A CYBERSECURITY CHECKLIST

Here are a few reminders about simple things you can do to help protect your computers and your money from online criminals.

- **Have computer security programs running and regularly updated to look for the latest threats.** Install anti-virus software to protect against malicious software (malware), which can steal information, such as account numbers and passwords, and use a firewall to prevent unauthorized access.
- **Be smart about where and how you connect to the internet for banking or other communications involving sensitive personal information.** Public Wi-Fi networks and computers at places such as libraries or hotel business centers can be risky if they don't have up-to-date security software.
- **Consider using a virtual private network (VPN).** A VPN establishes a secure and encrypted connection to provide greater privacy. For extra security, we also recommend using two-factor authentication when banking online.
- **Get to know standard internet safety features.** When banking or shopping online, look for a padlock symbol on a page (which means it is secure) and "https://" at the beginning of the web address (signifying the website is authentic and encrypts data during transmission).
- **Ignore unsolicited emails asking you to open an attachment or click on a link if you're not sure who truly sent it and why.** Cybercriminals are good at creating fake emails that look legitimate but can install malware. Ignore unsolicited requests to open attachments or files. Verify the supposed source actually sent the email to you by making contact using a published email address or telephone number. Ignore unsolicited requests for information, especially if they ask for information such as a Social Security number, bank account numbers or passwords.
- **Use the most secure process you can when logging in to financial accounts.** Create strong passwords that are hard to guess, change them regularly and try not to use the same passwords or personal identification numbers (PINs) for several accounts.
- **Be discreet when using social networking sites.** Criminals comb social media looking for information such as place of birth, mother's maiden name or a pet's name, in case those details can help them guess or reset passwords for online accounts.
- **Be careful when using smartphones and tablets.** Don't leave your mobile device unattended and use a password or other method to control access if it's stolen or lost.
- **Parents and caregivers should include children in their cybersecurity planning.** Talk with your children about being safe online, including the risks of sharing personal information with people they don't know, and ensure the devices they use have up-to-date security.
- **Small business owners should have policies and training for their employees.** Consider requiring information beyond a password to gain access to your business's network.

Heritage BANK

Information provided by the FDIC