



**Dog gone it!  
Don't even let Fido  
access your personal  
information...**

**Customers have an important role in protecting their bank accounts and detecting fraud. BEO's Internet and Mobile Banking services give you many tools to protect your personal information and to alert you about activity on your accounts, but you need to use them if you really want to protect your information!**

We're providing security tips & online security resources you can use to learn how to protect your accounts. Your online security is important to us; help us keep your information safe by taking measures to protect yourself!

Learn more about online security by visiting either of these websites:  
[www.staysafeonline.com](http://www.staysafeonline.com) & [www.idtheft.gov](http://www.idtheft.gov).

For more information on protecting your online accounts, go to  
[www.beobank.com](http://www.beobank.com)  
& click on *Customer Awareness*.

### **Key Features YOU can do to Protect Online Information**



**NEVER** reveal your User ID or password to anyone ■ **Log into your internet banking & check your activity at least weekly** ■ **Use a strong password & change it at least every three months** ■ **Disable the auto complete feature for usernames/passwords for your browser** ■ **Set up activity and balance alerts** ■ **Don't leave your computer in the middle of an online banking session...*sign off!*** ■ ***Sign off* on internet banking before visiting other internet sites** ■ **Business & Cash Management customers: use a dedicated PC & establish dual security controls** ■ **Check balances at the end of workday** ■ **Be alert to modified ACH & wire files. **And, most importantly, if you see suspicious activity, contact us immediately!****

### **Key Steps BEO takes to Protect Your Online Accounts**

➔ **Information Encoding.** We use the latest encoding technology to ensure that your private information cannot be intercepted. Encryption is a way to rewrite something in code, which can be decoded later with the right "key." When you request information about your accounts, the request is sent encrypted. We decode your request and send the requested information back to you in an encrypted format. When you receive the information, it is decoded so that you can read it.

➔ **Personally Selected Account Names.** Bank of Eastern Oregon does not display your account numbers over the Internet. Instead, we ask you to choose a "pseudo" name for each of your accounts. You can change your "pseudo" account name by selecting "Options" and then "Account" within your Internet Banking session.

➔ **Password Security System.** To keep unauthorized individuals from accessing your account by guessing your password, we have instituted a password security system. If your password is entered incorrectly several times, the online banking account is locked out. An email is sent to the email address on file to inform you of the locked out status. If you have forgotten your password or have accidentally locked yourself out of Internet Banking, please contact your local branch or you may also reset your own password. This procedure is found in your Internet Banking account under "Options."

➔ **Password Length & Strength.** Password length & strength is another factor we consider in keeping your accounts safe. The more complex the password, the harder it is to guess. Currently, we have this set to a minimum of 8 and maximum of 12 alpha/numeric character/special characters & the letters are case sensitive.

➔ **Multifactor Authentication.** After a brief monitoring period, you will be prompted to select some personal verification questions. During a future login we ask you to answer these questions if we don't recognize your computer or location from where you are logging in. Additionally, you will be asked to select a watermark for your Internet Banking account. This watermark will be displayed at each login and also on each page while you are on your Internet Banking account. This will assure you that you are accessing the secure Bank of Eastern Oregon Internet Banking at all times. Also, additional monitoring will be in place for dollar amount and volume of transaction. If any transaction presents a higher risk factor, the system will prompt for personal verification questions to ensure your identity prior to processing the transactions.

➔ **Automatic Logoff.** If you are logged onto Internet Banking, but do not perform an activity for 10 minutes, you will not be able to proceed until you "re-enter" your user ID and PIN.

➔ **Email Communications.** Please remember that email is not a secure method of communications, and you should be cautious when sending emails with personal information. If your information is very sensitive, or includes personal or confidential information, such as your bank account, charge card or social security number, you may want to contact us by postal mail or telephone. A list of branch addresses and phone number can be found on our website.

➔ **Web Browsers.** For a complete list of supported browsers, go to our Internet Banking log-in page.