WAKEFIELD
Co-operative
BANK

Bringing life to banking
Member FDIC / Member DIF

How do I protect myself?

We want your online banking experience to be enjoyable and safe. That's why we use 128-bit secure sockets layer (SSL) encryption, constantly updated and monitored systems along with multiple security layers and procedures. We also want to make you aware of several straightforward security tips to keep in mind:

1. Use a strong password. Choose passwords that are difficult for others to guess and use a different password for each of your online accounts.

2. Change your Passwords frequently. You can do this quickly and easily by logging in and visiting the Account Services tab, and then clicking on "Change My Profile".

3. Every time you access Online Banking your personal image and name will appear before you enter your password. Seeing your image and name will let you know that you are at our *real* site and not a fake or fraudulent site. This means it is safe to enter your password. If the correct image and name do not appear, do not enter your password and contact us immediately at 866-987-7601.

4. You may be asked to set-up several security questions that only you should know the answers to. Our security system will recognize the computers you normally use to access your online banking site. In the future, if you or someone else attempts to log in to your account from a new or unrecognized computer, you may need to answer some of your security questions before being allowed to continue.

5. From time to time you may be prompted to answer authentication questions before completing a payment or other transaction. These questions are compiled from public sources such as the department of motor vehicles and other public records. The questions should be easy for you to answer but difficult for others to guess the correct answer. For this reason, prompting you to answer these "out of wallet" questions on occasion provides you with additional assurance that we are doing all we can to protect your identity and make Online Banking even more secure.

6. Leave suspicious sites. If you suspect that a website is not what it purports to be, leave the site immediately. Do not follow any of the instructions it presents. For Microsoft Internet Explorer (IE) users setting your browser security setting to "high", a level that makes it more difficult to interact with some websites, is also recommended.

7. Be alert for scam emails. These may appear to come from a trusted business or friend, but actually are designed to trick you into downloading a virus or linking to a fraudulent website and disclosing sensitive information.

8. Though we will communicate with you over email from time to time, we will never request that you provide sensitive or personal information via email. Don't reply to any email that requests your personal information. Be very suspicious of any email from a business or person that asks for your password, Social Security number, or other highly sensitive information and/or one that sends you personal information and asks you to update or confirm it.

9. Open emails only when you know the sender. Be especially careful about opening an email with an attachment. We advise that you shouldn't open attachments unless you are confident that you can trust the source

10. Do not click on links in emails from unknown senders or on links in emails that are asking you to change or update personal information.

11. Do not send sensitive personal or financial information unless it is encrypted on a secure website. Regular emails are not encrypted and are more like sending a post card. Look for the padlock symbol to ensure that the site is running in secure mode before you enter confidential personal information.

12. Don't take anything for granted and only do business with companies you know and trust. Always keep in mind that forging emails and creating phony "look alike" websites designed to trick consumers and collect their personal information is not difficult. Make sure that websites on which you transact business post privacy and security statements, and review them carefully.

13. Make sure your home computer has the most current anti-virus software. Anti-virus software needs frequent updates to guard against new viruses. We recommend that you use a program that automatically upgrades your virus protection on a regular basis. If you currently do not have this automatic upgrade feature, make sure you update your virus detection program weekly and when you hear of a new virus. If your anti-virus product doesn't include spyware protection, we recommend that you install a reputable spyware detection product as well.

14. When your computer is not in use, shut it down or disconnect it from the Internet.

15. Act quickly if you suspect fraud. If you believe someone is trying to commit fraud and/or if you think you may have provided personal or account information in response to a fraudulent email or Web site, report the incident immediately, change your passwords and monitor your account activity frequently.

Cookies

In order to provide optimal security, performance and reliability, this service requires that cookies be enabled on your Web browser. Cookies are a small piece of information that a Web server can store on your browser so the system recognizes your actions during a session.

As you browse the Web, some cookies are "set" on your Web browser. For example, cookies are used to store preferences you have requested on frequently visited Web sites. When you close your browser, some cookies are stored in your computer's memory in a cookie file, while some expire immediately. All cookies have expiration dates.

Cookies cannot be used to obtain data from your computer, get your e-mail address or access sensitive or personal information. The only way that any private information could be part of your cookie file would be if you personally provided that information to a Web site. Also, each cookie can only be read at the site where the cookie was created.

REV June 2018