

NMEFCU Online

Our cyberbranch@home Online Guarantee

Accessing your account online shouldn't be a frightening experience. We want you to feel safe and secure every time you use the NMEFCU cyberbranch@home online services. That's why we've built a security system around NMEFCU's cyberbranch@home that safeguards your money and keeps your account information private.

We are confident of the security of our online account access. But you may still have concerns about the security of this new way to access your account.

Our Promise to You

If an unauthorized transaction was conducted on your account because of a breach on the NMEFCU data network, or as a result of data that was intercepted in conjunction with any transmission while you were connected to the NMEFCU cyberbranch@home online application, your liability on those unauthorized transactions will be zero (\$0.00). In the case of NMEFCU cyberbranch@home, the NMEFCU data network is defined as the point from your modem connection on the Internet to the final system on which a given transaction is accessed and stored at NMEFCU.

This includes funds removed from your accounts as a result of:

- Theft of your member numbers or password while using NMEFCU Online.
- Unauthorized online activity resulting in the removal of funds from your accounts.

Your Responsibility

Your use of NMEFCU cyberbranch@home confirms your agreement to and understanding of the provisions explained in our NMEFCU cyberbranch@home: Terms & Conditions, which describes in detail all aspects of using our service. You are responsible for maintaining the confidentiality of your personal identification and access information, member numbers, online passwords and other account data.

NMEFCU cannot be responsible for member errors or negligent use of the service and will not cover losses due to:

- Misuse of the service or member errors while entering information.
- Failure to maintain confidentiality of or sharing of passwords and/or access information leading to unauthorized access to accounts. This includes storing passwords (through functions such as "autocomplete") on any PC or device that may be collected and re-transmitted (as in the case with "spyware.")
- Failure to "Sign Off" when completing an online session, leaving a computer unattended during an online session, or storing identification or password information in a computer.
- Neglecting to report known unauthorized account access within 2 business days.