Security & Account Protection

Skowhegan Savings Protects You

ONLINE BANKING

In order to make our customer's online banking experience as secure as possible, Skowhegan Savings assigns unique user IDs/passwords, uses Multi-Factor Authentication and a security watermark feature (personal image). Multi-Factor Authentication will detect uncharacteristic activity or unusual behavior and when detected will prompt the user to answer security questions that are configured at initial enrollment. The personalized security watermark feature provides visual confirmation that the customer is logging into the authentic Skowhegan Savings' Internet Banking website. Customers are reminded about the importance of maintaining password confidentiality. Also, customers should regularly review their account statements.

We offer a variety of online security features:

PERSONAL SECURITY QUESTIONS

For your protection and to keep your accounts more secure, at one of your initial logins we will ask you to choose and answer Personal Security Questions. During future online sessions, we may ask you to answer these questions as added security to validate the identity of the individual attempting to access your Online Banking. Please choose answers that you will remember. Incorrectly answering questions can lead to your online account access being blocked and you will need to call customer service for assistance at 800.303.9511.

PERSONAL SECURITY IMAGE

We have enabled a Watermark security feature as an anti-phishing measure. At your initial enrollment, customers are prompted to select a picture from a vast library of images. Each time you login, verify the image is your selected Personal Identification Image before entering your password. If it is not your image DO NOT enter your password and contact customer service. This image will also display at the bottom of all Online Banking pages to validate that the customer is still genuinely connected to Skowhegan Savings' Online Banking.

SECURE TOKENS

For added security, secure tokens are available with the use of Online Banking. Business customers with ACH, Wires or Remote Deposit services are required to utilize secure tokens, however tokens are available for any customer interested in this added layer of security. (Fees may apply.) Secure tokens are issued and assigned to specific Online Banking access IDs. For active token users, online access is not granted until after successful entry of a user's ID, password and access code displaying on the assigned token.

AUTO LOGOFF

Users should immediately exit Online Banking when finished, however for added security, sessions will be automatically terminated after a period of inactivity to protect customer accounts and details.

DAILY MONITORING

Online Banking activity is monitored. Activity deemed out of routine for a customer, or trends of suspicious activity are detected and evaluated. When appropriate, customers are contacted to confirm if specified Online Banking activity is genuine. For security and account protection, blocks may be placed on Online Banking access until the unusual activity is verified.

ONE TIME PASSCODES

Additional user authentication may be required for certain higher risk Online Banking transactions. One time passcodes via text message will prompt immediately upon entry of a risk identified transaction to further protect customer accounts. Failure to enter the generated passcode will cancel the requested transaction.

ACCOUNT ACTIVITY ALERT MESSAGES

Customers should consistently monitor their account balances and activity. To make this even easier, we offer a variety of alert notifications. Customers select which notifications to activate, along with their desired method(s) of receiving notifications. Notifications may be generated to customers via email, text message or upon next Online Banking login session.

DEBIT CARDS

At Skowhegan Savings, our job is to take care of your money. To ensure that your funds are safe from fraud, we have an innovative service to help protect your ATM and debit card day and night. The service uses intelligence technology and a team of skilled fraud analysts. This service is completely free of charge, and it allows monitoring of your ATM and debit card transactions around the clock to protect you against fraud.

If at any time suspicious transactions are detected, a Risk Management specialist will contact you immediately. If fraud is confirmed, your card will be disabled. If you aren't available, your card will be assigned a 'watch' status until we know that all is well.

Protect Yourself

For the best security and protection, please follow the below guidance with regard to general account information and specific products or services connected to your personal and/or commercial accounts.

- Do not share your account number.
- Properly store or destroy your bank statements and account documents.
- Monitor your accounts regularly.
- Immediately report any unusual account activity.
- Keep your address and phone number up to date in case we need to contact you.
- Commercial customers should perform risk assessments for their business to gain awareness of the risk and threats to their confidential information or operations. Necessary internal controls should be established to mitigate as much risk as possible.

ONLINE BANKING

Skowhegan Savings takes many measures to protect your accounts and personal information, but it is important that you also safeguard this information. We will never email you asking for your personal information. Any email claiming to be the bank requesting personal information such as your social security number, IDs, or passwords should not be trusted or opened.

- Use complex passwords, with alpha-numeric and special character combinations
- Do not write down your password.

- Use a different password to access your online accounts than the ones you use for other applications.
- Always exit your Online Banking session before leaving your computer.

Keep your account safe and secure by using only trusted devices to access Online Banking. Be cautious of public internet connections. A combination of protective measures should be taken, including anti-virus software, anti-malware software, firewalls and secured internet connections.

COMMERICAL ONLINE BANKING

Commercial Online Banking users should take additional measures to safeguard their accounts and information.

- Utilize secure tokens. (This service is available for any commercial customer, however is mandatory for any online ACH, online Wire or Remote Deposit Capture users.)
- Activate permission controls specific to each user to minimize access to unnecessary accounts, information or transaction types.
- Utilize access time controls to prevent users from accessing accounts outside of normal business hours.
- Utilize IP restrict feature to prevent users from accessing accounts outside of your business office.
- Suspend user access when users will not require access for periods of time, such as vacations, sick days, etc.

MOBILE BANKING

At Skowhegan Savings we are very concerned about your security, no matter how you access your accounts. With mobile banking services available, we want to take a moment to share some important safety suggestions to help you avoid mobile banking fraud.

- Any time you login to Mobile Banking, be aware of the people around you. Don't disclose personal information, including account numbers or social security numbers, if someone else can read your screen or hear your voice.

- Always secure your phone with a password to prevent unauthorized access. It may be a bit of a hassle, but if your phone is ever lost or stolen, you'll be glad you took this extra precaution.

- Be sure to logout completely every time you finish a Mobile Web Banking session. This will prevent someone from having easy access to your information if they gain access to your phone.

- Don't save any financial or personal information on your phone, including PINs and Online Banking login information. If you lose your phone, not only have you lost that information, but it could fall into the hands of someone with bad intentions.

- Some web browsers have an "auto-fill" function that remember your username and password, and pre-fill these fields for you the next time you login. If you are prompted, tell your phone NOT to remember or auto-fill this information.

- Beware of third-party applications ("apps") for your phone. There are some programs that you can download that claim to organize your various online banking accounts or other passwords. Many of these are basically phishing scams designed to steal your information and send it to fraudsters.

- If you do lose your phone and you are worried about your Online Banking information being compromised, login to your account from another computer and change your password right away. If you can't get to a computer, call customer service at 800.303.9511.

- If you use Skowhegan Savings Mobile Text Banking, know that we will never send you an unsolicited message or ask you for a password or personal information via text. If you get a message requesting such information, do not respond.

- Periodically delete your archived Mobile Banking text messages.

- Being cautious when using Skowhegan Savings mobile banking doesn't take any extra time and will help minimize that you never have to worry when checking your accounts with your phone. If you have questions about accessing your Skowhegan Savings accounts on your phone, call customer service at 800.303.9511.

DEBIT CARD

For the best security and protection, please note the following tips for your debit card:

- Be certain to sign the back of you card immediately when received.
- Keep your Personal Identification Number (PIN) confidential and do not write it on your card.
- Use ATMs wisely. Always be alert and aware, especially in unfamiliar surroundings or at night.
- If your card is ever lost or stolen, please notify us immediately.

Fraudulent or Unauthorized Activity

CONTACT US

Skowhegan Savings' customer service team is available by calling 800.303.9511, by email at customerservice@skowheganssavings.com or by instant live chat through our website. Customer service is available M-F 8:00am-5:00pm and Saturday 8:30am-12:30pm. Any time you have concerns about your account, please contact us.

LOST OR STOLEN ATM/DEBIT CARD

When your ATM or Debit card is no longer in your possession, it must be cancelled to protect your account. If your card is lost or stolen, please call us at 800.303.9511. If you call after normal business hours, follow the menu prompt to cancel your card. Your call will be redirected to our service provider to ensure your card is cancelled immediately.

UNAUTHORIZED ACCOUNT ACTIVITY

If you notice an unfamiliar transaction on your account, please contact us immediately. Whether it is a debit card, ACH or in branch transaction, you must report the transaction timely. We will guide you through researching the transaction and disputing if necessary. Please call us at 800.303.9511 or visit a local branch office.

WE MAY CONTACT YOU

ONLINE BANKING

If we detect unusual Online Banking activity, we may contact you to confirm if the activity is genuine. For your protection, online access may be blocked until we reach you. Read more about this service and how "Skowhegan Savings Protects You" in the previous section.

DEBIT CARDS

Our risk management team monitors debit card activity 24 hours a day. If materially unusual transactions are presented against your card, we will connect with you to confirm if the transaction is genuine. If we cannot reach you, to protect your account your card may be blocked until we can. Read more about this service and how "Skowhegan Savings Protects You" in the previous section.

External Resources

IDENTITY THEFT

Not sure what to do if you've been a victim of identity theft? The Federal Trade Commission provides step by step instructions to guide you through reporting and recovering from identify theft. Visit their webpage at www.identitytheft.gov.

CREDIT REPORT

Detect identify theft quickly by monitoring your credit report regularly. You are entitled to one free credit report each year. Visit www.annualcreditreport.com for credit report information or to request a free report.

FDIC

Learn more about the Federal Deposit Insurance Corporation (FDIC) and your account coverage by visiting www.fdic.gov.

FFIEC – Consumer Help Center

The Federal Financial Institutions Examination Council (FFIEC) offers a Consumer Help Center at www.ffiec.gov. This council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB) and to make recommendations to promote uniformity in the supervision of financial institutions.