



Pioneer Federal Credit Union (PFCU) is always committed to ensuring the safety of our members' information and PFCU's internet banking environment is no exception. With more and more members using internet banking, unscrupulous individuals are working harder than ever to find new ways to scam unsuspecting individuals. One of the best defenses against fraud is to remain educated on cyber-safety. PFCU is dedicated to helping our members stay cyber-safe.

Tips on keeping yourself safe in the internet environment

- 1. Keep Information Private.** Be extremely careful if you have to use a library or other public computer to access your account online as fraudsters could have installed a keystroke logger to obtain your username, pin, answers to security questions, and password.

Fraudsters are known for masking emails and text messages to look like they come from a trusted sender. Do not send your account number or personal information via email or text messaging to anyone. Do not use a hyperlink that is located in an email to access PFCU's online banking website and always ensure the web address starts with https. PFCU uses Website identification which is located to the right of PFCU's web address.

If you receive a phone call from a person claiming to be a PFCU representative it is a good idea to ask for the representative's name and extension and inform the representative that you will call them right back. PFCU's call center will be able to direct your call to the extension given. DO NOT call the representative back on any number other than on a number that PFCU has given you to call (208-587-3304) or is located in your local telephone book. A best practice is to always initiate contact yourself.

- 2. Account Review.** PFCU encourages members to log into their accounts regularly to review account activity, even if you have not done any recent transactions. Early detection is a key component to stopping fraud quickly. If there are any concerns contact PFCU immediately at 208-587-3304.
- 3. Strong Password.** PFCU's VP of Information Systems encourages members to have a password that is at least 8 characters long with a mixture of upper and lower case letters, numbers, and special characters. Change your password regularly and do not give anyone your password or allow anyone else to use your password.
- 4. Website Redirection.** If you click on a hyperlink that redirects you to a website that does not look like it is operated by PFCU, use caution as PFCU may not operate that site. PFCU has pop up warnings on hyperlinks that we have placed on our website to inform you that you are being redirected to a site we do not operate. Use caution and contact PFCU if you suspect there is a problem.

5. **Always Logoff.** Always logoff your PFCU online banking session and DO NOT just close the browser.
6. **Assess your own risks.** PFCU encourages every member to do their own risk assessment on their online banking security controls such as, but not limited to: Storage of online banking information (account number, password, pin, answers to security questions), and the type of antivirus protection you use on your computer.

PFCU initiating contact with you

1. PFCU's employees will **NEVER** call, email, or send you a text messages asking for any of your electronic banking credentials. PFCU may inquire about your electronic banking credentials if you initiate contact and express online banking problems.
2. Card fraud detection may contact you on behalf of PFCU to verify unusual credit or debit card transactions. Card fraud detection will **NEVER** ask you for any of your electronic banking credentials. Card fraud detection will:
 - Introduce themselves to you as card fraud detection and that they are calling on behalf of Pioneer Federal Credit Union.
 - Card fraud detection will give you the last four of the card number they are contacting you about. **Do Not** give anyone claiming to be card fraud detection your full card number, expiration date, three digit security number (located on the back of your card), or your full social security number.
 - Card fraud detection will ask you to verify the transaction(s) in question.
 - Card fraud detection may ask you for information about your address or last four of your social security number.
 - Card fraud detection will only ever call you about credit or debit card transactions.

Protections under Regulation E

Regulation E, better known as the Electronic Fund Transfer Act (EFTA), outlines the rights, liabilities, and responsibilities of consumers that use electronic services covered under the EFTA and financial institutions that offer services covered under the EFTA.

❖ Examples of EFTA covered electronic services offered by PFCU

- ATM (Automated Teller Machine)
- ACH (Automated Clearing House)
- Debit Card Transactions (point-of-sale)

❖ Examples of services not covered by EFTA

- Share Drafts (checks)
- Wire transfers
- Internal transfers between members' accounts initiated through a member's online banking account

- Internal transfer requests made via telephone conversation or in person with a PFCU employee
- Internal transfers to a loan done through online banking, telephone conversation, or in person. Also includes internal recurring transfers that members have requested.

❖ The above are just examples and are not an exhausted list of EFTA covered and uncovered services. For more information on your rights, responsibilities, and liabilities under EFTA please review PFCU's terms and conditions disclosure that PFCU provided at account opening. You can also obtain a copy of the terms and conditions of your account on PFCU's website (www.pioneerfcu.org) by clicking on the disclosure info link at the bottom right hand corner.

Additional Resources

www.staysafeonline.com

www.ftc.gov

www.usa.gov

www.idtheft.gov

onguardonline.gov

PFCU Contact Information

If you suspect or notice any suspicious account activity or experience any information security-related events with PFCU's online banking you should immediately contact us at the following:

Pioneer Federal Credit Union
 Monday to Thursday 8 am to 5:30 pm
 Friday 8 am to 6:00 pm
 Excluding Holidays
 Phone: 208-587-3304

You can also go to one of PFCU's branch locations to report suspicious account activity or discuss any security-related events within PFCU's online banking (Lobby hours vary by branch).

Main Branch

250 W. 3rd S.
 Mountain Home, ID 83647

Base Branch

605 Gunfighter
 MHAFB, ID 83648

Glenns Ferry Branch

70 Commercial
 Glenns Ferry, ID 83623

PFCU Express Branch

3197 E. 8th North
 Mountain Home, ID 83647

Hailey Branch

841 N. Main
 Hailey, ID 83333

Meridian Branch

850 E. Fairview Ave
 Meridian, ID 83642

Jerome Branch

1865 S. Lincoln
 Jerome, ID 83338

Gooding Branch

1624 Main
 Gooding, ID 83330

Twin Falls Branch

1439 N. College Rd E.
 Twin Falls, ID 83301

Eagle Branch

1580 E State Street. #101
 Eagle, ID 83616

Nampa Branch

3000 12th Ave Road
 Nampa, ID 83686

Middleton Branch

551 S. Middleton Rd
 Middleton, ID 83644