SouthernFirst

Cybersecurity Checklist

THE BASICS

- **Be skeptical when anyone new reaches out to you**, especially if they are threatening in any way or using high-pressure tactics.
- **Slow down.** Taking the time to scrutinize requests and communications lowers your chance of accidentally falling victim to fraud.
- **Never share your passwords or pin numbers.**
- **When opening emails, expand the information to see who they are really from.** Beware of irregular sender addresses, misspelled domain names, and fragmented domains.
- **Carefully review the content of emails and text messages** for incorrect grammar, typos, and suspicious links and attachments.
- **Don't click on links or open attachments in unsolicited emails or text messages.**
- **Look for HTTPS at the beginning of website URLs** when you're logging into an account, ordering online, or entering any personal information into a website.
- **Create and save bookmarks for important banking and financial websites** you visit often to avoid inadvertently entering your credentials on a fraudulent site.
- **Monitor your bank statements and credit reports for suspicious activity.**
- **If you have concerns, call the number on the back of your card, or call your bank or banker directly.**

PASSWORDS

- Always change default passwords.
- Use complex passwords (16+ characters long and include upper and lowercase letters, numbers, and special characters).
- Try not to include information in your passwords that could easily be found online or on social media.
- Don't use the same password for multiple accounts.
- Change all passwords at least once per year.
- Use a password manager such as LastPass or 1Password.
- Turn on multi-factor authentication for all sites that offer it.

DATA MANAGEMENT

- Back up important files to a secure server, hard drive, or cloud storage.
- Set your phone to delete texts after a period of time (i.e., after 30 days).
- Decide on a retention time for emails as well (i.e., a year) and save older, important ones elsewhere (i.e., legal documents and contracts).
- Go through other services that store data for you like Google Drive, Dropbox, and OneDrive and delete unnecessary files.
- Clear your browser's history regularly.
- Delete online accounts you no longer use.
- When signing up for new online accounts, inquire about how your information will be stored and shared.

SouthernFirst

Cybersecurity Checklist

DEVICES

- [ ] Turn on automatic updates.
- [ ] Keep your web browser and browser plugins updated.
- [ ] Use anti-virus protection software.
- [ ] Use a 6+ character passcode on your phone.
- [ ] Do an audit of which apps have access to your contacts, location, camera, microphone, etc., and remove unncessary access.
- [ ] Use automatic screen lock settings.
- [ ] Check what is accessible on your phone's lock screen (i.e., text notifications).
- [ ] Use secure Wi-Fi networks and avoid public Wi-Fi.
- [ ] Secure your home Wi-Fi network, and create a separate Wi-Fi network for guests to use that is not connected to any of your devices.
- [ ] Do not use publicly available charging cables or USB ports to charge your devices.
- [ ] Leverage Find My iPhone/ Android Device Manager to prevent loss/ theft.
- [ ] Only install apps from trusted sources and delete apps you no longer use.

SOCIAL MEDIA

- [ ] Assume everything you post has the potential to become public.
- [ ] Assume everything you post online is permanent.
- [ ] Avoid sharing personally identifiable information online such as your email, address, phone number, date of birth, and social security number.
- [ ] Keep in mind if your posts could be taken out of context.
- [ ] Audit your privacy settings on each network, especially controls that determine who is eligible to see your posts.
- [ ] Check what content is viewable on your public profile.
- [ ] Review your friends or connections list for fake accounts.
- [ ] Decide if you want others to be able to see who you are connected with.
- [ ] Search yourself on social media and search engines regularly and attempt to remove information that is out of date or you don't want available.

HELPFUL APPS & SERVICES

Real-Time Alerts - Southern First customers can sign into personal online banking to set up customized text and email notifications for transactions, deposits, transfers, and more.*

SecurLOCK Equip - Control how your debit card is used with the SecurLOCK Equip app. Add your Southern First debit card to control when, where, and how it is used, set up instant alerts, turn your card on and off at the tap of a button, and more.

Zelle® - Southern First clients have access to Zelle® in the personal banking mobile app, a fast, easy, and secure way to send money to family and friends. Remember, only send money to people you know and trust. Southern First will never ask you to send money to yourself or unexpectedly call or text you about Zelle® or other payment apps.**

*Notifications for acount balance, loan balance, insufficient funds or overdrawn account, loan payments, and loan rate changes are only available on a daily basis. Message and data rates may apply.
**Additional fees may apply. Subject to terms and conditions. Mobile carrier fees may apply. The Zelle related trademarks are used under the license from Early Warning Services, LLC.

1-877-679-9646 | contactus@southernfirst.com | www.southernfirst.com