EAST WISCONSIN
SAVINGS BANK

Protect Yourself from Fraud

At East Wisconsin Savings Bank, your security is important to us. We're your partner in protecting what matters most by staying vigilant against fraud and scams.

Common Fraud Prevention Tips

Never Share Sensitive Information
We will never call, text, or email asking for:

- Online banking passwords
- Debit card PINs
- Full Social Security numbers

If someone contacts you requesting this information, hang up and contact the bank directly.

Be Suspicious of Urgent Requests
Scammers often create a sense of urgency by claiming:

- Your account will be closed
- A payment is overdue
- Your account has been locked
- You must act immediately to avoid penalties

Take a moment to verify the request before responding.

Watch for Phishing Emails and Text Messages
Before clicking any links:

- Verify the sender's email address
- Watch for misspellings or unusual wording
- Avoid opening unexpected attachments
- Navigate directly to known websites instead of using links

Monitor Your Accounts Regularly
Review your accounts frequently for:

- Unauthorized transactions
- Address changes you didn't request
- New accounts you didn't open
- Debit card purchases you don't recognize
- Report suspicious activity immediately.

Be Cautious with Phone Calls
Scammers can make phone numbers appear legitimate. If someone claiming to be from the bank requests sensitive information:

- Hang up.
- Call the bank directly using a trusted phone number.
- Verify the request by calling us directly before providing any information.

Protect Your Devices
Keep your devices secure by:

- Installing software updates promptly
- Avoiding public Wi-Fi for financial transactions
- Locking devices with passwords or biometrics

EAST WISCONSIN
SAVINGS BANK

What To Do If You Think You've Been Compromised

Step 1: Contact the Bank Immediately
If you believe your account or personal information may have been compromised, contact us as soon as possible. Notify us immediately if:

- You notice unauthorized transactions or account activity.
- Your debit card has been lost or stolen.
- You shared account information with a suspected scammer.
- You provided your online banking username, password, or verification code to an unauthorized person.

The sooner we are notified, the sooner we can take steps to secure your accounts and help minimize potential losses.

Step 2: EWSB Action
Once we are alerted to suspicious or fraudulent activity, we will take immediate action to help protect your accounts and personal information. Depending on the situation, we may:

- Restrict, freeze, or close affected accounts while allowing approved credits, such as payroll deposits, to continue when appropriate.
- Review recent account activity for unauthorized transactions, transfers, bill payments, external account links, scheduled payments, or newly added payees.
- Verify all account contact information to ensure email addresses, phone numbers, mailing addresses, security questions, and other profile details have not been altered by a fraudster.
- Reset and issue new online banking credentials, including a new username and password, when necessary. We may restrict online banking access until device is safe to use.
- Work directly with you to determine what information may have been compromised and discuss any additional protective measures that may be needed.

Step 3: Secure and Stay Vigilant
After your accounts have been secured, it's important to address the source of the compromise and take steps to prevent future incidents.

- Before restoring online banking access, ensure any affected computers, tablets, or mobile devices have been properly secured. If a fraudster gained access through a compromised device, simply changing passwords may not be enough. Malware, remote access software, or keylogging programs can continue to capture sensitive information. Professional scanning, cleaning, or reimaging of the device may be recommended.
- Continue monitoring your accounts and credit reports for unusual activity. Even after an issue has been resolved, fraudsters may attempt additional scams using information they previously obtained.
- Change passwords regularly and use unique, strong passwords for your financial and email accounts. Whenever available, enable multi-factor authentication.
- Stay alert for phishing emails, fraudulent websites, suspicious text messages, and unexpected phone calls. If something doesn't seem right, trust your instincts and contact us directly before taking action.