

ಇಂದೇ ಅಳವಡಿಸಿಕೊಳ್ಳಬೇಕಾದ ಒಂಬತ್ತು ಅಗತ್ಯ ಸೈಬರ್ ಭದ್ರತಾ ಅಭ್ಯಾಸಗಳು.



1. ನೀವು ಕ್ಲಿಕ್ ಮಾಡುವ ಮೊದಲು ಯೋಚಿಸಿ!

ಲಿಂಕ್‌ಗಳ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡುವ ಮೊದಲು ಅಥವಾ ಲಗತ್ತುಗಳನ್ನು ತೆರೆಯುವ ಮೊದಲು , ಅವುಗಳು ನಿಮಗೆ ತಿಳಿದಿರುವವರಿಂದ ಬಂದಂತೆ ಕಂಡುಬಂದರೂ ಸಹ ಎರಡು ಬಾರಿ ಯೋಚಿಸಿ

- ಅಜ್ಞಾತ ಲಿಂಕ್‌ಗಳ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡುವ ಬದಲು ಯಾವಾಗಲೂ, ತಿಳಿದಿರುವ, ಕಾನೂನುಬದ್ಧ ಮೂಲ
- (ಉದಾ. HTTPS) ವೆಬ್‌ಸೈಟ್‌ಗಳಿಗೆ ನ್ಯಾವಿಗೇಟ್ ಮಾಡಿ
- ಲಗತ್ತು ಅನಿರೀಕ್ಷಿತವಾಗಿ ಕಂಡುಬಂದರೆ, ವಿಶ್ವಾಸಾರ್ಹ ವಿಧಾನದ ಮೂಲಕ ಕಳುಹಿಸಿದವರೊಂದಿಗೆ ದೃಢೀಕರಿಸಿ ಅಥವಾ ಮುಂಜಾಗ್ರತೆ ವಹಿಸಿ ಕ್ಲಿಕ್ ಮಾಡದಿರಲು ಆಯ್ಕೆಮಾಡಿ.



2. ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯ ಅನುಮತಿಗಳನ್ನು ಪರಿಶೀಲಿಸಿ

ಖಾಸಗಿ ಮಾಹಿತಿಗಳ ರಿಕ್ವೆಸ್ಟ್ ಗಳನ್ನು ಯಾವಾಗಲೂ ದೃಢೀಕರಿಸಿ-ಅದು ನಿಮ್ಮದೇ ಆಗಿರಲಿ ಅಥವಾ ಬೇರೆಯವರದಾಗಿರಲಿ.

- ಸ್ಯಾಮರ್‌ಗಳು ವಿಶ್ವಾಸಾರ್ಹ ಸಂಪರ್ಕಗಳನ್ನು ಸುಲಭವಾಗಿ ಪ್ರತಿರೂಪಿಸಬಹುದು
- ಅಸಾಮಾನ್ಯ ಚಟುವಟಿಕೆಗಾಗಿ ಆರ್ಥಿಕ ವಿವರಣೆಗಳು ಮತ್ತು ಕ್ರೆಡಿಟ್ ವರದಿಗಳನ್ನು ನಿಯಮಿತವಾಗಿ ಪರಿಶೀಲಿಸಿ.
- ಅನೇಕ ಫಿಶಿಂಗ್ ಸಂದೇಶಗಳು ಪದ ಮತ್ತು ವ್ಯಾಕರಣ ದೋಷಗಳನ್ನು ಒಳಗೊಂಡಿರುತ್ತವೆ.
- ವಿನಂತಿಯು ನ್ಯಾಯಸಮ್ಮತವಾಗಿದೆಯೇ ಎಂದು ಪರಿಗಣಿಸಿ. ವ್ಯಕ್ತಿ ಅಥವಾ ಸಂಸ್ಥೆಗೆ ಆ ಮಾಹಿತಿಯ ಅವಶ್ಯಕತೆ ಇದೆಯೇ ಎಂದು ಪರಿಶೀಲಿಸಿ.



3. ನಿಮ್ಮ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ನಿಯಂತ್ರಿಸಿ

ನಿಮ್ಮ ಖಾತೆಗಳನ್ನು ಸುರಕ್ಷಿತವಾಗಿರಿಸಲು ಬಲವಾದ, ಸಂಕೀರ್ಣವಾದ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ರಚಿಸುವುದು ಮತ್ತು ಅವುಗಳನ್ನು ಬುದ್ಧಿವಂತಿಕೆಯಿಂದ ನಿರ್ವಹಿಸುವುದು ಅತ್ಯಗತ್ಯ.

- ವಿಭಿನ್ನ ಖಾತೆಗಳಿಗಾಗಿ ಅನನ್ಯ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ಬಳಸಿ.
- ವೃತ್ತಿ ಮತ್ತು ವೈಯಕ್ತಿಕ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ಪ್ರತ್ಯೇಕವಾಗಿ ಇರಿಸಿ.
- ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ಎಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.
- ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ಆಗಾಗ್ಗೆ ಬದಲಾಯಿಸಿ.
- ಬ್ರೌಸರ್‌ಗಳಲ್ಲಿ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ಉಳಿಸುವುದರಿಂದ ಹೊರಗುಳಿಯಿರಿ.
- ಹೆಚ್ಚಿನ ಭದ್ರತೆಗಾಗಿ ಬಹು ಅಂಶ ದೃಢೀಕರಣವನ್ನು (MFA) ಸಕ್ರಿಯಗೊಳಿಸಿ.



4. ನಿಮ್ಮ ಡಿವೈಸ್ ಗಳನ್ನು ಸುರಕ್ಷಿತಗೊಳಿಸಿ

ನಿಮ್ಮ ವರ್ಕ್ ಸ್ಪೇಸ್ ಅನ್ನು ಲಾಕ್ ಮಾಡಿ ಮತ್ತು ದೂರ ಹೋಗುವಾಗ ನಿಮ್ಮ ಡಿವೈಸ್ ಗಳನ್ನು ರಕ್ಷಿಸಿ.

- ಯಾವಾಗಲೂ ನಿಮ್ಮ ಕಂಪ್ಯೂಟರ್ ಪರದೆಯನ್ನು ಲಾಕ್ ಮಾಡಿ.
- ನಿಮ್ಮ ಫೋನ್ ಮತ್ತು ಪೋರ್ಟೆಬಲ್ ಸಾಧನಗಳನ್ನು ನಿಮ್ಮೊಂದಿಗೆ ತೆಗೆದುಕೊಳ್ಳಿ ಅಥವಾ ಅವುಗಳನ್ನು ಸುರಕ್ಷಿತವಾಗಿ ಸಂಗ್ರಹಿಸಿ.
- ಸಾಧ್ಯವಾದಾಗಲೆಲ್ಲಾ ಬಲವಾದ ದೃಢೀಕರಣ ವಿಧಾನಗಳನ್ನು ಬಳಸಿ.



5. ಪ್ರಮುಖ ಫೈಲ್‌ಗಳನ್ನು ಬ್ಯಾಕಪ್ ಮಾಡಿ

ನಿಮ್ಮ ನಿರ್ಣಾಯಕ ಡೇಟಾವನ್ನು ನಿಯಮಿತವಾಗಿ ಬ್ಯಾಕಪ್ ಮಾಡಲಾಗಿದೆಯೇ ಎಂದು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಿ.

- ಮೂಲ ಸ್ಥಳವಲ್ಲದೇ ಪ್ರತ್ಯೇಕ ಸ್ಥಳದಲ್ಲಿ ಬ್ಯಾಕಪ್‌ಗಳನ್ನು ಸಂಗ್ರಹಿಸಿ.
- ಸಂಸ್ಥೆಯ ಅನುಮೋದಿತ ಶೇಖರಣಾ ವ್ಯವಸ್ಥೆಯನ್ನು ಬಳಸಿ.
- ಬ್ಯಾಕಪ್‌ಗಳು ಸರಿಯಾಗಿ ಕಾರ್ಯನಿರ್ವಹಿಸುವುದನ್ನು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಲು ನಿಯಮಿತವಾಗಿ ಪರೀಕ್ಷಿಸಿ.



6. ಅನುಮಾನಾಸ್ಪದ ಚಟುವಟಿಕೆಗಳನ್ನು ವರದಿ ಮಾಡಿ

ಏನಾದರೂ ಅನುಮಾನಾಸ್ಪದವಾಗಿ ಕಂಡುಬಂದರೆ, ನಿಮ್ಮ ಪ್ರವೃತ್ತಿಯನ್ನು ನಂಬಿರಿ-ಅದನ್ನು ವರದಿ ಮಾಡಿ!

- ನಿಮ್ಮ ಮೇಲ್ವಿಚಾರಕರನ್ನು ಎಚ್ಚರಿಸಿ ಮತ್ತು ಶಂಕಿತ ಹಗರಣಗಳು ಅಥವಾ ಅನುಮಾನಾಸ್ಪದ ಚಟುವಟಿಕೆಗಳಿಗಾಗಿ ನಿಮ್ಮ ಸಂಸ್ಥೆಯ ವರದಿ ಮಾಡುವ ಪ್ರೋಟೋಕಾಲ್ ಅನ್ನು ಅನುಸರಿಸಿ.



7. ನೀವೂ ಕಲಿತು, ಇತರರಿಗೂ ತಿಳಿಸಿ

ಇತ್ತೀಚಿನ ಸೈಬರ್ ಭದ್ರತಾ ಬೆದರಿಕೆಗಳು ಮತ್ತು ಪ್ರವೃತ್ತಿಗಳ ಕುರಿತು ಅರಿಯಿರಿ.

- ತರಬೇತಿಗಳಿಗೆ ಹಾಜರಾಗಿ ಮತ್ತು ನಿಮಗೆ ಅವಕಾಶ ಸಿಕ್ಕಾಗಲೆಲ್ಲಾ ಸಹೋದ್ಯೋಗಿಗಳೊಂದಿಗೆ ನಿಮ್ಮ ಜ್ಞಾನವನ್ನು ಹಂಚಿಕೊಳ್ಳಿ.
- ಸೈಬರ್ ಬೆದರಿಕೆಗಳ ವಿರುದ್ಧ ಉತ್ತಮ ಮಾಹಿತಿಯುಳ್ಳ ತಂಡವು ನಿಮ್ಮ ಮೊದಲ ರಕ್ಷಣೆಯಾಗಿದೆ.



8. ಸುರಕ್ಷಿತ ನೆಟ್‌ವರ್ಕ್‌ಗಳನ್ನು ಬಳಸಿ

ಯಾವಾಗಲೂ ಸುರಕ್ಷಿತ ನೆಟ್‌ವರ್ಕ್‌ಗಳನ್ನು ಬಳಸಿ, ವಿಶೇಷವಾಗಿ ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯನ್ನು ವೀಕ್ಷಿಸುವಾಗ

- ಹಣಕಾಸಿನ ವಹಿವಾಟುಗಳು ಅಥವಾ ಸೂಕ್ಷ್ಮ ಕೆಲಸಗಳಿಗಾಗಿ ಸಾರ್ವಜನಿಕ Wi-Fi ಅನ್ನು ಬಳಸದಿರಿ.
- ಹೆಚ್ಚುವರಿ ರಕ್ಷಣೆಗಾಗಿ ಅಗತ್ಯವಿದ್ದಾಗ ವರ್ಚುವಲ್ ಪ್ರೈವೇಟ್ ನೆಟ್‌ವರ್ಕ್ (VPN) ಬಳಸಿ.



9. ಸಾಮಾಜಿಕ ಜಾಲತಾಣಗಳಲ್ಲಿ ಜಾಗರೂಕರಾಗಿರಿ

ನೀವು ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಹಂಚಿಕೊಳ್ಳುವ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯ ಪ್ರಮಾಣವನ್ನು ತಗ್ಗಿಸಿ. ಇದರಿಂದ ನೀವು ನಿಮ್ಮ ಗೌಪ್ಯತೆಯನ್ನು ರಕ್ಷಿಸಬಹುದು, ನಿಮ್ಮ ಸುರಕ್ಷತೆಯನ್ನು ಹೆಚ್ಚಿಸಬಹುದು ಮತ್ತು ಹೆಚ್ಚು ಸಕಾರಾತ್ಮಕ ಆನ್‌ಲೈನ್ ಅನುಭವವನ್ನು ಪಡೆಯಬಹುದು.

- ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮ ಪ್ಲಾಟ್‌ಫಾರ್ಮ್‌ಗಳಲ್ಲಿ ಗೌಪ್ಯತೆಯ ಸೆಟ್ಟಿಂಗ್‌ಗಳನ್ನು ಪರಿಶೀಲಿಸಿ.
- ಫ್ರೆಂಡ್ ರಿಕೆಸ್ಟ್‌ಗಳ ಬಗ್ಗೆ ಗಮನವಿರಲಿ ಹಾಗೆಯೇ ನಿಮ್ಮ ಮಾಹಿತಿಗೆ ಯಾರು ಪ್ರವೇಶವನ್ನು ಹೊಂದಿದ್ದಾರೆ ಎಂದು; ಲಾಕ್ ಮಾಡಿದ ಪ್ರೊಫೈಲ್‌ನಿಂದ ವಿನಂತಿಗಳನ್ನು ಸ್ವೀಕರಿಸಬೇಡಿ.
- ಸಂಭಾವ್ಯ ಅಪಾಯಗಳನ್ನು ಕಡಿಮೆ ಮಾಡಲು ನಿಮ್ಮ ಆನ್‌ಲೈನ್ ಉಪಸ್ಥಿತಿಯನ್ನು ನಿಯಮಿತವಾಗಿ ಪರಿಶೀಲಿಸಿ.

ನೆನಪಿಡಿ: ಸೈಬರ್ ಭದ್ರತೆ ಪ್ರತಿಯೊಬ್ಬರ ಜವಾಬ್ದಾರಿಯಾಗಿದೆ!