



## Protecting Your Online Information

Orion works hard to keep your Online & Mobile Banking experience safe and secure. Below is information that may help you keep your Orion accounts even safer. If you have any questions or concerns, please contact us.

### Will Orion ever contact me requesting my login information?

Under no circumstances will we contact you to obtain your Online or Mobile Banking credentials! It is common for fraudsters to email, text, or call a person, posing as their financial institution. Please do not fall into their traps. Always keep your information a secret. Call us immediately if you suspect anyone is trying to defraud you.

### What does Orion do to protect my Online & Mobile Banking accounts from fraud?

Orion uses advanced technology to monitor for unusual activity. Also, we will alert you whenever changes are made to your account settings, just in case those changes were made by an unauthorized user.

Your online transactions may be protected by the Electronic Fund Transfers Act. For details, please see the Electronic Fund Transfers section of Orion's Account Disclosures.

### What can I do to protect my Online & Mobile Banking accounts?

- Invest in antivirus software to help protect you when downloading information to your computer or mobile devices. Only use antivirus software that comes from a trusted source. Free downloads that claim to protect your computer may actually be spyware that puts your information at risk.
- Keep your login information private – do not write it down in a place where it can be lost or store it on your mobile device where it can be obtained by a potential fraudster.
- Set your mobile devices to require a password when they power-on or awake from sleep mode.
- Never set the app, web or client-text service on your computer or mobile device to automatically login to your bank account.
- Keep your other identifying information safe, like your Social Security Number and account numbers.
- Keep your mailing address, phone numbers, and email addresses up to date.
- Under the “Notify Me Alerts” tab in Orion Online Banking, set alerts to be emailed to you whenever there is activity. This helps protect you against Online Banking fraud as well as check and debit fraud, since all transactions are monitored.
- Always review your transactions – you may think that fraudsters will only go for big dollar amounts, but small transactions can add up over time, so please review each one.

- Do not login to your Online or Mobile Banking from public computers that you do not trust. Fraudsters may have installed programs to steal your information.
- Be sure your internet router has a firewall turned on. (This is the device that you probably connect your computer to for internet, with an Ethernet cable or by Wi-Fi. You may need to consult your owner's manual or your internet service provider for assistance.)
- Do not download programs or apps to your computer or mobile devices from sources you do not trust.

**Tip: Some websites, like [cnet.com](http://cnet.com) , review programs to ensure they do not contain spyware. Do your homework before you download!**

- For more tips, go to: [www.staysafeonline.org](http://www.staysafeonline.org)

## **I have a business account – should I do anything special?**

Business accounts commonly have multiple authorized users, so extra care should be taken. Be sure to remove a person's access if they leave employment or are on an unpaid or extended absence. Perform a risk assessment so that you understand your business's vulnerabilities, and implement procedures to help mitigate your risks.

## **Who do I contact if I notice suspicious account activity or am afraid my Online Banking account has been compromised?**

Please call Orion at 901-385-5200.