Availa Bank

We're *AVAILA*ble for YOU!

Use Data Privacy Day as an excuse to ensure your data is protected

In today's digital society, protecting data has become increasingly important – so much that there is a specific day set aside to commemorate how crucial it has become. January 28th is Data Privacy Day. With that in mind, Availa Bank wants to ensure consumers know how to determine their digital information is secure.

About 15 million people in the U.S. alone have their identities stolen each year, and those cases result in financial losses of around $50 billion. Practicing safe online behavior is one simple way that consumers can protect against becoming a victim of cybercrime.

10 simple ways to help secure your data

1. **Shred printed documents:** Make sure you shred any documents that contain sensitive information, such as Social Security, credit card or bank account numbers. That will prevent criminals from pulling them out of your trash.
2. **Set strong passwords:** Cybercriminals are becoming more sophisticated in how they are able to obtain victims' login information. Setting strong passwords that use a variety of letters, numbers and special characters helps prevent criminals from accessing your information.
3. **Be careful shopping online:** Online shopping has created an extra level of convenience, but with that conveniences comes another avenue for cybercriminals to compromise your data. Only shop from known and trusted sources, and be sure that the company's checkout website is secure. Before entering credit card info, make sure the word, "secure," or a closed padlock icon appear next to the URL in the web address bar.
4. **Lock your phone:** Your cell phone holds tons of your personal information. That makes locking your phone with a pass code crucial to ensuring thieves don't gain easy access to your bank accounts, email and other data.
5. **Know how to spot phishing scams:** Cybercriminals often gain access to personal information through phishing scams. Phishing is used to obtain sensitive information by disguising a fraudulent electronic communication as a trustworthy entity. When you click on a link and enter your information, it is automatically transferred to the criminal. Before clicking on any

links, examine the email carefully for signs that it may be fraudulent. Signs include misspelling, poor grammar or a return email address that doesn't match the organization name. If you are unsure whether the communication is fraudulent or not, contact the organization directly without clicking on any links.

6. **Check URLs before clicking on them:** Before clicking on a link, hover over it to see a preview of the URL. If it looks suspicious and does not actually contain the company name, do NOT click on it.
7. **Do NOT access accounts using public Wi-Fi:** Many businesses today offer unprotected Wi-Fi networks that customers can use for their convenience. Because they are unprotected, it is easier for cybercriminals to gain access to your accounts while you are connected to them. While it is OK to use such networks for general web browsing, it is unwise to use them to access any type of banking, credit card or shopping account.
8. **Review privacy settings on social media:** Most social media websites have privacy features that can be enabled to prevent people you don't know from seeing your social network activity. Explore the settings of the social networks you use to ensure that your accounts are private.
9. **Take advantage of two-factor authentication:** Many websites now offer an extra wall of security through two-factor authentication. Through two-factor authentication, you receive a temporary code through a text message that must be entered before you can log into your account. Because this code is sent to a device that only you have access to, it can prevent cybercriminals from accessing your count even if they are able to obtain your username and password.
10. **Monitor your credit report:** Your credit report can tell you whether your accounts have been compromised. Visit www.annualcreditreport.com to request your free report each year and examine it for suspicious activity.