Kennebec Savings Bank

Best Practices for Business Banking Security

Safeguarding your accounts is a top priority for Kennebec Savings Bank. We assign unique usernames and passwords, provide security tokens and multi-factor authentication (MFA) options, establish limits for Automated Clearing House (ACH), Remote Deposit Capture and Wire transactions, and monitor for suspicious login and file activity to help protect you and your data. However, despite our best efforts, we cannot control what is most often the initial point of compromise – the computer you use and the staff who process your transaction activities.

Review the checklists below and implement best practices to strengthen your security posture. You can also visit the resources on Kennebec Savings Bank's website for more tips and information at www.KennebecSavings.Bank/Security.

Prepare Yourself and Your Team

- ☐ Attend regular training regarding security best practices. Resources and webinars are available from consultants, vendors, and Kennebec Savings Bank. Helpful topics include creating secure passwords, using MFA and avoiding scams and fraudulent emails.
- ☐ Build a culture of verification. Employees must understand their role and responsibility in preventing fraud losses. Value and positively reinforce staff who take the time to question and report suspicious activity.
- ☐ Establish internal procedures and controls. A few "must have" guidelines include:
  - Acceptable use of work devices, including defining who can download and install software and documents. Limit computer use to work-related activities and avoid personal email use on business-owned devices.
  - Authorities, limits and accountability for dual control and signoffs, especially with transaction processing.
  - Expectations for verifying ACH, wire and other payment requests and instructions. It is common practice to call a known number or contact person to confirm instructions, especially when received via email.
- ☐ Do not share passwords and logins. Using the same password across several logins leaves you vulnerable if there is a compromise. Secure password management solutions may help employees track multiple logins.
- ☐ Review, update and retrain on your procedures at least annually, as well as anytime there is a change in staff (employee leaves or joins the team).
- ☐ Consider adjustments to policies and procedures for remote workforce, such as limiting access to financial systems to in-office employees.

Protect Your Systems & Exercise Caution with Email

- ☐ Assess the measures you have in place to safeguard against unauthorized access to the computers used for online banking activities.
- ☐ Question the authenticity of every email and do not open attachments or click links if the sender is unknown or unfamiliar. Fraudulent links and attachments in emails are a popular way for scammers to infect your computers, obtain access to your network, and contact your staff. Assess wither current anti-spam email tools should be strengthened.
- ☐ Install and regularly update software, firewall, malware and antivirus protection on your systems.
- ☐ If possible, avoid accessing financial services websites (such as online banking) on open Wi-Fi networks.

Protect Your Account Information

- ☐ Review account activity daily if possible and immediately report unusual or unauthorized transactions, as there is a limited recovery window for recovering funds. Leverage reporting and alerting tools from online banking as well as Positive Pay services.
- ☐ Restrict online account access to authorized personnel, and segregate responsibilities among different employees for payment, approval, deposit, and reconciliation activities whenever possible.
- ☐ Periodically review access rights and capabilities of key employees, and update Kennebec Savings Bank as soon as possible if you need to change online account access.
- ☐ Store check stock, signature stamps, monthly statements, online banking tokens and other account-sensitive items securely and with access control.

Use Your Resources

- ☐ Contact Kennebec Savings Bank as soon as possible if you have concerns regarding your accounts or online banking access. We can assist you with navigating challenges, disabling access, and updating signers.
- ☐ Obtain insurance to protect you against fraud losses.
- ☐ Bookmark and reference key industry resources for training, education and reporting incidents:
  - FBI Scams & Safety: https://www.fbi.gov/scams-and-safety
  - FBI's Internet Crime Complaint Center: https://www.ic3.gov
  - Financial Crimes Enforcement Network: www.fincen.gov
  - Your local payments association (NEACH): www.neach.org