – be sure to log-off immediately once you are finished.

- **SUNRISE BANKS ACH ORIGINATION —**
  - When sending an ACH file to debit a consumer (ex – employee, customer) you must have their written authorization for the debit entry before initiation of the ACH file. This authorization needs to be retained by your company for the life of the ACH debit entry(s), and upon termination of the entry(s), for a period of two years.
  - Please be prepared to provide a copy of the consumer written debit authorization to Sunrise Banks if requested. Per National Automated Clearing House Association rules; the individual, business and/or their financial institution can ask to see proof of this authorization.
  - Consider the use of templates for recurring ACH files to ensure recipient information remains consistent and file entry is limited to payment or collection amount.

- **SUNRISE BANKS EZ DEPOSIT —**
  - Practice separation of duties: Person opening mail is not person preparing, scanning and transmitting deposit to bank nor person reconciling the deposits.
  - Once checks have been scanned, use commercially reasonable methods to securely store all checks for a period of 60 days until they are destroyed. (This might include locked file/drawer or cabinet. Treat checks as cash.)
  - Shred and dispose of checks in a secured container.
  - Consider placing the computer that has EZ Deposit installed on it in a secured area where customers and/or vendors don't have access to it.

- **SUNRISE BANKS WIRE TRANSFER —**
  - Consider the use of templates for recurring Wire transfers to ensure recipient information remains consistent and file entry is limited to payment amount.
  - Set individual user limits for Wire transactions based on your business need.

At Sunrise Banks, we want to make sure that your business data remains safe. If you would like to learn about additional products and services that can help your business stay protected, contact us today at 651-265-5640.