HSBC

ಆನ್‌ಲೈನ್ ಸೆಕ್ಯೂರಿಟಿ ವೈಶಿಷ್ಟ್ಯಗಳು ಹಾಗೂ ಸುರಕ್ಷಿತ ಬಳಕೆಯ ಮಾರ್ಗಸೂಚಿಗಳು

ಒಟ್ಟಿಗೆ, ನಿಮ್ಮ ಆನ್‌ಲೈನ್ ಬ್ಯಾಂಕಿಂಗ್ ಅನ್ನು ಸುರಕ್ಷಿತವಾಗಿಡಲು ನಾವು ಹೇಗೆ ಸಹಾಯ ಮಾಡಬಹುದು ಎಂಬುದು ಇಲ್ಲಿದೆ .

ಒಂದು ಬ್ಯಾಂಕ್ ಅಗಿ ನಾವು ಭದ್ರತೆಯ ಬಗ್ಗೆ ಯೋಚಿಸುತ್ತಿದ್ದೇವೆ. ಇಂಟರ್‌ನೆಟ್‌ನ ಬೆಳವಣಿಗೆ ನಮ್ಮೆಲ್ಲರಿಗಾಗಿ ಹೆಚ್ಚಿನ ನಮ್ಯತೆಯನ್ನು ನೀಡುತ್ತದೆ, ಆದರೆ ಅದು ತರುವ ಹೊಸ ಅಪಾಯಗಳ ವಿರುದ್ಧ ರಕ್ಷಿಸಬೇಕು. ಎಚ್‌ಎಸ್‌ಬಿಸಿಯಲ್ಲಿ , ಯಾವುದೇ ಅನಧಿಕೃತ ಪ್ರವೇಶದಿಂದ ನಿಮ್ಮ ಖಾತೆಯನ್ನು ರಕ್ಷಿಸಲು ಗೌಪ್ಯತೆ, ತಂತ್ರಜ್ಞಾನ ಹಾಗೂ ಗುರುತಿಸುವಿಕೆ ಎಂಬ ಮೂರು ಪ್ರಮುಖ ಕ್ಷೇತ್ರಗಳ ಮೇಲೆ ಕೇಂದ್ರೀಸಿ ನಾವು ಉದ್ಯಮದ ಗುಣಮಟ್ಟ ದ ಸುರಕ್ಷತಾ ತಂತ್ರಜ್ಞಾನ ಹಾಗೂ ಆಚರಣೆಗಳನ್ನು ಬಳಸುತ್ತೇವೆ.

ನಿಮ್ಮ ಆನ್‌ಲೈನ್ ಬ್ಯಾಂಕಿಂಗ್ ಅನು ನಾವು ಹೇಗೆ ರಕ್ಷಿಸುತ್ತೇವೆ ಹಾಗೂ ನಿಮ್ಮ ಸ್ವಂತ ಆನ್‌ಲೈನ್ ಸುರಕ್ಷತೆಯನ್ನು ಸುಧಾರಿಸಲು ನೀವು ಯಾವ ಕ್ರಮಗಳನ್ನು ಕೈಗೊಳ್ಳಬಹುದು ಎಂಬುದನ್ನು ನೋಡಲು ಮುಂದೆ ಓದಿ.

ವಂಚನೆಯ ಪ್ರಕಾರಗಳು

ನಿಮ್ಮ ವೈಯಕ್ತಿಕ ಹಾಗೂ ಸುರಕ್ಷತಾ ವಿವರಗಳನ್ನು ನೀಡುವಂತೆ ಮೋಸಗಾರರು ನಿಮ್ಮನ್ನು ಮೋಸಗೊಳಿಸಲು ಪ್ರಯತ್ನಿಸುವ ವಿವಿಧ ಮಾರ್ಗಗಳಿವೆ. ಬ್ಯಾಂಕ್‌ನೊಂದಿಗೆ ನಿಮ್ಮ ಹಣಕಾಸಿನ ಮಾಹಿತಿಯ ಪ್ರವೇಶಾವಕಾಶವನ್ನು ಪಡೆಯಲು ಈ ವಿವರಗಳನ್ನು ಅವರು ಬಳಸುತ್ತಾರೆ ಹಾಗೂ ನಿಮ್ಮ ಖಾತೆಯಿಂದ ಅವರ ಖಾತೆಗಳಿಗೆ ಪಾವತಿಗಳನ್ನು ನೆಲೆಗೊಳಿಸುತ್ತಾರೆ.

ನೀವು ಎದುರಿಸಬಹುದಾದ ಕೆಲವು ಸಾಮಾನ್ಯ ವಂಚನೆಗಳು ಇಲ್ಲಿವೆ:

ಕ್ರೆಡಿಟ್/ಡೆಬಿಟ್ ಕಾರ್ಡ್ ಸ್ಕಿಮ್ಮಿಂಗ್ /ಕ್ಲೋನಿಂಗ್ :

ಕ್ರೆಡಿಟ್/ಡೆಬಿಟ್ ಕಾರ್ಡ್‌ನಲ್ಲಿನ ಮ್ಯಾಗ್ನೆಟಿಕ್ ಸ್ಟ್ರಿಪ್‌ನಿಂದ ಮಾಹಿತಿಯನ್ನು ಕದಿಯಬಹುದು. ಎಟಿಎಮ್‌ನ ಕಾರ್ಡ್ ಸ್ಲಾಟ್‌ನಲ್ಲಿ ಸ್ಕಿಮ್ಮಿಂಗ್ ಡಿವೈಸ್‌ಗಳನ್ನು ಮರೆಮಾಚುವ ಮೂಲಕ ಅಥವಾ ವಾಣಿಜ್ಯ ಪೇಮೆಂಟ್ ಟರ್ಮಿನಲ್‌ಗಳಲ್ಲಿ ನೀವು ಗಮನ ಹರಿಸದಿದ್ದಾಗ ಅವರು ಈ ಕೆಲಸವನ್ನು ಮಾಡುತ್ತಾರೆ. ಈ ಡಿವೈಸ್‌ಗಳು ನಿಮ್ಮ ಕಾರ್ಡ್ ವಿವರಗಳನ್ನು ಸ್ಕಾ ್ಯನ್ ಮಾಡುತ್ತವೆ ಹಾಗೂ ಸ್ಟೋರ್ ಮಾಡುತ್ತವೆ. ನಿಮ್ಮ ಪಿನ್‌ಅನ್ನು ಕದಿಯಲು, ವಂಚಕರು ಎಟಿಎಮ್‌ನಲ್ಲಿ ಅಥವಾ ವಾಣಿಜ್ಯ ಸಂಸ್ಥೆಯಲ್ಲಿ ವಿವೇಚನಾಯುಕ್ತ ಸ್ಥಳದಲ್ಲಿ ಕೆಮೆರಾವನ್ನು ಇರಿಸಬಹುದು.

ಯುಪಿಐ ಆ್ಯಪ್‌ಗಳಲ್ಲಿ ಹಗರಣ /ಪಾವತಿ ವಂಚನೆ

ಮೊಸಗಾರರು ಮೆಸೆಜಿಂಗ್ ಆ್ಯಪ್‌ಗಳ ಮೂಲಕ ನಿಮಗೆ ಕ್ಯೂಆರ್ ಕೋಡ್‌ಗಳನ್ನು ಕಳುಹಿಸಬಹುದು, ಅವರ ಖಾತೆಗೆ ಹಣವನ್ನು ವರ್ಗಾಯಿಸಲು ಕ್ಯೂಆರ್ ಕೋಡ್ ಅನ್ನು ಸ್ಕಾ ್ಯನ್ ಮಾಡಲು ಅಥವಾ ಱಕಲೆಕ್ಟ್ ಕೋರಿಕೆಯನ್ನುಱ ಅನುಮೋದಿಸಲು ನಿಮ್ಮನ್ನು ಕೇಳಬಹುದು. ನೀವು ಮಾರಾಟಮಾಡುತ್ತಿರುವ ಪ್ರಾಡಕ್ಟ್ ಖರಿದಿಸಲು ಅವರು ಬಯಸುತ್ತಾರೆ ಎಂದು ಹೇಳುವಂತಹ, ನಕಲಿ ಕಥೆಯನ್ನು ಹೇಳುವ ಮೂಲಕ ಅವರು ನಿಮ್ಮನ್ನು ಮೋಸಗೊಳಿಸಲು ಪ್ರಯತ್ನಿಸಬಹುದು. ಅವರು ಬ್ಯಾಂಕ್ ಅಥವಾ ಶಾಪಿಂಗ್ ಕಂಪನಿಯ ಕಾರ್ಯನಿರ್ವಾಹಕರಂತೆ ನಟಿಸಬಹುದು, ರಿಫಂಡ್‌ಗಳು/ ಕ್ಲೇಮ್ ಮಾಡದ ಕ್ಯಾಶ್ ಬ್ಯಾಕ್ ಆಫರ್‌ಗಳು ಅಥವಾ ರಿವಾರ್ಡ್ ಪಾಯಿಂಟ್ ಗಳನ್ನು ಪ್ರಕ್ರಿಯೆಗೊಳಿಸಲು ಮುಂದಾಗಬಹುದು. ನಂಬಿದ ವಿಕ್ಟಿಮ್‌ಗಳು ಆಗ ಕ್ಯೂಆರ್ ಕೋಡ್ ಅನ್ನು ಸ್ಕಾ ್ಯನ್ ಮಾಡುಬಹುದು ಅಥವಾ ತಮ್ಮ ಯುಪಿಐ ಪಿನ್ ಅನ್ನು ಬಳಸುವ ಮೂಲಕ ಱಕಲೆಕ್ಟ್ ರಿಕ್ವೆಸ್ಟ್ಱ ಅನ್ನು ಅನುಮೋದಿಸಬಹುದು, ಹಣವನ್ನು ವಂಚಕರ ಖಾತೆಗೆ ವರ್ಗಾಯಿಸಬಹುದು.

ಬಿಸಿನೆಸ್ ಇಮೇಲ್‌ಗಳು/ಮೆಸೆಜಿಂಗ್ ಆ್ಯಪ್‌ಗಳ ಮೂಲಕ ಪಾವತಿ ವಂಚನೆಗಳು

ವಂಚಕರು ನಿಮ್ಮ ಇಮೇಲ್‌ಗಳನ್ನು ಅಥವಾ ಚ್ಯಾಟ್‌ಗಳನ್ನು ಹ್ಯಾಕ್ ಮಾಡಬಹುದು, ಅಥವಾ ನಿಮ್ಮ ಬಗ್ಗೆ ಇನ್ನಷ್ಟು ತಿಳಿದುಕೊಳ್ಳಲು ಎನ್‌ಕ್ರಿಪ್ಟ್ ಮಾಡದ ಸಂದೇಶಗಳನ್ನು ತಡೆಯಬಹುದು. ಅವರು ನಿಮ್ಮ ಬಗ್ಗೆ ಇನ್ನಷ್ಟು ತಿಳಿದುಕೊಂಡ ನಂತರ, ಹ್ಯಾಕ್ ಮಾಡಿದ /ಒಪ್ಪಂದ ಮಾಡಿಕೊಂಡ /ಸ್ಪೂಫ್ಡ್ ಐಡಿಯಿಂದ ಸಂದೇಶಗಳನ್ನು ಕಳುಹಿಸುತ್ತಾರೆ, ಪ್ರೀತಿಪಾತ್ರರನ್ನು ಆಸ್ಪತ್ರೆಗೆ ಸೇರಿಸಲು ಅಥವಾ ಹೊಸಖಾತೆಗೆ ಪಾವತಿಸಬೇಕಾದ ಹಿಂದಿನ ಬಾಕಿಯ ಬಿಲ್‌ನಂತಹ ಕಾನೂನು ಬದ್ಧ ಉದ್ದೇಶಗಳಿಗಾಗಿ ತುರ್ತಾಗಿ ಹಣವನ್ನು ಪಾವತಿಸಲು ನಿಮ್ಮನ್ನು ಕೇಳುತ್ತಾರೆ. ಕೋರಿಕೆಯ ತುರ್ತು ಕಾರಣ ಅಥವಾ ಕೋರಿಕೆಯನ್ನು ನಂಬಬಹುದೆಂದು ಅವರು ಭಾವಿಸಿದ್ದರಿಂದ ವಿಕ್ಟಿಮ್‌ಗಳನ್ನು ಪಾವತಿ ಮಾಡಲು ಮೋಸಗೊಳಿಸಬಹುದು. ಹಾಗೂ ವಿಕ್ಟಿಮ್ ಸ್ವತಃ ಪಾವತಿ ಮಾಡಿದ್ದರಿಂದ, ಬ್ಯಾಂಕ್ ಅವರಿಗೆ ಕಳುಹಿಸುವ ವಹಿವಾಟಿನ ಅಲರ್ಟ್‌ಗಳಿಂದ ಗಾಬರಿಗೊಳ್ಳುವುದಿಲ್ಲ. ಅದು ಈ ರೀತಿಯ ವಂಚನೆಯನ್ನು ಕಂಡುಹಿಡಿಯುವುದನ್ನು ಕಷ್ಟಕರವಾಗಿಸುತ್ತದೆ.

ನಕಲಿ ಸಂಪರ್ಕ ಸಂಖ್ಯೆಗಳು :

ವಂಚಕರು ಬ್ಯಾಂಕ್‌ಗಳು ಹಾಗೂ ಸೇವಾ ಒದಗಣೆದಾರರ ಸಂಪರ್ಕ ಕೇಂದ್ರಗಳಿಗೆ ನಕಲಿ ಸಂಪರ್ಕ ವಿವರಗಳನ್ನು ಒದಗಿಸಬಹುದು. ಅನುಮಾನಪಡದ ವಿಕ್ಟಿಮ್‌ಗಳು ಸರ್ಚ್ ಎಂಜಿನ್ ಅನ್ನು ಬಳಸಿ ಸಂಪರ್ಕವಿವರಗಳಿಗಾಗಿ ನೋಡಬಹುದು ಹಾಗೂ ನಕಲಿ ನಂಬರ್‌ಗೆ ಕರೆಮಾಡಬಹುದು. ನಂತರ ಅವರನ್ನು ಱಪರಿಶೀಲನಾ ಪ್ರಕ್ರಿಯೆಗಳಱ ಮೂಲಕ ಕೊಂಡೊಯ್ಯಲಾಗುತ್ತದೆ ಹಾಗೂ ಅವರ ಡೆಬಿಟ್/ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್‌ಗಳು ಹಾಗೂ ಬ್ಯಾಂಕ್ ಖಾತೆಗಳ ಬಗ್ಗೆ ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯನ್ನು ಹಂಚಿಕೊಳ್ಳಲು ಅಲ್ಲಿ ಅವರನ್ನು ಮೋಸಗೊಳಿಸಲಾಗುತ್ತದೆ.

ನೀಮಗೆ ಅಗತ್ಯವಿರುವ ಸಂಪರ್ಕ ವಿವರಗಳಿಗಾಗಿ ನೋಡಲು ಬ್ಯಾಂಕ್ ಅಥವಾ ಸೇವಾ ಒದಗಣೆದಾರರ ಅಧಿಕೃತ ವೆಬ್‌ಸೈಟ್‌ಗೆ ಭೇಟಿ ನೀಡುವುದನ್ನು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳುವ ಮೂಲಕ ನೀವು ನಿಮ್ಮನ್ನು ರಕ್ಷಿಸಿಕೊಳ್ಳಬಹುದು. ಜಾಗರೂಕರಾಗಿರಿ ಹಾಗೂ ಮೊದಲು ಪರಿಶೀಲಿಸದೇ ಸರ್ಚ್ ಫಲಿತಾಂಶಗಳಲ್ಲಿ ಪ್ರದರ್ಶಿಸುವ ನಂಬರ್‌ಗಳಿಗೆ , ವಿಶೇಷವಾಗಿ ಅವು ಮೊಬೈಲ್ ನಂಬರ್ ಆಗಿರಬಹುದಾಗಿದ್ದರೆ ಕರೆಮಾಡಬೇಡಿ.

ಫಿಶಿಂಗ್ /ಸ್ಪೂಫಿಂಗ್ ಇಮೇಲ್ಸ್:

ವಂಚಕರು ಅವರು ಮಾಡಬಹುದಾದಂತೆ ಅನೇಕ ಇಮೇಲ್ ವಿಲಾಸಗಳಿಗೆ ಇಮೇಲ್ ಅನ್ನು ಕಳುಹಿಸುವ ಮೂಲಕ ವಿಕ್ಟಿಮ್‌ಗಳನ್ನು ಫಿಶ್ ಮಾಡಬಹುದು. ಬ್ಯಾಂಕ್, ಆನ್‌ಲೈನ್ ಪೇಮೆಂಟ್ ಸರ್ವಿಸ್, ರಿಟೇಲರ್ ಅಥವಾ ಇತರ ಸದೃಶ ಸೇವೆಯಂತಹ ಕಾನೂನುಬದ್ಧ ಸಂಸ್ಥೆಯ ಭಾಗವಾಗಿ ನಟಿಸುವಾಗ ಅವರು ಸಾಮಾನ್ಯವಾಗಿ ಇದನ್ನು ಮಾಡುತ್ತಾರೆ. ಅವರು ತಮ್ಮ ಐಡಿಯನ್ನು ಸ್ಪೂಫ್ ಮಾಡಬಹುದಾದ್ದರಿಂದ ಇಮೇಲ್ ಅನ್ನು ಸ್ವತಹ ಮೋಸಗಾರನಲ್ಲದೇ ಬೇರೊಬ್ಬರು ಕಳುಹಿಸಿದಂತೆ ಕಾಣುತ್ತದೆ.

ವೈಯಕ್ತಿಕ ಅಥವಾ ಹಣಕಾಸಿನ ಮಾಹಿತಿಗಾಗಿ ಕೇಳುವ ಇಮೇಲ್‌ಗಳಿಗೆ ಪ್ರತಿಕ್ರಿಯಿಸದೇ ಇರುವ ಮೂಲಕ ಫಿಶಿಂಗ್ ಹಗರಣದ ವಿರುದ್ಧ ನಿಮ್ಮನ್ನು ನೀವು ರಕ್ಷಿಸಿಕೊಳ್ಳಬಹುದು. ಅನುಮಾನಾಸ್ಪದ ಇಮೇಲ್‌ಗಳಲ್ಲಿನ ಲಿಂಕ್‌ಗಳನ್ನು ನೀವು ಎಂದಿಗೂ ಆಯ್ಕೆ ಮಾಡಬಾರದು.

ಎಚ್‌ಎಸ್‌ಬಿಸಿಯು ನಿಮ್ಮ ವೈಯಕ್ತಿಕ ಅಥವಾ ಸುರಕ್ಷತಾ ವಿವರಗಳನ್ನು ಇಮೇಲ್ ಮೂಲಕ ಬಹಿರಂಗಪಡಿಸಲು ಎಂದಿಗೂ ಕೇಳುವುದಿಲ್ಲ. ಎಚ್‌ಎಸ್‌ಬಿಸಿಯಿಂದ ಎಂದ ಎಂದ ಹೇಳಿಕೊಳ್ಳುವಂತಹ ಇಮೇಲ್ ಅನ್ನು ನೀವು ಸ್ವೀಕರಿಸಿದರೆ, ಅದಕ್ಕೆ ಪ್ರತಿಕ್ರಿಯಿಸಬೇಡಿ. ತಕ್ಷಣ ಇಮೇಲ್ ಅನ್ನು ಡಿಲೀಟ್ ಮಾಡಿ. ಹಾಗೂ ನೆನಪಿಟ್ಟುಕೊಳ್ಳಿ ,

ರುಜುವಾತುಗಳಾದಂತಹ–ನಿಮ್ಮ ಯೂಸರ್ ನೇಮ್ ಪಾಸ್‌ವರ್ಡ್ ಅಥವಾ ಇತರ ಸುರಕ್ಷತಾ ವವಿರಗಳನ್ನು –ಎಂದಿಗೂ ಯಾರೊಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.

ಮನಿ ಮ್ಯೂಲ್ /ಹೆಚ್ಚುವರಿ ಆದಾಯದ ಇಮೇಲ್ ಹಗರಣ :

ಮನಿ ಮ್ಯೂಲ್ ಹಗರಣದಲ್ಲಿ, ವಂಚಕರು ನಿಮ್ಮನ್ನು ಹಣ ವರ್ಗಾವಣೆಯೊಂದಿಗಿನ ಸಹಾಯಕ್ಕಾಗಿ ಕೇಳಬಹುದು. ಅವರು ನಿಮ್ಮ ಖಾತೆಗೆ ಹಣವನ್ನು ವರ್ಗಾಯಿಸಲು ಪ್ರಸ್ತಾವಿಸಬಹುದು ಹಾಗೆಯೇ ಅದನ್ನು ಮತ್ತೊಂದು ಖಾತೆಗೆ ವರ್ಗಾಯಿಸಲು ಅವರಿಗೆ ಸಹಾಯಮಾಡಬೇಕಾಗಬಹುದು. ಪ್ರತಿಯಾಗಿ ಅವರು ನಿಮಗೆ ಕಮಿಷನ್ ಕೊಡುವುದಾಗಿ ಹೇಳುತ್ತಾರೆ. ಅವರು ಸಾಮಾನ್ಯವಾಗಿ ಮನಿಲಾಂಡರಿಂಗ್‌ನಂತಹ ಅಪರಾಧಗಳಲ್ಲಿ ಅವರು ಒಳಗೊಂಡಿರುವುದರಿಂದ ಅಂತಹ ಕೋರಿಕೆಗಳನ್ನು ನೀವು ನಿರ್ಲಕ್ಷಿಸಬೇಕು. ಉದ್ದೇಶ ಪೂರ್ವಕವಾಗಿ ಭಾಗವಹಿಸುವ ಯಾರೊಬ್ಬರನ್ನಾದರೂ ಅಪರಾಧದಲ್ಲಿ ಶಾಮೀಲುದಾರರಾಗಿರುವವರನ್ನಾಗಿ ಪರಿಗಣಿಸಬಹುದು ಹಾಗೂ ಕಾನೂನಿನ ಕ್ರಮವನ್ನು ಎದುರಿಸಬೇಕಾಗಬಹುದು. ಇದು ಅತ್ಯಂತ ಚೆನ್ನಾಗಿ ತೋರುವುದು ನಿಜವಾದರೂ, ಬಹುಷಃ ಇದು ಒಂದು ಮೋಸವಾಗಿರುತ್ತದೆ!

ಮುಂಗಡ ಶುಲ್ಕ ವಂಚನೆ (“419” ಹಗರಣಗಳು):

ವಂಚಕರು ಸಾಮಾನ್ಯವಾಗಿ ಯುಎಸ್ ಡಾಲರ್‌ಗಳಲ್ಲಿ ದೊಡ್ಡ ಮೊತ್ತದ ಹಣವನ್ನು ನಂಬಲಾಗದ ರೀತಿಯಲ್ಲಿ ಸರಿಸಲು ಅವರಿಗೆ ಸಹಾಯ ಮಾಡುವದಕ್ಕಾಗಿ ನಿಮಗೆ ಯಥೇಚ್ಛ ಬಹುಮಾನವನ್ನು ನೀಡಲಾಗುವ ಕೋರದ ಪತ್ರಗಳನ್ನು ಅಥವಾ ಇಮೇಲ್‌ಗಳನ್ನು ಕಳುಹಿಸಬಹುದು. ಈ ವಂಚಕರು ನಿಜವಾಗಿಯು ನಿಮ್ಮ ಬ್ಯಾಂಕಿಂಗ್ ವಿವರಗಳನ್ನು ಹಿಂಬಾಲಿಸುತ್ತಾರೆ. ಅವರು ಡೀಲ್ ಅನ್ನು ಪೂರ್ಣಗೊಳಿಸಲು ಸಾಮಾನ್ಯವಾಗಿ ಶುಲ್ಕ , ಕೆಲವು ತೆರಿಗೆಗಳು ಅಥವಾ ಲಂಚವನ್ನು ಪಾವತಿಸಲು ನಿಮ್ಮನ್ನು ಕೇಳುತ್ತಾರೆ– ಇದು ಮುಂಗಡ ಶುಲ್ಕವಾಗಿರುತ್ತದೆ. ವಿಕ್ಟಿಮ್‌ಗಳು ಸಾಮಾನ್ಯವಾಗಿ ವಂಚಕರಿಗೆ ಇದನ್ನು ಪಾವತಿಸುವ ಮೂಲಕ ಕಳೆದುಕೊಳ್ಳುತ್ತಾರೆ.

ನಿಮ್ಮ ಇಂಟರ್‌ನೆಟ್ ಬ್ಯಾಂಕಿಂಗ್ ವಿವರಗಳನ್ನು ಯಾರಾದರೂ ಹೊಂದಿದ್ದಾರೆ ಎನ್ನುವ ಬಗ್ಗೆ ನಿಮಗೆ ಸಂದೇಹವಿದ್ದರೆ, ನೀವು ಆನ್‌ಲೈನ್ ಬಾಂಕಿಂಗ್‌ಗೆ ಲಾಗಾನ್ ಮಾಡಬೇಕು ಹಾಗೂ ತಕ್ಷಣ ನಿಮ್ಮ ಪಾಸ್‌ವರ್ಡ್ ಅನ್ನು ಬದಲಾಯಿಸಬೇಕು. ನಮ್ಮನ್ನು ಅಲರ್ಟ್ ಮಾಡಲು ಸಾಧ್ಯವಾದಷ್ಟು ಬೇಗ ನೀವು ನಮಗೆ ಕರೆ ಮಾಡಬೇಕು. ನಮ್ಮ ಲೈನ್‌ಗಳು 24/7* ತೆರೆದಿರುತ್ತವೆ. ನಮ್ಮ ಹಾಟ್‌ಲೈನ್ ನಂಬರ್‌ಗಳ ಲಿಸ್ಟ್ ಅನ್ನು ನೀವು ಇಲ್ಲಿ ಕಂಡುಕೊಳ್ಳಬಹುದು.

ಸೋಶಿಯಲ್ ಮೀಡಿಯಾ ಹ್ಯಾಕ್ಸ್ :

ಮೋಸಗಾರರು ಫೇಸ್‌ಬುಕ್, ವ್ಹಾಟ್ಸ್‌ಆ್ಯಪ್ ಅಥವಾ ಇನ್‌ಸ್ಟಾಗ್ರಾಂನಂತಹ ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮದ ಪ್ಲಾ್ಯಟ್‌ಫಾರ್ಮ್‌ಗಳಲ್ಲಿ ಆತ್ಮೀಯ ಸ್ನೇಹಿತ ಅಥವಾ ಸಂಬಂಧಿಯಂತೆ ನಟಿಸಬಹುದು, ಅವರಿಗೆ ತುರ್ತಾಗಿ ಹಣ ವರ್ಗಾಯಿಸಲು ನಿಮ್ಮನ್ನು ಕೇಳಿಕೊಳ್ಳುತ್ತಾರೆ. ನಿಮಗೆ ತಿಳಿದಿರುವ ವ್ಯಕ್ತಿಯಿಂದ ಅವರಿಗೆ ಕರೆ ಮಾಡಿಸುವ ಮೂಲಕ ಅಥವಾ ಇತರ ಚ್ಯಾನೆಲ್‌ಗಳ ಮೂಲಕ ಅವರನ್ನು ಸಂಪರ್ಕಿಸುವ ಮೂಲಕ ಕೋರಿಕೆಯು ಸಕಾರಣವಾಗಿದೆಯೇ ಎಂದು ನೀವು ಪರಿಶೀಲಿಸಬಹುದು.

ವಿಶಿಂಗ್ ಕರೆಗಳು

ವಂಚಕರು ಬ್ಯಾಂಕ್ ಸಿಬ್ಬಂದಿ ಅಥವಾ ಗ್ರಾಹಕ ಸೇವಾ ಕಾರ್ಯನಿರ್ವಾಹಕರಂತೆ ನಟಿಸಬಹುದು ಹಾಗೂ ಸಂಭಾವ್ಯ ವಿಕ್ಟಿಮ್‌ಗಳಿಗೆ ಅವರ ಬ್ಯಾಂಕ್ ಖಾತೆಯ ವಿವರಗಳಂತಹ ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯನ್ನು ಖರಿದಿಯಲು ಕರೆಮಾಡಬಹುದು. ವಿಕ್ಟಿಮ್‌ನ ವಿಶ್ವಾಸವನ್ನು ಗೆಲ್ಲಲು, ಅಪರಾಧಿಗಳು ಸಾಮಾಜಿಕ ಎಂಜಿನಿಯರಿಂಗ್ ಮೂಲಕ ಕಳುವು ಮಾಡಿರುವ ಸ್ವಲ್ಪ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ವಿಕ್ಟಿಮ್‌ಗೆ ಒದಗಿಸಬಹುದು. ಅವರು ಸ್ವಲ್ಪ ವಿಶ್ವಾಸವನ್ನು ಗಳಿಸಿದ ನಂತರ, ವಂಚಕರು ಅವರ ಬ್ಯಾಂಕ್ ವಿವರಗಳು ಹಾಗೂ ಒನ್–ಟೈಮ್ ಪಾಸ್‌ಕೋಡ್‌ಗಳಂತಹ(ಒಟಿಪಿಗಳಂತಹ) ಅವರ ಗೌಪ್ಯಮಾಹಿತಿಯನ್ನು ಒದಗಿಸುತ್ತಾರೆ ಎಂಬ ಭರವಸೆಯಲ್ಲಿ ಕೆಲವು ವಿಶೇಷ ಸೇವೆ ಅಥವಾ ಪ್ರಾಡಕ್ಟ್‌ಗಳ ಕೊಡುಗೆಯನ್ನು ನೀಡಬಹುದು.

ಟ್ರೋಜನ್ ವೈರಸ್‌ಗಳು

ಫೈಲ್‌ಗಳು, ಪೇಜ್‌ಗಳು ಅಥವಾ ಅ್ಯಟ್ಯಾಚ್‌ಮೆಂಟ್‌ಗಳನ್ನು ಒಳಗೊಂಡಿರುವ ಕೋರದ ಇಮೇಲ್‌ಗಳನ್ನು ನಿಮಗೆ ವಂಚಕರು ಕಳುಹಿಸಬಹುದಾಗಿದ್ದು ಅದನ್ನು ತೆರೆಯಲು ನಿಮಗೆ ಹೇಳುತ್ತಾರೆ. ಆದರೆ ಅವುಗಳನ್ನು ತರೆಯುವುದು ಎಂದರೆ ನಿಮ್ಮ ಆನ್‌ಲೈನ್ ಚಟುವಟಿಕೆಯನ್ನು ಹಾಗೂ ವಿವಿಧ ಸೈಟ್‌ಗಳಲ್ಲಿ ನೀವು ಏನನ್ನು ಟೈಪ್ ಮಾಡುತ್ತೀರಿ ಎನ್ನುವುದನ್ನೂ ಸಹ ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡುವ ಪ್ರೋಗ್ರಾಂ ಅನ್ನು ನಿಮ್ಮ ಕಂಪ್ಯೂಟರ್‌ನಲ್ಲಿ ರಹಸ್ಯವಾಗಿ ಅಳವಡಿಸಲಾಗುತ್ತದೆ ಎಂದರ್ಥ. ಈ ಪ್ರಕಾರ ಆನ್‌ಲೈನ್ ಶಾಪಿಂಗ್ ಮಾಡುವಾಗ ನೀವು ನಿಮ್ಮ ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ವಿವರಗಳನ್ನು ನೀವು ನಮೂದಿಸಿದಾಗ, ನೀವು ನಮೂದಿಸಿದ ಮಾಹಿತಿಯನ್ನು ಮೋಸಗಾರರಿಗೆ ನೋಡಲು ಸಾಧ್ಯವಾಗುತ್ತದೆ.

ಆನ್‌ಲೈನ್ ಸೆಕ್ಯುರಿಟಿಗಾಗಿ ಎಚ್‌ಎಸ್‌ಬಿಸಿ ಕೈಗೊಂಡ ಕ್ರಮಗಳು

ಬಹು -ಸ್ತರದ ಲಾಗಾನ್ ಪರಿಶೀಲನೆ

ನಿಮ್ಮ ಹಣಕಾಸಿನ ಮಾಹಿತಿಯನ್ನು ವಿಶಿಷ್ಟ ಯೂಸರ್‌ನೇಮ್ ಹಾಗೂ ಪಾಸ್‌ವರ್ಡ್‌ನ ಸಂಕೀರ್ಣ ಸಂಯೋಜನೆ, ಹಾಗೂ ಭೌತಿಕ ಸೆಕ್ಯೂರಿಟಿ ಡಿವೈಸ್/ಡಿಜಿಟಲ್ ಸೆಕ್ಯೂರ್ ಕೀಯಿಂದ ರಚಿಸಲಾದ ಒನ್–ಟೈಮ್ ಸೆಕ್ಯೂರಿಟಿ ಕೋಡ್‌ನಿಂದ ಸುರಕ್ಷಿತಗೊಳಿಸಲಾಗಿದೆ.

ವಹಿವಾಟಿನ ಪರಿಶೀಲನೆ

ಕಾರ್ಡ್‌ಗಳಲ್ಲಿನ 3ಡಿ ಸುರಕ್ಷಿತ ವಹಿವಾಟುಗಳು ವಹಿವಾಟು ಹಾಗೂ ಪಾವತಿ ವ್ಯವಸ್ಥೆಯಲ್ಲಿನ ನಂಬಿಕೆಯನ್ನು ಸುರಕ್ಷಿತಗೊಳಿಸಲು ಸಹಾಯ ಮಾಡುತ್ತದೆ. ವಹಿವಾಟಿಗಾಗಿ ಜನರೇಟ್ ಮಾಡಲಾದ ಒಟಿಪಿಗಳನ್ನು ಎಂದಿಗೂ ಯಾರೊಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.

128-ಬಿಟ್ ಸೆಕ್ಯೂರ್ ಸಾಕೆಟ್ ಲೇಯರ್ (ಎಸ್‌ಎಸ್‌ಎಲ್) ಎನ್‌ಕ್ರಿಪ್ಶನ್

ಎಚ್‌ಎಸ್‌ಬಿಸಿ ಇಂಟರ್‌ನೆಟ್ ಬ್ಯಾಂಕಿಂಗ್ ಸೆಷನ್‌ನಲ್ಲಿ ರವಾನಿಸುವ ಮಾಹಿತಿಗಾಗಿ 128–ಬಿಟ್ ಸೆಕ್ಯೂರ್ ಸಾಕೆಟ್ ಲೇಯರ್ (ಎಸ್‌ಎಸ್‌ಎಲ್) ಎನ್‌ಕ್ರಿಪ್ಶನ್ ಅನ್ನು ಬಳಸುತ್ತದೆ, ಇದನ್ನು ಎನ್ಕ್ರಿಪ್ಶನ್‌ಗಾಗಿ ಉದ್ಯಮದ ಮಾನದಂಡವಾಗಿ ಸ್ವೀಕರಿಸಲಾಗಿದೆ.

ಸ್ವಯಂಚಾಲಿತ “ಟೈಮ್ -ಔಟ್” ವೈಶಿಷ್ಟ್ಯತೆ

ಸುರಕ್ಷತಾ ಕ್ರಮವಾಗಿ, ನಿಮ್ಮ ಇಂಟರ್‌ನೆಟ್ ಬ್ಯಾಂಕಿಂಗ್ ಸೆಷನ್ ಬಳಸದ ಅವಧಿಯ ನಂತರ ಸ್ವಯಂಚಾಲಿತವಾಗಿ ಸ್ಥಗಿತಗೊಳ್ಳುತ್ತದೆ ಅಥವಾ ಟೈಮ್ –ಔಟ್ ಆಗುತ್ತದೆ. ನೀವು ನಿಮ್ಮ ಇಂಟರ್‌ನೆಟ್ ಬ್ಯಾಂಕಿಂಗ್ ಕೆಲಸವನ್ನು ಪೂರ್ಣಗೊಳಿಸಿದಾಗ ನಿಮ್ಮ ಇಂಟರ್‌ನೆಟ್ ಬ್ಯಾಂಕಿಂಗ್ ಸೆಷನ ಅನ್ನು ಯಾವಾಗಲು ಮುಕ್ತಾಯಗೊಳಿಸಬೇಕು.

ಸೆಕ್ಯೂರಿಟಿ ಡಿವೈಸ್ / ಡಿಜಿಟಲ್ ಸೆಕ್ಯೂರ್ ಕೀ

ಭೌತಿಕ ಸೆಕ್ಯೂರಿಟಿ ಡಿವೈಸ್ / ಡಿಜಿಟಲ್ ಸೆಕ್ಯೂರ್ ಕೀಯು ಆನ್‌ಲೈನ್ ಸುರಕ್ಷತೆಯನ್ನು ಉನ್ನತಮಟ್ಟಕ್ಕೆ ಕೊಂಡೊಯ್ಯುತ್ತದೆ. ನಿಮ್ಮ ಖಾತೆಗೆ ಲಾಗಾನ್ ಮಾಡಲು, ನೀವು ಎಂದಿನಂತೆ ನಿಮ್ಮ ಅಸ್ತಿತ್ವದಲ್ಲಿರುವ ಯೂಸರ್‌ನೇಮ್ ಹಾಗೂ ಪಾಸ್‌ವರ್ಡ್ ಅನ್ನು ನಮೂದಿಸಬೇಕಾಗುತ್ತದೆ, ಅದರ ನಂತರ ಭೌತಿಕ ಸುರಕ್ಷತಾ ಉಪಕರಣ/ಡಿಜಿಟಲ್ ಸುರಕ್ಷತಾ ಕೀಯಿಂದ ಜನರೇಟ್ ಮಾಡಲಾದ ವಿಶಿಷ್ಟ ಸುರಕ್ಷತಾ ಕೋಡ್ ಅನ್ನು ನಮೂದಿಸಬೇಕಾಗುತ್ತದೆ. ಈ 2–ಹಂತದ ದೃಢೀಕರಣ ಪ್ರಕ್ರಿಯೆಯು ನಿಮ್ಮ ಇಂಟರ್‌ನೆಟ್ ಬ್ಯಾಂಕಿಂಗ್‌ಗೆ ನೀವು ಪ್ರವೇಶಾವಕಾಶವನ್ನು ಪಡೆದಾಗ ವರ್ಧಿತ ಮಟ್ಟದ ಸುರಕ್ಷತೆಯನ್ನು ನಿಮಗೆ ಒದಗಿಸುತ್ತದೆ.

ಆನ್‌ಲೈನ್ ಸುರಕ್ಷತೆಯಲ್ಲಿ ನಿಮ್ಮ ಪಾತ್ರ

ಇಂಟರ್‌ನೆಟ್ ಬ್ಯಾಂಕಿಂಗ್ ಸುರಕ್ಷತೆಯನ್ನು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಲು ಮಾಡಬೇಕಾದ ಹಾಗೂ ಮಾಡಬಾರದ ಆಚರಣೆಗಳು

ಮಾಡಬೇಕಾದವುಗಳು

- ನಿಮ್ಮ ಕಂಪ್ಯೂಟರ್ ಅನ್ನು ಎಲ್ಲಾ ಸಮಯದಲ್ಲೂ ನೂತನ ಆ್ಯಂಟಿ –ವೈರಸ್ ಹಾಗೂ ಫೈರ್‌ವಾಲ್ ಪ್ರೊಟೆಕ್ಷನ್ ಸಾಫ್ಟ್‌ವೇರ್‌ನೊಂದಿಗೆ ರಕ್ಷಿಸಲಾಗಿರುವುದನ್ನು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಿ. ನೀವು ನೂತನ ರಕ್ಷಣೆಯನ್ನು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಲು ನಿಯಮಿತವಾಗಿ ಅಪ್‌ಡೇಟ್‌ಗಳನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡಿ.
- ನಿಮಗೆ ಸ್ಮರಣೀಯವಾದ ಆದರೆ ಬೇರೊಬ್ಬರಿಂದ ಊಹಿಸಲು ಸುಲಭವಲ್ಲದ ಪಾಸ್‌ವರ್ಡ್ ಅನ್ನು ಆಯ್ಕೆಮಾಡಿಕೊಳ್ಳಿ. ವರ್ಣಮಾಲೆ ಹಾಗೂ ಸಂಖ್ಯಾ ಅಕ್ಷರಗಳ ಸಂಯೋಜನೆಯನ್ನು ಹೊಂದಿರುವ ಪಾಸ್‌ವರ್ಡ್‌ಗಳು ಸಾಮನ್ಯವಾಗಿ ಊಹಿಸಲು ಕಷ್ಟವಾಗಿರುತ್ತದೆ (ಉದಾ. a7g3cy91)
- ನಿಮ್ಮ ಇಂಟರ್‌ನೆಟ್ ಬ್ಯಾಂಕಿಂಗ್ ಪಾಸ್‌ವರ್ಡ್ ಅನ್ನು ನಿಯಮಿತ ಆಧಾರದ ಮೇಲೆ ಬದಲಾಯಿಸಿ
- ಫಿಶಿಂಗ್ ಇಮೇಲ್ ಬಗ್ಗೆ ಎಚ್ಚರಿಕೆಯಿಂದಿರಿ. ವರ್ಣಮಾಲೆಗಳು ಹಾಗೂ ಅಕ್ಷರಗಳನ್ನು ಒಳಗೊಂಡು, ಯಾವಾಗಲೂ ಸಂಪೂರ್ಣ ಇಮೇಲ್ ವಿಳಾಸವನ್ನು ಎಚ್ಚರಿಕೆಯಿಂದ ಓದಿ.
- ಒಂದೇ ತರಹ ಕಾಣುವ ಇಮೇಲ್ ವಿಳಾಸದಿಂದ ಫಿಶಿಂಗ್ ಅನ್ನು ಮಾಡಲಾಗುತ್ತದೆ ಉದಾ. hsdc.co.in ಅಥವಾ hsbcbank.com. ನಿಮ್ಮ ಮೌಸ್ ಪಾಯಿಂಟರ್ ಅನ್ನು ಅದರ ನಿಜವಾದ ಗಮ್ಯಸ್ಥಾನವನ್ನು ಬಹಿರಂಗಪಡಿಸಲು ಯುಆರ್‌ಎಲ್ ಮೇಲೆ ರೋಲ್ ಮಾಡಿ; ನಿಮ್ಮ ಬ್ರೌಸರ್‌ನ ಕೆಳಗಿನ ಎಡ ಮೂಲೆಯಲ್ಲಿ ಇದನ್ನು ಪ್ರದರ್ಶಿಸಲಾಗುತ್ತದೆ. ಹೊಂದಿಕೆಯಾಗದಿದ್ದರೆ ಲಿಂಕ್ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡಬೇಡಿ. ಯುಆರ್‌ಎಲ್‌ನಲ್ಲಿ ಸ್ಪೆಲ್ಲಿಂಗ್ ಮಿಸ್ಟೇಕ್‌ಗಳು, ಕೆಟ್ಟ ವ್ಯಾಕರಣ ಅಥವಾ ಗೊಂದಲಮಯ ಅಕ್ಷರಗಳಂತಹ ಚಿಹ್ನೆಗಳಿಗಾಗಿ ವೀಕ್ಷಿಸಿ.
- ಅವಶ್ಯಕತೆ ಇಲ್ಲದಿದ್ದರೆ ನಿಮ್ಮ ಖಾತೆಯಿಂದ ಸೇರಿಸಲಾದ ಫಲಾನುಭವಿಗಳನ್ನು ತೆಗೆದುಹಾಕಿ
- ಲಾಗಾನ್ ವಿವರಗಳನ್ನು ನೆನಪಿಸಿಕೊಳ್ಳುವ ನಿಮ್ಮ ಕಂಪ್ಯೂಟರ್ ಅಥವಾ ಬ್ರೌಸರ್‌ಗಳಲ್ಲಿನ ಕಾರ್ಯಾತ್ಮಕತೆಯನ್ನು ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಿ.
- ನಿಮ್ಮ ಸಿಸ್ಟಮ್ ಹಾಗೂ ಬ್ರೌಸರ್ ಅನ್ನು ಅಪ್‌ಡೇಟ್ ಆಗಿ ಇಡಿ. ತಯಾರಕರು ತಮ್ಮ ಸಿಸ್ಟಮ್‌ಗಳು ಹಾಗೂ ಬ್ರೌಸರ್‌ಗಳಲ್ಲಿ ದೌರ್ಬಲ್ಯವನ್ನು ಕಂಡುಕೊಂಡಾಗ ನಿಯಮಿತವಾಗಿ ಸುರಕ್ಷತಾ ಪ್ಯಾಚ್‌ಗಳನ್ನು ಬಿಡುಗಡೆ ಮಾಡುತ್ತಾರೆ. ಈ ಅಪ್‌ಡೇಟ್‌ಗಳಿಗಾಗಿ ನಿಯಮಿತ ಆಧಾರದ ಮೇಲೆ ನಿಮ್ಮ ಸಾಫ್ಟ್‌ವೇರ್ ಒದಗಣೆದಾರರೊಂದಿಗೆ ಪರಿಶೀಲಿಸಿ.
- ನಿಮ್ಮ ಮೊಬೈಲ್ ಬ್ಯಾಂಕಿಂಗ್ ಅಪ್ಲಿಕೇಶನ್ ಅನ್ನು ಅಪ್‌ಡೇಟ್ ಆಗಿ ಇಟ್ಟುಕೊಳ್ಳಿ. ಡೌನ್‌ಲೋಡ್ ಹಾಗೂ ಅಪ್ಲಿಕೇಶನ್‌ನ ತರುವಾಯದ ಅಪ್‌ಡೇಟ್‌ಗಾಗಿ ಪ್ಲೇ ಸ್ಟೋರ್‌ಗೆ ಭೇಟಿ ನೀಡಿ. ವಿಶ್ವಾಸಾರ್ಹವಲ್ಲದ ಮೂಲಗಳಿಂದ ಇಮೇಲ್‌ನಲ್ಲಿನ ಲಿಂಕ್‌ಗಳನ್ನು ಆಧರಿಸಿ ಮೊಬೈಲ್ ಬ್ಯಾಂಕಿಂಗ್/ಪೇಮೆಂಟ್ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಎಂದಿಗೂ ಡೌನ್‌ಲೋಡ್ ಮಾಡಬೇಡಿ.
- ಎಚ್‌ಎಸ್‌ಬಿಸಿಯ ವೆಬ್‌ಸೈಟ್ ಅನ್ನು ತಲುಪಲು ಬ್ರೌಸರ್‌ನಲ್ಲಿ ಯಾವಾಗಲೂ ನಮ್ಮ ಯುಆರ್‌ಎಲ್ ಅನ್ನು ಟೈಪ್ ಮಾಡಿ.
- ಪ್ಯಾಡ್‌ಲಾಕ್ ಚಿಹ್ನೆ ಹಾಗೂ ಸೈಟ್ ಪ್ರಮಾಣಪತ್ರವನ್ನು ಪರಿಶೀಲಿಸಿ. ಸೈಟ್ ಪ್ರಮಾಣಪತ್ರವು ಎಚ್‌ಎಸ್‌ಬಿಸಿಗೆ ಸೇರಿರುವುದನ್ನು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಲು ಎಚ್‌ಎಸ್‌ಬಿಸಿ ಆನ್‌ಲೈನ್ ಬ್ಯಾಂಕಿಂಗ್‌ಗೆ ನೀವು ಲಾಗಿನ್ ಮಾಡಿದಾಗ ನಿಮ್ಮ ಬ್ರೌಸರ್‌ನ ಕೆಳಭಾಗದಲ್ಲಿರುವ ಪ್ಯಾಡ್‌ಲಾಕ್ ಚಿಹ್ನೆಯನ್ನು ಡಬಲ್–ಕ್ಲಿಕ್ ಮಾಡಿ. ಅನಕಲಿಟಸೈಟ್‌ನಲ್ಲಿ ನಿಮ್ಮ ವಿವರಗಳನ್ನು ನಮೂದಿಸಲು ನಿಮ್ಮನ್ನು ಮೋಸಗೊಳಿಸಲಾಗಿಲ್ಲ ಎಂದು ಖಚಿತಪಡಿಸುತ್ತದೆ.
- ನಿಮ್ಮ ಖಾತೆಗಳನ್ನು ನಿಯಮಿತವಾಗಿ ಪರಿಶೀಲಿಸಿ. ಯಾವುದೇ ವಹಿವಾಟುಗಳ ಬಗ್ಗೆ ಸಂದೇಹವಿದ್ದರೆ ವಿವರಗಳನ್ನು ಬರೆದಿಟ್ಟುಕೊಳ್ಳಿ ಹಾಗೂ ನಮಗೆ ಕರೆಮಾಡಿ.
- ಆನ್‌ಲೈನ್ ಬ್ಯಾಂಕಿಂಗ್ ಬಳಸಿದ ನಂತರ ಯಾವಾಗಲೂ ಲಾಗ್–ಔಟ್ ಮಾಡಿ. ಲಾಗ್–ಔಟ್ ಬಟನ್ ಅನ್ನು ಆಯ್ಕೆ ಮಾಡಿ ಹಾಗೂ ನೀವು ಸೇವೆಗೆ ಲಾಗ್ಡ್ ಇನ್ ಇರುವಾಗ ನಿಮ್ಮ ಪಿಸಿಯನ್ನು ಗಮನಿಸದೇ ಎಂದೂ ಹಾಗೇ ಬಿಡಬೇಡಿ.
- ಬ್ಯಾಂಕ್‌ಗಳು, ಆನ್‌ಲೈನ್ ಶಾಪಿಂಗ್ ವೆಬ್‌ಸೈಟ್ ಮುಂತಾದವರ ಕಸ್ಟಮರ್ ಕೇರ್ ನಂಬರ್‌ಗಳಿಗಾಗಿ ಹುಡುಕುತ್ತಿದ್ದರೆ ಇಂಟರ್‌ನೆಟ್‌ನಲ್ಲಿ ಬುದ್ಧಿವಂತಿಕೆಯಿಂದ ಹುಡುಕಿ. ಮೋಸಗಾರರು ಅವರಿಂದ ನಿರ್ವಹಿಸಲ್ಪಡುವ ಮೊಬೈಲ್ ನಂಬರ್‌ಗಳೊಂದಿಗೆ ಪರಿಣಾಮಗಳನ್ನು ಹಿಂತಿರುಗಿಸಲು ಹುಡುಕಾಟದಲ್ಲಿ ಕೈಚಳಕ ತೋರಿಸುತ್ತಾರೆ. ಬ್ಯಾಂಕ್‌ನ ಕಸ್ಟಮರ್ ಕೇರ್ ನಂಬರ್ ಅಥವಾ ಇ–ಕಾಮರ್ಸ್ ವೆಬ್‌ಸೈಟ್‌ನ ಬದಲಿಗೆ ಮೋಸಗಾರರಿಗೆ ಕರೆ ಮಾಡಲು ನಿಮ್ಮನ್ನು ಮೋಸಗೊಳಿಸಬಹುದು.
- ನಿಮ್ಮ ಬ್ಯಾಂಕ್‌ನ ಸಂಪರ್ಕ ಕೇಂದ್ರದ ನಂಬರ್ ಅನ್ನು ನಿಮ್ಮ ಡಿವೈಸ್‌ಗಳಲ್ಲಿ ಸ್ಟೋರ್ ಮಾಡಿ ಇಟ್ಟುಕೊಳ್ಳಿ ಅಥವಾ ನಿಮ್ಮ ಕ್ರೆಡಿಟ್/ಡೆಬಿಟ್ ಕಾರ್ಡ್‌ನ ಹಿಂಭಾಗದಲ್ಲಿ ಬರೆದ ನಂಬರ್ ಅನ್ನು ನೋಡಿ.
- ನಿಮ್ಮ ವೈಯಕ್ತಿಕ ಕಂಪ್ಯೂಟರ್ ಅಥವಾ ಮೊಬೈಲ್ ಉಪಕರಣಗಳಲ್ಲಿ ಸ್ಕ್ರೀನ್ ಶೇರಿಂಗ್ ಅಪ್ಲಿಕೇಶನಗಳ ಬಗ್ಗೆ ಜಾಗರೂಕರಾಗಿರಿ. ವಂಚಕರು ಅಂತಹ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡಲು ನಿಮ್ಮನ್ನು ಮೋಸಗೊಳಿಸಬಹುದು ಹಾಗೂ ನಿಮ್ಮಿಂದ ಕೋಡ್ ಅನ್ನು ಕೇಳುವ ಮೂಲಕ ಪ್ರವೇಶಾವಕಾಶವನ್ನು ಪಡೆಯಬಹುದು. ಒಮ್ಮೆ ಪ್ರವೇಶಾವಕಾಶವನ್ನು ಅನುಮತಿಸಿದ ನಂತರ, ಅವರು ನಿಮ್ಮ ಉಪಕರಣವನ್ನು ದೂರದಿಂದಲೇ ನೋಡಬಹುದು ಹಾಗೂ ನಿಯಂತ್ರಿಸಬಹುದು, ಹಾಗೂ ನಿಮ್ಮ ಖಾತೆಗಳಿಂದ ಪಾವತಿಗಳನ್ನು ಸಹ ಕಾರ್ಯಗತಗೊಳಿಸಬಹುದು.
- ನಿಮ್ಮ ಇಂಟರ್‌ನೆಟ್ ಸಂಪರ್ಕವನ್ನು ಸುರಕ್ಷಿತಗೊಳಿಸಿ. ನಿಮ್ಮ ಮನೆಯ ವೈರ್‌ಲೆಸ್ ನೆಟ್‌ವರ್ಕ್ ಅನ್ನು ಪಾಸ್‌ವರ್ಡ್‌ನೊಂದಿಗೆ ಯಾವಾಗಲೂ ರಕ್ಷಿಸಿ.

- ಕಮಿಷನ್ ಅಥವಾ ಸಹಾಯಕ್ಕಾಗಿ ಸಹ ನಿಮ್ಮ ಖಾತೆಯಲ್ಲಿ ಹಣವನ್ನು ಸಂಗ್ರಹಿಸುವ ಅಗತ್ಯವಿರುವ ಸ್ಕೀಮ್‌ಗಳು/ಕೊಡುಗೆಗಳ ಬಗ್ಗೆ ಜಾಗರೂಕರಾಗಿರಿ. ಅವರು ಮೋಸಗಾರರು ನಿಮ್ಮ ಖಾತೆಗೆ ಅಪರಾಧದ ಆದಾಯವನ್ನು ಕಳುಹಿಸಬಹುದು ಹಾಗೂ ಹಣವನ್ನು ವರ್ಗಾಯಿಸಲು ಅಥವಾ ಅವರಿಗೆ ನಗದನ್ನು ಕೊಡಲು ನಿಮಗೆ ಕೇಳಬಹುದು. ವಂಚಕರು ಹಣದ ಸುಳುವಿನಲ್ಲಿ ತಮ್ಮನ್ನು ಸಿಲುಕಿಸಿಕೊಳ್ಳಲು ಬಯಸುವುದಿಲ್ಲ ಹಾಗೂ ನಿಮ್ಮನ್ನು ಮನಿ ಮ್ಯೂಲ್ ಆಗಿ ಬಳಸ ಬಹುದು.
- ವಂಚನೆಯನ್ನು ವರದಿ ಮಾಡಲು ತಕ್ಷಣ ಬ್ಯಾಂಕ್ ಅನ್ನು ಸಂಪರ್ಕಿಸಿ.

ಮಾಡಬಾರದವುಗಳು

- ನೀವು ಇತರ ಸೇವೆಗೆ ಬಳಸುವ ಪಾಸ್‌ವರ್ಡ್ ಅನ್ನು ಬಳಸಬೇಡಿ. ನಿಮ್ಮ ಪಾಸ್‌ವರ್ಡ್ ಇಂಟರ್‌ನೆಟ್ ಬ್ಯಾಂಕಿಂಗ್‌ಗೆ ವಿಶಿಷ್ಟವಾಗಿರಬೇಕು.
- ಇಮೇಲ್/ಎಸ್‌ಎಮ್‌ಎಸ್‌ನಲ್ಲಿನ ಲಿಂಕ್‌ಗಳನ್ನು ಅಜಾಗರೂಕತೆಯಿಂದ ಕ್ಲಿಕ್ ಮಾಡಿದಾಗ ಅದು ತೆರೆಯುವ ವೆಬ್‌ಪೇಜ್‌ಗಳಲ್ಲಿ ಯೂಸರ್‌ಐಡಿ, ಪಾಸ್‌ವರ್ಡ್, ಕಾರ್ಡ್ ನಂಬರ್,ಸಮಾಪ್ತಿಯ ದಿನಾಂಕ ಸಿವಿವಿ,ಮುಂತಾದ ವಿವರಗಳನ್ನು ಬಹಿರಂಗಪಡಿಸಬೇಡಿ.
- ಬ್ಯಾಂಕ್ ಉದ್ಯೋಗಿಗಳು ಅಥವಾ ಸರ್ಕಾರಿ ಸಂಸ್ಥೆಗಳಾದಂತಹ ಐ.ಟಿ ವಿಭಾಗ, ಆರ್‌ಬಿಐ ಮುಂತಾದವುಗಳಿಂದ ಬಂದವರು ಎಂದು ಅವರು ಹೇಳಿಕೊಳ್ಳುತ್ತಿದ್ದರೂ ಸಹ ಅಂತಹ ವಿವರಗಳನ್ನು ಕೇಳುವ ಸಂದೇಶಗಳಿಗೆ ಪ್ರತಿಕ್ರಿಯಿಸ ಬೇಡಿ. ಎಚ್‌ಎಸ್‌ಬಿಸಿಯ ಸದಸ್ಯರು ಅಂತಹ ವಿವರಗಳನ್ನು ಎಂದಿಗೂ ಕರೆಮಾಡಿ ಕೇಳುವುದಿಲ್ಲ.
- ನಿಮ್ಮ ಪಾಸ್‌ವರ್ಡ್‌ನೊಂದಿಗೆ ನಿಮ್ಮ ಇಂಟರ್‌ನೆಟ್ ಬ್ಯಾಂಕಿಂಗ್ ಯೂಸರ್‌ನೇಮ್ ಅನ್ನು ಬರೆಯಬೇಡಿ. ನಿಮ್ಮ ಪಾಸ್‌ವರ್ಡ್ ಅನ್ನು ಗುರುತಿಸಬಹುದಾದ ರೂಪದಲ್ಲಿ ಬರೆಯಬೇಡಿ ಹಾಗೂ ನಿಮ್ಮ ಭೌತಿಕ ಸೆಕ್ಯೂರಿಟಿ ಡಿವೈಸ್/ಡಿಜಿಟಲ್ ಸೆಕ್ಯೂರ್ ಕೀಯೊಂದಿಗೆ ನಿಮ್ಮ ಲಾಗಾನ್ ವಿವರಗಳನ್ನು ಎಂದಿಗೂ ಬಿಡಬೇಡಿ.
- ನಿಮ್ಮ ಮೊಬೈಲ್ ಬ್ಯಾಂಕಿಂಗ್ ಆಪ್ಲಿಕೇಶನ್ ಅನ್ನು ಅಪ್‌ಡೇಟ್ ಮಾಡಿ ಇಟ್ಟುಕೊಳ್ಳಿ. ಅದನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡಲು ಹಾಗೂ ಅದರಲ್ಲಿ ಯಾವುದೇ ಅಪ್‌ಡೇಟ್‌ಗಳನ್ನು ಮಾಡಲು, ನಿಮ್ಮ ಉಪಕರಣದ ಅಧಿಕೃತ ಆ್ಯಪ್ ಸ್ಟೋರ್‌ಗೆ ಭೇಟಿನೀಡಿ.
- ವಿಶ್ವಾಸಾರ್ಹವಲ್ಲದ ಮೂಲಗಳ ಇಮೇಲ್‌ಗಳಲ್ಲಿನ ಲಿಂಕ್‌ಗಳಿಂದ ಮೊಬೈಲ್‌ಬ್ಯಾಂಕಿಂಗ್/ಪೇಮೆಂಟ್ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಎಂದಿಗೂ ಡೌನ್‌ಲೋಡ್ ಮಾಡಬೇಡಿ.
- ಆನ್‌ಲೈನ್ ವೆಬ್‌ಸೈಟ್‌ಗಳಲ್ಲಿ ಕಾರ್ಡ್ ನಂಬರ್ ಹಾಗೂ ಮುಕ್ತಾಯದ ದಿನಾಂಕಗಳನ್ನು ಸ್ಟೋರ್ ಮಾಡಿಟ್ಟುಕೊಳ್ಳುವುದರ ಬಗ್ಗೆ ಜಾಗರೂಕರಾಗಿರಿ. ವಿಶ್ವಾಸಾರ್ಹವಲ್ಲದ ವಿರಳವಾಗಿ ಬಳಸುವ ವೆಬ್‌ಸೈಟ್‌ಗಳಲ್ಲಿ ಈ ವಿವರಗಳನ್ನು ಸ್ಟೋರ್ ಮಾಡಬೇಡಿ.
- ಯಾರೊಂದಿಗೂ ನಿಮ್ಮ ಪಿನ್ ಅನ್ನು ಎಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ. ಅದನ್ನು ನೀವೇ ಬಳಸಿ.ನಿಮ್ಮ ಪಿನ್ ಬಹಿರಂಗವಾಗಿರುವ ಬಗ್ಗೆ ನಿಮಗೆ ಅನುಮಾನ ಬಂದರೆ, ಅದನ್ನು ತಕ್ಷಣ ಬದಲಾಯಿಸಿ.

ನಿಮ್ಮನ್ನು ಯುಪಿಐ ಪಿನ್‌ಗಾಗಿ ಕೇಳಿದರೆ, ನೆನಪಿಟ್ಟುಕೊಳ್ಳಿ, ನೀವು ಪಾವತಿಯನ್ನು ಮಾಡುತ್ತಿರುವಿರಿ. ಪಾವತಿಯನ್ನು ಸ್ವೀಕರಿಸಲು ನಿಮಗೆ ಯುಪಿಐ ಪಿನ್ ಅಗತ್ಯವಿರುವುದಿಲ್ಲ.

ಸಾರ್ವಜನಿಕ ಕಂಪ್ಯೂಟರ್‌ಗಳನ್ನು ಬಳಸುವಾಗ ಎಚ್ಚರಿಕೆಯಿಂದಿರಿ.

ಯಾವಾಗಲೂ

- ನೀವು ಕಂಪ್ಯೂಟರ್ ಅನ್ನು ಬಿಡುತ್ತಿದ್ದರೆ, ಅದು ಕೇವಲ ಒಂದು ಕ್ಷಣಕ್ಕಾದರೂ ಸಹ ಲಾಗ್ ಔಟ್ ಮಾಡಿ. ಸಾಧ್ಯವಾದರೆ, ನೀವು ಲಾಗ್ಡ್ ಇನ್ ಇರುವವರೆಗೂ ಕಂಪ್ಯೂಟರ್ ಅನ್ನು ಗಮನಿಸಿದೇ ಹಾಗೇ ಬಿಡಬೇಡಿ.
- ನೀವು ಕಂಪ್ಯೂಟರ್ ಅನ್ನು ಲಾಗ್ ಔಟ್ ಮಾಡುವ ಮೊದಲು ನಿಮ್ಮ ಬ್ರೌಸಿಂಗ್ ಹಿಸ್ಟ್ರಿಯನ್ನು ಡಿಲೀಟ್ ಮಾಡಿ: ಇಂಟರ್‌ನೆಟ್ ಬ್ರೌಸರ್‌ಗಳು ನಿಮ್ಮ ಪಾಸ್‌ವರ್ಡ್ ಹಾಗೂ ನೀವು ಭೇಟಿನೀಡಿದ ಪುಟಗಳ ಬಗ್ಗೆ ಮಾಹಿತಿಯನ್ನು ಸಂಗ್ರಹಿಸುತ್ತವೆ. ಇಂಟರ್‌ನೆಟ್ ಬ್ರೌಸರ್‌ನ ಟೂಲ್ಸ್ ಮೆನುಗೆ ಹೋಗಿ ಹಾಗೂ ಆಪ್ಶನ್‌ಗಳನ್ನು ಅಥವಾ ಇಂಟರ್‌ನೆಟ್ ಆಪ್ಶನ್‌ಗಳನ್ನು ಸಿಲೆಕ್ಟ್ ಮಾಡಿ. ಬ್ರೌಸರ್‌ನ ಯಾವುದೇ ಆಟೋ ಕಂಪ್ಲೀಟ್ ಫಂಕ್ಷನ್ ಟರ್ನ್ ಆಫ್ ಆಗಿದೆಯೇ ಎಂದು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಿ, ಯಾವುದೇ ಕುಕೀಗಳನ್ನು ಡಿಲೀಟ್ ಮಾಡಿ, ಹಾಗೂ ಹಿಸ್ಟ್ರಿಯನ್ನು ಕ್ಲಿಯರ್ ಮಾಡಿ.
- ಗ್ರಂಥಾಲಯಗಳು, ಇಂಟರ್‌ನೆಟ್ ಕೆಫೆಗಳು ಹಾಗೂ ಶಾಲೆಗಳನ್ನು ಒಳಗೊಂಡು ನಿಮ್ಮ ಬ್ಯಾಂಕಿಂಗ್ ಕೆಲಸವನ್ನು ಮಾಡಲು ನೀವು ಸಹಾಯ ಮಾಡಬಹುದಾದರೆ ಸಾರ್ವಜನಿಕ ಕಂಪ್ಯೂಟರ್‌ಗಳನ್ನು ಬಳಸದಿರಲು ಪ್ರಯತ್ನಿಸಿ.

ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯನ್ನು ಟೈಪ್ ಮಾಡಬೇಡಿ. ಎಲ್ಲಾ ಮುನ್ನೆಚ್ಚರಿಕೆಗಳನ್ನು ಅನುಸರಿಸುತ್ತಿದರೂ ಸಹ, ಸಾರ್ವಜನಿಕ ಕಂಪ್ಯೂಟರ್‌ನಲ್ಲಿ ಕೀಸ್ಟ್ರೋಕ್ ಲಾಗರ್ ಎಂದು ಕರೆಯಲ್ಪಡುವ ದುರುದ್ದೇಶಪೂರಿತ ಸಾಫ್ಟ್‌ವೇರ್ ಅನ್ನು ಅದರಲ್ಲಿ ಅಳವಡಿಸಿರಬಹುದು. ಈ ಪ್ರೋಗ್ರಾಂಗಳು ನಿಮ್ಮ ಪಾಸ್‌ವರ್ಡ್, ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ನಂಬರ್ ಹಾಗೂ ಬ್ಯಾಂಕ್ ವಿವರಗಳನ್ನು ಕದಿಯಬಹುದು. ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯನ್ನು ಬಹಿರಂಗಗೊಳಿಸಬಹುದಾದ ಯಾವುದೇ ಹಣಕಾಸಿನ ವಹಿವಾಟುಗಳನ್ನು ಮಾಡಬೇಡಿ.

ಪ್ರಮುಖ ಅಂಶ – ಎಚ್‌ಎಸ್‌ಬಿಸಿ ಎಂದು ಹೇಳಿಕೊಳ್ಳುವ ವಿಶ್ವಾಸಾರ್ಹವಲ್ಲದ ಮೂಲದಿಂದ ನೀವು ಎಂದಾದರೂ ಇಮೇಲ್ ಅನ್ನು , ಅಥವಾ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಅರಸುವ ಕೋರದ ಇಮೇಲ್ ಅನ್ನು ಸ್ವೀಕರಿಸಿದರೆ; ಹೆಚ್ಚಿನ ತನಿಖೆಗಾಗಿ ನಮಗೆ **phishing@hsbc.com**ಗೆ ಅವುಗಳನ್ನು ವರದಿ ಮಾಡಿ.