FirsTrust

CYBERSECURITY CHECKLIST

Based on the answers given on the Cyber Scorecard, review the checklist for the key activities needed to be performed to reduce your risk.

	Checklist	Completed?
1	Enable two-factor authorization on all your accounts that contain personally identifiable information, e.g., email, banking, and other financial accounts.	
1	Consider downloading a password manager and install in on all your computers and devices including cell phones.	
2	Install a VPN program on your laptop and cell phones for safe WiFi.	
3	Change your router's default username and password (factory settings are easily guessed).	
3	Set your router's encryption setting to WPA2 or WPA3.	
3	Check your router's firmware and update if needed.	
4	Create text or email alerts in your bank accounts and credit cards. They typically offer multiple types of alerts include one associated with spending habits.	
5	Place a free credit freeze on your credit at all 3 bureaus (Equifax, Experian & TransUnion).	
5	If you have children under the age of 18, place a credit freeze on their credit files at all 3 bureaus as well.	
6	If your passwords are easily-guessable, update them. Do not re-use them on multiple sites. As mentioned above, consider using a password manager. (Note: As of 2021, Microsoft recommends passwords are at least 8 characters in length and are not easily-guessable; for example, password123, 1234567890)	
7	Install an antivirus program with auto update turned on.	
8	Install a backup program on your computer that updates regularly.	
9	Set your software programs for auto update including operating systems, Microsoft products, etc.	
10	If applicable, install an anti-virus application on your non-Apple cell phones.	
11	Never click on a link that you were not expecting to receive. Instead, open a new browser window and go to that site intentionally. Neverl click on a link sent in a text unless you were expecting it. Call the company's listed phone number to verify any suspicious activity. (NOTE: Companies will not call you on the phone to request sensitive information or to log onto your computer. If this happens, hang up and report the call to the intended party immediately.)	
11	Report fraudulant activity to the government: Text/Phone calls->ReportFraud.ftc.gov; Internet->www.ic3.gov	
12	Ask your neighbors or do a google search to locate a local resource that can assist you with fixing your computer in the event of an attack. For training, contact your local community colleges; many offer low cost computer training courses.	
13	Purchase a document shredder and use it for documents that contain personally identifiable information.	

Great job in securing your electronic devices and lowering your cybersecurity risk!