Consumer Online Security Tips

Contact Us

Call Us

Report Fraud or Suspicious Activity
1-800-488-2265
Report a Lost or Stolen Credit Card
1-800-996-2638

Email Us

Report Suspicious Emails
abuse@bankofthewest.com

Protecting the security of your personal information is a high priority at Bank of the West. While there are numerous security measures Bank of the West uses to identify suspicious activity and to keep your information safe, there are steps you should also take to protect yourself. Bank of the West recommends the following security tips to help you protect yourself from unauthorized access to your accounts and personal information.

If you have recently identified unauthorized account activity on an account, a compromised Online Banking Profile, or believe your personal devices (computer, laptop, tablets, smart phone, etc.) have been infected with malware, please report the activity immediately by contacting our Customer Service department, or visiting any Bank of the West location. You should also ensure all personal devices are secure and clean of viruses and malicious software before you use them to re-establish online banking services and change passwords for your financial, personal, and email accounts. We also recommend consulting a computer security professional for support. For additional fraud prevention and security information, visit the Security Center on bankofthewest.com.

Tips for protecting your online identity:

1.	**Keep your operating systems, web browsers, and other applications on all personal devices (computer, laptop, tablet, smart phone, etc.) updated with the latest security patches:** Most internet service providers offer an automatic update feature to help you stay up to date; ensure this feature is turned on.
2.	**Protect your personal and online account information:** • Never share your user name or password with anyone. • Avoid login features that save usernames and passwords. • Use unique passwords for your important accounts such as online banking and email and use strong passwords that are difficult to guess but easy enough to not be written down or saved on computer. Change your passwords regularly and use combinations of letters, numbers, and special characters such as # and @ when possible. For example, “1jwCamp!” is a stronger password than “jwcamps” • Never use your Social Security Number (SSN), name, or date of birth as a username or password. • Never leave your device unattended while handling bank-related business. • Never access banking information or financial services at public internet locations. • Clear browsing history and cookies stored on your hard drive. • Beware of scams, no matter how urgent someone claims a deal, job offer or plea for assistance, you should research and confirm its legitimacy before responding. • If your computer is infected with a virus, use a separate secure device to change passwords on all your financial, personal and email accounts.

3.	**Install antivirus and/or other protection software on all personal devices:** Purchase or subscribe to an antivirus service to help keep your computer virus free. Make sure your software is updated regularly and always running to stay protected. Beware of scams involving pop-ups or phone calls from software companies claiming to provide security support by downloading software. These are attempts to download spyware onto personal devices; confirm legitimacy before responding. Help protect yourself, your personal information and your devices with the below security tools offered by Bank of the West. **Visit https://www.bankofthewest.com/security-center-personal/protection-tools.html for access to these tools:** ➢ **McAfee AntiVirus Plus:** As a Bank of the West customer you are entitled to a 12 month trial1 of McAfee AntiVirus Plus. ➢ **Trusteer Rapport:** Trusteer Rapport helps to create a safe connection between your web browser and Online Banking. It helps shield your information from malware and helps you protect yourself from phishing techniques. Trusteer Rapport is an online fraud software application from Trusteer2 that is free to download and use. [1]Auto-renewal – Prior to the end of your 12-month trial period, McAfee will use the payment information in its files to automatically renew your subscription at the then-current retail price for the service you ordered. To change your payment information, cancel or ament your subscription, go to "My Account" on the McAfee website or contact McAfee customer service at (866) 622-3911. [2]Bank of the West and Trusteer are separate legal entities, which are not affiliated with each other in any way by common ownership, management, control or otherwise. The content, availability and processing accuracy of their web sites and products are the responsibility of each respective company. Bank of the West does not control or guarantee Trusteer Rapport, makes no representations or warranties; and assumes no responsibility concerning Trusteer Rapport. Trusteer is solely responsible for customer service support and the performance and maintenance of Trusteer Rapport.
4.	**Reconcile your bank account frequently and immediately report any unauthorized activity:** Review your account details and transaction history at least once a week (or more) in an effort to promptly identify unauthorized or suspicious activity. Notify your financial institution **immediately** if you identify any unauthorized or suspicious activity.
5.	**Be wary of "Phishing", "Smishing" and "Vishing"** Criminals will use emails, text messages and phone calls in an effort to steal your personal information or infect your personal device. The request appears to be from valid companies or financial institutions requesting confidential information. Bank of the West will never send unsolicited communications asking for confidential information. **Do not respond to unsolicited requests for personal information.** Contact your financial institution at a trusted number to verify requests. **Be on Guard:** • Just browsing to a malicious website could infect your device with malicious software; make sure the website is secure. Look for "secure transaction" symbols such as the lock symbol (see the lower right-hand corner of your web browser window or on the toolbar), or "https://…" in the address bar of the website. The "s" indicates "secured" and means the web page uses encryption. • Be cautious of attachments, never open attachments, click on links, or respond to emails from suspicious or unknown senders. • Criminals may send you attachments or links that will lead you to spoofed sites or cause you to inadvertently download malicious software to your computer. Do not respond to any communication asking for confirmation of personal information. Personal information includes but is not limited to name, address, phone number, email address, Social Security Number, financial information such as account numbers, etc. • Do not respond to unexpected text messages or automated voice messages. • Look for spelling and grammatical errors as these are often an indication of fraudulent emails or websites. • Report any suspicious email purporting to be from Bank of the West by forwarding it to: abuse@bankofthewest.com. • Do not include account or sensitive information in emails. If you use Online Banking, send a secure message through the Message Center function of your Online Banking service. **Visit the Security Center at bankofthewest.com for additional information about Online Fraud Scams.**

6.	**Read Online Banking messages and visit the Security Center at bankofthewest.com:** https://www.bankofthewest.com/security-center-personal.html Keep up to date with Online Banking messages from Bank of the West. We'll communicate information when we hear of phishing emails circulating, provide latest system enhancements for security, and other important information that may impact you.
7.	**Use Online Banking tools and services:** Utilize the services Online Banking offers, such as email alert notifications. Being alerted to changes in profile and activity can help you quickly identify unauthorized access to your accounts. Visit **bankofthewest.com** for a full list of services and tools.
8.	**Review your credit report at least twice a year:** Check for unauthorized changes and new accounts in your name. Consumers can obtain free copies of their credit reports once each year from each of the three major credit reporting agencies. Be sure to review the credit report of your minor children. See the Federal Trade Commission's website http://www.ftc.gov/bcp/edu/microsites/freereports/index.shtml for more information.
9.	**Don't overshare personal information online** Information that you share on social networking websites, such as photos, location "check-ins", and other personal details about your life, may be sought by fraudsters in their attempts to commit financial fraud or identity theft. In addition, anything posted online may remain out there permanently, which is why it is important to be cautious of what you post. Consider the below tips when sharing your personal information online. • **Do not settle for the default settings.** Limit information sharing to a small group, or only those closest to you. • **Validate your friends.** Be wary of people that you meet online that you have not met in person, including job offers and financial transactions. • **Think before you post.** Recent news of data breaches teaches us that anything that we post online, even items meant to be private, may become public. Before you say or upload something, think about the impact if it became public. What information is contained in the picture? What does the post say about you? • **Guard your location.** Do not tell criminals when you are not at home. Your location information could be used for cyber stalking or to take your valuables when you are not at home. Keep in mind, status updates and photos taken with smartphones may contain embedded GPS coordinates that allow fraudsters to know where you are or have been. If you want to post photos of your vacation, considering waiting until you are back at home. • **Do not overshare.** Social media sites may ask for your personal information (address, phone number, SSN, date of birth, etc.) which can be used by identity thieves to gain access to your bank account. • **Parent-strong.** Teach your children the risks associated with the internet and potential risks of sharing personal details online.

In South Dakota, Bank of the West operates under the name Bank of the West California

BANK OF THE WEST
BNP PARIBAS GROUP