BNH
Bank of New Hampshire

Fraud Prevention *starts with you.*

At Bank of New Hampshire, your security is our top priority. Fraud is becoming more common and scammers are using new tricks to target people every day. It can happen to anyone, even when you're careful.

The good news is there are simple steps you can take to stay safe. By staying informed, watching for warning signs and using trusted tools, you can greatly reduce your risk. This guide will walk you through practical tips to help keep you and your information protected.

Look for .bank *to Stay Safe.*

Bank of New Hampshire's official website domain is **BNH.Bank**. These domains, also known as website URLs, are exclusively reserved for verified financial institutions. (Dot)Bank domains ensure legitimacy and help protect you from scams and fraudsters.

VERIFIED WITH .Bank

www.bnh.bank ✓

www.bnh.com ✗

Common Scams *to be Aware of*

Spoofed Website Alert
Scammers create fake bank websites to steal login info. Always type your bank's web address directly and use caution with search engine links.

Romance Scams:
Fraudsters create fake relationships to manipulate victims into sending money.

Phishing & Smishing Scams:
Fake emails or text messages designed to look like they're from trusted organizations asking you to click on a link and provide personal information.

Refund or Overpayment Scams:
Scammers may claim you're owed a refund or say you overpaid, then ask for account access or a return payment. Do not send money or share info.

Cryptocurrency Scams:
Scammers may pressure you to deposit money into a crypto ATM. No legitimate business will ever ask for payment this way.

Fake Check Fraud:
Scammers issue fake checks that look real and try to deceive you into accepting them as payment.

Business Email Compromise (BEC):
Cybercriminals impersonate trusted partners or executives and request wire transfers or sensitive information.

Social Media Scams:
Scammers impersonate friends or family members on social media to ask for money or gifts.

Fraud tactics change fast
Visit our Fraud Prevention page for the latest updates.

Revised 01.09.2025

BNH Mobile Banking Tools *for Businesses & Consumers*

PositivePay for Business

- Submit a daily file of issued checks
- Checks are validated by check number, amount and payee name
- Discrepancies are flagged for your review
- Helps detect check fraud as it happens

ACH Filter for Business

- Detects unauthorized ACH transactions
- Lets you set custom rules for debits & credits
- Improves account control and visibility
- Helps reduce fraud losses and processing delays

BNH Mobile Banking App for Everyone

- **Account Alerts:** Get real-time notifications for account activity.
- **eStatements:** Access paper-free statements.
- **Two-Factor Authentication:** Strong login security for all authorized users.

GET IT ON Google Play

Download on the App Store

BNH Card Control App for Everyone

CardControl

- Instantly lock or unlock your card
- Get real-time transaction alerts
- Set spending, location and merchant controls
- 24/7 fraud monitoring and support
- Control international transactions anytime

GET IT ON Google Play

Download on the App Store

Fraud Tips *to Remember*

1. Do not allow anyone to access your computer.
2. Keep your online banking credentials and secure access codes private.
3. Stay aware of phishing emails and unexpected links.
4. Do not act on urgent requests. Scammers prey on stress responses and quick negligent actions.
5. Send sensitive information only through encrypted email or secure fax.
6. Always use a password manager to keep your login credentials secure.
7. Use a unique password for every account.
8. Enable Multi-Factor Authentication when possible.
9. Don't access sensitive information or complete transactions on public or unknown networks.
10. Secure and shred sensitive documents.
11. Stay up-to-date on the latest trending scams and spread the word to friends and family.
12. Review recurring payments regularly for unexpected changes.
13. Monitor account activity regularly using the BNH Online Banking desktop site or mobile app.
14. Always log out of your accounts after each session, especially on shared or public devices.
15. If something feels off: First, stop. Then, call BNH, a family member or the police.

You've got people.

BNH.Bank | 1.800.832.0912 | Member FDIC

What to Do *if You Fall Victim*

Call the Bank right away to report suspicious activity and lock or freeze your card if needed using the BNH CardControl app.

Update passwords and security credentials for your online banking and any related accounts.

Review recent transactions carefully and note any unauthorized charges.

Keep records of evidence such as emails, texts and screenshots for investigations.

Report to authorities like the FTC or local police and continue monitoring your accounts closely.

Where to Turn *for Support*

BNH Fraud Prevention Page
Tips to help you recognize, avoid and report scams
800.832.0912 | BNH.Bank/fraud-prevention

NH Financial Abuse Specialty Team (NH FAST)
Scam & elder abuse prevention
888.397.3742 | stayconnectednh.org

NH Bankers Association
Fraud prevention guides
603.224.5373 | nhbankers.com

American Bankers Association® | Banks Never Ask That
National scam awareness campaign
800.226.5377 | aba.com | banksneveraskthat.com

AARP Fraud Watch Network
Tips, alerts and guidance for all ages
877.908.3360 | aarp.org/money/scams-fraud