ಮೋಸಗಾರರು ಇಲ್ಲಿದ್ದಾರೆ,
ಮೋಸಗಾರರು ಅಲ್ಲಿದ್ದಾರೆ,
ಎಲ್ಲಿಯೂ ಸಿಕ್ಕಿಹಾಕಿಕೊಳ್ಳಬೇಡಿ!

#BankingDhyaanSe 2.0

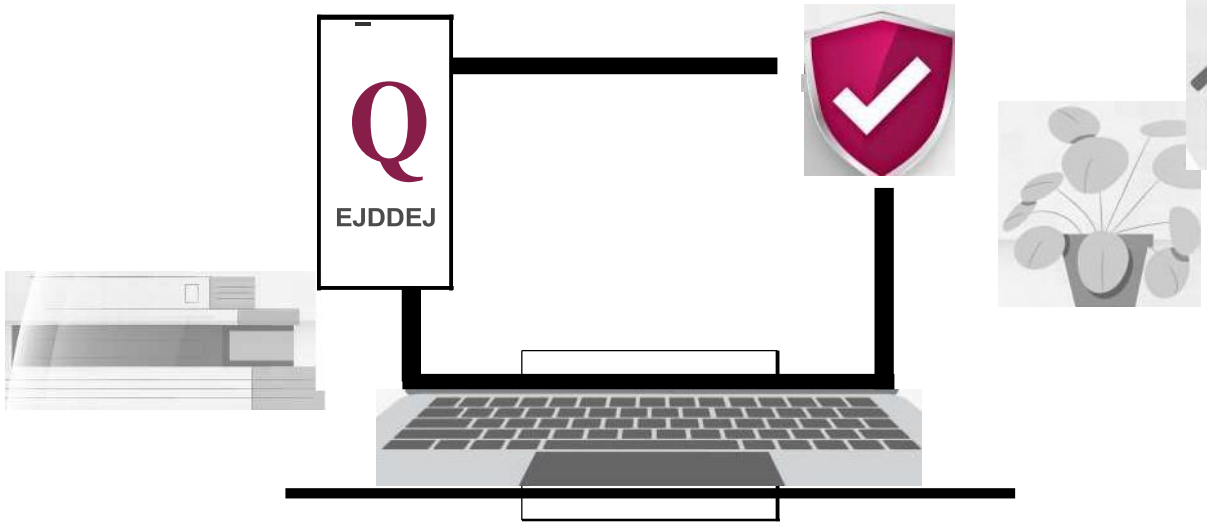
AXIS BANK

ನೀವು ಸಂಪಾದಿಸಲು ಕಷ್ಟಪಟ್ಟು ಕೆಲಸ ಮಾಡುತ್ತೀರಿ, ನಿಮ್ಮ ಗಳಿಕೆಯನ್ನು ಏಕೆ ಸುರಕ್ಷಿತವಾಗಿಡಬಾರದು?

ಆಕ್ಸಿಸ್ ಬ್ಯಾಂಕ್ ವಂಚನೆ ಜಾಗೃತಿ ಕಿರುಪುಸ್ತಕ #BankingDhyaanSe 2.0 ಗೆ ಸ್ವಾಗತ,
ಹಣಕಾಸಿನ ಹಗರಣಗಳನ್ನು ಅರ್ಥಮಾಡಿಕೊಳ್ಳಲು ಮತ್ತು ತಡೆಗಟ್ಟಲು ನಿಮ್ಮ ಕೀಲಿಕೈ. ವೇಗವಾಗಿ ವಿಕಸನಗೊಳ್ಳುತ್ತಿರುವ ಡಿಜಿಟಲ್ ಯುಗದಲ್ಲಿ, ಜ್ಞಾನವು ವಂಚಕರ ವಿರುದ್ಧ ನಿಮ್ಮ ರಕ್ಷಾಕವಚವಾಗಿದೆ. ಈ ಮಾರ್ಗದರ್ಶಿ ಪುಸ್ತಕವು ನಿಮಗೆ ಒಳನೋಟಗಳು, ನಿಜ ಜೀವನದ ಉದಾಹರಣೆಗಳು ಮತ್ತು ನೀವು ಕಷ್ಟಪಟ್ಟು ಸಂಪಾದಿಸಿದ ಹಣವನ್ನು ರಕ್ಷಿಸಲು ಪ್ರಾಯೋಗಿಕ ಸಲಹೆಗಳನ್ನು ಒದಗಿಸುತ್ತದೆ.

ಬ್ಯಾಂಕಿಂಗ್ ನಲ್ಲಿ ನಿಮ್ಮ ವಿಶ್ವಾಸಾರ್ಹ ಪಾಲುದಾರರಾಗಿ, ಆಕ್ಸಿಸ್ ಬ್ಯಾಂಕ್ ಡಿಜಿಟಲ್ ಲ್ಯಾಂಡ್‌ಸ್ಕೇಪ್ ಅನ್ನು ವಿಶ್ವಾಸದಿಂದ ನ್ಯಾವಿಗೇಟ್ ಮಾಡಲು ನಿಮಗೆ ಸಹಾಯ ಮಾಡಲು ಸಮರ್ಪಿತವಾಗಿದೆ. ಮೋಸದ ವಿರುದ್ಧ ಜಾಗರೂಕರಾಗಿರೋಣ ಮತ್ತು ಒಟ್ಟಿಗೆ ಉಜ್ವಲ ಆರ್ಥಿಕ ಭವಿಷ್ಯವನ್ನು ಭದ್ರಪಡಿಸೋಣ.

OTP ಹಗರಣಗಳು



ನಿಮ್ಮ ಅಭೇದ್ಯ ಡಿಜಿಟಲ್ ಸಾಮ್ರಾಜ್ಯವನ್ನು ಪ್ರವೇಶಿಸಲು ಒನ್-ಟೈಮ್ ಪಾಸ್‌ವರ್ಡ್ ಒಂದು ಚಿನ್ನದ ಕೀಯಾಗಿದೆ.

ಕುತಂತ್ರಿಗಳು ನಿಮ್ಮ ಅಮೂಲ್ಯವಾದ ಕೀಲಿಯನ್ನು ಕದಿಯದಂತೆ ತಡೆಯಲು, ನೀವು ನಿಮ್ಮ ಕೋಟೆಯ ಕಾವಲುಗಾರರಾಗಿರಬೇಕು!

OTPಗಳನ್ನು ಗೌಪ್ಯವಾಗಿರಿಸಿ: ಫೋನ್ ಕರೆಗಳು, ಇ-ಮೇಲ್‌ಗಳು, ಪಠ್ಯ ಸಂದೇಶಗಳು ಅಥವಾ ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮಗಳ ಮೂಲಕ OTPಗಳನ್ನು ಯಾರೊಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ ಮತ್ತು ಜಾಗರೂಕ ಕಾವಲುಗಾರನಂತೆ ಜಾಗರೂಕರಾಗಿರಿ.

ವಿನಂತಿಗಳನ್ನು ಪರಿಶೀಲಿಸಿ: ನಂಬಿ ಆದರೆ ಪರಿಶೀಲಿಸಿ. OTP ವಿನಂತಿಯು ನೀಲಿ ಬಣ್ಣದಿಂದ ಪಾಪ್ ಅಪ್ ಆಗಿದ್ದರೆ ಅಥವಾ ಅನುಮಾನಸ್ಪದವಾಗಿದ್ದರೆ, ಅವಸರಪಡಬೇಡಿ. ನೀವು ಪ್ರತಿಕ್ರಿಯಿಸುವ ಮೊದಲು ಅದರ ಸತ್ಯಾಸತ್ಯತೆಯನ್ನು ಎರಡು ಬಾರಿ ಪರಿಶೀಲಿಸಿ.

ಅಧಿಕೃತ ವೆಬ್‌ಸೈಟ್‌ಗಳು ಅಥವಾ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಬಳಸಿ: OTP ಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳುವಾಗ ಸುರಕ್ಷಿತವಾಗಿರಿ. ಯಾವಾಗಲೂ ಅಧಿಕೃತ ಸೈಟ್ ಅಥವಾ ಅಪ್ಲಿಕೇಶನ್‌ಗೆ ನೇರವಾಗಿ ಭೇಟಿ ನೀಡಿ - ಶಾರ್ಟ್‌ಕಟ್‌ಗಳಿಲ್ಲ. ಟೈಪ್ ಮಾಡುವುದು ಯಾವುದೇ ದಿನ ಲಿಂಕ್‌ಗಳನ್ನು ಕ್ಲಿಕ್ ಮಾಡುವುದನ್ನು ಮೀರಿಸುತ್ತದೆ.

ತುರ್ತು ವಿನಂತಿಗಳ ಬಗ್ಗೆ ಜಾಗರೂಕರಾಗಿರಿ: ನಿಮ್ಮ OTPಯನ್ನು ಹಂಚಿಕೊಳ್ಳುವಂತೆ ನಿಮ್ಮ ಮೇಲೆ ಒತ್ತಡ ಹೇರಲು ಸ್ಕ್ಯಾಮರ್ಗಳು ಆಗಾಗ್ಗೆ ತುರ್ತು ಪ್ರಜ್ಞೆಯನ್ನು ಸೃಷ್ಟಿಸುತ್ತಾರೆ. ಒಂದು ಹೆಜ್ಜೆ ಹಿಂದೆ ಸರಿದು, ವಿಮರ್ಶಾತ್ಮಕವಾಗಿ ಯೋಚಿಸಿ ಮತ್ತು ಕಾರ್ಯನಿರ್ವಹಿಸುವ ಮೊದಲು ವಿನಂತಿಯನ್ನು ಸ್ವತಂತ್ರವಾಗಿ ಪರಿಶೀಲಿಸಿ.

ಎರಡು-ಅಂಶಗಳ ದೃಢೀಕರಣವನ್ನು ಸಕ್ರಿಯಗೊಳಿಸಿ: 2FA (ಎರಡು-ಅಂಶಗಳ ದೃಢೀಕರಣ) ನೊಂದಿಗೆ ಭದ್ರತೆಯನ್ನು ದ್ವಿಗುಣಗೊಳಿಸಿ. ಅಪ್ಲಿಕೇಶನ್ ಆಧಾರಿತ ಅಥವಾ ಹಾರ್ಡ್‌ವೇರ್ ಟೋಕನ್‌ಗಳಂತಹ ರಾಕ್-ಸಾಲಿಡ್ ಆಯ್ಕೆಗಳನ್ನು ಆರಿಸಿ. ಅದು ಯಾವುದೇ ದಿನ SMS OTPಗಳನ್ನು ಮೀರಿಸುತ್ತದೆ.

ದಯವಿಟ್ಟು ನೆನಪಿಡಿ, ಬ್ಯಾಂಕ್ ನಿಮ್ಮ CVV, OTP, PIN, ಕಾರ್ಡ್ ಸಂಖ್ಯೆ, ಪಾಸ್‌ವರ್ಡ್ ಇತ್ಯಾದಿಗಳನ್ನು ಕೇಳುವುದಿಲ್ಲ. ಈ ವಿವರಗಳನ್ನು ಯಾರೊಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.

ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ಹಗರಣಗಳು

ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ಹಗರಣಗಳನ್ನು ಮರೆಮಾಚುವ ಮತ್ತು ಹುಡುಕುವ ಬಚ್ಚಿಕೊಳ್ಳುವ ಆಟವೆಂದು ಕಲ್ಪಿಸಿಕೊಳ್ಳೋಣ. ಸ್ಕ್ಯಾಮರ್ ತಮ್ಮ ನಿಜವಾದ ಉದ್ದೇಶಗಳನ್ನು ಮರೆಮಾಚಲು ಹೇಗೆ ಪ್ರಯತ್ನಿಸುತ್ತಾರೆಯೋ, ಹಾಗೆಯೇ ಅವರು ನಿಮ್ಮ ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ಮಾಹಿತಿಯನ್ನು ಬಹಿರಂಗಪಡಿಸಲು ನಿಮ್ಮನ್ನು ಮೋಸಗೊಳಿಸಬಹುದು.

ಅವರ ಬಲೆಗೆ ಬೀಳುವುದನ್ನು ತಪ್ಪಿಸಲು, ಈ ಸಲಹೆಗಳನ್ನು ನೆನಪಿನಲ್ಲಿಡಿ:

ಫಿಶರ್‌ಗಳ ಬಗ್ಗೆ ಎಚ್ಚರದಿಂದಿರಿ: ಸ್ಕ್ಯಾಮರ್‌ಗಳು ನಿಮ್ಮ ಬ್ಯಾಂಕ್ ಅಥವಾ ಪರಿಚಿತ ಕಂಪನಿಯಿಂದ ಬಂದವರಂತೆ ನಟಿಸಬಹುದು. ಅವರ ತಂತ್ರಗಳಿಗೆ ಬೀಳಬೇಡಿ; ಅವರ ಗುರುತನ್ನು ಪರಿಶೀಲಿಸಿ.

ನಿಮ್ಮ ಸ್ಟೇಟ್‌ಮೆಂಟ್‌ಗಳನ್ನು ಪರಿಶೀಲಿಸಿ: ನಿಮ್ಮ ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ಸ್ಟೇಟ್‌ಮೆಂಟ್‌ಗಳನ್ನು ನಿಯಮಿತವಾಗಿ ಪರಿಶೀಲಿಸಿ. ನೀವು ಅಪರಿಚಿತ ಖರ್ಚುಗಳು ಅಥವಾ ಶುಲ್ಕಗಳನ್ನು ಗುರುತಿಸಿದರೆ, ಅದು ಆಟದಲ್ಲಿ ಅಡಗಿರುವ ಆಟಗಾರರನ್ನು ಕಂಡುಹಿಡಿದಂತೆ- ಅವರನ್ನು ತಕ್ಷಣ ಪರಿಹರಿಸಿ.

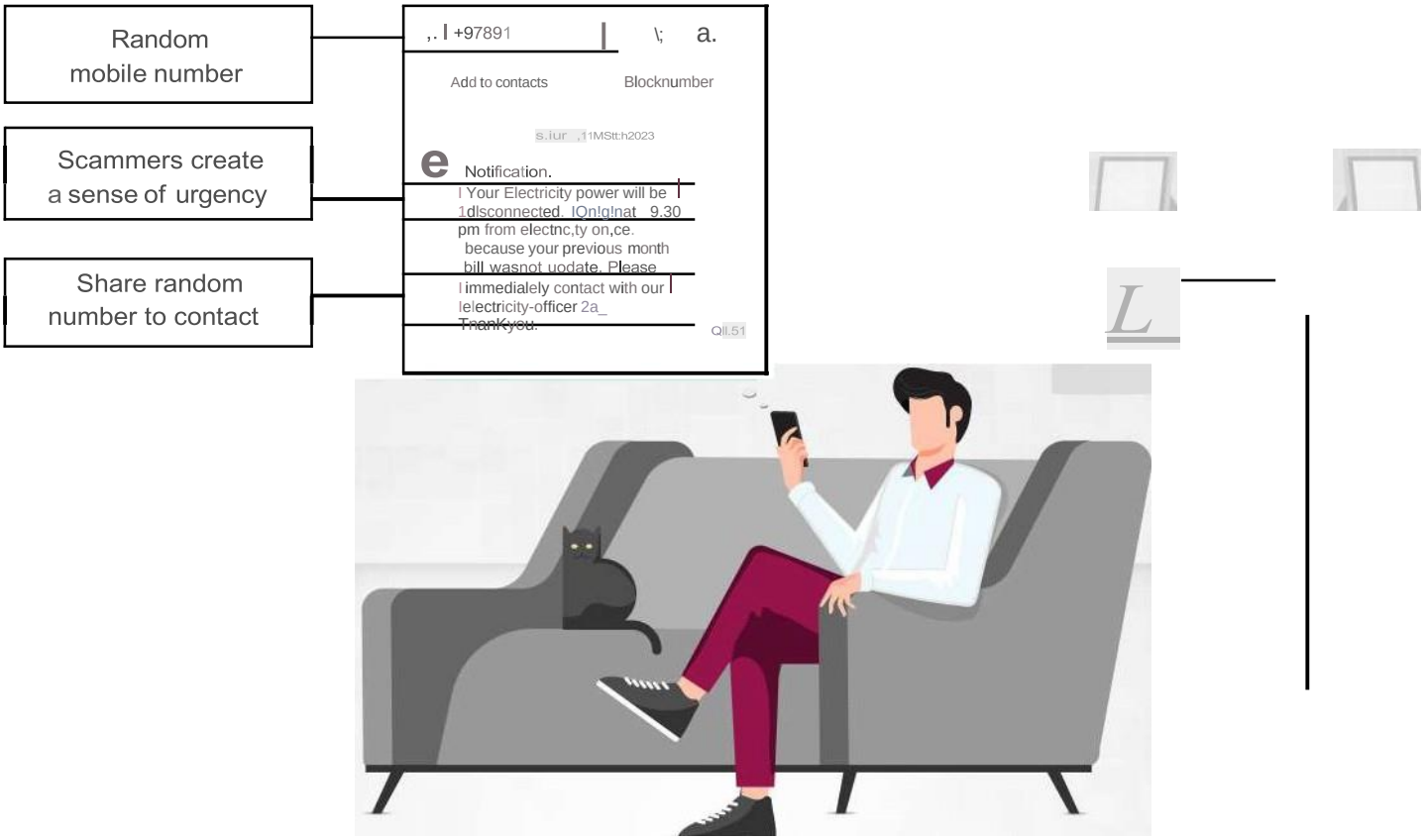
ವಹಿವಾಟು ಮಿತಿಗಳನ್ನು ಹೊಂದಿಸಿ: ನಿಮ್ಮ ಎಲ್ಲಾ ಪಾವತಿ ಚಾನೆಲ್ ಗಳಲ್ಲಿ ವಹಿವಾಟು ಮಿತಿಗಳನ್ನು ಹೊಂದಿಸಿ ಮತ್ತು ನಿಮ್ಮ ಅಗತ್ಯಕ್ಕೆ ಅನುಗುಣವಾಗಿ 'ಬಳಕೆಯನ್ನು ನಿರ್ವಹಿಸಿ' ವಿಭಾಗವನ್ನು ಗ್ರಾಹಕೀಯಗೊಳಿಸಿ.

ಸುರಕ್ಷಿತ ಸೈಟ್‌ಗಳು ಮಾತ್ರ: ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಶಾಪಿಂಗ್ ಮಾಡುವಾಗ, ವೆಬ್‌ಸೈಟ್ ಸುರಕ್ಷಿತವಾಗಿದೆ ಎಂದು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಿ (URL ನಲ್ಲಿ "https" ಗಾಗಿ ನೋಡಿ). ಇದು ಆಟಕ್ಕೆ ಸುರಕ್ಷಿತ ಆಟದ ಮೈದಾನವನ್ನು ಆಯ್ಕೆ ಮಾಡಿದಂತೆ.

ಅಪ್‌ಡೇಟ್ ಆಗಿರಿ: ನೀವು ಆಟದಲ್ಲಿ ಹೊಸ ತಂತ್ರಗಳನ್ನು ಕಲಿಯುವಂತೆಯೇ ಇತ್ತೀಚಿನ ಹಗರಣ ತಂತ್ರಗಳ ಮೇಲೆ ಕಣ್ಣಿಡಿ. ಈ ರೀತಿಯಾಗಿ, ನೀವು ಸ್ಕ್ಯಾಮರ್‌ಗಳನ್ನು ಮೀರಿಸಲು ಸಿದ್ಧರಾಗುತ್ತೀರಿ.

ವಿದ್ಯುತ್ ಬಿಲ್ ಹಗರಣಗಳು

ನಕಲಿ SMS ಗುರುತಿಸುವುದು ಹೇಗೆ?



ಇದನ್ನು ಕಲ್ಪಿಸಿಕೊಳ್ಳಿ: ನೀವು ಮನೆಯಲ್ಲಿ ವಿಶ್ರಾಂತಿ ಸಂಜೆಯನ್ನು ಆನಂದಿಸುತ್ತಿದ್ದೀರಿ, ನಿಮ್ಮ ನೆಚ್ಚಿನ ಪ್ರದರ್ಶನವನ್ನು ಅತಿಯಾಗಿ ವೀಕ್ಷಿಸುತ್ತಿದ್ದೀರಿ, ನಿಮ್ಮ ಫೋನ್ ಒಳಬರುವ ಸಂದೇಶದೊಂದಿಗೆ ಸದ್ದು ಮಾಡುತ್ತದೆ. ಇದು ನಿಮ್ಮ ವಿದ್ಯುತ್ ಪೂರೈಕೆದಾರ, ಮತ್ತು ನಿಮ್ಮ ಇತ್ತೀಚಿನ ಬಿಲ್ ಗೆ ನೀವು ಅತಿಯಾದ ಮೊತ್ತವನ್ನು ಪಾವತಿಸಬೇಕಾಗಿದೆ ಎಂದು ಅವರು ಹೇಳುತ್ತಿದ್ದಾರೆ.

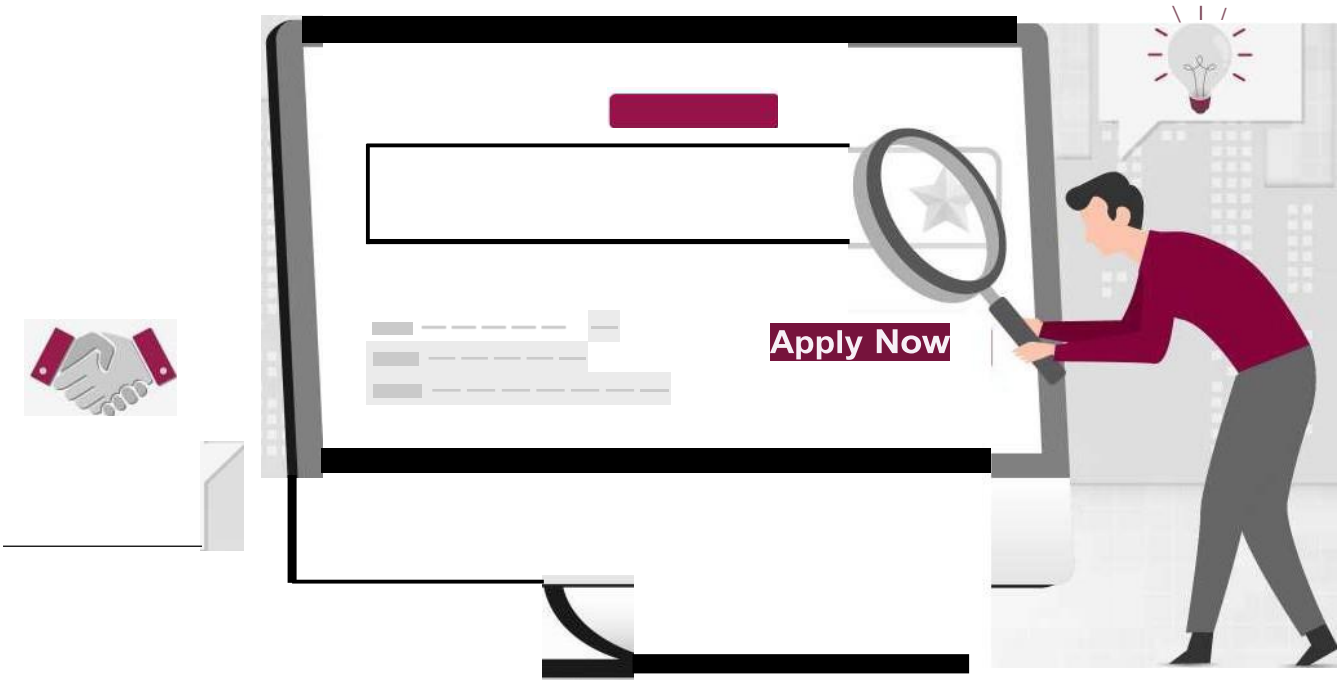
ನೀವು ಭಯಭೀತರಾಗುವ ಮೊದಲು, ಇದನ್ನು ಪರಿಗಣಿಸಿ: ವಿದ್ಯುತ್ ಬಿಲ್ ವಂಚನೆ, ರಹಸ್ಯ ಭೂತದಂತೆ, ಯಾವುದೇ ಮುನ್ಸೂಚನೆಯಿಲ್ಲದೆ ನಿಮ್ಮ ಜೀವನದಲ್ಲಿ ನುಸುಳಬಹುದು.

ನಿಮ್ಮ ಗೌಪ್ಯ ವಿವರಗಳನ್ನು ಯಾರೊಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ ಅಥವಾ ಅನಪೇಕ್ಷಿತ ಲಿಂಕ್‌ಗಳನ್ನು ಕ್ಲಿಕ್ ಮಾಡಬೇಡಿ.

ಬಿಲ್ ಪಾವತಿಗಳನ್ನು ಮಾಡಲು ಅಧಿಕೃತ ಮತ್ತು ಸುರಕ್ಷಿತ ವೆಬ್‌ಸೈಟ್‌ಗಳನ್ನು ಮಾತ್ರ ಬಳಸಿ.

ನೆನಪಿಡಿ, ವಿದ್ಯುತ್ ಇಲಾಖೆಯು ವೈಯಕ್ತಿಕ ವಿವರಗಳನ್ನು ಅಥವಾ ಯಾದೃಚ್ಛಿಕ / ನೋಂದಾಯಿಸದ ಸಂಖ್ಯೆಗಳ ಮೂಲಕ ಪಾವತಿಗಳನ್ನು ಎಂದಿಗೂ ಕೇಳುವುದಿಲ್ಲ.

ಉದ್ಯೋಗ ಹಗರಣಗಳು



ನೀವು ಉದ್ಯೋಗ ಪಟ್ಟಿಗಳ ಮೂಲಕ ಸ್ಕ್ರೋಲ್ ಮಾಡುತ್ತಿದ್ದೀರಿ ಎಂದು ಕಲ್ಪಿಸಿಕೊಳ್ಳಿ ಮತ್ತು ಇದ್ದಕ್ಕಿದ್ದಂತೆ ನೀವು ಉದ್ಯೋಗದ ಪ್ರಸ್ತಾಪವನ್ನು ಮುಗ್ಗರಿಸುತ್ತೀರಿ ಅದು ನಿಜವಾಗಲು ತುಂಬಾ ಒಳ್ಳೆಯದು. ಅನಿಯಮಿತ ರಜೆಯ ದಿನಗಳು, ನಿಮ್ಮ ಪೈಜಾಮಾದಲ್ಲಿ ಕೆಲಸ, ಮತ್ತು ಡೇಟಾ ಎಂಟ್ರಿಗಾಗಿ ಆರು-ಅಂಕಿಯ ಸಂಬಳ? ನನ್ನನ್ನು ಸೈನ್ ಅಪ್ ಮಾಡಿ!

ನೀವು ಆ "ಈಗ ಅನ್ವಯಿಸಿ" ಬಟನ್ ಒತ್ತುವ ಮೊದಲು ಕಾಯಿರಿ!

ಕಂಪನಿಯ ಬಗ್ಗೆ ಸಂಶೋಧಿಸಿ: ಕಂಪನಿಯನ್ನು ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ನೋಡಿ ಮತ್ತು ಅದು ಪ್ರತಿಷ್ಠಿತವಾಗಿದೆ ಎಂದು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಿ. ವಂಚಕರು ಸಾಮಾನ್ಯವಾಗಿ ಮನವೊಲಿಸುವ ವೆಬ್‌ಸೈಟ್‌ಗಳೊಂದಿಗೆ ನಕಲಿ ಕಂಪನಿಗಳನ್ನು ರಚಿಸುತ್ತಾರೆ.

ಮುಂಗಡವಾಗಿ ಪಾವತಿಸಬೇಡಿ: ನೀವು ಕೆಲಸ ಮಾಡಲು ಪ್ರಾರಂಭಿಸುವ ಮೊದಲು ಕಾನೂನುಬದ್ಧ ಉದ್ಯೋಗದಾತರು ತರಬೇತಿ, ಸಾಮಗ್ರಿಗಳು ಅಥವಾ ಹಿನ್ನೆಲೆ ಪರಿಶೀಲನೆಗಳಿಗೆ ಪಾವತಿಸಲು ನಿಮ್ಮನ್ನು ಕೇಳುವುದಿಲ್ಲ.

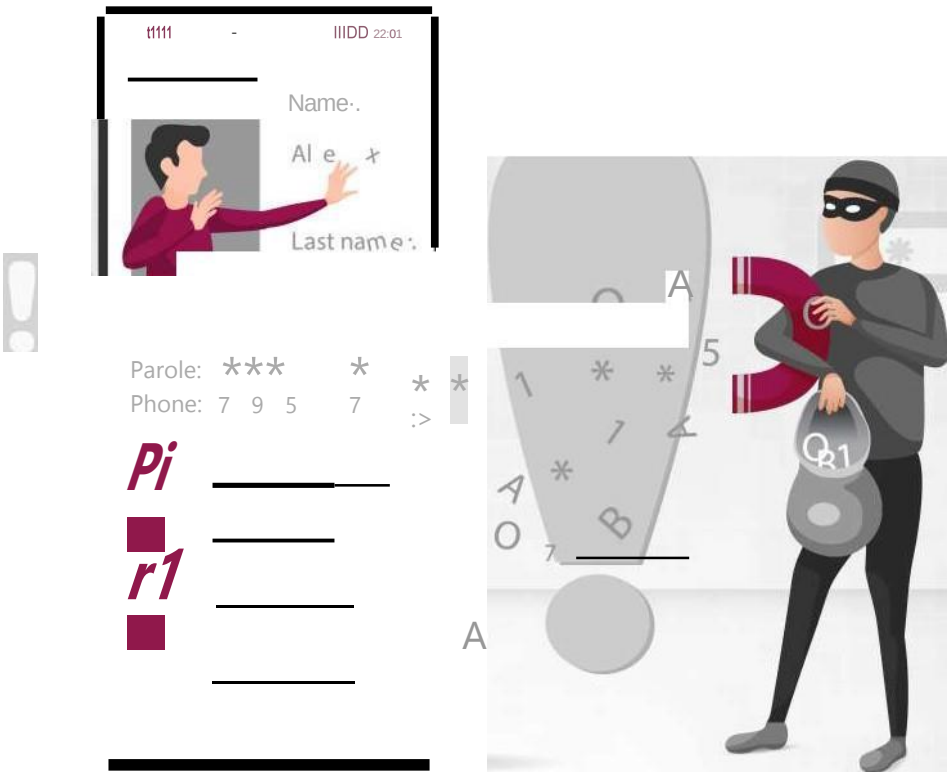
ರೆಡ್ ಫ್ಲಾಗ್ ಮೇಲೆ ನಿಗಾ ಇರಿಸಿ: ನಿಮ್ಮ ಸಾಮಾಜಿಕ ಭದ್ರತೆ ಸಂಖ್ಯೆ ಅಥವಾ ಹಣಕಾಸಿನ ವಿವರಗಳಂತಹ ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯನ್ನು ಈಗಿನಿಂದಲೇ ಒದಗಿಸುವ ಕೆಲಸವು ನಿಮಗೆ ಅಗತ್ಯವಿದ್ದರೆ ಜಾಗರೂಕರಾಗಿರಿ.

ಬಾಡಿಗೆಗೆ ತುಂಬಾ ತ್ವರಿತ: ಸಂದರ್ಶನ ಅಥವಾ ಹೆಚ್ಚಿನ ಮಾಹಿತಿಯನ್ನು ವಿನಿಮಯ ಮಾಡಿಕೊಳ್ಳದೆಯೇ ನಿಮಗೆ ಸ್ಥಳದಲ್ಲೇ ಕೆಲಸ ನೀಡಿದರೆ, ಅದು ಹಗರಣವಾಗಿರಬಹುದು.

ನಿಮ್ಮ ಪ್ರವೃತ್ತಿಯನ್ನು ನಂಬಿರಿ: ಏನಾದರೂ ತೊಂದರೆಯಾದರೆ, ನಿಮ್ಮ ಕರುಳನ್ನು ನಂಬಿ ಮತ್ತು ಎಚ್ಚರಿಕೆಯಿಂದ ಮುಂದುವರಿಯಿರಿ ಅಥವಾ ದೂರ ಹೋಗಿ.

ನೆನಪಿಡಿ, ಉದ್ಯೋಗ ಹುಡುಕಾಟದಲ್ಲಿ ನಿಮ್ಮ ವೈಯಕ್ತಿಕ ಮತ್ತು ಹಣಕಾಸಿನ ಮಾಹಿತಿಯನ್ನು ರಕ್ಷಿಸುವುದು ನಿಮ್ಮ ಮೊದಲ ಆದ್ಯತೆಯಾಗಿರಬೇಕು.

ಕರೆ ವಂಚನೆ ಹಗರಣ



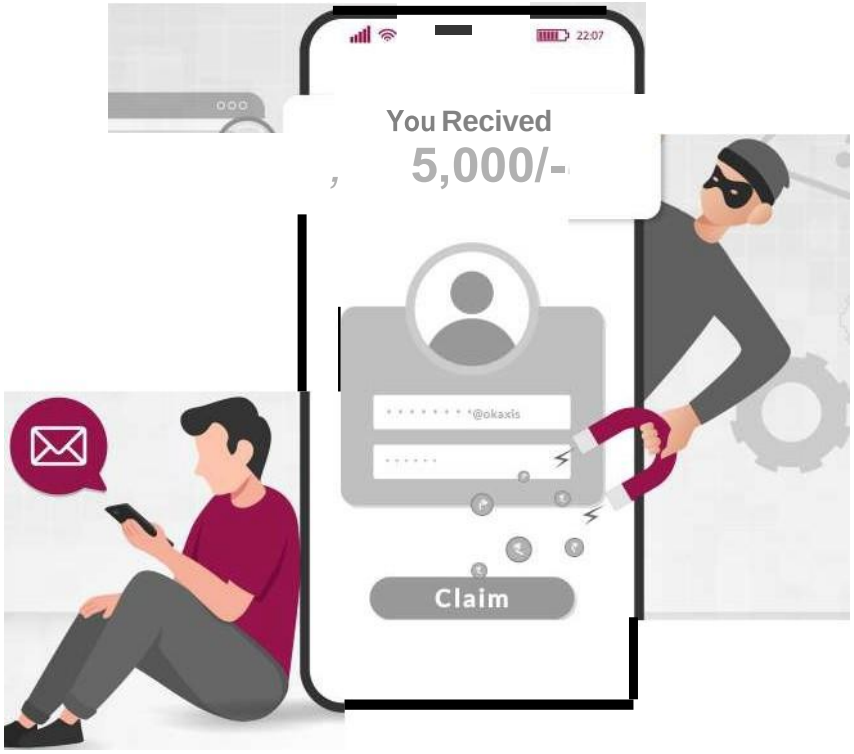
ಜಾದೂಗಾರನು ವಿಷಯಗಳನ್ನು ವಾಸ್ತವವಾಗಿ ಇರುವುದಕ್ಕಿಂತ ಭಿನ್ನವಾಗಿ ಕಾಣುವಂತೆ ಹೇಗೆ ಮಾಡಬಹುದು, ಸ್ಕ್ಯಾಮರ್‌ಗಳು ನಿಮ್ಮ ಕಾಲರ್ ಐಡಿಯನ್ನು ನೀವು ತಿಳಿದಿರುವ ಅಥವಾ ನಂಬುವ ವ್ಯಕ್ತಿ ಎಂದು ತೋರುವಂತೆ ಮಾಡಲು ನಿರ್ವಹಿಸಬಹುದು - ಈ ಸಂದರ್ಭದಲ್ಲಿ, ನಿಮ್ಮ ಬ್ಯಾಂಕ್. ಇದು ಅವರ ನಿಜವಾದ ಗುರುತಿಗಾಗಿ ಡಿಜಿಟಲ್ ವೇಷದಂತೆ..
ಈ ಸ್ನೀಕಿ ಟ್ರಿಕ್‌ನಿಂದ ನಿಮ್ಮನ್ನು ರಕ್ಷಿಸಿಕೊಳ್ಳಲು, ಈ ಸಲಹೆಗಳನ್ನು ನೆನಪಿಡಿ:

ಎಚ್ಚರಿಕೆಯಿಂದ ಪರಿಶೀಲಿಸಿ: ಕಾಲರ್ ಐಡಿ ಪರಿಚಿತವಾಗಿರುವಂತೆ ತೋರುತ್ತಿದ್ದರೂ ಸಹ, ಸಂದೇಹದಿಂದ ಇರಿ. ಯಾರಾದರೂ ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯನ್ನು ಕೇಳಿದರೆ, ಇತರ ವಿಧಾನಗಳ ಮೂಲಕ ಅವರ ಗುರುತನ್ನು ಎರಡು ಬಾರಿ ಪರಿಶೀಲಿಸಿ.
ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಹಂಚಿಕೊಳ್ಳಬೇಡಿ: ಕರೆ ಮಾಡಿದವರು ನ್ಯಾಯಸಮ್ಮತವಾಗಿ ತೋರಿದರೂ ಸಹ, ಫೋನ್‌ನಲ್ಲಿ ವೈಯಕ್ತಿಕ ಅಥವಾ ಹಣಕಾಸಿನ ಮಾಹಿತಿಯನ್ನು ಎಂದಿಗೂ ನೀಡಬೇಡಿ. ವಿಶ್ವಾಸಾರ್ಹ ಸಂಖ್ಯೆಯನ್ನು ಬಳಸಿಕೊಂಡು ಸ್ವಗಿತಗೊಳಿಸಿ ಮತ್ತು ಮರಳಿ ಕರೆ ಮಾಡಿ.
ಖಾಸಗಿಯಾಗಿರಿ: ನೀವು ಲೈನ್‌ನಲ್ಲಿ ಅಥವಾ ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮದಲ್ಲಿ ಯಾವ ವೈಯಕ್ತಿಕ ವಿವರಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳುತ್ತೀರಿ ಎಂಬುದರ ಕುರಿತು ಜಾಗರೂಕರಾಗಿರಿ. ವಂಚಕರು ತಮ್ಮ ವಂಚನೆಯ ಕರೆಗಳನ್ನು ಹೆಚ್ಚು ಮನವರಿಕೆ ಮಾಡಲು ಈ ಮೂಲಗಳಿಂದ ಮಾಹಿತಿಯನ್ನು ಸಂಗ್ರಹಿಸುತ್ತಾರೆ.
ಕರೆ ನಿರ್ಬಂಧಿಸುವಿಕೆಯನ್ನು ಬಳಸಿ: ನಿಮ್ಮ ಫೋನ್ ವಾಹಕದಿಂದ ಒದಗಿಸಲಾದ ಕರೆ ನಿರ್ಬಂಧಿಸುವ ಅಪ್ಲಿಕೇಶನ್‌ಗಳು ಅಥವಾ ವೈಶಿಷ್ಟ್ಯಗಳನ್ನು ಅನ್ವೇಷಿಸಿ. ಸಂಭಾವ್ಯ ಹಗರಣ ಕರೆಗಳನ್ನು ಫಿಲ್ಟರ್ ಮಾಡಲು ಅವರು ಸಹಾಯ ಮಾಡಬಹುದು.

Google ಅಥವಾ ಯಾವುದೇ ಹುಡುಕಾಟ ಎಂಜಿನ್‌ನಲ್ಲಿ ಫೋನ್ ಸಂಖ್ಯೆಗಳನ್ನು ಹುಡುಕಬೇಡಿ. ನೀವು ಹಾಗೆ ಮಾಡಿದರೆ, ಘಟಕ ಅಥವಾ ವ್ಯಾಪಾರಿ ನಿಮಗೆ ಕಳುಹಿಸಿದ ಯಾವುದೇ ಲಿಂಕ್‌ಗಳನ್ನು ಕ್ಲಿಕ್ ಮಾಡಬೇಡಿ.

ಹೆಚ್ಚುವರಿಯಾಗಿ, ಅಧಿಕೃತ ಅಪ್ಲಿಕೇಶನ್ ಸ್ಟೋರ್‌ಗಳಿಂದ ನಿಮ್ಮ ಸಾಧನಗಳಲ್ಲಿ ಡೌನ್‌ಲೋಡ್ ಮಾಡಲಾದ ಬ್ಯಾಂಕಿಂಗ್ ಅಪ್ಲಿಕೇಶನ್‌ಗಳ ಇತ್ತೀಚಿನ ಆವೃತ್ತಿಗಳನ್ನು ನೀವು ಹೊಂದಿರುವಿರಾ ಎಂಬುದನ್ನು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಿ.
ದಯವಿಟ್ಟು ಇದನ್ನು ನಿಯತಕಾಲಿಕವಾಗಿ ಪರಿಶೀಲಿಸಿ.
ನೆನಪಿಡಿ, ನಿಜ ಜೀವನದಲ್ಲಿ ನೀವು ಮುಖವಾಡ ಧರಿಸಿದ ಅಪರಿಚಿತರನ್ನು ನಂಬದಂತೆಯೇ, ಫೋನ್‌ನಲ್ಲಿ ಮುಖವಾಡ ಧರಿಸಿದ ಕರೆ ಮಾಡುವವರನ್ನು ನಂಬಬೇಡಿ. ಜಾಗರೂಕರಾಗಿರಿ!

UPI ಮರುಪಾವತಿ ಹಗರಣ



ನೀವು UPI ಮರುಪಾವತಿ ಅಧಿಸೂಚನೆಯನ್ನು ಗುರುತಿಸಿದಾಗ ನಿಮ್ಮ ಫೋನ್ ಮೂಲಕ ನೀವು ಸ್ಕ್ರೋಲ್ ಮಾಡುತ್ತಿದ್ದೀರಿ ಎಂದು ಕಲ್ಪಿಸಿಕೊಳ್ಳಿ ಮತ್ತು ಇದ್ದಕ್ಕಿದ್ದಂತೆ, ನೀವು ಅವಸರದಲ್ಲಿದ್ದೀರಿ! ಆದರೆ ನಿರೀಕ್ಷಿಸಿ. ಇದು UPI ಮರುಪಾವತಿ ಹಗರಣವಾಗಿರಬಹುದು!

UPI ಅಥವಾ ಏಕೀಕೃತ ಪಾವತಿಗಳ ಇಂಟರ್ಫೇಸ್ ನಮ್ಮ ದೈನಂದಿನ ಜೀವನದ ಭಾಗವಾಗಿದೆ. ನಿಮ್ಮ ಸ್ಥಳೀಯ ಕಿರಾನಾ ಸ್ಟೋರ್‌ಗಳಲ್ಲಿ ಪಾವತಿಸುವುದರಿಂದ ಹಿಡಿದು ಫೋನ್‌ಗಳನ್ನು ರೀಚಾರ್ಜ್ ಮಾಡುವುದರಿಂದ ಫ್ಲೈಟ್ ಟಿಕೆಟ್‌ಗಳನ್ನು ಕಾಯ್ದಿರಿಸುವವರೆಗೆ, ನಾವು ವಿವಿಧ ವಿಷಯಗಳಿಗೆ UPI ಪಾವತಿಯನ್ನು ಬಳಸುತ್ತೇವೆ. ಆದ್ದರಿಂದ UPI ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಬಳಸಿಕೊಂಡು ಜನರನ್ನು ಮೋಸಗೊಳಿಸಲು ಸ್ಕ್ಯಾಮ್‌ಸ್ಟರ್‌ಗಳು ಹೊಸ ವಿಧಾನಗಳನ್ನು ಅಳವಡಿಸಿಕೊಳ್ಳಲು ಪ್ರಾರಂಭಿಸಿದ್ದಾರೆ.

ಅವರ ಅಧಿಕೃತ ಪರಿಭಾಷೆ ಮತ್ತು ವೃತ್ತಿಪರ ಭಾಷೆಗೆ ಎಂದಿಗೂ ಬೀಳಬೇಡಿ. ಕೆಳಗಿನ ಸಲಹೆಗಳನ್ನು ನೆನಪಿನಲ್ಲಿಡಿ:

ಲಿಂಕ್‌ಗಳ ಬಗ್ಗೆ ಎಚ್ಚರದಿಂದಿರಿ: ವಂಚಕರು ನಿಮಗೆ ಲಿಂಕ್ ಕಳುಹಿಸಬಹುದು, ಮರುಪಾವತಿಯನ್ನು ಪಡೆಯಲು ನೋಂದಾಯಿಸಲು ನಿಮ್ಮನ್ನು ಒತ್ತಾಯಿಸುತ್ತಾರೆ.

ಅಧಿಕ ಒತ್ತಡದ ತಂತ್ರಗಳು: ತ್ವರಿತ ಹಣಕ್ಕಾಗಿ ತಕ್ಷಣವೇ ಬ್ಯಾಂಕ್ ವಿವರಗಳನ್ನು ಅಥವಾ UPI ಪಿನ್ ಅನ್ನು ಭರ್ತಿ ಮಾಡಲು ಅವರು ನಿಮಗೆ ಒತ್ತಡ ಹೇರುತ್ತಾರೆ.

ಅರ್ಹತೆಯನ್ನು ಪರಿಶೀಲಿಸಿ: ನೀವು ಮರುಪಾವತಿಗೆ ಅರ್ಹರಾಗಿದ್ದೀರಿ ಎಂದು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಿ. ಹೌದು ಎಂದಾದರೆ, ವಿಶ್ವಾಸಾರ್ಹ ಮೂಲವನ್ನು ಪರಿಶೀಲಿಸಿ.

ನೆನಪಿಡಿ, ಬ್ಯಾಂಕ್ ಅಥವಾ ಇತರ ಅಧಿಕಾರಿಗಳು ಅಂತಹ ಸೂಕ್ಷ್ಮ ವಿವರಗಳನ್ನು ಎಂದಿಗೂ ಕೇಳುವುದಿಲ್ಲ.

ಫಿಶಿಂಗ್ ಹಗರಣ

ನಿಮ್ಮ ಸ್ವಂತ ವ್ಯವಹಾರವನ್ನು ಗಮನದಲ್ಲಿಟ್ಟುಕೊಂಡು ನೀವು ಸ್ಪಷ್ಟವಾದ ಕೊಳದಲ್ಲಿ ಶಾಂತಿಯುತವಾಗಿ ಈಜುವ ಮೀನು ಎಂದು ಊಹಿಸಿ. ಇದ್ದಕ್ಕಿದ್ದಂತೆ, ಹೊಳೆಯುವ, ಪ್ರಲೋಭನಗೊಳಿಸುವ ಬೆಟ್ ನಿಮ್ಮ ಮುಂದೆ ತೂಗಾಡುತ್ತದೆ. ನೀವು ಆಸಕ್ತಿ ಹೊಂದಿದ್ದೀರಿ ಆದರೆ ನಿರೀಕ್ಷಿಸಿ - ಏನೋ ಫೀಶಿಂಗ್!

ಫಿಶಿಂಗ್ ಹಗರಣಗಳೊಂದಿಗೆ ಡಿಜಿಟಲ್ ಕ್ಷೇತ್ರದಲ್ಲಿ ಇದು ನಿಖರವಾಗಿ ಸಂಭವಿಸುತ್ತದೆ.

ಸೈಬರ್ ಕ್ರಿಮಿನಲ್‌ಗಳು ನಿಮ್ಮನ್ನು ಮೋಸಗೊಳಿಸಲು ನಂಬಲರ್ಹ ವ್ಯಕ್ತಿಗಳಂತೆ ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯನ್ನು ಬಹಿರಂಗಪಡಿಸಲು ಪ್ರಯತ್ನಿಸುತ್ತಾರೆ, ಮೀನುಗಳು ಬೆಟ್‌ನಿಂದ ಆಮಿಷಕ್ಕೆ ಒಳಗಾಗುತ್ತವೆ. ಅವರು ನಕಲಿ ಇಮೇಲ್‌ಗಳು, ಸಂದೇಶಗಳು ಅಥವಾ ವೆಬ್‌ಸೈಟ್‌ಗಳನ್ನು ಕಳುಹಿಸುತ್ತಾರೆ ಅದು ಅಸಲಿ ಎಂದು ತೋರುತ್ತದೆ, ಆಗಾಗ್ಗೆ ಬ್ಯಾಂಕ್‌ಗಳು, ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮಗಳು ಅಥವಾ ನಿಮ್ಮ ಬಾಸ್ ಅನ್ನು ಅನುಕರಿಸುತ್ತದೆ.
ಈ ಡಿಜಿಟಲ್ ಕೊಕ್ಕೆಗಳನ್ನು ತಪ್ಪಿಸಿಕೊಳ್ಳಲು, ಈ ಸಲಹೆಗಳನ್ನು ನೆನಪಿಡಿ:

URLಗಳನ್ನು ಎರಡು ಬಾರಿ ಪರಿಶೀಲಿಸಿ: ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಹಂಚಿಕೊಳ್ಳಬೇಡಿ:

ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಹಂಚಿಕೊಳ್ಳಬೇಡಿ: ಕಾನೂನುಬದ್ಧ ಘಟಕಗಳು ಇಮೇಲ್ ಮೂಲಕ ಸೂಕ್ಷ್ಮ ವಿಷಯವನ್ನು ಕೇಳುವುದಿಲ್ಲ.

ಸಂಶಯಾಸ್ಪದವಾಗಿ ಇರಿ: ಅನಿರೀಕ್ಷಿತ ವಿನಂತಿಗಳು? ಕಾರ್ಯನಿರ್ವಹಿಸುವ ಮೊದಲು ಇತರ ವಿಧಾನಗಳ ಮೂಲಕ ಪರಿಶೀಲಿಸಿ

ಭದ್ರತಾ ಸಾಫ್ಟ್‌ವೇರ್ ಅನ್ನು ನವೀಕರಿಸಿ: ಇತ್ತೀಚಿನ ರಕ್ಷಣೆಗಳೊಂದಿಗೆ ನಿಮ್ಮ ಡಿಜಿಟಲ್ ಕೊಳವನ್ನು ಕಾಪಾಡಿ.

ಎಚ್ಚರಿಕೆಯ ಮೀನಿನಂತೆಯೇ, ಜಾಗರೂಕರಾಗಿರಿ ಮತ್ತು ಅಂತರ್ಜಾಲದ ವಿಶಾಲ ಸಾಗರದಲ್ಲಿ ಚುರುಕಾಗಿ ಈಜಿಕೊಳ್ಳಿ!

ವಿಷಿಂಗ್ ಹಗರಣ

a

ನಿಮ್ಮ ಫೋನ್ ರಿಂಗ್ ಆಗುತ್ತದೆ, ಮತ್ತು ಇದು ನಿಮ್ಮ ಬ್ಯಾಂಕ್ ಎಂದು ಕರೆಯಲಾಗುವ ನಿಮ್ಮ ಖಾತೆಗೆ ಧಕ್ಕೆಯಾಗಿದೆ ಎಂದು ಹೇಳಿಕೊಳ್ಳುವ 'ತುರ್ತು' ಕರೆಯೊಂದಿಗೆ, ಅಥವಾ ಬಹುಶಃ ಇದು ನಿಮ್ಮ ಅದೃಷ್ಟದ ದಿನ ಎಂದು ಹೇಳಿಕೊಳ್ಳುವ 'ವಿಜೇತ' ಕರೆ, ಮತ್ತು ನೀವು ಬಹುಮಾನ ಗೆದ್ದಿದ್ದೀರಿ! ಫೋನ್ ಹಿಡಿದುಕೊಳ್ಳಿ (ಅಕ್ಷರಶಃ)!

ಅಂತಹ ಹಗರಣಗಳಿಂದ ಸುರಕ್ಷಿತವಾಗಿರಲು, ಈ ಕೆಳಗಿನ ಸಲಹೆಗಳನ್ನು ನೆನಪಿಡಿ:

ನಿಮ್ಮ ವೈಯಕ್ತಿಕ ವಿವರಗಳನ್ನು ಎಂದಿಗೂ ಫೋನ್ ಅಲ್ಲಿ ಹೇಳಬೇಡಿ.

<@)>

ಷರ್ಲಾಕ್ ಹೋಮ್ಸ್ ಆಗಿರಿ ಮತ್ತು ಆ ಕರೆ ಮಾಡಿದವರ ಗುರುತನ್ನು ಪರಿಶೀಲಿಸಿ.

ನಾಟಕವನ್ನು ಒಪ್ಪಿಕೊಳ್ಳಬೇಡಿ! ಅವರು ಹೆಚ್ಚು ಮಾತನಾಡಿದಷ್ಟು ಶಾಂತವಾಗಿರಿ.

ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಅಪರಿಚಿತರೊಂದಿಗೆ ಮಾಹಿತಿಯನ್ನು ಹಂಚಿಕೊಳ್ಳುವ ಬಗ್ಗೆ ಜಾಗರೂಕರಾಗಿರಿ - ನಿಮ್ಮ ವಿಷಯವನ್ನು ಸುರಕ್ಷಿತವಾಗಿರಿಸಲು ಸ್ಮಾರ್ಟ್ ಆಗಿರಿ!

UPI ಸ್ಕ್ಯಾಮ್‌ಗಳು - ಹಣಕ್ಕಾಗಿ ವಿನಂತಿ ಆಯ್ಕೆ

+75,000/

-75,000/-

ಸ್ನೇಹಾ ತನ್ನ ಪೀಠೋಪಕರಣಗಳನ್ನು ಆನ್‌ಲೈನ್ ಖರೀದಿ ಮತ್ತು ಮಾರಾಟದ ಅಪ್ಲಿಕೇಶನ್‌ನಲ್ಲಿ ಜಾಹೀರಾತು ಮಾಡಿದರು. ಅರೆಸೇನಾಪಡೆಯ ಸಿಬ್ಬಂದಿ ಎಂದು ಹೇಳಿಕೊಳ್ಳುವ ಖರೀದಿದಾರರೊಬ್ಬರು ವಾಟ್ಸಾಪ್‌ನಲ್ಲಿ ಪಾವತಿಗಾಗಿ ಕ್ಯೂಆರ್ ಕೋಡ್ ಕಳುಹಿಸಿದ್ದಾರೆ. ಸ್ನೇಹಾ ಅದನ್ನು ಸ್ಕ್ಯಾನ್ ಮಾಡಿ 75,000 ಕಳೆದುಕೊಂಡರು.

ಇದು ಪರಿಚಿತವಾಗಿದೆಯೇ? ನಿಮ್ಮ ಆಗಾಗ್ಗೆ UPI ಪಾವತಿ ಪ್ಲಾಟ್‌ಫಾರ್ಮ್‌ಗಳ ಬಳಕೆಯಿಂದಾಗಿ UPI ವಂಚನೆಗೆ ಬಲಿಯಾಗುವ ಭಯವಿದೆಯೇ?

ಯಾವಾಗಲೂ ನೆನಪಿಡಿ:

UPI ಪಿನ್ ಪಾವತಿಯನ್ನು ಮಾಡಲು ಮಾತ್ರ ಅಗತ್ಯವಿದೆ ಮತ್ತು ಯಾವುದೇ ಪಾವತಿಯನ್ನು ಸ್ವೀಕರಿಸುವುದಿಲ್ಲ.

ನಿಲ್ಲಿಸಿ, ಪಾವತಿಯನ್ನು ಸ್ವೀಕರಿಸಲು ನಿಮ್ಮ UPI ಪಿನ್ ಕೇಳಿದಾಗ! ಇದು ವಾಸ್ತವವಾಗಿ ಪಾವತಿ ವಿನಂತಿಯಾಗಿರಬಹುದು ಮತ್ತು ಸಂಗ್ರಹಣೆಯ ವಿನಂತಿಯಲ್ಲ.

ನಿಮ್ಮ OTP, UPI ಪಿನ್ ಅಥವಾ ಯಾವುದೇ ಗೌಪ್ಯ ವಿವರಗಳನ್ನು ಯಾರೊಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.

ಯಾವುದೇ ಪಾವತಿಯನ್ನು ಪ್ರಾರಂಭಿಸುವ ಮೊದಲು UPI ಅಪ್ಲಿಕೇಶನ್‌ನಲ್ಲಿ ಯಾವಾಗಲೂ ಮೊಬೈಲ್ ಸಂಖ್ಯೆ ಮತ್ತು ಹೆಸರನ್ನು ಪರಿಶೀಲಿಸಿ.

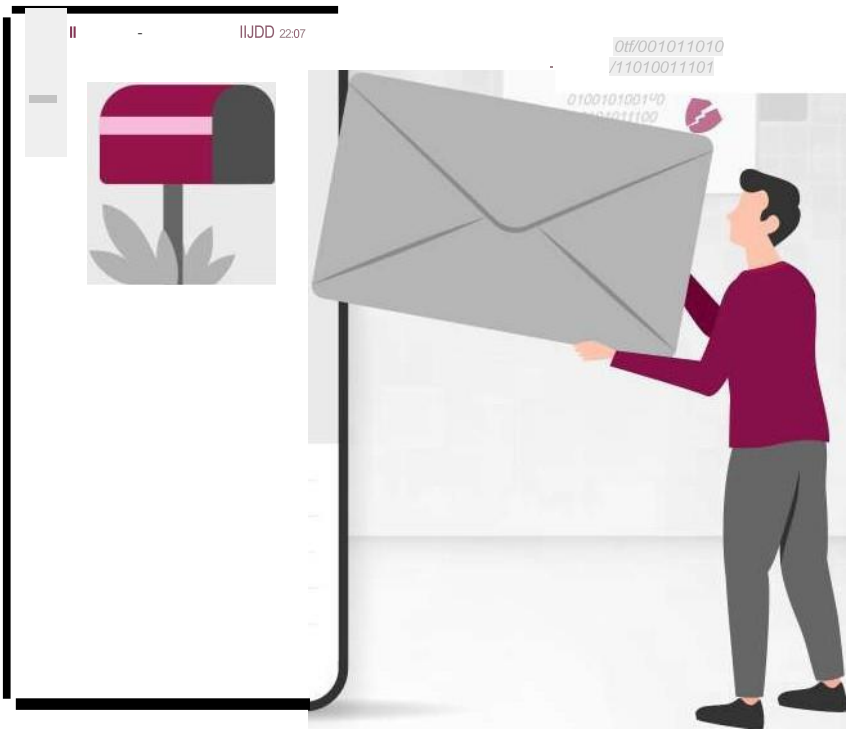
QR ಕೋಡ್ ಸ್ಕ್ಯಾನ್ ವಂಚನೆ

ಪಾವತಿ ಅಪ್ಲಿಕೇಶನ್‌ಗಳಲ್ಲಿ ಕ್ಯೂಆರ್ ಕೋಡ್‌ಗಳನ್ನು ಎಚ್ಚರಿಕೆಯಿಂದ ಸ್ಕ್ಯಾನ್ ಮಾಡಿ; ಅವು ಹಣ ವರ್ಗಾವಣೆಗಾಗಿ ಖಾತೆ ವಿವರಗಳನ್ನು ಒಳಗೊಂಡಿರುತ್ತವೆ..

ಹಣವನ್ನು ಸ್ವೀಕರಿಸಲು QR ಕೋಡ್‌ಗಳನ್ನು ಸ್ಕ್ಯಾನ್ ಮಾಡಬೇಡಿ; ಬಾರ್‌ಕೋಡ್‌ಗಳು / ಕ್ಯೂಆರ್ ಕೋಡ್‌ಗಳನ್ನು ಸ್ಕ್ಯಾನ್ ಮಾಡುವುದು ಅಥವಾ ಮೊಬೈಲ್ ಬ್ಯಾಂಕಿಂಗ್ ಪಿನ್ (ಎಂ-ಪಿನ್), ಪಾಸ್‌ವರ್ಡ್‌ಗಳು ಇತ್ಯಾದಿಗಳನ್ನು ನಮೂದಿಸುವುದು ಹಣವನ್ನು ಸ್ವೀಕರಿಸಲು ವಹಿವಾಟುಗಳಲ್ಲಿ ಅನಗತ್ಯವಾಗಿರುತ್ತದೆ.

ವಿವೇಚನಾರಹಿತ ಆತುರ ಅಥವಾ ಅವಸರವನ್ನು ತೋರಿಸುವ ಖರೀದಿದಾರ/ಮಾರಾಟಗಾರನು ಹೆಚ್ಚಾಗಿ ವಂಚಕನಾಗಿರಬಹುದು. ಶಾಂತವಾಗಿರಿ, ಯಾವಾಗಲೂ ಸ್ಪಷ್ಟೀಕರಣವನ್ನು ಪಡೆದುಕೊಳ್ಳಿ ಮತ್ತು ಅಗತ್ಯ ಪ್ರಶ್ನೆಗಳನ್ನು ಕೇಳಿ.

ಪರಿಶೀಲಿಸದ ಮೊಬೈಲ್ ಅಪ್ಲಿಕೇಶನ್ ವಂಚನೆಗಳು



ನಿಮ್ಮ ನೆಚ್ಚಿನ ಅಧಿಕೃತ ಘಟಕದಿಂದ ಅಸಲಿ ಅಪ್ಲಿಕೇಶನ್‌ನಂತೆ ಕಾಣುವ ಲಿಂಕ್‌ನೊಂದಿಗೆ, ಅಸ್ತಿತ್ವದಲ್ಲಿದೆ ಎಂದು ನಿಮಗೆ ತಿಳಿದಿಲ್ಲದ ದೀರ್ಘಕಾಲ ಕಳೆದುಹೋದ ಸೋದರಸಂಬಂಧಿಯಿಂದ ನೀವು SMS, ಇಮೇಲ್ ಅಥವಾ ಸಂದೇಶವನ್ನು ಸ್ವೀಕರಿಸುತ್ತೀರಿ..
ಒಂದು ನಿಮಿಷ ತಡೆದುಕೊಳ್ಳಿ! ಇವು ಸ್ನೇಹಿ ಡೌನ್‌ಲೋಡ್‌ಗಳಲ್ಲ; ನೀವು ಖಂಡಿತವಾಗಿಯೂ ಹಾಜರಾಗಲು ಬಯಸದ ಡಿಜಿಟಲ್ ಪಾರ್ಟಿಗೆ ಅವು ಆಹ್ವಾನಗಳಾಗಿವೆ!
ವಂಚಕರು SMS, ಇಮೇಲ್ ಅಥವಾ ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮಗಳ ಮೂಲಕ ನಕಲಿ ಅಪ್ಲಿಕೇಶನ್ ಲಿಂಕ್‌ಗಳನ್ನು ಕಳುಹಿಸುತ್ತಾರೆ ಅದು ಕಾನೂನುಬದ್ಧವಾದವುಗಳಂತೆ ಕಾಣುತ್ತದೆ. ಅವರು ಬಳಕೆದಾರರನ್ನು ಅವುಗಳ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡಲು ಮನವೊಲಿಸುತ್ತಾರೆ, ಇದು ಅಜ್ಞಾತ ಅಪ್ಲಿಕೇಶನ್‌ಗಳ ಡೌನ್‌ಲೋಡ್‌ಗೆ ಕಾರಣವಾಗುತ್ತದೆ. ಒಮ್ಮೆ ಸ್ಥಾಪಿಸಿದ ನಂತರ, ಸ್ಕ್ಯಾಮರ್‌ಗಳು ಗೌಪ್ಯ ಮಾಹಿತಿ ಮತ್ತು OTP ಗಳನ್ನು ಒಳಗೊಂಡಂತೆ ಸಾಧನಕ್ಕೆ ಪ್ರವೇಶವನ್ನು ಪಡೆಯುತ್ತಾರೆ.

ಅಪರಿಚಿತ ಮೂಲಗಳಿಂದ ಅಥವಾ ಅಪರಿಚಿತರ ಕೋರಿಕೆಯ ಮೇರೆಗೆ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡುವುದನ್ನು ತಪ್ಪಿಸಿ.

ಡೌನ್‌ಲೋಡ್ ಮಾಡುವ ಮೊದಲು ಅಪ್ಲಿಕೇಶನ್ ಪ್ರಕಾಶಕರು ಮತ್ತು ಬಳಕೆದಾರರ ರೇಟಿಂಗ್‌ಗಳನ್ನು ಪರಿಶೀಲಿಸಿ.

ಅನುಮತಿಗಳು ಮತ್ತು ಅಪ್ಲಿಕೇಶನ್ ವಿನಂತಿಗಳನ್ನು ಪರಿಶೀಲಿಸಿ (ಉದಾ. ಸಂಪರ್ಕಗಳು, ಫೋಟೋಗಳು) ಮತ್ತು ಅಗತ್ಯವನ್ನು ಮಾತ್ರ ನೀಡಿ.

ನೆನಪಿಡಿ, ಬ್ಯಾಂಕ್ ಅಥವಾ ಇತರ ಅಧಿಕಾರಿಗಳು ಅಂತಹ ಸೂಕ್ಷ್ಮ ವಿವರಗಳನ್ನು ಎಂದಿಗೂ ಕೇಳುವುದಿಲ್ಲ.

ಎಟಿಎಂ ಕಾರ್ಡ್ ಸ್ಕಿಮ್ಮಿಂಗ್ ವಂಚನೆ

ಡಿಜಿಟಲ್ ಪಿಕ್‌ಪಾಕೆಟಿಂಗ್‌ನಂತೆ ಎಟಿಎಂ ಸ್ಕಿಮ್ಮಿಂಗ್ ಬಗ್ಗೆ ಯೋಚಿಸಿ. ನೀವು ಹಣವನ್ನು ಹಿಂಪಡೆಯಲು ಅಥವಾ ನಿಮ್ಮ ಬ್ಯಾಲೆನ್ಸ್ ಪರಿಶೀಲಿಸಲು ATM ಅನ್ನು ಬಳಸುವಾಗ, ವಂಚಕರು ನಿಮ್ಮ ಕಾರ್ಡ್ ಮಾಹಿತಿಯನ್ನು ದಾಖಲಿಸಲು ಯಂತ್ರದಲ್ಲಿ ಗುಪ್ತ ಸಾಧನಗಳನ್ನು ಹೊಂದಿಸುತ್ತಾರೆ. ಈ ಸಾಧನಗಳು ನಕಲಿ ಕಾರ್ಡ್ ಸ್ಲಾಟ್ ಅಥವಾ ಚಿಕ್ಕ ಕ್ಯಾಮೆರಾದಂತೆ ಅಪ್ರಜ್ಞಾಪೂರ್ವಕವಾಗಿರಬಹುದು.

ಎಟಿಎಂ ಪರೀಕ್ಷಿಸಿ: ATM ಅನ್ನು ಬಳಸುವ ಮೊದಲು ಯಾವುದೇ ಅಸಾಮಾನ್ಯ ಲಗತ್ತುಗಳು, ಸಡಿಲವಾದ ಭಾಗಗಳು ಅಥವಾ ಗುಪ್ತ ಕ್ಯಾಮೆರಾಗಳಿಗಾಗಿ ಯಾವಾಗಲೂ ಕಾರ್ಡ್ ಸ್ಲಾಟ್ ಮತ್ತು ಕೀಪ್ಯಾಡ್ ಅನ್ನು ಪರಿಶೀಲಿಸಿ.

ನಿಮ್ಮ ಪಿನ್ ಅನ್ನು ಕವರ್ ಮಾಡಿ: ನಿಮ್ಮ ಕೈ ಅಥವಾ ದೇಹದಿಂದ ನಿಮ್ಮ ಪಿನ್ ನಮೂದನ್ನು ರಕ್ಷಿಸಿ, ಕ್ಯಾಮರಾಗಳು ಅಥವಾ ನೋಡುಗರಿಗೆ ನೋಡಲು ಕಷ್ಟವಾಗುತ್ತದೆ.

ಸ್ಟೇಟ್‌ಮೆಂಟ್‌ಗಳನ್ನು ನಿಯಮಿತವಾಗಿ ಪರಿಶೀಲಿಸಿ: ನಿಮ್ಮ ಬ್ಯಾಂಕ್ ಸ್ಟೇಟ್‌ಮೆಂಟ್‌ಗಳು ಮತ್ತು ವಹಿವಾಟುಗಳ ಮೇಲೆ ನಿಗಾ ಇರಿಸಿ. ಯಾವುದೇ ಅಪರಿಚಿತ ಚಟುವಟಿಕೆಯನ್ನು ತಕ್ಷಣವೇ ನಿಮ್ಮ ಬ್ಯಾಂಕ್‌ಗೆ ವರದಿ ಮಾಡಿ.

ಕರೆಗಳ ಬಗ್ಗೆ ಎಚ್ಚರದಿಂದಿರಿ: ನಿಮ್ಮ ಬ್ಯಾಂಕ್‌ನಿಂದ ಬಂದವರು ಎಂದು ಹೇಳಿಕೊಳ್ಳುವ ಯಾರಾದರೂ ಕರೆ ಮಾಡಿ ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯನ್ನು ಕೇಳಿದರೆ, ಜಾಗರೂಕರಾಗಿರಿ. ಬ್ಯಾಂಕ್‌ಗಳು ಫೋನ್‌ನಲ್ಲಿ ಪಿನ್‌ಗಳು ಅಥವಾ ಪೂರ್ಣ ಕಾರ್ಡ್ ಸಂಖ್ಯೆಗಳನ್ನು ಕೇಳುವುದು ಅಪರೂಪ.

ಸುರಕ್ಷಿತ ಎಟಿಎಂಗಳನ್ನು ಬಳಸಿ: ಚೆನ್ನಾಗಿ ಬೆಳಗುವ ಪ್ರದೇಶಗಳಲ್ಲಿ ಅಥವಾ ಬ್ಯಾಂಕ್ ಶಾಖೆಗಳಿಗೆ ಲಗತ್ತಿಸಲಾದ ಎಟಿಎಂಗಳನ್ನು ಆಯ್ಕೆ ಮಾಡಿ, ಏಕೆಂದರೆ ಅವುಗಳು ಟ್ಯಾಂಪರ್ ಆಗುವ ಸಾಧ್ಯತೆ ಕಡಿಮೆ.

ನವೀಕೃತವಾಗಿರಿ: ನಿಮ್ಮನ್ನು ಉತ್ತಮವಾಗಿ ರಕ್ಷಿಸಿಕೊಳ್ಳಲು ಇತ್ತೀಚಿನ ವಂಚನೆಗಳು ಮತ್ತು ವಂಚನೆ ತಂತ್ರಗಳ ಕುರಿತು ಮಾಹಿತಿಯಲ್ಲಿರಿ.

ನೆನಪಿಡಿ, ಜಾಗರೂಕರಾಗಿರಿ ಮತ್ತು ಈ ಸಲಹೆಗಳನ್ನು ಅನುಸರಿಸುವುದು ಎಟಿಎಂ ಕಾರ್ಡ್ ಸ್ಕಿಮ್ಮಿಂಗ್ ವಂಚನೆಗೆ ಬಲಿಯಾಗುವುದನ್ನು ತಪ್ಪಿಸಲು ಮತ್ತು ನಿಮ್ಮ ಹಣಕಾಸುವನ್ನು ಸುರಕ್ಷಿತವಾಗಿರಿಸಲು ಸಹಾಯ ಮಾಡುತ್ತದೆ.

ರಿಮೋಟ್ ಪ್ರವೇಶ ವಂಚನೆ

ಸ್ಕ್ಯಾಮರ್‌ಗಳು ಗ್ರಾಹಕರನ್ನು ಸ್ಕ್ರೀನ್ ಶೇರಿಂಗ್ ಆ್ಯಪ್ ಡೌನ್‌ಲೋಡ್ ಮಾಡುವಂತೆ ಆಮಿಷವೊಡ್ಡುತ್ತಾರೆ. ಅದರೊಂದಿಗೆ, ಅವರು ನಿಮ್ಮ ಸಾಧನಕ್ಕೆ ನುಸುಳುತ್ತಾರೆ, ನಿಮ್ಮ ಮೇಲೆ ಕಣ್ಣಿಡುತ್ತಾರೆ ಮತ್ತು ನಿಮ್ಮ ಹಣಕಾಸಿನ ಮಾಹಿತಿಯನ್ನು ಸ್ವೈಪ್ ಮಾಡುತ್ತಾರೆ. ನಂತರ, ಅವರು ನಿಮ್ಮ ಹಣದಿಂದ ಶಾಪಿಂಗ್ ಹೋಗುತ್ತಾರೆ!
ಅಂತಹ ವಂಚನೆಗಳಿಂದ ದೂರವಿರಲು, ಈ ಸಲಹೆಗಳನ್ನು ನೆನಪಿಡಿ:

ಕರೆ ಮಾಡುವವರನ್ನು ಪರಿಶೀಲಿಸಿ: ಅವರು ಪ್ರತಿನಿಧಿಸುವುದಾಗಿ ಹೇಳಿಕೊಳ್ಳುವ ಸಂಸ್ಥೆಯ ಅಧಿಕೃತ ಸಂಪರ್ಕ ಮಾಹಿತಿಯನ್ನು ಸ್ವತಂತ್ರವಾಗಿ ಹುಡುಕುವ ಮೂಲಕ ಕರೆ ಮಾಡುವವರ ಗುರುತನ್ನು ಯಾವಾಗಲೂ ಎರಡು ಬಾರಿ ಪರಿಶೀಲಿಸಿ.

ಅವಸರದ ನಿರ್ಧಾರ ಬೇಡ: ಒತ್ತಡದಲ್ಲಿ ಹಠಾತ್ ನಿರ್ಧಾರಗಳನ್ನು ತೆಗೆದುಕೊಳ್ಳಬೇಡಿ. ಪ್ರವೇಶವನ್ನು ನೀಡುವ ಮೊದಲು ಅಥವಾ ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯನ್ನು ಹಂಚಿಕೊಳ್ಳುವ ಮೊದಲು ಯೋಚಿಸಲು ಮತ್ತು ಪರಿಶೀಲಿಸಲು ನಿಮ್ಮ ಸಮಯವನ್ನು ತೆಗೆದುಕೊಳ್ಳಿ.

ನಿಮ್ಮ ಸಾಧನಗಳನ್ನು ಸುರಕ್ಷಿತಗೊಳಿಸಿ: ಇತ್ತೀಚಿನ ಭದ್ರತಾ ಪ್ಯಾಚ್‌ಗಳೊಂದಿಗೆ ನಿಮ್ಮ ಸಾಧನಗಳನ್ನು ನವೀಕರಿಸಿ ಮತ್ತು ಪ್ರತಿ ಖಾತೆಗೆ ಬಲವಾದ, ಅನನ್ಯ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ಬಳಸಿ.

ನೀವೇ ಶಿಕ್ಷಣ ಮಾಡಿಕೊಳ್ಳಿ: ಸಾಮಾನ್ಯ ಹಗರಣಗಳು ಮತ್ತು ತಂತ್ರಗಳ ಬಗ್ಗೆ ತಿಳಿಯಿರಿ ಇದರಿಂದ ಅವುಗಳು ಸಂಭವಿಸಿದಾಗ ನೀವು ಅವುಗಳನ್ನು ಗುರುತಿಸಬಹುದು.

ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಕಾಪಾಡಿ: ವಿನಂತಿಯ ನ್ಯಾಯಸಮ್ಮತತೆಯ ಬಗ್ಗೆ ನಿಮಗೆ ಖಚಿತವಿಲ್ಲದಿದ್ದರೆ ಫೋನ್, ಇಮೇಲ್ ಅಥವಾ ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ವೈಯಕ್ತಿಕ ಅಥವಾ ಹಣಕಾಸಿನ ವಿವರಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳುವ ಬಗ್ಗೆ ಜಾಗರೂಕರಾಗಿರಿ.

ನಿಮ್ಮ ಡಿಜಿಟಲ್ ಜೀವನದಲ್ಲಿ ನುಸುಳಲು ಪ್ರಯತ್ನಿಸುತ್ತಿರುವ ರಿಮೋಟ್ ಆಕ್ಸೆಸ್ ವಂಚಕರ ವಿರುದ್ಧ ವರ್ಚುವಲ್ ಬಾಗಿಲನ್ನು ಲಾಕ್ ಮಾಡಲು ಜಾಗರೂಕರಾಗಿರಿ.
ದಯವಿಟ್ಟು ಗಮನಿಸಿ - ನೀವು ಕಪ್ಪು / ಖಾಲಿ ಪರದೆಯನ್ನು ಗಮನಿಸಿದರೆ, ದಯವಿಟ್ಟು ನಿಮ್ಮ ಸಿಸ್ಟಂನಲ್ಲಿ ಯಾವುದೇ ಕ್ರಿಯೆಯನ್ನು ಮುಂದುವರಿಸಬೇಡಿ. ನಿಮ್ಮ ಪರದೆಯು ಇತರರಿಗೆ ಗೋಚರಿಸಬಹುದು ಎಂಬುದರ ಸಂಕೇತವಾಗಿರಬಹುದು.

ಸಿಮ್ ಸ್ವಾಪ್ ಹಗರಣ

ಸ್ಕ್ಯಾಮರ್‌ಗಳು ಫೋನ್ ಹೀಸ್ಟ್ ಅನ್ನು ಎಳೆಯುವುದನ್ನು ಕಲ್ಪಿಸಿಕೊಳ್ಳಿ! ಅವರು ನಿಮ್ಮಂತೆ ನಟಿಸುತ್ತಾರೆ, ಅವರು ತಮ್ಮ ಸಿಮ್ ಕಾರ್ಡ್ ಕಳೆದುಕೊಂಡಿದ್ದಾರೆ ಮತ್ತು ಬಾರ್ನ್-ಅವರು ನಿಮ್ಮ ಸಂಖ್ಯೆಯನ್ನು ಪಡೆದುಕೊಂಡಿದ್ದಾರೆ ಎಂದು ಹೇಳುತ್ತಾರೆ. ಅದರೊಂದಿಗೆ, ಅವರು ನಿಮ್ಮ ಬ್ಯಾಂಕ್ ಅಥವಾ ಇಮೇಲ್‌ನಂತಹ ನಿಮ್ಮ ಆನ್‌ಲೈನ್ ಖಾತೆಗಳಿಗೆ ಕ್ಯಾಶ್ ಮಾಡುತ್ತಾರೆ ಮತ್ತು ಗೊಂದಲವನ್ನು ಉಂಟುಮಾಡುತ್ತಾರೆ!
ಸ್ವಾಪ್ ಹಗರಣವನ್ನು ನಿಲ್ಲಿಸಿ! ಕೆಳಗಿನ ಸಲಹೆಗಳನ್ನು ನೆನಪಿಡಿ.

ಸಿಮ್ ಕಾರ್ಡ್ ಗುರುತಿನ ವಿವರಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.

ನಿಮ್ಮ ಫೋನ್‌ನ ನೆಟ್‌ವರ್ಕ್ ಪ್ರವೇಶವನ್ನು ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡಿ.

ಸ್ವಲ್ಪ ಸಮಯದವರೆಗೆ ಯಾವುದೇ ನೆಟ್‌ವರ್ಕ್ ಇಲ್ಲದಿದ್ದರೆ, ನಕಲಿ ಸಿಮ್‌ಗಳನ್ನು ಪರಿಶೀಲಿಸಲು ನಿಮ್ಮ ಆಪರೇಟರ್ ಅನ್ನು ಸಂಪರ್ಕಿಸಿ.

ನಿಮ್ಮ ಡಿಜಿಟಲ್ ಜೀವನದಲ್ಲಿ ನುಸುಳಲು ಪ್ರಯತ್ನಿಸುತ್ತಿರುವ ರಿಮೋಟ್ ಆಕ್ಸೆಸ್ ವಂಚಕರ ವಿರುದ್ಧ ವರ್ಚುವಲ್ ಬಾಗಿಲನ್ನು ಲಾಕ್ ಮಾಡಲು ಜಾಗರೂಕರಾಗಿರಿ.

ಮೋಸದ ವಹಿವಾಟನ್ನು ವರದಿ ಮಾಡುವುದು ಹೇಗೆ?

www.axisbank.com ಗೆ ಭೇಟಿ ನೀಡಿ > ಬೆಂಬಲ > 'ನಮ್ಮನ್ನು ಇಲ್ಲಿಗೆ ತಲುಪಿ' ವಿಭಾಗಕ್ಕೆ ಸ್ಕ್ರಾಲ್ ಮಾಡಿ > ನಮ್ಮೊಂದಿಗೆ ಮಾತನಾಡಿ > 'ವಂಚನೆ ಅಥವಾ ವಿವಾದವನ್ನು ವರದಿ ಮಾಡಿ' ಆಯ್ಕೆಮಾಡಿ > ವಂಚನೆ ವರದಿ ಮಾಡಿ > ನಿಮ್ಮ ಪ್ರಶ್ನೆಯ ಡ್ರಾಪ್-ಡೌನ್ ಪಟ್ಟಿಯಿಂದ ಸಂಬಂಧಿತ ಆಯ್ಕೆಯನ್ನು ಆರಿಸಿ> ಕರೆ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡಿ

RBI ಗೆ ದೂರು ಸಲ್ಲಿಸಲು, https://cms.rbi.org.in ಗೆ ಭೇಟಿ ನೀಡಿ

ಟೋಲ್-ಫ್ರೀ ಸಂಖ್ಯೆ 14448 ಗೆ ಕರೆ ಮಾಡಿ (ಸೋಮವಾರದಿಂದ ಶುಕ್ರವಾರದವರೆಗೆ, 9:30 ರಿಂದ ಸಂಜೆ 5:15 ರವರೆಗೆ, ರಾಷ್ಟ್ರೀಯ ರಜಾದಿನಗಳನ್ನು ಹೊರತುಪಡಿಸಿ).

ದೈಹಿಕ ದೂರನ್ನು ಕಳುಹಿಸಿ: 'ಕೇಂದ್ರೀಕೃತ ರಸೀದಿ ಮತ್ತು ಸಂಸ್ಕರಣಾ ಕೇಂದ್ರ, 4 ನೇ ಮಹಡಿ, ಭಾರತೀಯ ರಿಸರ್ವ್ ಬ್ಯಾಂಕ್, ಸೆಕ್ಟರ್ -17, ಸೆಂಟ್ರಲ್ ವಿಸ್ತಾ, ಚಂಡೀಗಢ - 160 017' ಗೆ ಪತ್ರ / ಪೋಸ್ಟ್. ಅಗತ್ಯವಿರುವ ಸ್ವರೂಪದ ಕುರಿತು ಹೆಚ್ಚಿನ ವಿವರಗಳಿಗಾಗಿ ದಯವಿಟ್ಟು https://cms.rbi.org.in ಗೆ ಭೇಟಿ ನೀಡಿ.

ಸೈಬರ್ ಅಪರಾಧವನ್ನು ವರದಿ ಮಾಡಲು, ಸಹಾಯವಾಣಿ ಸಂಖ್ಯೆ 155260 ಅಥವಾ 1930 ಅನ್ನು ಡಯಲ್ ಮಾಡಿ ಅಥವಾ ರಾಷ್ಟ್ರೀಯ ಸೈಬರ್ ಅಪರಾಧ ವರದಿ ಪೋರ್ಟಲ್ (www.cybercrime.gov.in) ನಲ್ಲಿ ಘಟನೆಯನ್ನು ವರದಿ ಮಾಡಿ.