At Bank of New Hampshire, we pride ourselves on keeping your money and information safe, and we need your help to do this most effectively!

With instances of fraud becoming more widespread, it is important that you understand what you can do to keep your money and information safe. Fraud can happen at any time to anyone, and we know that losing money to fraud can be devastating.

Steps you take today can help prevent you from becoming a fraud victim, and protect you from more severe impacts if you do become a fraud victim.

Bank of New Hampshire

BankNH.com **1.800.832.0912**

Rev 4/21

FRAUD PREVENTION

Bank of New Hampshire

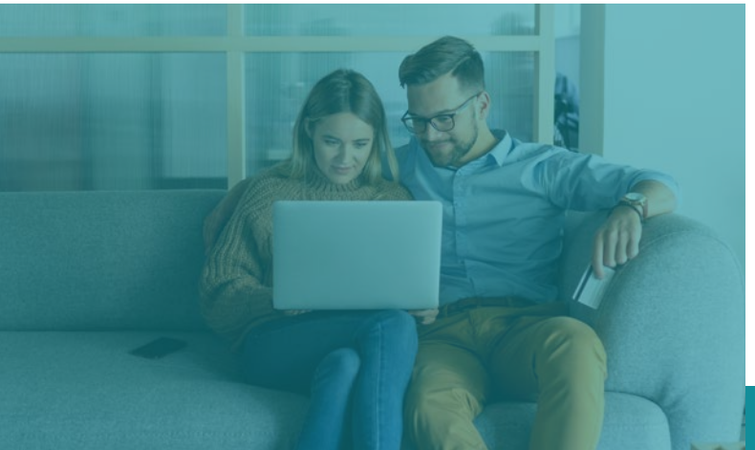
BEST PRACTICES AND TIPS TO PREVENT FRAUD

NEVER

- Allow access to your computer.
- Click on an unknown link or email that you were not expecting.
- Access important information or complete transactions on public/unknown networks.
- Use the same password more than once if you use a password manager.

ALWAYS

- Monitor account activity regularly using online banking.
- Be suspicious of ACH activity from unknown parties.
- Keep your login credentials secure and confidential.
- Send sensitive information securely through secure/encrypted email or fax.
- Use caution when giving out information over the phone.
- Monitor accounts for suspicious activity.



INSTANCES OF FRAUD AND STEPS TO TAKE

LOST/STOLEN DEBIT OR CREDIT CARD

- Report lost/stolen card to the creditor/bank and request the card be closed.
- Review your account for suspicious activity and report to the creditor/bank.
- The creditor/bank may request that you file a police report.

COMPROMISED COMPUTER

- Report the situation to your bank.
- Bring your computer to a technician that can clean your computer of any malware or viruses that it may have been infected with.
- Change all account passwords after your computer has been cleaned.
- Review your account for suspicious activity and report to the creditor/bank.
- The creditor/bank may request that you file a police report.

COMPROMISED BANK ACCOUNT

- Notify creditor/bank of suspicious activity and request to freeze or close the account to cease the unauthorized use of your account.
- The creditor/bank may request that you file a police report.

IDENTITY THEFT

- Maintain a written chronology of steps you took, the date, the time, contact telephone numbers, person you spoke to and any relevant reports, reference numbers and instructions.
- Notify all affected creditors or banks.
- Contact the three major credit bureaus and request a copy of your credit report.

EQUIFAX
Equifax.com/personal/credit-report-services
1.800.685.1111

EXPERIAN
Experian.com/help
1.888.397.3742

TRANSUNION
TransUnion.com/credit-help
1.888.909.8872

- Review report for suspicious activity and request that your credit be frozen.
- If your license or SSI card was stolen, replace your stolen identification.
- File a police report with your local department and keep a copy for your records.
- Change all account passwords.
- Contact your telephone and utility companies.
- If you have been victimized by an internet scam, report it to the internet Crime Complaint Center online by going to www.ic3.gov or by calling 1.800.221.4424.
- File a complaint with the Federal Trade Commission (FTC) at www.ftc.gov.