Protecting Yourself and Your Personal Information

Cybercriminals are always looking for new ways to steal your data, and they become even more brazen during times of crisis. Learn what you can do to protect yourself from ongoing cyberthreats.

Use Strong Passwords

- Create strong and unique password phrases that are at least 12 characters long using uppercase, lowercase, alphanumeric, and special characters
  For example: tH35Ky1sN0T81uE! (Theskyisnotblue!)
- Don't use common words or personal information, like your name or date of birth
- Use a password manager to generate strong passwords that will be stored in a secure vault, so you'll only need to remember one
- Change your password at least every 180 days

Safeguard Your Accounts

- Be proactive—monitor your accounts regularly for unusual activity, especially during the holiday season
- Set up fraud alerts on all your accounts and promptly report unauthorized transactions
- Enable multifactor authentication to reduce the risk of your account being compromised

Secure Your Device

- Use passcodes and lock screens on your mobile devices and computers
- Don't store bank account information or passwords on your mobile devices
- Use antivirus and antimalware software and keep it updated

Avoid Phone Scams and Social Engineering Attacks

- Beware of callers who create a sense of urgency and pressure you to comply with demands
- Never disclose login credentials or nonpublic personal information (NPI) over the phone
- Ask probing questions to identify unknown callers and their intentions
- Avoid malicious software downloaded on your system and don't click on unknown links to "verify" your information, especially those requesting financial details or passwords

Derrell Crimm, CFP®
AC Financial Partners
1800 International Park Drive | Suite 10 | Birmingham, AL 35243
205.235.3500 | 205.235.5170 fax | www.acfinancialpartners.com | derrell.crimm@acfinancialpartners.com

Watch Out for Phishing Attempts

- Never click on any unknown links within emails, especially those asking to verify nonpublic personal information (NPI)
- Ignore emails with urgent requests requiring an immediate response
- Avoid poorly written emails that include suspicious attachments or links
- Beware of communications from a public email domain, such as Yahoo! or Google, or a misspelled name, such as "Commonwaelth"

Use Public Wi-Fi with Caution

- Avoid sending personal information on a public wireless network, like those in a coffee shop, library, airport, hotel, and other public places

Report Suspicious Emails

- Notify your email provider, such as Yahoo!, Gmail, or any other relevant providers

Please contact your advisor if you have questions or concerns.