Protecting Your Online Data: Don't Become a Victim!

CYBERSECURITY CHECKLIST:

1. **Utilize computer security programs.** Have computer security programs running and regularly updated to look for the latest threats. For example, install anti-virus software to protect against malware (malicious software) that can steal information such as account numbers and passwords, and use a firewall to prevent unauthorized access to your computer.
2. **Be aware of where and how you connect to the Internet.** Be cautious 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.
3. **Study up on basic standards of Internet safety.**It pays to become familiar with standard Internet security protocols. For example, when banking or shopping online, look for a padlock symbol on a page (that means it is secure) and "https://" at the beginning of the Web address—this signifies that the website is authentic and encrypts data during transmission.
4. **Ignore unsolicited emails with suspicious attachments.** Cybercriminals excel at creating fake emails that look legitimate, but can install malware. If you're uncertain you know who sent it and why, your best bet is to either ignore an unsolicited request to open attachments or files. Or, independently verify that the supposed source actually sent the email to you by making contact using a published email address or telephone number.

5. **Be suspicious of strangers asking for personal info.** If someone contacts you unexpectedly online and asks for your personal information, it's highly unlikely it's legitimate. A sound strategy is to ignore unsolicited requests for information, no matter how real they appear, especially if you're asked for information such as a Social Security number, bank account numbers and passwords.
6. **Use secure processes when logging into financial accounts.** Exactly what are some of the most secure steps you can take when logging into financial accounts? Create "strong" passwords that are extremely difficult to guess. Change them often. And don't use the same passwords or PINs (personal identification numbers) for multiple accounts.
7. **Be discreet when using social networking sites.** Criminals comb social media sites looking for information such as someone's 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.
8. **Be careful when using smartphones and tablets.** Never leave your mobile device unattended and use a device password or other method to control access if it's stolen or lost.
9. **Include your children in cybersecurity plannin.** If you're a parent or caregive, include your children in your cybersecurity measures. Talk about being safe online, including the risks of sharing personal information with people they don't know, and make sure the devices they use to connect to the Internet have up-to-date security.
10. **Businesses should train employees in cybersecurity.** Small business owners are wise to have policies and training for their employees on topics similar to those provided here, plus other issues that are specific to the business. For example, consider requiring more information beyond a password to gain access to your business's network, and additional safety measures, such as requiring confirmation calls with your financial institution before certain electronic transfers are authorized.

For more cybersecurity information, go to: www.riverhillsbank.com/cybersecurity

RiverHills Bank

Member FDIC

EQUAL HOUSING LENDER