## OTHER IMPORTANT TIPS TO CONSIDER

Here are some other important tips to help you better protect yourself:

- Never share User ID's, passwords, PIN numbers, dynamic tokens, etc. with anyone. Do not leave them in an area that is not locked or secured.
- Do not use the same login or password on any other website or software.
- Obtain and install antivirus, anti-malware and anti-spyware software, and consider installation of a firewall and make sure it is automatically updated by the vendor or take necessary steps to keep it updated.
- Limit or eliminate unnecessary web surfing and/or email activity on computers used for online banking.
- Educate all company personnel on good cyber security practices, such as clearing the internet browser's cache before and after visiting websites.
- Verify use of a secure session (https:// and not http://) for online banking sessions.
- Avoid saving passwords to a computer.
- Never leave a computer unattended when using any online banking service, and always lock your computer when away.
- Be cautious of accessing a financial institution's website for online banking from a public computer such as at a hotel, library, coffee shop or other public wireless access point.
- Be suspicious of any employment position that requires use of a personal account for business purposes. Such offers for employment as a mystery shopper, payment processor, etc. where you are required to use your personal account for someone else's business purposes, may not be legitimate.
- Be cautious of requests to move business funds through personal accounts.
- If you are approached to participate in such schemes, immediately contact local law enforcement, the FBI or the Secret Service to let them know.

You can also learn about online safety at the following websites:

www.ftc.gov
www.idtheft.gov
www.onguardonline.gov

Rev. 10/2014

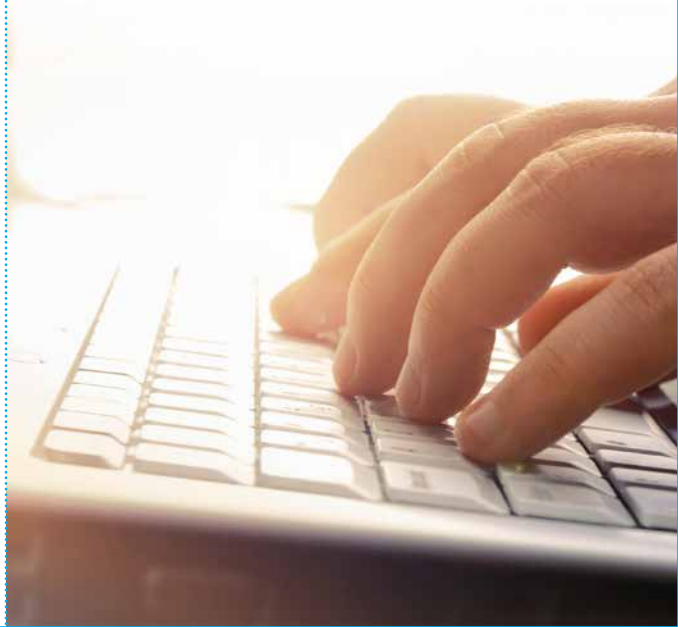
Federally insured by NCUA EQUAL HOUSING LENDER

HAWAII STATE
FEDERAL CREDIT UNION

# Online Banking Awareness and Education

Hawaii State FCU Online Banking provides highly secure, easy access to your HSFCU accounts products and services 24 hours a day, seven days a week

www.HawaiiStateFCU.com | (808) 587-2700



# MEMBER AWARENESS AND EDUCATION TO PROMOTE ONLINE BANKING SECURITY

At Hawaii State FCU, the safety and security of your financial information is of utmost importance to us. It is equally important for YOU to be educated and informed about the types of online fraud and theft that could compromise your personal information and finances. Please read the following important information on how to keep your accounts safe.

## MEMBER CONTACT

Hawaii State FCU or any of its employees will never call, email or otherwise contact you and ask for your user name, password or other online banking credentials. If you are contacted by anyone requesting this information, DO NOT provide the information and contact Hawaii State Federal Credit Union immediately by phone at (808) 587-2700 Island of O'ahu; (888) 586-1056 (Toll Free) Neighbor Islands and elsewhere in the U.S.

## ACCESSING ONLINE BANKING

For your safety, accessing our Online Banking services requires more than the traditional account number and password. In order to access Online Banking, you will need to access your account(s) using your User ID and password. You may change your password within Online Banking by clicking on the Preference link. We recommend that you change your password regularly. For security purposes, it is recommended that you memorize your password and do not write it down. You are responsible for keeping your password, account numbers, and other account data confidential. This is extremely important to prevent unauthorized access to or use of your account. You agree that you will be responsible for all transfers and payments made from your account by anyone you authorize to use your account, whether such use is pursuant to or beyond your instructions.

HAWAII STATE
FEDERAL CREDIT UNION

## ELECTRONIC FUND TRANSFERS: YOUR RIGHTS AND RESPONSIBILITIES

If you believe your Password has been lost or stolen and you notify us within two Business Days after you learn of the loss or theft, you can lose no more than $50.00 if someone uses your Password to conduct unauthorized electronic funds transfers without your permission. If you do NOT notify us within two Business Days after you learn of the loss or theft of your Password, and we can prove we could have stopped someone from using your Password to conduct unauthorized electronic funds transfers without your permission if you had told us, you could lose as much as $500.00. After 60 days, you could be legally liable for the full amount. You may use Online Banking to conduct transactions to view account information, transfer funds among linked accounts, and initiate bill payments.

The "Electronic Fund Transfers" disclosure provided to you at the time of account opening provides detailed information. We will provide to you, upon request, a free printed copy of this disclosure.

## BUSINESS/COMMERCIAL ACCOUNTS

Business/Commercial members, it is critical you implement sound security practices within your place of business to reduce the risk of fraud and unauthorized transactions from occurring. We recommend you perform regular risk assessments to determine any potential exposure you may have related to Online Banking activities.

## BE AWARE OF PHISHING EMAILS

Phishing e-mail messages and the websites they link to, typically use familiar logos and familiar graphics to deceive individuals into thinking the sender or website owner is a government agency or a company they know. Sometimes the phisher urges intended victims to "confirm" account information that has been "stolen" or "lost". Other times, the phisher entices victims to reveal personal information by telling them they have won a special prize or earned an exciting reward. There is no way to absolutely eliminate the risk of receiving a phishing attempt. The most important thing to remember is not to respond.