



Online Banking Security Checklist

Coastal Community Bank wants to help keep you and your account safe. Here are some steps you should take to ensure that you are not putting yourself at risk for unauthorized access or fraud when accessing your account online.

- Change your access password at least every four months. Do not allow your internet browser or Windows to remember your internet banking password.
- Monitor your transaction history regularly. Set Online Banking alerts to notify you of unusual purchases or activity. (You can find *Manage Alerts* under the *Administration* Tab in Coastal's online banking.)
- Keep your anti-virus, anti-spam, and anti-spyware programs up to date on all computers and devices.
- Never access your bank accounts or shop online using a public computer or un-secured Wi-Fi connection.
- Make purchases online from only trusted companies with a secure payment site. The company web address should begin with https.
- Never enter your online banking password into a website that is not the Coastal Community Bank login page. We will never ask for your online password on a form, by phone, or in an email.
- Never disclose your passwords to anyone including family or friends. Do not write down your password, or store it on your computer.
- Never provide personal information (i.e. Social Security number or account number) in response to a phone or email inquiry that you didn't initiate.
- Do not send confidential information by email. Contact your Coastal Banker for instructions for secure message delivery.
- If you are unsure of the authenticity of an e-mail you receive from Coastal, call us to verify before submitting personal information.
- Be wary of emails from people you don't know or trust. Never click on a link or an attachment in an email from a source you don't know or trust.
- Don't leave your computer or mobile device unattended while logged in to online banking. Be sure you click the "log off" button when finished. We also recommend that you close out of your browser completely at the end of each online banking session.
- Notify Coastal Community Bank immediately if you think your computer or password has been compromised.



For more information or to find additional tips to protect your home or business, try one of these helpful resources:

National Consumer Protection Week — www.ncpw.gov

Federal Trade Commission — www.ftc.gov

Microsoft's Malware Protection Center — www.microsoft.com/security/portal/mmpc/

For the location of the branch nearest you, call 425-257-9000 or visit www.coastalbank.com.