



## TIPS TO SAFEGUARD YOUR INFORMATION

BCU values your trust and respects your privacy. Protecting the confidentiality of members' financial information is vital to BCU. We know that keeping your personal information secure is an important responsibility you have entrusted in us and we take every precaution to ensure security in every aspect of our operations.

But, every day, unscrupulous individuals are busy developing new scams targeting the unsuspecting public.

In today's high tech world, we are able to do things more quickly and conveniently electronically; whether it is to send a letter via email, pay bills, or go shopping online. With this increase in speed and convenience also comes increased risk. One of the best ways to avoid fraud is to become an educated consumer. Please take a moment to read this important information on how to keep safe when conducting business online.

## HOW TO KEEP YOURSELF SAFE IN CYBERSPACE

- 1. Set good passwords.** A good password is a combination of upper and lower case letters and numbers and is hard to guess. Change your password frequently. Don't write it down or share it with others.
- 2. Don't reveal personal information via email.** Emails and text messages can be masked to look like they come from a trusted sender when they are actually from someone else. Play it safe. Do not send your personal information such as account numbers, social security numbers, passwords, or other personal information via email or text messaging.
- 3. Don't download that file!** Opening files attached to emails can be dangerous especially when they are from someone you don't know as they may allow harmful malware or viruses to be downloaded onto your computer. Make sure you have a good up-to-date antivirus program on your computer and all electronic devices.
- 4. Links aren't always what they seem.** Never log in from a link embedded in an email message. Criminals can use fake email addresses and make fake web pages that mimic the page you would expect. To avoid falling into their trap, type in the URL address directly and then log in.
- 5. Websites aren't always what they seem.** Be aware that if you navigate to a website from a link you don't type, you may end up at a site that looks like the correct one, when in fact it's not. Take time to verify the web page you're visiting matches exactly with the URL you'd expect.
- 6. Log off from sites when you are done.** When you are ready to leave a site you have logged in to, log off rather than just closing the page.
- 7. Monitor account activity.** Monitor your account activity regularly either online or by reviewing your monthly statements and report any unauthorized transactions right away.
- 8. Assess your risk.** We recommend periodically assessing your online banking risk and putting into place increased security controls where weaknesses are found.
- 9. Be extra diligent with business accounts.** Business accounts are at an even greater risk as you often need to allow sharing of account information and passwords in order to conduct business. In addition to all of the other precautions listed above, other items to consider when assessing your business online banking risk are:
  - Who has access to your online business accounts?
  - How and where are user names and passwords stored?
  - How strong are your passwords and how often are they changed? Are they changed before or immediately after terminating an employee who had access to them?
  - Do you have dual controls or other checks and balances with respect to access to online banking transactions?

## WHAT TO EXPECT FROM BCU

BCU will NEVER call, email, or otherwise contact you to ask for your user name, password, or other online banking credentials.

BCU will NEVER contact you to ask for your credit card or debit card number, PIN, or 3-digit security code.

BCU may:

- Verify your street address
- Verify the last four digits of your social security number
- Ask for your mother's maiden name
- Ask for the last four digits of your card number
- Ask to verify the amount of your last transaction or payment
- Ask for your account password

If you are ever uncomfortable with a call you receive and feel you may be the victim of someone trying to access your personal information, please hang up and call us back at 888.729.6728.

## RIGHT AND RESPONSIBILITIES

The federal government has put in place rights and responsibilities for both you and the credit union. These rights and responsibilities are described in the account information disclosures you received when you opened your account with BCU. If you have any questions about this information, please contact the credit union at 616.452.2161 or 888.729.6728.

## ADDITIONAL PRECAUTIONS TO HELP PREVENT IDENTITY THEFT

It is a good idea to be diligent in handling anything with sensitive information. Below is a list of basic precautions you should always take:

- Be prepared by photocopying credit and debit cards and other account information so if something gets stolen you know which accounts to cancel.
- Keep records of all online purchases with dates and order numbers.
- Keep all credit card receipts and compare them with your statement.
- Be wary of anyone asking for personal information.
- Do not give out your social security number unless it is absolutely necessary.
- Take outgoing mail with checks or personal information directly to the post office.
- When making an online purchase, navigate directly to the retailer's site, do not follow links.
- Shred all documents with personal information before throwing them away.
- Do not have your driver's license, social security number, or phone printed on your checks.

If you notice suspicious account activity or experience security-related events, immediately contact your local BCU branch manager for assistance or call us at 616.452.2161 or 888.729.6728. We're here to help.