Direct Financial®

Digital Banking

Safety and Security

Protecting You and Your Account

Direct Financial uses cutting-edge security technologies to safeguard your online transactions and personal information.

CONSUMER PROTECTIONS UNDER REG E

As a NEFCUOnline user, you have the advantage of being able to log in to your Direct Financial accounts on a regular basis to monitor activity.

In the event that you detect a fraudulent and/or unauthorized transaction, the consumer protections provided under Reg E can help you limit your liability and recover losses according to how soon you report them.

Notify us AT ONCE by:

- **Calling:** 800.400.8790
- **Writing:** NEFCU
  141 Harvest Lane
  Williston, VT 05495

You must notify us within 60 days after the fraudulent and/or unauthorized transaction first appears on your statement.

For more information, including your security responsibilities (ie. control and confidentiality of your password), please refer to the Electronic Fund Transfers Disclosure.

What WE Do to Secure Your Account

Direct Financial is dedicated to protecting your account information and we maintain physical, electronic and procedural safeguards that comply with federal regulations. We have taken many precautions to ensure your information is secure when you use online or mobile banking services including, but not limited to:

ENCRYPTION

Encryption protects your information while it is in transit between your browser and our servers. The data is changed into code and "scrambled" making it nearly impossible to read or alter. NEFCUOnline uses 128-bit Secure Sockets Layer (SSL) protocol to ensure that your connection and any information transmitted is protected.

USERNAME AND PASSWORD PROTECTION

NEFCUOnline requires a strong username and password to protect your account. Alternatively, biometric authentication (Touch ID, Fingerprint ID and Face ID) is available on the NEFCU Mobile App. For added security, if there are too many invalid authentication attempts, your account access is automatically locked.

MULTIFACTOR AUTHENTICATION

NEFCUOnline uses an extra layer of security beyond the username and password to protect against fraud and identity theft. Access is only possible from devices that you have registered and linked to your accounts, or by using a one-time secure access code delivered to you via text, phone or email. You are in control of which computers and mobile devices are allowed to access your accounts, and no access is allowed without using either a registered device or a one-time secure access code.

SESSION TIMEOUT

After a period of inactivity (20 minutes for online banking and 5 minutes for mobile banking), your session will automatically timeout. This feature keeps others from viewing or continuing activity if you leave your device unattended.

LAST VISIT DATE

By displaying the last visit date, you can easily monitor usage of your account. As an additional safety precaution, your account access will be disabled if you haven't logged in to digital banking in the past year.

What YOU Can Do to Secure Your Account

Direct Financial takes numerous steps to keep your accounts and personal information secure, but you also play a vital role in maintaining the security of your banking information. Here are some things you can do to help keep digital banking safe and secure.

ONLINE SECURITY BEST PRACTICES

Use a secure browser and trusted computer.

- Install real-time antivirus and antispyware protection and allow for automatic scanning and updates.
- Install security updates to operating systems and all applications as they become available.
- Install a personal firewall and secure wireless networks.
- Disable autoplay to prevent the launching of executable files.
- Disable file sharing if it is not needed.
- Do not use computers accessible to the public to conduct transactions online.
- Do not reply to or click on any links in unsolicited emails.

Create a strong password and keep it confidential.

- Create a different password for all the different systems you use.
- Use unpredictable passwords with a combination of letters, numbers and special characters.
- Never use birth dates, first names, pet names, addresses, phone numbers, or Social Security numbers as your password.
- You shouldn't use the "remember password" feature of a web browser for online banking or transactional Web sites.
- Never share your password or login information with anyone.

Logout, disconnect and shut down.

- Always logout from online banking or any other Web site that you've logged into with a username and password.
- Do not leave your computer unattended while logged in to online banking.
- When a computer is not in use, disconnect it from the Internet or shut it down.

MOBILE SECURITY BEST PRACTICES

Maintain physical control of your mobile device.

- Enable your mobile device's screen lock and passcode.
- Keep the device with you or secure the device when not in use.
- Consider utilizing a "remote wiping" service that, in the event your mobile device is lost or stolen, provides the ability to remotely erase all of its data.
- Delete all information stored on a device before the device changes ownership. Use a "hard factory reset" to permanently erase all content and settings.

Keep your mobile device updated.

- Set your device to install app and system updates automatically, if possible. These updates often include security fixes.
- Do not hack, 'jailbreak' or modify the device as it may disable important security features.
- Only download applications from trusted sources (such as the App Store or Google Play). Review the privacy policy and data access of any app before installing it.

Use your mobile device securely.

- Use trusted networks. Connecting your device to unknown wireless networks can expose your data. Switch to your cellular data plan to access online banking.
- Disable features not actively in use such as Wi-Fi and Bluetooth.
- Avoid links from unknown sources including emails and social media posts.
- Never store usernames and passwords on the device.
- Always logout when finished with an app rather than just closing it.

If you have any questions, contact a Member Service Representative using our Live Chat option in online or mobile banking, or call us at 800-400-8790.