-Alert Message-

× THINK BEFORE YOU CLICK!!! Don't be a victim of FRAUD or RAMSONWARE. Scammers are trying hard to steal your information. NEVER click on links provided in an email or text message. NEVER give out your personal or banking information. When in doubt, STOP and call us at 608-929-4515. We are here to help!

HIGHLAND STATE BANK

Online Banking

Login Enroll | Forgot Password

Toggle navigation

- Checking
- Home
- Savings
- Lending
- Wealth Management
- Resources
  - Helpful Links
  - Cyber Security
  - eStatements
  - Debit Card Replacement
  - Change of Address Form
- About Us
  - Our History
  - Hours and Location
  - Contact Us
  - Community Reinvestment Act Public File

Cyber Security

- Print Format
- PDF

Resources Cyber Security

Important Notice

We will never request personal or account information from you by email or telephone. In addition, our regulators or insurers will never call you to “verify” your information or to “confirm” our records. We will also never ask you to enter your account number, PIN number or any other information in a form provided in an email. If you receive any such requests, do not respond, and contact us immediately.

If you are an online banking customer, never reveal your password or PIN to anyone. If you feel the security of your password has been breached, contact us immediately.

Protect Yourself From Identity Theft

Identify theft occurs when someone uses your personal information, such as your name, social security number, account number or other identifying information without your permission. Identity theft is a serious crime. People whose identities have been stolen can spend months or years cleaning up the mess thieves have made of their good name and credit record.

If you think your identity has been stolen, here’s what to do now:

- Contact the fraud departments of any one of the three major credit bureaus to place a fraud alert on your credit file. The fraud alert requests creditors to contact you before opening any new accounts or making any changes to existing accounts. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will be automatically notified.
- Close the accounts that you know or believe have been tampered with or opened fraudulently. Use the ID Theft Affidavit when disputing new Unauthorized accounts.
- File a police report. Get a copy of the report to submit to your creditors and others that may require proof of the crime.

- File your complaint with the FTC. The FTC maintains a database of identity theft cases used by law enforcement.

Beware of Unsolicited “Phoney” Emails

Be cautious of emails and web sites coming from parties pretending to be real companies that request personal or financial information. Customers are led to believe the request is from the real company when it is in fact a malicious attempt to collect customer information for the purpose of committing fraud.

Tips to help you:

- Never provide sensitive personal or financial information in response to an email.
- Look for misspelled words.
- If the email requests that you click on a link provided in the message, do not click it because it may take you to a fraudulent site. Instead, type the company’s web address in the address bar. When the site opens, look for messages regarding fraudulent messages and scams that have been brought to their attention.

Routing Number

- 075905554

NMLS Number

- 402232

Contact Us

P.O. Box 286
541 Main Street
Highland, WI 53543
(608) 929-4515

Quick Links

Copyright © Highland State Bank. All rights reserved.