BLACK

Top Ten Cyber Security Tips

1. Limit the personal information given to online services and frequently monitor your credit score and bank accounts for signs of fraudulent activity. Report anything suspicious to your financial institution immediately.

2. Never send sensitive information in an unencrypted form. Look for the green lock in your browser on websites.

3. If you are storing sensitive data or information on a removable drive, use an encrypted drive or encrypt the files themselves.

4. Be aware of emails that you are not expecting that contain attachments; verify the validity of the attachment from the sender prior to opening it. If the message appears suspicious, do not open the attachment. Spear-phishing emails often appear to be from a colleague or corporation known by the target, but contain an attachment that is actually a virus or Trojan.

5. Exercise caution when following links on social media sites or in emails, as they could be scams. Enable your email server so that it disables auto-clicking on links will protect against some phishing scams and other unsolicited emails.

6. Download trusted applications and limit the sensitive activities that take place on your mobile devices. While malware exists for all mobile operating systems, Android is by far the most vulnerable due to its susceptibility of system attacks and viruses. iOS products—such as the iPhone and the iPad—are generally more secure than their Android counterparts because Apple fully vets all applications before they are available on the App Store.

7. Be aware of your surroundings when at an ATM or other point of sale; always cover the number pad when entering PIN numbers during a transaction to prevent someone from recording your PIN.

8. Shred sensitive paper documents.

9. Sign up for a credit monitoring service that provides you with alerts. You can also lock your credit by contacting the credit bureaus.

10. Always use two-factor authentication with any websites, social media accounts, or services that have sensitive information. Use a password manager such as LastPass to help manage complex passwords.