ಇಂಟರ್ನೆಟ್ ಬ್ಯಾಂಕಿಂಗ್ ಅನ್ನು ಸುರಕ್ಷಿತವಾಗಿ ಬಳಸುವ ಸಲಹೆಗಳು

ಇಂದು , ಬಿಲ್ ಪಾವತಿಗಳು, ಹಣ ವರ್ಗಾವಣೆ ಅಥವಾ ನಿಶ್ಚಿತ ಠೇವಣಿ ರಚನೆಯಾಗಿದ್ದಲ್ಲಿ, ಇಂಟರ್ನೆಟ್ ಬ್ಯಾಂಕಿಂಗ್ ನಿಮಗೆ ಇದನ್ನು ತ್ವರಿತ ಮತ್ತು ಅನುಕೂಲಕರ ರೀತಿಯಲ್ಲಿ ಮಾಡಲು ಅನುಮತಿಸುತ್ತದೆ. ಬ್ಯಾಂಕಿನಲ್ಲಿ ಹೋಗುವುದಕ್ಕೆ ಬದಲಾಗಿ ಮತ್ತು ನಿರಂತರವಾಗಿ ಸರದಿಯಲ್ಲಿ ಕಾಯುವ ಬದಲಾಗಿ, ಇಂಟರ್ನೆಟ್ ಬ್ಯಾಂಕಿಂಗ್ ಕೆಲವು ಬ್ಯಾಂಕಿಂಗ್ ಕಾರ್ಯಗಳನ್ನು ಕೆಲವು ಕ್ಲಿಕ್ಗಳ ಮೂಲಕ ಪ್ರವೇಶಿಸಬಹುದು. ಆದಾಗ್ಯೂ, ನಿಮ್ಮ ಗೌಪ್ಯ ಬ್ಯಾಂಕಿಂಗ್ ಮಾಹಿತಿಯನ್ನು ಪಡೆದುಕೊಳ್ಳುವ ಫಿಶಿಂಗ್ ಅಪಾಯದ ಕಾರಣದಿಂದಾಗಿ ಈ ಸೌಲಭ್ಯವನ್ನು ಜಾಗರೂಕತೆಯಿಂದ ಬಳಸಬೇಕಾಗಿದೆ. ಇಂಟರ್ನೆಟ್ ಬ್ಯಾಂಕಿಂಗ್ಗಾಗಿ ಏಳು ಸ್ಮಾರ್ಟ್ ಸುಳಿವುಗಳು ಕೆಳಗೆ ಪಟ್ಟಿಮಾಡಲಾಗಿದೆ :

1. **ನಿಮ್ಮ ಪಾಸ್ವರ್ಡ್ ನಿಯಮಿತವಾಗಿ ಬದಲಾಯಿಸಿ**

   ನಿಮ್ಮ ಇಂಟರ್ನೆಟ್ ಬ್ಯಾಂಕಿಂಗ್ ಖಾತೆಗೆ ನೀವು ಮೊದಲ ಬಾರಿಗೆ ಲಾಗಿನ್ ಮಾಡಿದರೆ, ಬ್ಯಾಂಕ್ ಒದಗಿಸಿದ ಗುಪ್ತಪದವನ್ನು ನೀವು ಬಳಸಬೇಕಾಗುತ್ತದೆ. ಆದಾಗ್ಯೂ, ನಿಮ್ಮ ಖಾತೆಯನ್ನು ಸುರಕ್ಷಿತವಾಗಿರಿಸಲು ನೀವು ಈ ಪಾಸ್ವರ್ಡ್ ಅನ್ನು ಬದಲಾಯಿಸಬೇಕಾಗಿದೆ. ಹೆಚ್ಚುವರಿಯಾಗಿ, ನಿಯಮಿತ ಮಧ್ಯಂತರದಲ್ಲಿ ನಿಮ್ಮ ಪಾಸ್ವರ್ಡ್ ಅನ್ನು ಬದಲಿಸಿಕೊಳ್ಳಿ. ಹೆಚ್ಚು ಮುಖ್ಯವಾಗಿ, ಎಲ್ಲಾ ಸಮಯದಲ್ಲೂ ಗುಪ್ತಪದವನ್ನು ರಹಸ್ಯವಾಗಿ ಇರಿಸಿ.

2. **ಲಾಗಿನ್ ಮಾಡಲು ಸಾರ್ವಜನಿಕ ಕಂಪ್ಯೂಟರ್ಗಳನ್ನು ಬಳಸಬೇಡಿ**

   ಸೈಬರ್ ಕೆಫೆಗಳಲ್ಲಿ ಅಥವಾ ಗ್ರಂಥಾಲಯಗಳಲ್ಲಿನ ಸಾಮಾನ್ಯ ಕಂಪ್ಯೂಟರ್ಗಳಲ್ಲಿ ನಿಮ್ಮ ಬ್ಯಾಂಕ್ ಖಾತೆಗೆ ಲಾಗಿಂಗ್ ಮಾಡುವುದನ್ನು ತಪ್ಪಿಸಿ. ಇವುಗಳು ಕಿಕ್ಕಿರಿದ ಸ್ಥಳಗಳಾಗಿವೆ, ಮತ್ತು ನಿಮ್ಮ ಪಾಸ್ವರ್ಡ್ ಅನ್ನು ಇತರರು ಪತ್ತೆಹಚ್ಚುವ ಅಥವಾ ನೋಡಬಹುದಾದ ಹೆಚ್ಚಿನ ಅವಕಾಶಗಳಿವೆ. ಅಂತಹ ಸ್ಥಳಗಳಿಂದ ನೀವು ಲಾಗಿನ್ ಮಾಡಬೇಕಾದರೆ, ನೀವು ಸಂಗ್ರಹ ಮತ್ತು ಬ್ರೌಸಿಂಗ್ ಇತಿಹಾಸವನ್ನು ತೆರವುಗೊಳಿಸಿ, ಕಂಪ್ಯೂಟರ್ನಿಂದ ತಾತ್ಕಾಲಿಕ ಫೈಲ್ಗಳನ್ನು ಅಳಿಸಿಹಾಕುವುದನ್ನು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಿ. ಅಲ್ಲದೆ, ಬ್ರೌಸರ್ ನಿಮ್ಮ ID ಮತ್ತು ಪಾಸ್ವರ್ಡ್ ಅನ್ನು ನೆನಪಿಟ್ಟುಕೊಳ್ಳಲು ಎಂದಿಗೂ ಅನುಮತಿಸುವುದಿಲ್ಲ.

3. **ನಿಮ್ಮ ವಿವರಗಳನ್ನು ಯಾರೊಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ**

   ಫೋನ್ ಅಥವಾ ಇಮೇಲ್ ಮೂಲಕ ನಿಮ್ಮ ಗೌಪ್ಯ ಮಾಹಿತಿಯನ್ನು ನಿಮ್ಮ ಬ್ಯಾಂಕ್ ಎಂದಿಗೂ ಕೇಳುವುದಿಲ್ಲ. ಹಾಗಾಗಿ ನೀವು ಬ್ಯಾಂಕಿನಿಂದ ಅಥವಾ ನಿಮ್ಮ ವಿವರಗಳನ್ನು ಕೋರುವ ಇಮೇಲ್ನಿಂದ ಸ್ಪಷ್ಟ ದೂರವಾಣಿ ಕರೆಯನ್ನು ಪಡೆಯುತ್ತೀರಾ, ನಿಮ್ಮ ಲಾಗಿನ್ ಮಾಹಿತಿಯನ್ನು ನೀಡುವುದಿಲ್ಲ. ಬ್ಯಾಂಕ್ನ ಅಧಿಕೃತ ಲಾಗಿನ್ ಪುಟದಲ್ಲಿ ಮಾತ್ರ ನಿಮ್ಮ ಲಾಗಿನ್ ID ಮತ್ತು ಪಾಸ್ವರ್ಡ್ ಅನ್ನು ಬಳಸಿ, ಇದು ಸುರಕ್ಷಿತ ವೆಬ್ಸೈಟ್ ಆಗಿರಬೇಕು. ಲಾಗ್ ಇನ್ ಮಾಡುವಾಗ URL ನಲ್ಲಿ 'https: //' ನೋಡಿ; ಇದರರ್ಥ ವೆಬ್ಸೈಟ್ ಸುರಕ್ಷಿತವಾಗಿದೆ.

4. **ನಿಮ್ಮ ಉಳಿತಾಯ ಖಾತೆಯನ್ನು ನಿಯಮಿತವಾಗಿ ಪರಿಶೀಲಿಸುತ್ತಿರಿ**

   ಯಾವುದೇ ವಹಿವಾಟನ್ನು ಆನ್ಲೈನ್ನಲ್ಲಿ ಮಾಡಿದ ನಂತರ ನಿಮ್ಮ ಖಾತೆಯನ್ನು ಪರಿಶೀಲಿಸಿ. ನಿಮ್ಮ

ಖಾತೆಯಿಂದ ಸರಿಯಾದ ಮೊತ್ತವನ್ನು ಕಡಿತಗೊಳಿಸಲಾಗಿದೆಯೆ ಎಂದು ಪರಿಶೀಲಿಸಿ. ಮೊತ್ತದಲ್ಲಿ ಯಾವುದೇ ವ್ಯತ್ಯಾಸಗಳನ್ನು ನೀವು ನೋಡಿದರೆ, ತಕ್ಷಣವೇ ಬ್ಯಾಂಕ್ಗೆ ತಿಳಿಸಿ.

5. **ಯಾವಾಗಲೂ ಪರವಾನಗಿ ಪಡೆದ ಆಂಟಿ-ವೈರಸ್ ಸಾಫ್ಟ್ವೇರ್ ಅನ್ನು ಬಳಸಿ**

   ನಿಮ್ಮ ಕಂಪ್ಯೂಟರ್ ಅನ್ನು ಹೊಸ ವೈರಸ್ಗಳಿಂದ ರಕ್ಷಿಸಲು, ನೀವು ಯಾವಾಗಲೂ ಪರವಾನಗಿ ಪಡೆದ ಆಂಟಿ-ವೈರಸ್ ಸಾಫ್ಟ್ವೇರ್ ಅನ್ನು ಬಳಸುತ್ತಿದ್ದಾರೆ ಎಂದು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಿ. ವಿರೋಧಿ ವೈರಸ್ ತಂತ್ರಾಂಶಗಳ ಪೈರೇಟೆಡ್ ಆವೃತ್ತಿಗಳು ಉಚಿತವಾಗಿ ಲಭ್ಯವಾಗಬಹುದು, ಆದರೆ ಅವರು ನಿಮ್ಮ ಕಂಪ್ಯೂಟರ್ ಅನ್ನು ಆನ್ಲೈನ್ ಜಗತ್ತಿನಲ್ಲಿ ಪ್ರಚಲಿತದಲ್ಲಿರುವ ಹೊಸ ವೈರಸ್ಗಳಿಂದ ರಕ್ಷಿಸಲು
   ವಿಫಲವಾಗಬಹುದು. ಹೆಚ್ಚುವರಿಯಾಗಿ, ನೀವು ಸಾಫ್ಟ್ವೇರ್ನಲ್ಲಿ ನವೀಕರಣಗಳಿಗಾಗಿ ನಿಯತಕಾಲಿಕವಾಗಿ ಅಧಿಸೂಚನೆಗಳನ್ನು ಪಡೆಯುತ್ತೀರಿ. ನಿಮ್ಮ ವಿರೋಧಿ ವೈರಸ್ ಅನ್ನು ನೀವು ನವೀಕರಿಸಿದ್ದೀರಿ ಎಂದು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಿ, ಆದ್ದರಿಂದ ನಿಮ್ಮ ಗೌಪ್ಯ ಮಾಹಿತಿಯನ್ನು ಯಾವಾಗಲೂ ರಕ್ಷಿಸಲಾಗುತ್ತದೆ.

6. **ಬಳಕೆಯಲ್ಲಿಲ್ಲದಿದ್ದಾಗ ಇಂಟರ್ನೆಟ್ ಸಂಪರ್ಕವನ್ನು ಕಡಿತಗೊಳಿಸಿ**

   ಹೆಚ್ಚಿನ ಬ್ರಾಡ್ಬ್ಯಾಂಡ್ ಬಳಕೆದಾರರು ತಮ್ಮ ಕಂಪ್ಯೂಟರ್ನಲ್ಲಿ ಇಂಟರ್ನೆಟ್ ಸಂಪರ್ಕವನ್ನು ಬಳಸದೆ ಇರುವಾಗ ಅವುಗಳನ್ನು ಸಂಪರ್ಕ ಕಡಿತಗೊಳಿಸುವುದಿಲ್ಲ. ದುರುದ್ದೇಶಪೂರಿತ ಹ್ಯಾಕರ್ಸ್ ಇಂಟರ್ನೆಟ್ ಸಂಪರ್ಕದ ಮೂಲಕ ನಿಮ್ಮ ಕಂಪ್ಯೂಟರ್ ಅನ್ನು ಪ್ರವೇಶಿಸಬಹುದು ಮತ್ತು ನಿಮ್ಮ ರಹಸ್ಯವಾದ ಬ್ಯಾಂಕಿಂಗ್ ಮಾಹಿತಿಯನ್ನು ಕದಿಯಬಹುದು. ನಿಮ್ಮ ಡೇಟಾವನ್ನು ರಕ್ಷಿಸಲು, ನೀವು ಇಂಟರ್ನೆಟ್ನಲ್ಲಿ ಬೇಡವಾದಾಗ ನೀವು ಸಂಪರ್ಕ ಕಡಿತಗೊಳಿಸುತ್ತೀರಿ ಎಂದು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಿ.

7. **ನಿಮ್ಮ ಇಂಟರ್ನೆಟ್ ಬ್ಯಾಂಕಿಂಗ್ URL ಟೈಪ್ ಮಾಡಿ**

   ಇಮೇಲ್ನಲ್ಲಿ ನೀಡಲಾದ ಲಿಂಕ್ಗಳನ್ನು ಕ್ಲಿಕ್ ಮಾಡುವುದರ ಬದಲು ಬ್ರೌಸರ್ನ ವಿಳಾಸ ಪಟ್ಟಿಯಲ್ಲಿ ನಿಮ್ಮ ಬ್ಯಾಂಕ್ URL ಅನ್ನು ಟೈಪ್ ಮಾಡಲು ಸುರಕ್ಷಿತವಾಗಿದೆ. ಮೋಸದ ವೆಬ್ಸೈಟ್ಗಳ ಲಿಂಕ್ಗಳೊಂದಿಗೆ ವಂಚನೆದಾರರು ಇಮೇಲ್ಗಳನ್ನು ಕಳುಹಿಸುವ ನಿದರ್ಶನಗಳಿವೆ, ಅದು ಬ್ಯಾಂಕಿನ ಮೂಲ ವೆಬ್ಸೈಟ್ನಂತೆಯೇ ವಿನ್ಯಾಸಗೊಳಿಸಲಾಗಿದೆ. ಅಂತಹ ವೆಬ್ಸೈಟ್ನಲ್ಲಿ ನೀವು ನಿಮ್ಮ ಲಾಗಿನ್ ವಿವರಗಳನ್ನು ನಮೂದಿಸಿದ ನಂತರ, ನಿಮ್ಮ ಖಾತೆಯನ್ನು ಪ್ರವೇಶಿಸಲು ಮತ್ತು ನಿಮ್ಮ ಹಣವನ್ನು ಕದಿಯಲು ಅವುಗಳನ್ನು ಬಳಸಬಹುದು. ಲಾಗ್ ಆನ್ ಮಾಡುವಾಗ, URL ನಲ್ಲಿ 'https: //' ಅನ್ನು ಪರಿಶೀಲಿಸಿ ಮತ್ತು ಇದು ನಿಮ್ಮ ಬ್ಯಾಂಕಿನ ಅಧಿಕೃತ ವೆಬ್ಸೈಟ್ ಎಂದು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಿ.