Safeguarding Your Information

In today's high tech world, we are able to do things more quickly and conveniently electronically, whether it is sending a letter via email, paying bills or even shopping online. With this increase in speed and convenience also comes increased risk. Every day, unscrupulous individuals are busy developing new scams targeting the unsuspecting public. At Belvoir Federal Credit Union, the security of our member's information is a priority. We are strongly committed to the safety and confidentiality of your records.

Belvoir Federal employs full-time staff dedicated to continually monitoring networks for suspicious activity. We have a wide range of security measures, including:

- An intrusion detection system;
- Network traffic filtering;
- Multiple layers of continuous antivirus software scanning; and
- Annual network security assessments conducted by certified third party professionals.

All Belvoir Federal employees are required to attend mandatory security training and follow industry best practices. We have developed an Incident Response Plan based on industry best practices to provide clear directions for handling network security incidents. We are fully prepared to handle all aspects of sensitive data protection, from classification of critical assets to detailed steps regarding malicious software containment.

One of the best ways to avoid fraud is to become an educated consumer and we would like to help you in this endeavor. Please take a moment to read this important information on how to keep yourself and your information safe when conducting business online.

How to Keep Yourself Safe in Cyberspace

An important part of online safety is knowledge. The more you know, the safer you'll be. Here are some great tips on how to stay safe in cyberspace:

1. Set complex passwords. A complex password is a combination of upper and lower case letters and numbers, and is one that is not easily guessed. 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 are coming 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 etc. via email or texting.

3. Don't download that file! Opening files attached to emails can be dangerous as they can allow harmful malware or viruses to be downloaded onto your computer. Make sure you have a recognized antivirus program (i.e. Symantec/Norton, McAfee, etc.) on your computer that is up-to-date. Most importantly, don't open attachments from people you don't know.

4. Links aren't always what they seem. Never log in from a link that is 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 that trap, type in the URL address directly and then log in.

14040 Central Loop. Woodbridge, VA 22193   •   703.730.1800   •   703.730.1410 -fax   •   www.BelvoirCreditUnion.org

1 | P a g e   R e v . 1 2 / 1 1

5. Web sites aren't always what they seem. Be aware that if you navigate to a Web site 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 that the Web page you're visiting matches exactly with the URL that you'd expect.

6. Logoff from sites when you are done. When you are ready to leave a site you have logged in to, logoff 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, particularly for members with business accounts. Some items to consider when assessing your 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 Belvoir Federal

Online Banking, Bill Pay and e-Statements

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

For your safety, accessing our online conveniences requires more than the traditional account number and passcode. Multi-Factor Authentication (MFA) provides an extra level of security for your account information. With MFA, when you log into our online banking website, you will be prompted for your username and password (the first factor), a unique phrase and identification of a picture that you've chosen (the second factor) and in some cases, the answer to one of several security questions the you've chosen (the third factor). Taken together, these multiple factors provide increased security for your Belvoir Federal account(s).

Credit and Debit Cards

Belvoir Federal will NEVER contact you and ask for your credit or debit card number, PIN or 3-digit security code. Please see below for more information about how our Fraud and Card Service Departments approach member service calls.

If you receive a call from our Fraud department:

They will identify themselves as the Fraud Detection department calling on behalf of Belvoir Federal and what card number they are calling to verify transactions on.

14040 Central Loop. Woodbridge, VA 22193   •   703.730.1800   •   703.730.1410 -fax   •   www.BelvoirCreditUnion.org

2 | P a g e   R e v . 1 2 / 1 1

If you are available to answer the phone then the system will go through different prompts to verify who they are speaking with and then verify the zip code and then if all matches it will go into the transaction verification. If the transactions are valid it will update the account. If there is any question about the transactions being verified then the call will be transferred to a live representative.

If you are uncomfortable with the call, please hang up and call back on the 800 number on the back of your card.

If the Fraud department leaves a message, they will:
- Identify themselves as the Fraud Detection department calling on behalf of Belvoir Federal.
- Tell you the card type and number they are calling to verify transactions on.
- Ask you to call an 800 number.

When you call the 800 number you will be asked to do the following by the interactive voice response system:
- Enter your 10 digit phone number where the call was received; or
- Enter your 16 digit credit or debit card number; and
- Enter the last four digits of your Social Security Number.

If you choose to speak with a representative they will ask for a combination of three of the items below:
- Your mother's maiden name;
- The last four digits of your Social Security Number;
- Your address;
- Your date of birth; or
- Any other personal information that may be on your credit or debit card account.

Rights and Responsibilities

With respect to online banking and electronic fund transfers, 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 disclosures you received when you opened your account with Belvoir Federal. You can also find them online under the disclosures link at www.belvoircreditunion.org/disclosures. Ultimately, if you notice suspicious account activity or experience security-related events, please contact the credit union immediately at 703-730-1800 or 1-888-503-2328.

14040 Central Loop. Woodbridge, VA 22193   •   703.730.1800   •   703.730.1410 -fax   •   www.BelvoirCreditUnion.org

3 | P a g e   R e v . 1 2 / 1 1