ಅನುಬಂಧ 7: ಗ್ರಾಹಕ ಜಾಗೃತಿ ಬೆದರಿಕೆ ಹಾಗೂ ವಂಚನೆ

ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮ ತಂತ್ರಗಳು, ಮೊಬೈಲ್ ಫೋನ್ ಕರೆಗಳು ಸೇರಿದಂತೆ ಹೊಸ ವಿಧಾನಗಳನ್ನು ಬಳಸಿ ನಿರ್ಲಜ್ಜ ಅಂಶಗಳು ಸಾರ್ವಜನಿಕರನ್ನು ವಂಚಿಸುತ್ತಿವೆ ಮತ್ತು ತಪ್ಪುದಾರಿಗೆಳೆಯುತ್ತಿವೆ ಎಂದು ಗಮನಿಸಲಾಗಿದೆ. ಲಿಂಕ್‌ಗಳು, ತಪ್ಪು ಅಧಿಸೂಚನೆಗಳು, ಅನಧಿಕೃತ ಕ್ಯುಆರ್ ಕೋಡ್‌ಗಳು, ಇತ್ಯಾದಿ, ಯಾವುದೇ ರೀತಿಯಲ್ಲಿ ಬ್ಯಾಂಕ್‌ಗಳು ಮತ್ತು ಹಣಕಾಸು ಸೇವಾ ಪೂರೈಕೆದಾರರಿಂದ ರಿಯಾಯಿತಿಗಳು/ಪ್ರತಿಕ್ರಿಯೆಯನ್ನು ತ್ವರಿತಗೊಳಿಸುವಲ್ಲಿ ಸಹಾಯ ಮಾಡುವ ಭರವಸೆ ನೀಡುವ ಮೂಲಕ ವಂಚಿಸುತ್ತಿವೆ.

ಯೂಸರ್ ಐಡಿ, ಲಾಗಿನ್/ಟ್ರಾನ್ಸಾಕ್ಷನ್ ಪಾಸ್‌ವರ್ಡ್, ಒನ್ ಟೈಮ್ ಪಾಸ್‌ವರ್ಡ್ (ಓಟಿಪಿ), ಡೆಬಿಟ್/ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ವಿವರಗಳಾದ ಪಿನ್, ಸಿವಿವಿ, ಮುಕ್ತಾಯ ದಿನಾಂಕ ಮತ್ತು ಇತರ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯಂತಹ ಗೌಪ್ಯ ವಿವರಗಳನ್ನು ಪಡೆಯಲು ವಂಚಕರು ಪ್ರಯತ್ನಿಸುತ್ತಾರೆ. ವಂಚಕರು ಬಳಸುವ ವಿಶಿಷ್ಟ ವಿಧಾನಗಳೆಂದರೆ:

- ಕೆವೈಸಿ ಅಪ್ಡೇಟ್, ಖಾತೆ/ಸಿಮ್ ಕಾರ್ಡ್ ಆನ್ ಬ್ಲಾಕ್ ಮಾಡುವುದು, ಡೆಬಿಟ್ ಮಾಡಿದ ಮೊತ್ತವನ್ನು ಕ್ರೆಡಿಟ್ ಮಾಡುವುದು ಇತ್ಯಾದಿ ನೆಪದಲ್ಲಿ ಗೌಪ್ಯ ವಿವರಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳಲು ಗ್ರಾಹಕರನ್ನು ಆಕರ್ಷಿಸಲು ಬ್ಯಾಂಕ್/ಬ್ಯಾಂಕ್ ಅಲ್ಲದ ಇ-ವ್ಯಾಲೆಟ್ ಪೂರೈಕೆದಾರರು/ಟೆಲಿಕಾಂ ಸೇವಾ ಪೂರೈಕೆದಾರರಿಂದ ನಟಿಸುವ ವಿಶಿಂಗ್-ಫೋನ್ ಕರೆಗಳು.
- ಮೋಸ- ವಂಚನೆಯ ಇಮೇಲ್‌ಗಳು ಮತ್ತು/ಅಥವಾ ಎಸ್ಎಂಎಸ್‌ಗಳು ಗ್ರಾಹಕರು ತಮ್ಮ ಬ್ಯಾಂಕ್/ಇ-ವ್ಯಾಲೆಟ್ ಪೂರೈಕೆದಾರರಿಂದ ಸಂವಹನವು ಹುಟ್ಟಿಕೊಂಡಿದೆ ಮತ್ತು ಗೌಪ್ಯ ವಿವರಗಳನ್ನು ಹೊರತೆಗೆಯಲು ಲಿಂಕ್‌ಗಳನ್ನು ಹೊಂದಿದೆ ಎಂದು ಭಾವಿಸುವಂತೆ ಮಾಡಲು ವಿನ್ಯಾಸಗೊಳಿಸಲಾಗಿದೆ.
- ದೂರದಿಂದ ಪ್ರವೇಶ – ಗ್ರಾಹಕರ ಸಾಧನದಲ್ಲಿ ಡೇಟಾವನ್ನು ಪ್ರವೇಶಿಸಬಹುದಾದ ತಮ್ಮ ಮೊಬೈಲ್ ಫೋನ್/ಕಂಪ್ಯೂಟರ್‌ನಲ್ಲಿ ಅಪ್ಲಿಕೇಶನ್ ಅನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡಲು ಗ್ರಾಹಕರನ್ನು ಆಕರ್ಷಿಸುವ ಮೂಲಕ.
- ಹಣವನ್ನು ಸ್ವೀಕರಿಸಲು 'ನಿಮ್ಮ ಯುಪಿಐ ಪಿನ್ ನಮೂದಿಸಿ' ಎನ್ನುವಂತಹ ಸಂದೇಶಗಳೊಂದಿಗೆ ನಕಲಿ ಪಾವತಿ ವಿನಂತಿಗಳನ್ನು ಕಳುಹಿಸುವ ಮೂಲಕ ಯುಪಿಐ ನ 'ಮನವಿ ಸಂಗ್ರಹಿಸಿ' ವೈಶಿಷ್ಟ್ಯವನ್ನು ದುರುಪಯೋಗಪಡಿಸಿಕೊಳ್ಳುತ್ತಾರೆ.
- ವೆಬ್ಪುಟಗಳು/ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮಗಳಲ್ಲಿ ಬ್ಯಾಂಕ್‌ಗಳು/ಇ-ವ್ಯಾಲೆಟ್ ಪೂರೈಕೆದಾರರ ನಕಲಿ ಸಂಪರ್ಕ ಸಂಖ್ಯೆಗಳು ಮತ್ತು ಸರ್ಚ್ ಇಂಜಿನ್‌ಗಳು ಇತ್ಯಾದಿಗಳಿಂದ ಪ್ರದರ್ಶಿಸಲಾಗುತ್ತದೆ.

ಯಾವುದೇ ಡಿಜಿಟಲ್ (ಆನ್‌ಲೈನ್/ಮೊಬೈಲ್) ಬ್ಯಾಂಕಿಂಗ್/ಪಾವತಿ ವಹಿವಾಟುಗಳನ್ನು ನಡೆಸುವಾಗ ಎಲ್ಲಾ ಮುನ್ನೆಚ್ಚರಿಕೆಗಳನ್ನು ತೆಗೆದುಕೊಳ್ಳುವ ಮೂಲಕ ಸುರಕ್ಷಿತ ಡಿಜಿಟಲ್ ಬ್ಯಾಂಕಿಂಗ್ ಅನ್ನು ಅಭ್ಯಾಸ ಮಾಡಲು ಡಿಸಿಬಿ ಬ್ಯಾಂಕ್ ಸಾರ್ವಜನಿಕರನ್ನು ಒತ್ತಾಯಿಸುತ್ತದೆ. ಇವುಗಳು ಹಣಕಾಸಿನ ಮತ್ತು/ಅಥವಾ ಇತರ ನಷ್ಟವನ್ನು ತಡೆಯಲು ಸಹಾಯ ಮಾಡುತ್ತವೆ.

ಸುರಕ್ಷಿತ ಡಿಜಿಟಲ್ ಬ್ಯಾಂಕಿಂಗ್ ಅಭ್ಯಾಸಗಳು

- ನಿಮ್ಮ ಖಾತೆಯ ವಿವರಗಳಾದ, ಖಾತೆ ಸಂಖ್ಯೆ, ಲಾಗಿನ್ ಐಡಿ, ಪಾಸ್‌ವರ್ಡ್, ಪಿನ್, ಯುಪಿಐ-ಪಿನ್, ಒಟಿಪಿ, ಎಟಿಎಂ/ಡೆಬಿಟ್ ಕಾರ್ಡ್/ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ವಿವರಗಳನ್ನು ಯಾರೊಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ, ಬ್ಯಾಂಕ್ ಅಧಿಕಾರಿಗಳೊಂದಿಗೆ ಸಹ ಅಲ್ಲ, ಅವರು ನಿಜವಾಗಿದ್ದರೂ ಸಹ.
- ಕೆವೈಸಿ ಅಪ್ಡೇಟ್ ಮಾಡದಿರುವ ನೆಪದಲ್ಲಿ ನಿಮ್ಮ ಖಾತೆಯನ್ನು ನಿರ್ಬಂಧಿಸುವ ಬೆದರಿಕೆಯ ಯಾವುದೇ ಫೋನ್ ಕರೆ/ಇಮೇಲ್ ಮತ್ತು ಅದನ್ನು ನವೀಕರಿಸಲು ಲಿಂಕ್ ಅನ್ನು ಕ್ಲಿಕ್ ಮಾಡಲು ಸಲಹೆ ನೀಡುವುದು ವಂಚಕರ ಸಾಮಾನ್ಯ ಕಾರ್ಯವಾಗಿದೆ. ಕೆವೈಸಿಯನ್ನು ನವೀಕರಿಸಲು/ತ್ವರಿತಗೊಳಿಸಲು ಕೊಡುಗೆಗಳಿಗೆ ಪ್ರತಿಕ್ರಿಯಿಸಬೇಡಿ. ನಿಮ್ಮ ಬ್ಯಾಂಕ್/ಎನ್‌ಬಿಎಫ್‌ಸಿ/ ಇ-ವ್ಯಾಲೆಟ್ ಪೂರೈಕೆದಾರರ ಅಧಿಕೃತ ವೆಬ್‌ಸೈಟ್ ಅನ್ನು ಯಾವಾಗಲೂ ಪ್ರವೇಶಿಸಿ ಅಥವಾ ಶಾಖೆಯನ್ನು ಸಂಪರ್ಕಿಸಿ.
- ನಿಮ್ಮ ದೂರವಾಣಿ ಅಥವಾ ಸಾಧನದಲ್ಲಿ ಯಾವುದೇ ಅಪರಿಚಿತ ಅಪ್ಲಿಕೇಶನ್ ಅನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡಬೇಡಿ. ಅಪ್ಲಿಕೇಶನ್ ನಿಮ್ಮ ಗೌಪ್ಯ ಡೇಟಾವನ್ನು ರಹಸ್ಯವಾಗಿ ಪ್ರವೇಶಿಸಬಹುದು.
- ಹಣದ ಸ್ವೀಕೃತಿಯನ್ನು ಒಳಗೊಂಡಿರುವ ವಹಿವಾಟುಗಳಿಗೆ ಬಾರ್‌ಕೋಡ್‌ಗಳು ಅಥವಾ ಕ್ಯುಆರ್ ಕೋಡ್‌ಗಳನ್ನು ಸ್ಕ್ಯಾನ್ ಮಾಡುವ ಅಥವಾ ಎಂಪಿನ್ ನಮೂದಿಸುವ ಅಗತ್ಯವಿಲ್ಲ. ಹೀಗಾಗಿ, ಹಾಗೆ ಮಾಡಲು ಕೇಳಿದರೆ ಜಾಗರೂಕರಾಗಿರಿ.
- ಸಂಪರ್ಕ ವಿವರಗಳಿಗಾಗಿ ಬ್ಯಾಂಕ್/ಎನ್‌ಬಿಎಫ್‌ಸಿ/ ಇ-ವ್ಯಾಲೆಟ್ ಪೂರೈಕೆದಾರರ ಅಧಿಕೃತ ವೆಬ್‌ಸೈಟ್ ಅನ್ನು ಯಾವಾಗಲೂ ಪ್ರವೇಶಿಸಿ. ಇಂಟರ್ನೆಟ್ ಸರ್ಚ್ ಇಂಜಿನ್‌ಗಳಲ್ಲಿನ ಸಂಪರ್ಕ ಸಂಖ್ಯೆಗಳು ಮೋಸವಾಗಿರಬಹುದು.

- ಕಾಗುಣಿತ ದೋಷಗಳಿಗಾಗಿ ಇಮೇಲ್‌ಗಳು ಮತ್ತು ಎಸ್ ಎಂ ಎಸ್ ನಲ್ಲಿ ಸ್ವೀಕರಿಸಿದ ಯು ಆರ್ ಎಲ್ ಗಳು ಮತ್ತು ವಲಯದ ಹೆಸರುಗಳನ್ನು ಪರಿಶೀಲಿಸಿ. ಆನ್‌ಲೈನ್ ಬ್ಯಾಂಕಿಂಗ್‌ಗಾಗಿ ಪರಿಶೀಲಿಸಿದ, ಸುರಕ್ಷಿತ ಮತ್ತು ವಿಶ್ವಾಸಾರ್ಹ ವೆಬ್‌ಸೈಟ್‌ಗಳು ಮತ್ತು ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಮಾತ್ರ ಬಳಸಿ, ಎಂದರೆ, ''https'' ನಿಂದ ಪ್ರಾರಂಭವಾಗುವ ವೆಬ್‌ಸೈಟ್‌ಗಳನ್ನು ಮಾತ್ರ ಬಳಸಿ. ಅನುಮಾನಾಸ್ಪದ ಯು ಆರ್ ಎಲ್ ಅಥವಾ ವೆಬ್‌ಸೈಟ್ ಅನ್ನು ತಕ್ಷಣವೇ ಸ್ಥಳೀಯ ಪೊಲೀಸ್/ಸೈಬರ್ ಕ್ರೈಮ್ ಶಾಖೆಗೆ ಸೂಚಿಸಬೇಕು.

● ನೀವು ಪ್ರಾರಂಭಿಸದ ವಹಿವಾಟಿಗಾಗಿ ನಿಮ್ಮ ಖಾತೆಯನ್ನು ಡೆಬಿಟ್ ಮಾಡಲು ಓಟಿಪಿ ಸ್ವೀಕರಿಸಿದರೆ, ತಕ್ಷಣವೇ ನಿಮ್ಮ ಬ್ಯಾಂಕ್/ಇ-ವ್ಯಾಲೆಟ್ ಪೂರೈಕೆದಾರರಿಗೆ ತಿಳಿಸಿ. ವಹಿವಾಟು ಮಾಡದಿದ್ದಕ್ಕಾಗಿ ನೀವು ಡೆಬಿಟ್ ಎಸ್ ಎಂ ಎಸ್ ಸ್ವೀಕರಿಸಿದರೆ, ತಕ್ಷಣವೇ ನಿಮ್ಮ ಬ್ಯಾಂಕ್/ಇ-ವ್ಯಾಲೆಟ್ ಪೂರೈಕೆದಾರರಿಗೆ ತಿಳಿಸಿ ಮತ್ತು ಯುಪಿಐ ಸೇರಿದಂತೆ ಎಲ್ಲಾ ಡೆಬಿಟ್ ವಿಧಾನಗಳನ್ನು ನಿರ್ಬಂಧಿಸಿ. ನಿಮ್ಮ ಖಾತೆಯಲ್ಲಿ ಯಾವುದೇ ಮೋಸದ ಚಟುವಟಿಕೆಯನ್ನು ನೀವು ಅನುಮಾನಿಸಿದರೆ, ಇಂಟರ್ನೆಟ್/ಮೊಬೈಲ್ ಬ್ಯಾಂಕಿಂಗ್‌ಗಾಗಿ ಸಕ್ರಿಯಗೊಳಿಸಲಾದ ಫಲಾನುಭವಿಗಳ ಪಟ್ಟಿಗೆ ಸೇರ್ಪಡೆಗಾಗಿ ಪರಿಶೀಲಿಸಿ.

● ನಿಮ್ಮ ಬ್ಯಾಂಕ್/ಇ-ವ್ಯಾಲೆಟ್ ಖಾತೆಗೆ ಲಿಂಕ್ ಮಾಡಲಾದ ನಿಮ್ಮ ಇಮೇಲ್‌ನ ಪಾಸ್‌ವರ್ಡ್ ಅನ್ನು ಹಂಚಿಕೊಳ್ಳಬೇಡಿ. ಇ-ವಾಣಿಜ್ಯ/ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮ ಸೈಟ್‌ಗಳು ಸಾಮಾನ್ಯ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ಹೊಂದಿಲ್ಲ ಮತ್ತು ನಿಮ್ಮ ಬ್ಯಾಂಕ್ ಖಾತೆ ಮತ್ತು ಇಮೇಲ್ ಅನ್ನು ನಿಮ್ಮ ಬ್ಯಾಂಕ್ ಖಾತೆಗೆ ಲಿಂಕ್ ಮಾಡಬೇಡಿ. ಸಾರ್ವಜನಿಕ, ಮುಕ್ತ ಅಥವಾ ಉಚಿತ ವೈ-ಫೈ ಅಥವಾ ಇಂಟರ್ನೆಟ್ ನೆಟ್‌ವರ್ಕ್‌ಗಳ ಮೂಲಕ ಬ್ಯಾಂಕಿಂಗ್ ಮಾಡುವುದನ್ನು ತಪ್ಪಿಸಿ.

● ಯಾವುದೇ ವೆಬ್‌ಸೈಟ್/ಅಪ್ಲಿಕೇಶನ್ನಲ್ಲಿ ನಿಮ್ಮ ಇಮೇಲ್ ಬಳಕೆದಾರ ಐಡಿ ನೋಂದಾಯಿಸುವಾಗ ನಿಮ್ಮ ಇಮೇಲ್ ಪಾಸ್‌ವರ್ಡ್ ಅನ್ನು ''ಪಾಸ್‌ವರ್ಡ್'' ಎಂದು ಹೊಂದಿಸಬೇಡಿ. ನಿಮ್ಮ ಇಮೇಲ್ ಅನ್ನು ಪ್ರವೇಶಿಸಲು ಬಳಸುವ ಪಾಸ್‌ವರ್ಡ್, ವಿಶೇಷವಾಗಿ ನಿಮ್ಮ ಬ್ಯಾಂಕ್ ಖಾತೆಯೊಂದಿಗೆ ಲಿಂಕ್ ಮಾಡಿದ್ದರೆ, ವಿಶಿಷ್ಟವಾಗಿರಬೇಕು ಮತ್ತು ಇಮೇಲ್ ಪ್ರವೇಶಕ್ಕಾಗಿ ಮಾತ್ರ ಬಳಸಬೇಕು ಮತ್ತು ಯಾವುದೇ ಇತರ ವೆಬ್‌ಸೈಟ್ ಅಥವಾ ಅಪ್ಲಿಕೇಶನ್ ಅನ್ನು ಪ್ರವೇಶಿಸಲು ಅಲ್ಲ.

● ವಿದೇಶಿ ರವಾನೆ, ಕಮಿಷನ್ ಸ್ವೀಕೃತಿ ಅಥವಾ ಲಾಟರಿಯ ಗೆಲುವಿಗಾಗಿ ಆರ್‌ಬಿಐನಲ್ಲಿ ನಿಮ್ಮ ಪರವಾಗಿ ಹಣವನ್ನು ಠೇವಣಿ ಮಾಡುವ ಸಲಹೆಯಿಂದ ದಾರಿತಪ್ಪಬೇಡಿ.

● ನಿಮ್ಮ ಹಣಕಾಸು ಸೇವಾ ಪೂರೈಕೆದಾರರಿಂದ ಎಚ್ಚರಿಕೆಗಳಿಗಾಗಿ ನಿಮ್ಮ ಇಮೇಲ್ ಮತ್ತು ಫೋನ್ ಸಂದೇಶಗಳನ್ನು ನಿಯಮಿತವಾಗಿ ಪರಿಶೀಲಿಸಿ. ಹೆಚ್ಚಿನ ನಷ್ಟವನ್ನು ತಡೆಗಟ್ಟಲು ಕಾರ್ಡ್, ಖಾತೆ, ವ್ಯಾಲೆಟ್ ಅನ್ನು ನಿರ್ಬಂಧಿಸಲು ನಿಮ್ಮ ಖಾತೆಯಲ್ಲಿನ ಯಾವುದೇ ಅನಧಿಕೃತ ವಹಿವಾಟನ್ನು ತಕ್ಷಣವೇ ನಿಮ್ಮ ಬ್ಯಾಂಕ್/ಎನ್ ಬಿ ಎಫ್ ಸಿ/ಸೇವಾ ಪೂರೈಕೆದಾರರಿಗೆ ವರದಿ ಮಾಡಿ.

● ನಿಮ್ಮ ಎಟಿಎಂ, ಡೆಬಿಟ್ ಮತ್ತು ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್‌ಗಳನ್ನು ಸುರಕ್ಷಿತಗೊಳಿಸಿ ಮತ್ತು ವಹಿವಾಟುಗಳಿಗೆ ದೈನಂದಿನ ಮಿತಿಯನ್ನು ಹೊಂದಿಸಿ. ನೀವು ಮಿತಿಗಳನ್ನು ಹೊಂದಿಸಬಹುದು ಮತ್ತು ದೇಶೀಯ/ಅಂತರರಾಷ್ಟ್ರೀಯ ಬಳಕೆಗಾಗಿ ಸಕ್ರಿಯಗೊಳಿಸಬಹುದು/ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಬಹುದು. ಇದು ವಂಚನೆಯಿಂದಾಗುವ ನಷ್ಟವನ್ನು ಮಿತಿಗೊಳಿಸಬಹುದು