

When you use the internet to visit us, whether it's to learn about our services, to review your account or to transact other business you are entering a secure area.

Here are just a few of the safeguards we have in place to help ensure your personal security when visiting us online:

- **Your Password – We'll ask you to develop a secret password that only you will know. Only then will you be able to review personal information about your account.**
- **Our Privacy Policies – Our entire staff is dedicated to protecting the personal privacy of you, our customer. We have stringent privacy policies in place, and have instituted bank-wide measures to assure that they are strictly observed.**
- **Encryption Software – 'cryptographic software' makes it possible to scramble a message between two parties in a way that allows the message to be decoded only by one of the two parties.**

**WHEN YOU BANK WITH
FOUNDERS COMMUNITY BANK
YOU CAN BANK WITH
CONFIDENCE...ONLINE, ON
THE PHONE OR IN PERSON.**

Banking Hours

Lobby Hours:

Monday-Thursday 9:00 a.m. to 5:00 p.m.
Friday 9:00 a.m. to 6:00 p.m.

Walk-up Window:

Monday-Thursday 8:00 a.m. to 9:00 a.m.
& 5:00 p.m. to 6:00 p.m.
Friday 8:00 a.m. to 9:00 a.m.

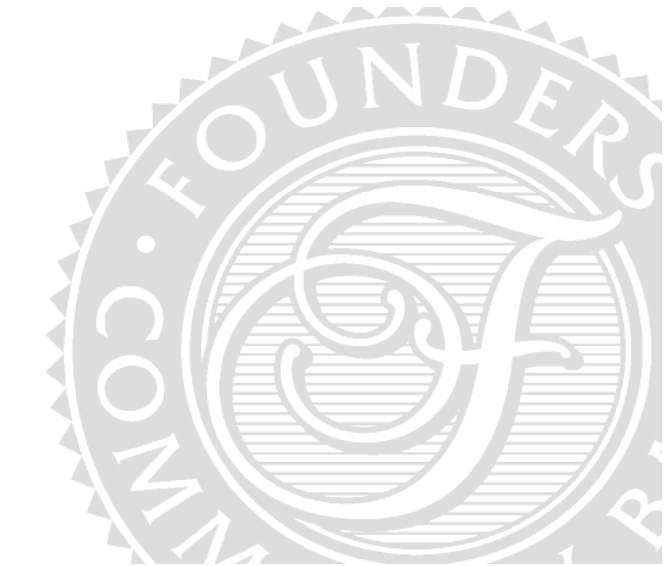
237 Higuera Street
San Luis Obispo, CA 93401
Tel (805) 543-6500
Fax (805) 543-6599
24 hour phone service (888) 543-6595
www.founderscommunitybank.com

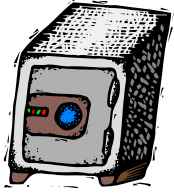
**Member
FDIC**



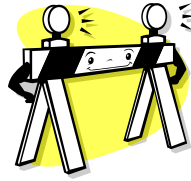
FOUNDERS
COMMUNITY BANK

'PHISHING' AND INTERNET SECURITY






Safe Online Banking



Technology, accountability and ongoing communication help us insure that your online banking experience is safe and secure, however we would like to make you aware of ‘phishing’.

Phishing is the widespread use of email and other internet scams to fraudulently obtain information from you.

Identity thieves will send emails to bank customers asking them to ‘verify’ information or otherwise divulge personal data.

 *We never send emails requesting personal information. We will never ask you to click on a special site link to do so. While emails of this nature may look like they are from us, and even use our logo, they are most likely a ‘phishing’ scam. Do not answer them. If you receive an email purporting to be from us, do not hesitate to call us to confirm it.*

When you bank online with us, your transaction is safeguarded by the full extent of available technology.

Some Helpful Hints

- ☑ Do you have an account with the ‘company’ that sent you the e-mail? If not this could be a ‘phishing’ scam.
- ☑ Never click on a link from an unknown person; viruses and spyware can be transmitted that way.
- ☑ Don’t reply to a possible phishing e-mail. If you do, you have just told the scammer that he has reached a good e-mail address, and that has invited even more spam and scams into your inbox.
- ☑ If you think the request for information may be legitimate, do not click on the link, but instead open a new Web browser and go directly to that company’s site.
- ☑ Before entering your personal information or credit card numbers on a Web site, look for signs that the site is secure. Sometimes it will be a ‘locked’

yellow padlock icon, usually in the lower right corner. Also, Web addresses for secure sites usually begin with ‘https,’ the ‘s’ being the letter that tells you the site is secure.

- ☑ Keep tabs on your credit card usage and immediately report any unfamiliar activity to your bank.
- ☑ Do not complete forms in e-mail messages that ask for personal information.
- ☑ Ensure that your internet browser and operating system are up to date with the most recent security releases.

Most importantly, if there is ever a question, pick up the phone and call us. We are here to make your banking easier, not something to worry about.

