ಸುರಕ್ಷಿತ ಮತ್ತು ಜವಾಬ್ದಾರಿಯುತ ಬ್ಯಾಂಕಿಂಗ್ ಬಳಕೆಯ ಮಾರ್ಗಸೂಚಿಗಳು

ಹಣವನ್ನು ಮೊಬೈಲ್ ಬ್ಯಾಂಕಿಂಗ್ ಅಥವಾ ಇಂಟರ್ನೆಟ್ ಬ್ಯಾಂಕಿಂಗ್ ಮೂಲಕ ಆಗಿರಲಿ, ಶಾಖೆ ಅಥವಾ ATM ನಿಂದ ಆಗಿರಲಿ ವಿಥ್ಡ್ರಾವಲ್ ಮಾಡುವಾಗ, ಸುರಕ್ಷಿತ ಬ್ಯಾಂಕಿಂಗ್ ಅನುಭವವನ್ನು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಲು ನೀವು ತೆಗೆದುಕೊಳ್ಳಬೇಕಾದ ಕೆಲವು ಮೂಲಭೂತ ಮುನ್ನೆಚ್ಚರಿಕೆಗಳಿವೆ. ಇಕ್ವಿಟಾಸ್ ಸ್ಮಾಲ್ ಫೈನಾನ್ಸ್ ಬ್ಯಾಂಕ್ (ESFB) ನಲ್ಲಿ ನಾವು ಸುರಕ್ಷಿತ ಬ್ಯಾಂಕಿಂಗ್ ಅಭ್ಯಾಸ ಮಾಡುವುದನ್ನು ನಂಬುತ್ತೇವೆ. ನಮ್ಮ ಡೇಟಾಬೇಸ್‌ನಲ್ಲಿ ನಿಮ್ಮ ಸಂಪರ್ಕ ವಿವರಗಳು ನವೀಕೃತವಾಗಿವೆ ಎಂದು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳುವುದರೊಂದಿಗೆ ಇದು ಪ್ರಾರಂಭವಾಗುತ್ತದೆ, ಇದರಿಂದ ಎಚ್ಚರಿಕೆಗಳು ಅನಪೇಕ್ಷಿತ ಸ್ವೀಕೃತದಾರರಿಗೆ ಹೋಗುವುದಿಲ್ಲ. ನೀವು ವಿದೇಶಕ್ಕೆ ಪ್ರಯಾಣಿಸುತ್ತಿದ್ದರೆ, ನಿಮ್ಮ ಇಮೇಲ್ ID ಬ್ಯಾಂಕ್‌ನಲ್ಲಿ ನೋಂದಾಯಿಸಲಾಗಿದೆಯೇ ಎಂದು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಿ.

ಮಾಡಬೇಕು ಮತ್ತು ಮಾಡಬಾರದ ವಿಷಯಗಳ ಪಟ್ಟಿ:

ನಿಮ್ಮ ಖಾತೆ/ಕಾರ್ಡ್ ಬ್ಲಾಕ್ ಆಗುವುದು ನಿಮ್ಮ KYC ವಿವರಗಳನ್ನು ಅಪ್‌ಡೇಟ್ ಮಾಡದಿದ್ದರೆ, ಹೆಚ್ಚಿದ ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ಮಿತಿಯನ್ನು ಪಡೆದುಕೊಳ್ಳಿ, ಕ್ಯಾಶ್‌ಬ್ಯಾಕ್ ಪಾಯಿಂಟ್‌ಗಳು/ಬಹುಮಾನಗಳನ್ನು ಗಳಿಸಿದ್ದೀರಿ ಅಥವಾ ಸಾಲ ನೀಡುತ್ತೀವಿ / ಸಾಲದ ಮೇಲೆ ಟಾಪ್-ಅಪ್ ಮಾಡುತ್ತೀವಿ ಎಂದು ಹೇಳುವ ನೆಪದಲ್ಲಿ ನಿಮಗೆ ಕರೆಗಳು / SMS / ಇಮೇಲ್‌ಗಳ ಮೂಲಕ ನಿಮ್ಮನ್ನು ಗುರಿಯಾಗಿಸುವ ವಂಚಕರ ಬಗ್ಗೆ ಎಚ್ಚರದಿಂದಿರಿ.

ಇಂತಹ ವಂಚನೆಗಳಿಗೆ ಬಲಿಯಾಗಬೇಡಿ.

ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ನಿಮ್ಮನ್ನು ಸುರಕ್ಷಿತವಾಗಿರಿಸಲು ಮಾಡಬೇಕಾಗಿರುವುದು ಮತ್ತು ಮಾಡಬಾರದಂತಹ ಕೆಲವು ಮಾಹಿತಿ ಇಲ್ಲಿವೆ:

ಮಾಡಬೇಕು

- ಬ್ಯಾಂಕ್ ಸಂಪರ್ಕ ವಿವರಗಳಿಗಾಗಿ ಯಾವಾಗಲೂ ಅಧಿಕೃತ ವೆಬ್‌ಸೈಟ್‌ಗೆ ಭೇಟಿ ನೀಡಿ
- ನಿಮ್ಮ ಸಂಪರ್ಕ ವಿವರಗಳನ್ನು ಯಾವಾಗಲೂ ಬ್ಯಾಂಕ್‌ನೊಂದಿಗೆ ನವೀಕರಿಸಿ ಮತ್ತು ವಹಿವಾಟು ಎಚ್ಚರಿಕೆಗಳನ್ನು ಪಡೆಯಲು ಸಬ್‌ಸ್ಕ್ರೈಬ್ ಮಾಡಿ
- ನಿಮ್ಮ ಕಂಪ್ಯೂಟರ್/ಮೊಬೈಲ್‌ನಲ್ಲಿ ಅಸಲಿ ಆಂಟಿ-ವೈರಸ್ ಮತ್ತು ಆಂಟಿ-ಮಾಲ್‌ವೇರ್ ಸಾಫ್ಟ್‌ವೇರ್ ಅನ್ನು ಇನ್ಸ್ಟಾಲ್ ಮಾಡಿ ಮತ್ತು ಅದನ್ನು ಅಪ್ಡೇಟ್ ಮಾಡುತ್ತಾ ಇರಿ
- ನಿಮ್ಮ ಪಾಸ್‌ವರ್ಡ್ ಅನ್ನು ಕಠಿಣ ಮತ್ತು ಅನನ್ಯವಾಗಿರಿಸಿಕೊಳ್ಳಿ
- ನಿಮ್ಮ ಕಾರ್ಡ್ ಸಂಖ್ಯೆಗಳು, ಪಾಸ್‌ವರ್ಡ್‌ಗಳು ಅಥವಾ ಯಾವುದೇ ಇತರ ವೈಯಕ್ತಿಕ/ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯನ್ನು ಸಂಗ್ರಹಿಸದಂತೆ ತಡೆಯಲು ನಿಮ್ಮ ಬ್ರೌಸರ್‌ನ ಆಟೋಕಾಂಪ್ಲೀಟ್ ಸೆಟ್ಟಿಂಗ್ಸ್ ಅನ್ನು ಆಫ್ ಮಾಡಿ
- ಪ್ಲೇ ಸ್ಟೋರ್ ಅಥವಾ ಆಪ್ ಸ್ಟೋರ್‌ನಿಂದ ಯಾವುದೇ ಆಪ್ ಅನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡುವ ಮೊದಲು ಜಾಗರೂಕರಾಗಿರಿ
- ವಹಿವಾಟು ಮಾಡುವಾಗ ನಿಮ್ಮ ವೆಬ್ ಬ್ರೌಸರ್‌ನ ಸ್ಟೇಟಸ್ ಬಾರ್‌ನ ಪ್ಯಾಡ್‌ಲಾಕ್ ಸೈನ್ ಅಥವಾ https ಅನ್ನು ನೋಡಿ
- ಸೂಕ್ಷ್ಮ ವಿವರಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳಲು ಕೇಳುವ ಸಂದೇಶಗಳಲ್ಲಿನ ಸ್ಪೆಲ್ಲಿಂಗ್ ದೋಷಗಳಿಗೆ ಯಾವಾಗಲೂ ಗಮನ ಕೊಡಿ, ಏಕೆಂದರೆ ಇದು ನಕಲಿ ಸಂದೇಶಗಳನ್ನು ಗುರುತಿಸಲು ನಿಮಗೆ ಸಹಾಯ ಮಾಡುತ್ತದೆ.

ಮಾಡಬಾರದು

- PIN, ಪಾಸ್‌ವರ್ಡ್, OTP ಅಥವಾ ಕಾರ್ಡ್ ವಿವರಗಳಂತಹ ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯನ್ನು ಯಾರೊಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ
- ನಿಮ್ಮ ಬ್ಯಾಂಕ್ ಖಾತೆಯನ್ನು ಪ್ರವೇಶಿಸುವಾಗ ಸಾರ್ವಜನಿಕ ವೈ-ಫೈ ಅಥವಾ ಉಚಿತ VPN/ಸಾರ್ವಜನಿಕ ಕಂಪ್ಯೂಟರ್‌ಗಳನ್ನು ಬಳಸುವುದನ್ನು ತಪ್ಪಿಸಿ
- ಅಜ್ಞಾತ ಮೂಲಗಳು/ಕಳುಹಿಸುವವರ IDs ಗಳಿಂದ ಸ್ವೀಕರಿಸಿದ ಲಿಂಕ್‌ಗಳ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡಬೇಡಿ
- ಸಾಮಾನ್ಯವಾಗಿ ಬಳಸುವ ಪಾಸ್‌ವರ್ಡ್‌ಗಳಿಂದ ದೂರವಿರಿ ಉದಾ 123456, ಹೆಸರುಗಳು, ಜನ್ಮದಿನ ಇತ್ಯಾದಿ.
- ನಿಮ್ಮ ಬ್ಯಾಂಕಿಂಗ್ ಪಾಸ್‌ವರ್ಡ್ ಅನ್ನು ಎಲ್ಲಿಯಾದರೂ ಬರೆಯುವುದನ್ನು ಮತ್ತು ಅದನ್ನು ಬ್ರೌಸರ್‌ಗಳಲ್ಲಿ ಸೇವ್ ಮಾಡುವುದನ್ನು ತಪ್ಪಿಸಿ
- ರಿಮೋಟ್ ಶೇರಿಂಗ್ ಆಪ್ ಗಳನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡಬೇಡಿ ಉದಾ: ಎನಿಡೆಸ್ಕ್
- UPI ಮೂಲಕ ಹಣವನ್ನು ಸ್ವೀಕರಿಸಲು QR ಕೋಡ್ ಅನ್ನು ಸ್ಕ್ಯಾನ್ ಮಾಡಬೇಡಿ ಅಥವಾ PIN ಅಥವಾ OTP ಅನ್ನು ನಮೂದಿಸಬೇಡಿ
- ATM ನಲ್ಲಿ ಅಪರಿಚಿತರಿಂದ ಸಹಾಯ ಪಡೆಯಬೇಡಿ

ನೆನಪಿನಲ್ಲಿಡಿ:

ESFB ಅಥವಾ ಅದರ ಸಿಬ್ಬಂದಿಗಳು/ಪ್ರತಿನಿಧಿಗಳು ನಿಮ್ಮ ವೈಯಕ್ತಿಕ ಖಾತೆಯ ಮಾಹಿತಿಯನ್ನು ಎಂದಿಗೂ ಕೇಳುವುದಿಲ್ಲ.

1. ಪಾಸ್ವರ್ಡ್ ರಕ್ಷಣೆ

ಸಾಮಾನ್ಯವಾಗಿ ಜನರು ಒಂದೇ ಅಥವಾ ಒಂದೇ ರೀತಿಯ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ಬಹು ಖಾತೆಗಳಿಗೆ ಬಳಸುತ್ತಾರೆ ಎಂದು ಹ್ಯಾಕರ್‌ಗಳಿಗೆ ತಿಳಿದಿದೆ. ನಿಮ್ಮ ಬ್ಯಾಂಕಿಂಗ್ ಪಾಸ್‌ವರ್ಡ್, ಅಮೆಜಾನ್ ಪಾಸ್‌ವರ್ಡ್ ಮತ್ತು ಇಮೇಲ್ ಪಾಸ್‌ವರ್ಡ್ ಒಂದೇ ಆಗಿದ್ದರೆ, ಒಂದು ಸೈಟ್‌ನಲ್ಲಿನ ದೌರ್ಬಲ್ಯವು ಇನ್ನೊಂದು ಸೈಟ್‌ಗೆ ಅಪಾಯವನ್ನುಂಟುಮಾಡುತ್ತದೆ.

ಪಾಸ್ವರ್ಡ್ ಊಹಿಸಲು ಸುಲಭವಾಗುವಂತೆ ಮಾಡುವುದು ಯಾವುದು?

ಒಮ್ಮೆ ಹ್ಯಾಕರ್‌ಗಳು ಡೇಟಾ ಉಲ್ಲಂಘನೆಯಿಂದ ಇಮೇಲ್ ವಿಳಾಸಗಳ ಲಿಸ್ಟ್ ಅನ್ನು ಪಡೆದರೆ, ಅವರು ಈಗಾಗಲೇ ಉತ್ತಮ ಪ್ರಾರಂಭ ಮಾಡಿದ್ದಾರೆ. ಅಲ್ಲಿಂದ, ಅವರು ತಮ್ಮ ಆಯ್ಕೆಯ ವೆಬ್‌ಸೈಟ್ ಅನ್ನು ಆರಿಸಬೇಕಾಗುತ್ತದೆ ಮತ್ತು ಅತ್ಯಂತ ಜನಪ್ರಿಯ ಪಾಸ್‌ವರ್ಡ್‌ಗಳೊಂದಿಗೆ ಸೇರ್ಪಡೆಗೊಂಡ ಇಮೇಲ್‌ಗಳನ್ನು ಪ್ರಯತ್ನಿಸಬೇಕು. ಹಲವು ಖಾತೆಗಳಿಗೆ ಹೊಂದಾಣಿಕೆಯಾಗುವ ಸಾಧ್ಯತೆ ಹೆಚ್ಚು.

ನಿಮ್ಮ ಖಾತೆಯನ್ನು ಹ್ಯಾಕ್ ಮಾಡುವುದನ್ನು ತಪ್ಪಿಸಲು, ನೀವು ತಪ್ಪಿಸಬೇಕಾದ ಕಳಪೆ ಪಾಸ್‌ವರ್ಡ್‌ಗಳ ಪಟ್ಟಿ ಇಲ್ಲಿದೆ:

- ಎಲ್ಲಾ ಪಾಸ್‌ವರ್ಡ್‌ಗಳಲ್ಲಿ ಅತ್ಯಂತ ಸಾಮಾನ್ಯವಾದ 123456 ಅನ್ನು ಬಳಸುವುದನ್ನು ತಪ್ಪಿಸಿ.
- ಅಕ್ಷರವನ್ನು ಚಿಹ್ನೆಗೆ ಬದಲಾಯಿಸುವುದು ಉದಾ p@ssw0rd! ಇದು ಹ್ಯಾಕರ್‌ಗಳಿಗೆ ತಿಳಿದಿರುವ ಒಂದು ಸ್ಪಷ್ಟವಾದ ಸಾಮಾನ್ಯ ಟ್ರಿಕ್ ಆಗಿದೆ. ಪಾಸ್ವರ್ಡ್ ಕ್ರ್ಯಾಕಿಂಗ್ ಪ್ರೋಗ್ರಾಂಗಳು ಪ್ರತಿಯೊಂದು ಭಾಷೆಯಲ್ಲಿ ಈ ಸಂಯೋಜನೆಗಳ ಪ್ರತಿಯೊಂದು ಪ್ರಕಾರವನ್ನು ಒಳಗೊಂಡಿರುತ್ತವೆ.
- ಕೆಲವು ಅಸ್ಪಷ್ಟ ಪದಗಳನ್ನು ಬಳಸಿ ಮತ್ತು ನಿಮ್ಮ ನೆಚ್ಚಿನ ಕ್ರೀಡಾ ತಂಡ ಅಥವಾ ಪಾಪ್ ಸಂಸ್ಕೃತಿಯ ಉಲ್ಲೇಖಗಳನ್ನು ಬಳಸುವುದನ್ನು ತಪ್ಪಿಸಿ.
- ಸನ್‌ಶೈನ್ ಅಥವಾ ಮಂಕಿಯಂತಹ ಏಕ ಪದಗಳನ್ನು ಬಳಸುವುದರಿಂದ ಮತ್ತು ಕೊನೆಯಲ್ಲಿ ಯಾವುದೇ ಸಂಖ್ಯೆಗಳು ಅಥವಾ ವಿರಾಮಚಿಹ್ನೆಗಳನ್ನು ಸೇರಿಸುವುದರಿಂದ ಬಲವಾದ ಪಾಸ್‌ವರ್ಡ್ ಆಗುವುದಿಲ್ಲ. ಬದಲಾಗಿ, ನಿಮ್ಮ ಪಾಸ್‌ವರ್ಡ್ ಅನ್ನು ಬಲಗೊಳಿಸಲು ಪದಗುಚ್ಛ ಅಥವಾ ವಾಕ್ಯವನ್ನು ಬಳಸಿ.
- ಸಾಮಾನ್ಯ ಮಾದರಿಯನ್ನು ಬಳಸುವುದನ್ನು ತಪ್ಪಿಸಿ ಉದಾ111111, abc123 ಅಥವಾ 654321.

ಪಾಸ್ವರ್ಡ್ ಅನ್ನು ಯಾವುದು ಪ್ರಬಲವಾಗಿಸುತ್ತದೆ?

- ಸಂಬಂಧವಿಲ್ಲದ ಪದಗಳನ್ನು ಸಂಯೋಜಿಸುವುದು.
- ಸಂಪೂರ್ಣ ಪದಗುಚ್ಛವನ್ನು ಬಳಸುವುದು ಮತ್ತು ಕೆಲವು ಅಕ್ಷರಗಳನ್ನು ವಿಶೇಷ ಅಕ್ಷರಗಳು ಮತ್ತು ಸಂಖ್ಯೆಗಳಿಗೆ ಬದಲಾಯಿಸುವುದು.
- ಕ್ಯಾಪಿಟಲ್ ಮತ್ತು ಸ್ಮಾಲ್ ಲೆಟರ್, ಚಿಹ್ನೆಗಳು ಮತ್ತು ನಂಬರ್‌ಗಳ ಸಂಯೋಜನೆಯನ್ನು ಬಳಸಿ.
- ನಿಮ್ಮ ಪಾಸ್‌ವರ್ಡ್ ಉದ್ದವಾದಷ್ಟೂ ಅದು ಬಲವಾಗಿರುತ್ತದೆ.
- ಪ್ರತಿ ಖಾತೆಗೆ ವಿಭಿನ್ನ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ಬಳಸಿ.

2. ಡೆಬಿಟ್ ಕಾರ್ಡ್‌ಗಳು

ಡೆಬಿಟ್ ಮತ್ತು ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ವಂಚನೆಯನ್ನು ತಪ್ಪಿಸಲು ಮತ್ತು ಸುರಕ್ಷಿತ ಮತ್ತು ತೊಂದರೆ-ಮುಕ್ತ ಬ್ಯಾಂಕಿಂಗ್ ಅನುಭವವನ್ನು ಆನಂದಿಸಲು ನಿಮಗೆ ಸಹಾಯ ಮಾಡುವ ಕೆಲವು ಮಾಡಬೇಕಾದ ಮತ್ತು ಮಾಡಬಾರದ ಸಂಗತಿಗಳು ಇಲ್ಲಿವೆ.

ಮಾಡಬೇಕು

- ವೆಲ್‌ಕಮ್ ಕಿಟ್ ಅನ್ನು ಸ್ವೀಕರಿಸಿದ ನಂತರ, ಲಕೋಟೆಯನ್ನು ಸೀಲ್ಡ್ ಆಗಿದೆಯೇ ಎಂದು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಿ. ಯಾವುದೇ ತಿದ್ದುಪಡಿಯ ಸೂಚನೆ ಕಂಡುಬಂದಲ್ಲಿ, ತಕ್ಷಣವೇ ಬ್ಯಾಂಕ್ ಅನ್ನು ಸಂಪರ್ಕಿಸಿ.
- ಕಾರ್ಡ್‌ನ ಹಿಂಬದಿಯಲ್ಲಿ ತಕ್ಷಣವೇ ಸಹಿ ಮಾಡಿ.
- ಕಾರ್ಡ್ ಅನ್ನು ಸ್ವೀಕರಿಸಿದ ನಂತರ ಅದರ PIN ಅನ್ನು ಬದಲಾಯಿಸಿ. ಸಾಧ್ಯವಾದರೆ, ಸಂಪೂರ್ಣ ರಕ್ಷಣೆಗಾಗಿ ಪ್ರತಿ ಆರು ತಿಂಗಳಿಗೊಮ್ಮೆ ಮಾಡಿ.
- ನಿಮ್ಮ ಕಾರ್ಡ್‌ಗಳನ್ನು ಸುರಕ್ಷಿತವಾಗಿ ಇರಿಸಿ. ನಷ್ಟ ಅಥವಾ ಕಳ್ಳತನದ ಸಂದರ್ಭದಲ್ಲಿ, ತಕ್ಷಣವೇ ಬ್ಯಾಂಕ್ಗೆ ತಿಳಿಸಿ.
- ಹೊಸ ಅಥವಾ ನವೀಕರಿಸಿದ ಕಾರ್ಡ್ ಅನ್ನು ಸ್ವೀಕರಿಸಿದ ನಂತರ, ಹಳೆಯ ಕಾರ್ಡ್ ಅನ್ನು ಅಡ್ಡವಾಗಿ ಕತ್ತರಿಸಿ ಅದನ್ನು ಬಿಸಾಡಿ.
- ವಿದೇಶ ಪ್ರವಾಸದ ನಂತರ PIN ಬದಲಾಯಿಸುವುದು ಸೂಕ್ತ.
- ನಿಮ್ಮ PIN ಅನ್ನು ಎಲ್ಲಿಯಾದರೂ ಬರೆಯುವ ಬದಲು ನೆನಪಿಟ್ಟುಕೊಳ್ಳಲು ಪ್ರಯತ್ನಿಸಿ.
- ಭೌತಿಕ ಕೀಬೋರ್ಡ್ ಬಳಸುವುದನ್ನು ತಪ್ಪಿಸಿ ಮತ್ತು ನಿಮ್ಮ ಲ್ಯಾಪ್‌ಟಾಪ್ ಅಥವಾ ಮೊಬೈಲ್‌ನಲ್ಲಿ ನಿಮ್ಮ ರುಜುವಾತುಗಳನ್ನು ಇನ್‌ಪುಟ್ ಮಾಡಲು ವರ್ಚುವಲ್ ಕೀಪ್ಯಾಡ್ (ಶೋ ಇಮೇಜ್) ಬಳಸಿ.
- ನಿಮ್ಮ PIN ಅನ್ನು ಎಲ್ಲಿಯಾದರೂ ನಮೂದಿಸುವಾಗ ಜಾಗರೂಕರಾಗಿರಿ - ATM, ಕಾರ್ಡ್ ಮೆಷಿನ್, ಇತ್ಯಾದಿ.
- ಯಾವುದೇ ಕಾರ್ಡ್ ಚಟುವಟಿಕೆಯಲ್ಲಿ ನಿರಂತರ ಎಚ್ಚರಿಕೆಗಳಿಗಾಗಿ ನಿಮ್ಮ ಇಮೇಲ್ ಮತ್ತು ಫೋನ್ ಸಂಖ್ಯೆಯನ್ನು ನವೀಕರಿಸಿ. ನಿಮ್ಮ ವಹಿವಾಟುಗಳು ಮತ್ತು ಖರೀದಿಗಳನ್ನು ಟ್ರ್ಯಾಕ್ ಮಾಡಿ ಮತ್ತು ಯಾವುದೇ ಅಸಾಮಾನ್ಯ ವಹಿವಾಟುಗಳನ್ನು ತಕ್ಷಣವೇ ಬ್ಯಾಂಕ್‌ಗೆ ವರದಿ ಮಾಡಿ.

- ವೀಸಾ (VbV) ಅಥವಾ ಮಾಸ್ಟರ್‌ಕಾರ್ಡ್ ಸುರಕ್ಷಿತ ಕೋಡ್ (MCSC) ಮೂಲಕ ಪರಿಶೀಲಿಸಲಾದ ರೂಪದಲ್ಲಿ ನಿಮ್ಮ ಕಾರ್ಡ್ 3D ಸುರಕ್ಷಿತವಾಗಿದೆ ಎಂದು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಿ. ಇದು ಈಗ ಆನ್‌ಲೈನ್ ವಹಿವಾಟುಗಳಿಗೆ ಕಡ್ಡಾಯವಾಗಿದೆ ಮತ್ತು ಎಲ್ಲಾ ESFB ಕಾರ್ಡ್‌ಗಳು ಇದನ್ನು ಹೊಂದಿವೆ.
- ಪಾವತಿ ಮಾಡುವ ಮೊದಲು ವೆಬ್‌ಸೈಟ್ ಸುರಕ್ಷಿತವಾಗಿದೆಯೇ ಎಂದು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಲು ಯಾವಾಗಲೂ ವೆಬ್‌ಸೈಟ್‌ನ url ಅನ್ನು ಪರಿಶೀಲಿಸಿ. ತ್ವರಿತ ಪರಿಶೀಲನೆ: ನಿಮ್ಮ ಬ್ರೌಸರ್‌ನಲ್ಲಿ ಲಾಕ್ ಐಕಾನ್ (https://show lock symbol) ಇದೆ ಎಂದು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಿ, ಇದು ಸೂಕ್ಷ್ಮ ಡೇಟಾವನ್ನು ರವಾನಿಸುವಾಗ ವೆಬ್‌ಸೈಟ್ ಎನ್‌ಕ್ರಿಪ್ಶನ್ ತಂತ್ರಜ್ಞಾನವನ್ನು ಬಳಸುತ್ತಿದೆ ಎಂದು ಸೂಚಿಸುತ್ತದೆ. ಲಾಕ್ ಅನ್ನು ಕ್ಲಿಕ್ ಮಾಡಿದಾಗ ನೀವು ಡಿಜಿಟಲ್ ಪ್ರಮಾಣಪತ್ರ ಮತ್ತು ವೆಬ್‌ಸೈಟ್‌ಗೆ ಸಂಬಂಧಿಸಿದ ಇತರ ವಿವರಗಳನ್ನು ನೋಡಬಹುದು. ಅಂತಹ ಪರಿಶೀಲನೆ ಲಭ್ಯವಿದ್ದರೆ ಮಾತ್ರ ಮುಂದುವರಿಯಿರಿ
- ಒಂದು ಸೈಟ್ ಡೊಮೇನ್ ಹೆಸರಿನ ಬದಲಿಗೆ IP ವಿಳಾಸ ಅಥವಾ ಸಂಖ್ಯಾತ್ಮಕ ವಿಳಾಸವನ್ನು ಪ್ರದರ್ಶಿಸುತ್ತಿದ್ದರೆ, ಆ ಸೈಟ್‌ನ url ಅನ್ನು ಪರಿಶೀಲಿಸಿ ಏಕೆಂದರೆ ಅಂತಹ ಸೈಟ್ ಅಸಲಿ ಆಗಿರುವುದಿಲ್ಲ.

ಮಾಡಬಾರದು:

- ಇಕ್ವಿಟಾಸ್ ಸ್ಮಾಲ್ ಫೈನಾನ್ಸ್ ಬ್ಯಾಂಕ್ ಎಂದಿಗೂ ಕಾರ್ಡ್ ವಿವರಗಳನ್ನು ಕೇಳುವುದಿಲ್ಲ ಎಂಬುದನ್ನು ನೆನಪಿಡಿ ಉದಾಹರಣೆಗೆ ನಿಮ್ಮ ಕಾರ್ಡ್‌ನ ಮುಂಭಾಗ ಮತ್ತು ಹಿಂಭಾಗದ ಮಾಹಿತಿ
- ಯಾರಾದರೂ ಬ್ಯಾಂಕ್ ಪ್ರತಿನಿಧಿ ಎಂದು ಹೇಳಿಕೊಂಡು ನಿಮ್ಮ ಕಾರ್ಡ್ ಕೇಳಿದರೆ, ಅದನ್ನು ಅವರಿಗೆ ನೀಡಬೇಡಿ.
- ಕಾರ್ಡ್ ಸಂಖ್ಯೆ, ಎಕ್ಸ್ಪೈರಿ ದಿನಾಂಕ, CVV, PIN ಅಥವಾ OTP ಯಂತಹ ನಿಮ್ಮ ಕಾರ್ಡ್ ವಿವರಗಳನ್ನು ಯಾರೊಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ, ಅವರು ಬ್ಯಾಂಕ್ ಅಧಿಕಾರಿ ಎಂದು ಹೇಳಿಕೊಂಡರೂ ಸಹ.
- ಆನ್‌ಲೈನ್ ಮರ್ಚೆಂಟ್ ವೆಬ್‌ಸೈಟ್‌ಗಳಲ್ಲಿ ನಿಮ್ಮ ಕಾರ್ಡ್ ವಿವರಗಳನ್ನು ಸೇವ್ ಮಾಡಬೇಡಿ.
- ನಿಮ್ಮ ಕಾರ್ಡ್ ವಿವರಗಳು, ATM PIN, CVV, UPI PIN ಇತ್ಯಾದಿಗಳನ್ನು ಕೇಳುವ ಇನ್‌ಪುಟ್ ಕ್ಷೇತ್ರಗಳೊಂದಿಗೆ ಇಮೇಲ್‌ಗಳಲ್ಲಿ ನಿಮ್ಮ ವಿವರಗಳನ್ನು ಎಂದಿಗೂ ನಮೂದಿಸಬೇಡಿ.
- ಗೇಮಿಂಗ್ ವೆಬ್‌ಸೈಟ್‌ಗಳು, ಅಶ್ಲೀಲ ವೆಬ್‌ಸೈಟ್‌ಗಳು, ಲಾಟರಿ, ಜೂಜಾಟ ಮತ್ತು ಹೆಚ್ಚಿನವುಗಳಂತಹ ಅನಧಿಕೃತ ಪಾವತಿ ಗೇಟ್‌ವೇಗಳಲ್ಲಿ ನಿಮ್ಮ ಕಾರ್ಡ್‌ಗಳನ್ನು ಬಳಸುವುದನ್ನು ತಪ್ಪಿಸಿ.
- ಖಾಲಿ ಅರ್ಜಿ ನಮೂನೆಗೆ ಎಂದಿಗೂ ಸಹಿ ಮಾಡಬೇಡಿ ಮತ್ತು ಅದನ್ನು ಬ್ಯಾಂಕ್ ಪ್ರತಿನಿಧಿಯಿಂದ ನಂತರ ಭರ್ತಿ ಮಾಡಲಾಗುವುದು ಎಂದು ಭರವಸೆ ನೀಡಿದರೂ ಸಹ ಸಹಿ ಮಾಡಬೇಡಿ

3. UPI

ಮಾಡಬೇಕು:

- ಮಾನ್ಯ ಪ್ಲಾಟ್‌ಫಾರ್ಮ್‌ಗಳ ಮೂಲಕ UPI ಅಪ್ಲಿಕೇಶನ್ ಅನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡಿ ಅಂದರೆ ಗೂಗಲ್ ಪ್ಲೇ ಸ್ಟೋರ್ ಇತ್ಯಾದಿ.
- ನಿಮ್ಮ ಮೂಲ ಶಾಖೆ/ನೆಟ್ ಬ್ಯಾಂಕಿಂಗ್/UPI ಮೂಲಕ ಮೊಬೈಲ್ ಬ್ಯಾಂಕಿಂಗ್‌ಗಾಗಿ ನೋಂದಾಯಿಸಿ.
- ನೀವು ಸಂಪೂರ್ಣ ಗೌಪ್ಯತೆಯಿಂದ ಲಾಗಿನ್ ಆಗಿರುವುದನ್ನು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಿ ಮತ್ತು UPI ವಹಿವಾಟುಗಳನ್ನು ಪ್ರಾರಂಭಿಸಿ.
- ಟ್ರಾನ್ಸಾಕ್ಷನ್ ಅನ್ನು ಪೂರ್ಣಗೊಳಿಸಿದ ನಂತರ, ನೀವು ಅಪ್ಲಿಕೇಶನ್‌ನಿಂದ ಯಶಸ್ವಿಯಾಗಿ ಲಾಗ್ ಔಟ್ ಆಗಿರುವಿರಿ ಎಂದು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಿ.
- ಪ್ರತಿ ವಹಿವಾಟಿಗೆ ನಿಮ್ಮ ನೋಂದಾಯಿತ ಮೊಬೈಲ್ ಸಂಖ್ಯೆಗೆ ನೀವು sms ಎಚ್ಚರಿಕೆಯನ್ನು ಪಡೆಯುತ್ತೀರಿ. ನಿಮ್ಮ ಖಾತೆಯಲ್ಲಿ ಯಾವುದೇ ಅನಧಿಕೃತ UPI ವಹಿವಾಟು ಕಂಡುಬಂದರೆ, ದಯವಿಟ್ಟು ತಕ್ಷಣ ನಿಮ್ಮ ಶಾಖೆಯನ್ನು ಸಂಪರ್ಕಿಸಿ.
- ಯಾವುದೇ ವಿಫಲ ವಹಿವಾಟಿನ ಸಂದರ್ಭದಲ್ಲಿ, ದಯವಿಟ್ಟು ವೆಬ್‌ಸೈಟ್ ಮತ್ತು ಅಪ್ಲಿಕೇಶನ್‌ನಲ್ಲಿ ನೀಡಲಾದ ಮಾರ್ಗದರ್ಶನ ಅನುಸರಿಸಿ ದೂರನ್ನು ಮುಂದಕ್ಕೆ ಕೊಂಡೊಯ್ಯಿರಿ.
- ನಿಮ್ಮ UPI ಅಪ್ಲಿಕೇಶನ್ ಪಾಸ್‌ವರ್ಡ್ ಮತ್ತು UPI PIN / MPIN ಅನ್ನು ಆಗಾಗ್ಗೆ ಬದಲಾಯಿಸಿ.
- ನಿಮ್ಮ ಮೊಬೈಲ್ ಬ್ಯಾಂಕಿಂಗ್/UPI ಗೆ ಅನಧಿಕೃತ ಪ್ರವೇಶವಿದ್ದರೆ, ದಯವಿಟ್ಟು ATM / ಇಂಟರ್ನೆಟ್ ಬ್ಯಾಂಕಿಂಗ್ / ಆಧಾರ್ ಶಾಖೆಯ ಮೂಲಕ (ಅಥವಾ ದಯವಿಟ್ಟು ನಮ್ಮ ಸಂಪರ್ಕ ಕೇಂದ್ರವನ್ನು ಸಂಪರ್ಕಿಸಿ) ತಕ್ಷಣವೇ ನೋಂದಣಿ ರದ್ದು ಮಾಡಿ.
- ನಿಮ್ಮ ಮೊಬೈಲ್ ಫೋನ್ ಕಳೆದುಹೋದರೆ/ಕದ್ದಿದ್ದರೆ, ದಯವಿಟ್ಟು ಮೂಲ ಶಾಖೆ / ನೆಟ್ ಬ್ಯಾಂಕಿಂಗ್ / ATM / ಸಂಪರ್ಕ ಕೇಂದ್ರದ ಮೂಲಕ ನಿಮ್ಮ ಮೊಬೈಲ್ ಬ್ಯಾಂಕಿಂಗ್ ನೋಂದಣಿಯನ್ನು ತಕ್ಷಣವೇ ರದ್ದುಗೊಳಿಸಿ.
- ನಿಮ್ಮ ವಿನಂತಿಯಿಲ್ಲದೆಯೇ ನಿಮ್ಮ ಮೊಬೈಲ್ ಬ್ಯಾಂಕಿಂಗ್ / ಮೊಬೈಲ್ ಸಂಖ್ಯೆಯನ್ನು ಡಿ-ರಿಜಿಸ್ಟರ್ಡ್ / ಡೀಆಕ್ಟಿವೇಟ್ ಮಾಡಿದ್ದರೆ ಅಥವಾ ಈ ನಿಟ್ಟಿನಲ್ಲಿ ನೀವು ಕರೆಯನ್ನು ಸ್ವೀಕರಿಸಿದರೆ, ಯಾರಾದರೂ ನಿಮ್ಮನ್ನು ನಕಲಿ SIM ಪಡೆಯಲು / ನಿಮ್ಮ MPIN / OTP (ಒಂದು ಬಾರಿ ಪಾಸ್‌ವರ್ಡ್) ಬದಲಾಯಿಸಿ ಎಂದು ಕೇಳುತ್ತಿರಬಹುದು. ರುಜುವಾತುಗಳನ್ನು ಕದಿಯಲು ಪ್ರಯತ್ನಿಸುತ್ತಿರಬಹುದು. ಅಂತಹ ಪರಿಸ್ಥಿತಿಯಲ್ಲಿ, ದಯವಿಟ್ಟು ತಕ್ಷಣ ನಿಮ್ಮ ಮೂಲ ಶಾಖೆಯನ್ನು ಸಂಪರ್ಕಿಸಿ.

ಮಾಡಬಾರದು:

- ದಯವಿಟ್ಟು ನಿಮ್ಮ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳಬೇಡಿ / ಅದನ್ನು ನಿಮ್ಮ ಮೊಬೈಲ್ ಹ್ಯಾಂಡ್‌ಸೆಟ್‌ನಲ್ಲಿ ಸಂಗ್ರಹಿಸಬೇಡಿ.
- ನಿಮ್ಮ ಅಪ್ಲಿಕೇಶನ್ ಪಾಸ್‌ವರ್ಡ್ ಅಥವಾ UPI PIN / MPIN ಅನ್ನು ನೀವು ನಮೂದಿಸುವುದನ್ನು ಯಾರಿಗೂ ನೋಡಲು ಬಿಡಬೇಡಿ.
- ಸುಲಭವಾಗಿ ಊಹಿಸಬಹುದಾದ ಅಪ್ಲಿಕೇಶನ್ / UPI PIN / MPIN ಅನ್ನು ಎಂದಿಗೂ ಬಳಸಬೇಡಿ ಉದಾ: 1111/2222/1234/ಹುಟ್ಟಿದ ವರ್ಷ, ಮೊಬೈಲ್ ಸಂಖ್ಯೆ/ದೂರವಾಣಿ ಸಂಖ್ಯೆ.
- ಬೇರೆಯವರ ಸಾಧನದಲ್ಲಿ UPI ಅಪ್ಲಿಕೇಶನ್ ಅನ್ನು ಇನ್ಸ್ಟಾಲ್ ಮಾಡಬೇಡಿ ಮತ್ತು ಬಳಸಬೇಡಿ.
- ಇಕ್ವಿಟಾಸ್ ಬ್ಯಾಂಕ್ ನಿಮ್ಮ UPI / ಮೊಬೈಲ್ ಬ್ಯಾಂಕಿಂಗ್ ಪಾಸ್‌ವರ್ಡ್‌ಗಾಗಿ ಕರೆ / ಇಮೇಲ್ ಮಾಡುವುದಿಲ್ಲ. ಯಾವುದೇ ಕರೆ ಮಾಡುವವರು ನಮ್ಮ ಬ್ಯಾಂಕ್ / ಸಂಪರ್ಕ ಕೇಂದ್ರದಿಂದ ಬಂದವರಂತೆ ನಟಿಸಿದರೆ, ದಯವಿಟ್ಟು ಅಂತಹ ವಿನಂತಿಗಳನ್ನು ನಿರ್ಲಕ್ಷಿಸಿ ಏಕೆಂದರೆ ಅವುಗಳು ಮೋಸದ ಘಟಕಗಳಾಗಿವೆ.
- ನಿಮ್ಮ ನೋಂದಾಯಿತ SIM ಕಾರ್ಡ್ ಮತ್ತು ಡೆಬಿಟ್ ಕಾರ್ಡ್ ಅನ್ನು ಎಂದಿಗೂ ಒಟ್ಟಿಗೆ ಇಟ್ಟುಕೊಳ್ಳಬೇಡಿ, ಏಕೆಂದರೆ ಎರಡೂ ಕಳೆದುಹೋಗುವ ಅಪಾಯವಿದೆ, ಇದು ನಿಮ್ಮ ಖಾತೆಯನ್ನು ಯಾರಾದರೂ ಪ್ರವೇಶಿಸಲು ಕಾರಣವಾಗಬಹುದು.

సురక్షిత మరియు బాధ్యతాయుతమైన బ్యాంకింగ్ ఉపయోగపు మార్గదర్శకాలు

అది మొబైల్ బ్యాంకింగ్ అయినా లేదా ఇంటర్నెట్ బ్యాంకింగ్ అయినా, బ్రాంచ్ లేదా ATM నుండి విత్‌డ్రాయల్ అయినా, సురక్షితమైన బ్యాంకింగ్ అనుభవాన్ని నిర్ధారించుకోవడానికి గాను తగు శ్రద్ధ వహించి మరియు కొన్ని ప్రాథమిక జాగ్రత్తలను పాటించాల్సి ఉంటుంది. ఈక్విటాస్ స్మాల్ ఫైనాన్స్ బ్యాంక్ (ESFB) వద్ద, మేము సురక్షిత బ్యాంకింగ్ ఆచరణను విశ్వసిస్తాము. మీ సంప్రదింపు వివరాలు మా డేటాబేస్‌లో అప్‌డేట్ చేయబడి ఉండే విధంగా నిర్ధారించుకోవడంతో ఇది మొదలవుతుంది, తద్వారా అలర్టులు అనుద్దేశిత స్వీకర్తలకు వెళ్లకుండా ఉంటాయి. మీరు గనక విదేశాలకు ప్రయాణిస్తున్న పక్షములో, మీ ఇమెయిల్ ID బ్యాంక్ తో రిజిస్టర్ చేయబడినట్లు నిర్ధారించుకోండి.

చేయదగిన మరియు చేయకూడని పనుల జాబితా:

మీ ఖాతా/కార్డ్ బ్లాక్ చేయబడినందువల్ల మీ KYC వివరాలను అప్‌డేట్ చేసుకోవాలని, క్రెడిట్ కార్డ్ పరిమితి పెరుగుదలను పొందమని, క్యాష్‌బ్యాక్ పాయింట్‌లు/రివార్డ్‌లు సంపాదించుకొమ్మని లేదా లోన్/లోన్ పైన టాప్-అప్ పొందమనేటటువంటి సాకులతో కాల్స్/ SMS/ ఇమెయిల్స్ ద్వారా మిమ్మల్ని లక్ష్యంగా చేసుకునే మోసగాళ్ల పట్ల జాగ్రత్త వహించండి. అట్టి స్కామ్‌లకు బలి కావద్దు.

అట్టి స్కామ్‌లకు బలి కావద్దు.

మిమ్మల్ని మీరు రక్షించుకొని మరియు ఆన్‌లైన్ యందు సురక్షితంగా ఉండేందుకు చేయవలసిన మరియు చేయకూడని పనులు ఇక్కడ ఉన్నాయి:

చేయదగినవి

- బ్యాంక్ యొక్క సంప్రదింపు వివరాల కోసం ఎల్లప్పుడూ అధికారిక వెబ్‌సైట్‌ను మాత్రమే సందర్శించండి
- మీ సంప్రదింపు వివరాలను ఎల్లప్పుడూ బ్యాంకుతో అప్‌డేట్ చేసుకోండి మరియు లావాదేవీ అలర్టులను పొందడానికి గాను సబ్‌స్క్రైబ్ చేసుకోండి
- మీ కంప్యూటర్/మొబైల్ యందు ప్రశస్తమైన యాంటీ-వైరస్ మరియు యాంటీ-మాల్వేర్ సాఫ్ట్‌వేర్‌లను ఇన్‌స్టాల్ చేసుకోండి మరియు దానిని ఎప్పటికప్పుడు తాజాగా ఉంచుకోండి
- మీ పాస్‌వర్డ్ ని బలమైనదిగా మరియు విశిష్టమైనదిగా ఉంచుకోండి
- మీ కార్డ్ నంబరు, పాస్‌వర్డ్‌లు లేదా ఏదైనా ఇతర వ్యక్తిగత/సున్నితమైన సమాచారం నిల్వ చేయబడకుండా ఉండటానికి గాను మీ బ్రౌజర్ యొక్క ఆటోకంప్లీట్ సెట్టింగ్‌లను ఆఫ్ చేయండి
- ప్లే స్టోర్ లేదా యాప్ స్టోర్ నుండి ఏవైనా యాప్స్ డౌన్‌లోడ్ చేసుకునే ముందు జాగ్రత్త వహించండి
- లావాదేవీ చేస్తున్నప్పుడు మీ వెబ్ బ్రౌజర్ యొక్క స్టేటస్ బార్ లో ప్యాడ్‌లాక్ గుర్తు లేదా https కోసం చూడండి
- సున్నితమైన వివరాలను పంచుకొమ్మని అడిగే సందేశాలలో స్పెల్లింగ్ దోషాల కోసం ఎల్లప్పుడూ చూడండి, ఎందుకంటే అవి నకిలీలను గుర్తించడంలో మీకు సహాయపడతాయి.

చేయకూడనివి

- PIN, పాస్‌వర్డ్‌లు, OTP లేదా కార్డ్ వివరాల వంటి సున్నితమైన వివరాలను ఎవ్వరితోనూ ఎప్పటికీ పంచుకోవద్దు
- మీ బ్యాంక్ ఖాతాను ప్రాప్యత చేసుకుంటున్నప్పుడు పబ్లిక్ వై-ఫై లేదా ఉచిత VPN/పబ్లిక్ కంప్యూటర్లను ఉపయోగించడం మానుకోండి
- అపరిచిత మూలములు/పంపినవారి IDల నుండి అందుకున్న లింక్‌లపై క్లిక్ చేయవద్దు
- 123456, పేర్లు, పుట్టినరోజు మొదలగు సామాన్యంగా ఉపయోగించబడే పాస్‌వర్డ్‌లకు దూరంగా ఉండండి.
- మీ బ్యాంకింగ్ పాస్‌వర్డ్‌ను మరెక్కడైనా వ్రాసి ఉంచడం మరియు దానిని బ్రౌజర్లపై సేవ్ చేయడం మానుకోండి
- రిమోట్ షేరింగ్ యాప్స్ డౌన్‌లోడ్ చేసుకోవద్దు ఉదా. అనీడెస్క్
- UPI ద్వారా డబ్బును అందుకోవడానికి QR కోడ్‌ని స్కాన్ చేయవద్దు లేదా PIN లేదా OTP ని ఎంటర్ చేయవద్దు
- ATM వద్ద కొత్తవారితో సహాయము తీసుకోవద్దు.

గుర్తుంచుకోండి:

ESFB లేదా దాని ఉద్యోగులు/ప్రతినిధులు మీ వ్యక్తిగత ఖాతా సమాచారాన్ని ఎప్పటికీ అడగబోరు.

1. పాస్ వర్డ్ రక్షణ

వ్యక్తులు అనేక ఖాతాల కోసం ఒకే లేదా సారూప్యమైన పాస్‌వర్డ్‌లను ఉపయోగిస్తున్నారని హ్యాకర్లకు తెలుసు. మీ బ్యాంకింగ్ పాస్‌వర్డ్, అమెజాన్ పాస్‌వర్డ్ మరియు ఇమెయిల్ పాస్‌వర్డ్ ఒకటే అయి ఉంటే, ఒక సైట్ యందలి నిస్సహాయత ఇతర సైట్లను ప్రమాదంలో పడేయగలదు.

ఒక పాస్‌వర్డ్ ని ఊహించడానికి ఏది సులభతరం చేస్తుంది?

ఒక డేటా అతిక్రమణ నుండి హ్యాకర్లు ఇమెయిల్ చిరునామాల జాబితాను పొందారంటే, వారు అప్పటికే మంచిగా మొదలు పెట్టారని అర్థం. అక్కడ నుండి, వారు తమకు నచ్చిన వెబ్‌సైట్‌ను ఎంచుకుని, అత్యంత ప్రజాదరణ పొందిన పాస్‌వర్డ్‌లతో జాబితా చేయబడిన ఇమెయిల్స్ ని ప్రయత్నించడం కొనసాగిస్తారు. ఆ ప్రయత్నంలో కొన్ని ఖాతాలను పొందగల అవకాశాలు ఉండనే ఉంటాయి.

మీ ఖాతా హ్యాక్ కాకుండా నివారించడానికి, మీరు తప్పనిసరిగా నివారించాల్సిన చెత్త పాస్‌వర్డ్‌ల జాబితా ఇక్కడ ఉంది:

- అన్ని పాస్‌వర్డ్‌ల పైకి అత్యంత సామాన్యమైన 123456 ఉపయోగించడం మానండి.
- p@ssw0rd! లాగా ఒక అక్షరాన్ని గుర్తుకు మార్చడం వంటిది కూడా హ్యాకర్లకు బాగా తెలిసిన ఒక స్పష్టమైన ట్రిక్. పాస్‌వర్డ్ క్రాకింగ్ ప్రోగ్రాములు ప్రతి భాషలోనూ ఈ సమ్మేళనాల యొక్క ప్రతి రకాన్నీ కలిగి ఉంటాయి.
- కొంతవరకూ అస్పష్టమైన వాటిని ఉపయోగించండి మరియు మీ అభిమాన క్రీడా జట్టు పేర్లను లేదా పాశ్చాత్య సంస్కృతి సూచికలను ఉపయోగించకుండా ఉండండి.
- సన్‌షైన్ లేదా మంకీ వంటి సింగిల్ పదాలు వాడటం మరియు చివర ఒక అంకె లేదా విరామ చిహ్నాలను జోడించడం మాత్రాన అది బలమైన పాస్‌వర్డ్ కాజాలదు. అందుకు బదులుగా, మీ పాస్‌వర్డ్ ని బలంగా చేయడానికి ఒక వాక్యాంశం లేదా వాక్యాన్ని ఉపయోగించండి.
- 111111, abc123 లేదా 654321 వంటి సాధారణ పోకడలను ఉపయోగించడం మానండి.

ఒక పాస్‌వర్డ్ ని ఏది బలంగా చేస్తుంది?

- పొంతన లేని పదాలను కలపడం.
- ఒక సంపూర్ణ వాక్యాంశాన్ని ఉపయోగించడం మరియు కొన్ని అక్షరాలను ప్రత్యేక అక్షరాలు మరియు అంకెలుగా మార్చడం.
- పెద్ద మరియు చిన్న అక్షరాలు, గుర్తులు మరియు అంకెల కలయికను ఉపయోగించండి.
- మీ పాస్‌వర్డ్ ఎంత పొడవుగా ఉంటే అంత బలంగా అవుతుంది.
- ప్రతీ ఖాతా కోసం విభిన్న పాస్‌వర్డ్ లను ఉపయోగించండి.

2. డెబిట్ కార్డులు

డెబిట్ మరియు క్రెడిట్ కార్డ్‌ల మోసాలను నివారించడానికి మరియు సురక్షితమైన మరియు ఆటంకాలు లేని బ్యాంకింగ్ అనుభవాన్ని ఆనందించడానికి మీకు సహాయపడే కొన్ని 'చేయదగిన మరియు చేయకూడని పనులు' ఇక్కడ ఉన్నాయి.

చేయదగినవి

- స్వాగత కిట్ అందుకున్న మీదట, ఆ ఎన్వలప్ సీలు చేయబడి ఉన్నట్లుగా నిర్ధారించుకోండి. అది తారుమారు చేయబడినట్లుగా ఏ మాత్రం సూచన ఉన్నా, వెంటనే బ్యాంకును సంప్రదించండి.
- కార్డు యొక్క వెనుక వైపున వెంటనే సంతకం చేయండి.
- కార్డును అందుకున్న తర్వాత దాని PIN మార్చివేయండి. సంపూర్ణ రక్షణ కోసం, ప్రతి ఆరు నెలలకు ఒకసారి దానిని మార్చడం ఉత్తమం.
- మీ కార్డులను భద్రంగా ఉంచుకోండి. ఒకవేళ పోగొట్టుకున్నా లేదా చోరీ చేయబడినా, వెంటనే బ్యాంకుకు తెలియజేయండి.
- కొత్తది లేదా అప్‌గ్రేడ్ చేయబడిన కార్డును అందుకున్న తర్వాత, పాతదానిని ఐమూలగా కత్తిరించి పారవేయండి.
- ఒక విదేశీ పర్యటన తర్వాత PIN ని మార్చడం మంచిదని సలహా ఇవ్వబడుతోంది.
- మీ PIN ని మరెక్కడైనా వ్రాసి ఉంచుకోవడానికి బదులు దానిని జ్ఞాపకం ఉంచుకోవడానికి ప్రయత్నించండి.
- ఫిజికల్ కీబోర్డులను వాడకుండా ఉండండి మరియు మీ ల్యాప్ టాప్ లేదా మొబైల్‌లో మీ క్రెడెన్షియల్స్ ఇన్‌పుట్ చేయడానికి వర్చువల్ కీప్యాడ్ (ఇమేజ్ చూపించు) ఉపయోగించండి.
- ఎక్కడైనా మీ PIN ఎంటర్ చేస్తున్నప్పుడు చాలా జాగ్రత్తగా ఉండండి – ATM అయినా, కార్డ్ మెషీన్లు అయినా.
- ఏదైనా కార్డ్ యాక్టివిటీపై క్రమం తప్పకుండా అలర్టుల కోసం మీ ఇమెయిల్ మరియు ఫోన్ నంబర్‌ను అప్‌డేట్ చేయండి. మీ లావాదేవీలు మరియు కొనుగోళ్లపై ఒక కన్నేసి ఉంచండి మరియు జరిగిన ఏవైనా అసాధారణ లావాదేవీలను వెంటనే బ్యాంకుకు తెలియజేయండి.

- మీ కార్డుల కోసం వెరిఫైడ్ బై వీసా (VbV) లేదా మాస్టర్‌కార్డ్ సెక్యూర్ కోడ్ (MCSC) రూపంలో మీకు 3D భద్రత ఉండేలా చూసుకోండి. ఇది ఇప్పుడు ఆన్‌లైన్ లావాదేవీలన్నింటికీ తప్పనిసరి అంశము మరియు ESFB కార్డులు అన్నీ దీన్ని కలిగి ఉన్నాయి.
- చెల్లింపు చేయడానికి ముందు ఆ వెబ్‌సైట్ సురక్షితమైనదేనా అని నిర్ధారించుకోవడానికి గాను ఎల్లప్పుడూ వెబ్‌సైట్ యొక్క url ని చెక్ చేసుకోండి. త్వరిత చెక్: మీ బ్రౌజరుపై ఒక లాక్ చిహ్నం (https://show lock symbol) ఉన్నట్లుగా నిర్ధారించుకోండి, సున్నితమైన డేటాను ప్రసారం చేస్తున్నప్పుడు వెబ్‌సైట్ ఎన్‌క్రిప్షన్ టెక్నాలజీని ఉపయోగిస్తున్నట్లుగా అది సూచిస్తుంది. లాక్ పై క్లిక్ చేయడం ద్వారా మీరు డిజిటల్ సర్టిఫికెట్ మరియు వెబ్‌సైట్‌కు సంబంధించిన ఇతర వివరాలను చూడవచ్చు. ఒకవేళ అటువంటి వెరిఫికేషన్ ఉంటేనే ముందుకు వెళ్ళండి
- సైట్ ఒకవేళ డొమైన్ పేరుకు బదులుగా IP చిరునామా లేదా అంకెల చిరునామాను ప్రదర్శిస్తున్నదేమో సైట్‌ల url ని చెక్ చేయండి, అటువంటి సైట్‌లు ప్రశస్తమైన సైట్‌లు కాకపోవచ్చు.

చేయకూడనివి

- ఈక్విటాస్ స్మాల్ ఫైనాన్స్ బ్యాంక్ ఎప్పటికీ మిమ్మల్ని మీ కార్డు ముందువైపు మరియు వెనుకవైపు కాపీ వంటి వివరాలను అడగదని జ్ఞాపకం ఉంచుకోండి.
- ఎవరైనా సరే బ్యాంక్ ప్రతినిధిని అని చెప్పుకుని, మీ కార్డు కోసం అడిగితే, దానిని వారికి అప్పగించకండి.
- బ్యాంక్ అధికారులమని చెప్పుకున్నా సరే ఎవ్వరికీ కార్డ్ నంబర్, ముగింపు గడువు తేదీ, CVV, PIN లేదా OTP వంటి మీ కార్డ్ వివరాలను ఇవ్వవద్దు.
- ఆన్‌లైన్ మర్చంట్ వెబ్‌సైట్‌లపై మీ కార్డు వివరాలను సేవ్ చేయవద్దు.
- మీ కార్డుల వివరాలు, ATM PIN, CVV, UPI PIN మొదలగు వాటిని అడిగే ఇన్‌పుట్ ఫీల్డులతో కూడిన ఇమెయిల్స్ లో మీ వివరాలను ఎప్పటికీ ఎంటర్ చేయవద్దు.
- గేమింగ్ వెబ్‌సైట్‌లు, అశ్లీల వెబ్‌సైట్‌లు, లాటరీ, జూదం మరియు మొదలగువంటి అనధికారిక చెల్లింపు గేట్‌వేలపై మీ కార్డులను ఉపయోగించడం మానుకోండి.
- బ్యాంక్ ప్రతినిధిచే ఆ తదుపరి పూరించబడుతుందనే వాగ్దానం మీద ఎప్పుడూ ఖాళీ దరఖాస్తు ఫారముపై సంతకం చేయవద్దు.

3. UPI

చేయదగినవి:

- చెల్లుబాటు అయ్యే ప్లాట్‌ఫారమ్‌లు అంటే గూగుల్ ప్లే స్టోర్ మొదలగు వాటి ద్వారా UPI అప్లికేషన్‌ను డౌన్‌లోడ్ చేసుకోండి.
- మొబైల్ బ్యాంకింగ్ కోసం మీ బేస్ బ్రాంచ్/నెట్ బ్యాంకింగ్/UPI ద్వారా రిజిస్టర్ చేసుకోండి.
- మీరు సంపూర్ణమైన గోప్యతతో UPI లావాదేవీని లాగిన్ చేసి మొదలుపెట్టేలా నిర్ధారించుకోండి.
- లావాదేవీని పూర్తి చేసుకున్న తర్వాత, అప్లికేషన్ నుండి మీరు విజయవంతంగా లాగ్ అవుట్ అయినట్లు నిర్ధారించుకోండి.
- ప్రతి లావాదేవీకీ, మీరు మీ రిజిస్టర్డ్ మొబైల్ నంబరుకు SMS అలర్టును అందుకుంటారు. మీరు మీ ఖాతాలో ఏదైనా అనధికారిక UPI లావాదేవీని కనుగొన్నట్లయితే, దయచేసి వెంటనే మీ బ్రాంచ్‌ని సంప్రదించండి.
- ఏవైనా లావాదేవీలు విఫలమైన పక్షములో, దయచేసి వెబ్‌సైట్ మరియు అప్లికేషన్ పైన అందించబడిన ఎస్కలేషన్ మ్యాట్రిక్స్‌ని అనుసరించండి.
- మీ UPI అప్లికేషన్ పాస్‌వర్డ్ మరియు UPI PIN / MPIN ని తరచుగా మారుస్తూ ఉండండి.
- మీ మొబైల్ బ్యాంకింగ్/ UPI అనధికారికంగా ప్రాప్యత చేసుకోబడిన పక్షములో, దయచేసి వెంటనే ATM / ఇంటర్నెట్ బ్యాంకింగ్ / బేస్ బ్రాంచ్ ద్వారా డీరిజిస్టర్ చేసుకోండి (లేదా దయచేసి మా సంప్రదింపు కేంద్రాన్ని సంప్రదించండి).
- ఒకవేళ మీ మొబైల్ ఫోన్ పోగొట్టుకుపోయినా / చోరీ అయినా, దయచేసి బేస్ బ్రాంచ్ / నెట్ బ్యాంకింగ్ / ATM / సంప్రదింపు కేంద్రం ద్వారా వెంటనే మీ మొబైల్ బ్యాంకింగ్‌ను డీరిజిస్టర్ చేసుకోండి.
- ఒకవేళ మీ అభ్యర్థన లేకుండానే మీ మొబైల్ బ్యాంకింగ్ / మొబైల్ నంబర్ డీరిజిస్టర్ / డీయాక్టివేట్ చేయబడి ఉంటే లేదా ఈ విషయంలో మీకు కాల్ వచ్చినట్లయితే, ఎవరో ఒకరు డూప్లికేట్ SIM పొందడానికి ప్రయత్నించవచ్చు/ mPIN / OTP (వన్ టైమ్ పాస్‌వర్డ్) వంటి మీ క్రెడెన్షియల్స్ చోరీ చేయడానికి ప్రయత్నిస్తూ ఉండవచ్చు. ఈ ఉదంతంలో, దయచేసి వెంటనే మీ బేస్ బ్రాంచ్‌ను సంప్రదించండి.

చేయకూడనివి:

- దయచేసి మీ పాస్‌వర్డ్‌లను ఎవ్వరికీ తెలియజేయవద్దు / మీ మొబైల్ హ్యాండ్‌సెట్‌లో నిల్వ చేయవద్దు.
- మీరు మీ అప్లికేషన్ పాస్‌వర్డ్ లేదా UPI PIN / MPIN ని ఎంటర్ చేస్తూ ఉండగా ఎవ్వరినీ చూడనివ్వవద్దు.
- సులభంగా ఊహించగలిగే అప్లికేషన్/ UPI PIN / MPINని ఎప్పటికీ ఉపయోగించవద్దు, ఉదా: 1111/2222/1234/ పుట్టిన సంవత్సరం, మొబైల్ నంబర్/ టెలిఫోన్ నంబర్.
- మరొకరి పరికరం పైన UPI అప్లికేషన్‌ను ఇన్‌స్టాల్ చేసి ఉపయోగించుకోవద్దు.
- ఈక్విటాస్ బ్యాంక్ మీ UPI / మొబైల్ బ్యాంకింగ్ పాస్‌వర్డ్‌లను అడుగుతూ కాల్స్ / ఇమెయిల్స్ చేయదు. ఒకవేళ కాల్ చేసిన వ్యక్తి ఎవరైనా మా బ్యాంక్ / సంప్రదింపు కేంద్రం నుండి వచ్చినట్లు నటిస్తే, దయచేసి అటువంటి అభ్యర్థనలను అంగీకరించవద్దు, ఎందుకంటే అవి మోసపూరిత సంస్థలు అయి ఉంటాయి.
- మీ రిజిస్టర్డ్ SIM కార్డ్ మరియు డెబిట్ కార్డులను ఎప్పుడు కూడా కలిపి తీసుకువెళ్లవద్దు, ఎందుకంటే ఈ రెండింటినీ పోగొట్టుకునే ప్రమాదం ఉంది, దానివల్ల ఎవరైనా మీ ఖాతాకు ప్రాప్యతను పొందవచ్చు.

<u>സുരക്ഷിത, ഉത്തരവാദിത്ത ബാങ്കിംഗ് ഉപയോഗ മാർഗ്ഗനിർദ്ദേശങ്ങൾ</u>

മൊബൈൽ ബാങ്കിംഗോ ഇൻറിർനെറ്റ് ബാങ്കിംഗോ, ബ്രാഞ്ചിൽ നിന്നോ ATM നിന്നോ ഉള്ള പിൻവലിക്കലോ ആകട്ടെ, സുരക്ഷിതമായ ബാങ്കിംഗ് അനുഭവം ഉറപ്പാക്കാൻ ഒരു വ്യക്തി ചില അടിസ്ഥാന മുൻകരുതലുകൾ പാലിക്കുകയും ശ്രദ്ധിക്കുകയും വേണം. ഇകിറ്റാസ് സ്മോൾ ഫിനാൻസ് ബാങ്കിൽ (ESFB) ഞങ്ങൾ സുരക്ഷിത ബാങ്കിംഗിൽ വിശ്വസിക്കുന്നു. നിങ്ങളുടെ ബന്ധപ്പെടാനുള്ള വിശദാംശങ്ങൾ ഞങ്ങളുടെ ഡാറ്റാബേസിൽ അപ്ഡേറ്റ് ചെയ്തിട്ടുണ്ടെന്ന് ഉറപ്പാക്കിക്കൊണ്ട് ഇത് ആരംഭിക്കുന്നു, അതിനാൽ അലേർട്ടുകൾ ഉദ്ദേശിക്കാത്ത സ്വീകർത്താക്കളിലേക്ക് പോകില്ല. നിങ്ങൾ വിദേശത്തേക്ക് യാത്ര ചെയ്യുകയാണെങ്കിൽ, നിങ്ങളുടെ ഇമെയിൽ ID ബാങ്കിൽ രജിസ്റ്റർ ചെയ്തിട്ടുണ്ടെന്ന് ഉറപ്പാക്കുക.

ചെയ്യേണ്ടതും ചെയ്യരുതാത്തതുമായവയുടെ പട്ടിക:

നിങ്ങളുടെ അക്കൗണ്ട്/കാർഡ് ബ്ലോക്ക് ചെയ്തിരിക്കുന്നതിനാൽ നിങ്ങളുടെ KYC വിശദാംശങ്ങൾ അപ്ഡേറ്റ് ചെയ്യുക, വർദ്ധിച്ച ക്രെഡിറ്റ് കാർഡ് പരിധി പ്രയോജനപ്പെടുത്തുക, ക്യാഷ്ബാക്ക് പോയിന്റുകൾ/പാരിതോഷികങ്ങൾ നേടുക അല്ലെങ്കിൽ ഒരു വായ്പ/ വായ്പയിലെ ടോപ്പ്-അപ്പ് നേടുക തുടങ്ങിയ വ്യാജേന ഫോൺ/SMS/ഇ-മെയിലുകൾ വഴി നിങ്ങളെ ലക്ഷ്യമിടുന്ന തട്ടിപ്പുകാരെ സൂക്ഷിക്കുക. ഇത്തരം തട്ടിപ്പുകള്ക്ക് ഇരയാകരുത്.

ഇത്തരം തട്ടിപ്പുകള്ക്ക് ഇരയാകരുത്.

സ്വയം പരിരക്ഷിക്കാനും ഓൺലൈനിൽ സുരക്ഷിതമായി തുടരാനും ചെയ്യേണ്ടതും ചെയ്യരുതാത്തതുമായ കാര്യങ്ങൾ ചുവടെകൊടുക്കുന്നു:

ചെയ്യേണ്ടവ

- ബാങ്കുമായി ബന്ധപ്പെടുവാനുള്ള വിശദാംശങ്ങൾക്കായി എപ്പോഴും ഔദ്യോഗിക വെബ്സൈറ്റ് സന്ദർശിക്കുക
- ഇടപാട് അറിയിപ്പുകൾ ലഭിക്കുന്നതിന് നിങ്ങളുടെ ബന്ധപ്പെടുവാനുള്ള വിശദാംശങ്ങൾ ബാങ്കുമായി എല്ലായ്പ്പോഴും പുതുക്കി സബ്സ്ക്രൈബ് ചെയ്യുക
- നിങ്ങളുടെ കമ്പ്യൂട്ടറിൽ/മൊബൈലിൽ യഥാർത്ഥ ആൻറി-വൈറസും ആൻറി-മാൽവെയർ സോഫ്റ്റ്വെയറും ഇൻസ്റ്റാൾ ചെയ്ത് അത് അപ്ഡേറ്റ് ചെയ്ത് നിലനിർത്തുക
- നിങ്ങളുടെ പാസ്വേഡ് ശക്തവും സമാനതകളില്ലാത്തതുമായി സൂക്ഷിക്കുക
- നിങ്ങളുടെ കാർഡ് നമ്പറോ പാസ്വേഡുകളോ മറ്റേതെങ്കിലും വ്യക്തിഗത/സൂക്ഷ്മ വിവരങ്ങളോ ശേഖരിക്കുന്നത് ഒഴിവാക്കുവാന് ബ്രൗസറിൻറെ ഓട്ടോ കംപ്ലീറ്റ് സെറ്റിംഗ്സ് ഓഫ് ചെയ്യുക.
- പ്ലേ സ്റ്റോറിൽ നിന്നോ ആപ്പ് സ്റ്റോറിൽ നിന്നോ ഏതെങ്കിലും ആപ്പുകൾ ഡൗൺലോഡ് ചെയ്യുന്നതിന് മുമ്പ് ശ്രദ്ധിക്കുക
- ഇടപാട് നടത്തുമ്പോൾ നിങ്ങളുടെ വെബ് ബ്രൗസറിൻറെ സ്റ്റാറ്റസ് ബാറിൽ പാഡ്ലോക്ക് അടയാളം അല്ലെങ്കിൽ https -നായി നോക്കുക
- വ്യാജങ്ങൾ തിരിച്ചറിയാൻ നിങ്ങളെ സഹായിക്കുമെന്നതിനാല് തന്ത്രപ്രധാനമായ വിശദാംശങ്ങൾ പങ്കിടാൻ ആവശ്യപ്പെടുന്ന സന്ദേശങ്ങളിലെ അക്ഷരപ്പിശകുകൾ എല്ലായ്പ്പോഴും ശ്രദ്ധിക്കുക.

ചെയ്യരുതാത്തവ

- PIN, പാസ്വേഡുകൾ, OTP അല്ലെങ്കിൽ കാർഡ് വിശദാംശങ്ങൾ എന്നിവ പോലുള്ള സെൻസിറ്റീവ് വിശദാംശങ്ങൾ ആരുമായും പങ്കിടരുത്
- നിങ്ങളുടെ ബാങ്ക് അക്കൗണ്ട് ആക്സസ് ചെയ്യുമ്പോൾ പൊതു വൈഫൈ അല്ലെങ്കിൽ സൗജന്യ VPN/പബ്ലിക് കമ്പ്യൂട്ടറുകൾ ഉപയോഗിക്കുന്നത് ഒഴിവാക്കുക
- അജ്ഞാത ഉറവിടങ്ങള്/ID-കള്-ൽ നിന്ന് നിന്ന് ലഭിക്കുന്ന ലിങ്കുകളിൽ ക്ലിക്ക് ചെയ്യരുത്
- സാധാരണയായി ഉപയോഗിക്കുന്ന 123456, പേരുകൾ, ജന്മദിനം തുടങ്ങിയ പാസ്വേഡുകളിൽ നിന്ന് വിട്ടുനിൽക്കുക.
- നിങ്ങളുടെ ബാങ്കിംഗ് പാസ്വേഡ് എവിടെയെങ്കിലും എഴുതുന്നതും ബ്രൗസറുകളിൽ സേവ് ചെയ്യുന്നതും ഒഴിവാക്കുക
- റിമോട്ട് ഷെയറിംഗ് ആപ്പുകൾ ഡൗൺലോഡ് ചെയ്യരുത് ഉദാ. ആനിഡെസ്ക്
- UPI വഴി പണം സ്വീകരിക്കുന്നതിന് QR കോഡ് സ്കാൻ ചെയ്യുകയോ PIN അല്ലെങ്കില് OTPനൽകുകയോ ചെയ്യരുത്
- ATM-ൽ അപരിചിതരുടെ സഹായം സ്വീകരിക്കരുത്

ഓർക്കുക:

ESFB അല്ലെങ്കിൽ അതിൻറെ ജീവനക്കാർ/പ്രതിനിധികൾ ഒരിക്കലും നിങ്ങളുടെ സ്വകാര്യ അക്കൗണ്ട് വിവരങ്ങൾ ചോദിക്കില്ല.

1. **പാസ്സ്‌വേർഡ് സംരക്ഷണം**

ഒന്നിലധികം അക്കൗണ്ടുകൾക്കായി ആളുകൾ ഒരേ പാസ്‌വേഡുകൾ അല്ലെങ്കിൽ സമാനമായവ ഉപയോഗിക്കുന്നുണ്ടെന്ന് ഹാക്കർമാർക്കറിയാം. നിങ്ങളുടെ ബാങ്കിംഗ് പാസ്‌വേഡ്, ആമസോൺ പാസ്‌വേഡ്, ഇമെയിൽ പാസ്‌വേഡ് എന്നിവ ഒന്നുതന്നെയാണെങ്കിൽ, ഒരു സൈറ്റിലെ കേടുപാടുകൾ മറ്റുള്ളവയെ അപകടത്തിലാക്കാം.

എന്താണ് ഒരു പാസ്‌വേഡ് ഊഹിക്കാൻ എളുപ്പമാക്കുന്നത്?

ഹാക്കർമാർ ഒരു ഡാറ്റാ ലംഘനത്തിലൂടെ ഇമെയിൽ വിലാസങ്ങളുടെ ഒരു ലിസ്റ്റ് സ്വന്തമാക്കിക്കഴിഞ്ഞാൽ, അവർക്ക് ഇതിനകം തന്നെ നല്ല തുടക്കമുണ്ട്. അവിടെ നിന്ന്, അവർക്ക് ഇഷ്ടമുള്ള ഒരു വെബ്‌സൈറ്റ് തിരഞ്ഞെടുത്ത് ഏറ്റവും ജനപ്രിയമായ പാസ്‌വേഡുകൾ ഉപയോഗിച്ച് ലിസ്റ്റുചെയ്ത ഇമെയിലുകൾ പരീക്ഷിക്കുകയും ചെയ്യും. കുറച്ച് അക്കൗണ്ടുകളിൽ കയറാൻ സാധ്യതയുണ്ട്.

നിങ്ങളുടെ അക്കൗണ്ട് ഹാക്ക് ചെയ്യപ്പെടാതിരിക്കാൻ, നിങ്ങൾ ഒഴിവാക്കേണ്ട ഏറ്റവും മോശം പാസ്‌വേഡുകളുടെ ഒരു ലിസ്റ്റ് ഇതാ:

- പാസ്‌വേഡുകളില് ഏറ്റവും സാധാരണമായ 123456 ഉപയോഗിക്കുന്നത് ഒഴിവാക്കുക.
- p@ssw0rd! എന്നതു പോലെ ഒരു ചിഹ്നത്തിലേക്ക് ഒരു അക്ഷരം മാറ്റുന്നു! ഹാക്കർമാർക്ക് അറിയാവുന്ന ഒരു വ്യക്തമായ തന്ത്രമാണ്. പാസ്‌വേഡ് ക്രാക്കിംഗ് പ്രോഗ്രാമുകളിൽ ഓരോ ഭാഷയിലും ഈ കോമ്പിനേഷനുകളുടെ ഓരോ തരവും അടങ്ങിയിരിക്കുന്നു.
- അവ്യക്തമായ എന്തെങ്കിലും ഉപയോഗിക്കുക, നിങ്ങളുടെ പ്രിയപ്പെട്ട സ്പോർട്സ് ടീമിൻറെ പേരുകൾ അല്ലെങ്കിൽ പോപ്പ് കൾച്ചർ റഫറൻസുകൾ ഉപയോഗിക്കുന്നത് ഒഴിവാക്കുക.
- സൺഷൈൻ അല്ലെങ്കിൽ മങ്കി പോലുള്ള ഒറ്റവാക്കുകൾ ഉപയോഗിച്ച് അവസാനം ഒരു അക്കമോ വിരാമചിഹ്നമോ ചേർക്കുന്നത് ശക്തമായ പാസ്‌വേഡ് ഉണ്ടാക്കില്ല. പകരം, നിങ്ങളുടെ പാസ്‌വേഡ് ശക്തമാക്കാൻ ഒരു വാക്യമോ ഖണ്ഡികയോ ഉപയോഗിക്കുക.
- 111111, abc123 അല്ലെങ്കിൽ 654321 പോലുള്ള സാധാരണ പാറ്റേണുകൾ ഉപയോഗിക്കുന്നത് ഒഴിവാക്കുക.

എന്താണ് പാസ്‌വേഡ് ശക്തമാക്കുന്നത്?

- ബന്ധമില്ലാത്ത വാക്കുകൾ കൂട്ടിച്ചേർക്കുന്നു.
- ഒരു മുഴുവൻ വാക്യവും ഉപയോഗിക്കുകയും ചില അക്ഷരങ്ങൾ പ്രത്യേക അക്ഷരങ്ങളിലേക്കും അക്കങ്ങളിലേക്കും മാറ്റുകയും ചെയ്യുന്നു.
- വലിയക്ഷരങ്ങളും ചെറിയ അക്ഷരങ്ങളും ചിഹ്നങ്ങളും അക്കങ്ങളും സംയോജിപ്പിച്ച് ഉപയോഗിക്കുക.
- നിങ്ങളുടെ പാസ്‌വേഡ് ദൈർഘ്യമേറുന്തോറും, അവ ശക്തവുമാകുന്നു.
- ഓരോ അക്കൗണ്ടിനും വ്യത്യസ്ത പാസ്‌വേഡുകൾ ഉപയോഗിക്കുക.

2. ഡെബിറ്റ് കാർഡുകള്

ഡെബിറ്റ്, ക്രെഡിറ്റ് കാർഡുകളിലെ തട്ടിപ്പുകൾ ഒഴിവാക്കാനും സുരക്ഷിതവും തടസ്സരഹിതവുമായ ബാങ്കിംഗ് അനുഭവം ആസ്വദിക്കാനും നിങ്ങളെ സഹായിക്കുന്ന ചില 'ചെയ്യേണ്ടവയും ചെയ്യരുതാത്തവയും' ചുവടെ കൊടുത്തിരിക്കുന്നു.

ചെയ്യേണ്ടവ

- വെല്കം കിറ്റ് ലഭിച്ചാൽ, കവർ സീൽ ചെയ്തിട്ടുണ്ടെന്ന് ഉറപ്പാക്കുക. കൃത്രിമം നടന്നതായി എന്തെങ്കിലും സൂചനയുണ്ടെങ്കിൽ ഉടൻ ബാങ്കുമായി ബന്ധപ്പെടുക.
- കാർഡിൻറെ മറുവശത്ത് ഉടൻ ഒപ്പിടുക.
- കാർഡ് ലഭിച്ചതിന് ശേഷം അതിൻറെ PIN മാറ്റുക. പൂർണ്ണമായ സംരക്ഷണത്തിനായി, ഓരോ ആറുമാസത്തിലും അങ്ങനെ ചെയ്യുക.
- നിങ്ങളുടെ കാർഡുകൾ സുരക്ഷിതമായി സൂക്ഷിക്കുക. നഷ്ടപ്പെടലോ മോഷണമോ ഉണ്ടായാൽ ഉടൻ ബാങ്കിനെ അറിയിക്കുക.
- പുതിയതോ അപ്‌ഗ്രേഡുചെയ്തതോ ആയ കാർഡ് ലഭിച്ചതിന് ശേഷം, പഴയത് ഡയഗണലായി മുറിച്ച് ഉപേക്ഷിക്കുക.
- ഒരു വിദേശ യാത്രയ്ക്ക് ശേഷം PIN മാറ്റുന്നത് നല്ലതാണ്.
- നിങ്ങളുടെ PIN എവിടെയും എഴുതുന്നതിനുപകരം അത് ഓർത്തുവയ്ക്കാന് ശ്രമിക്കുക.
- ഫിസിക്കൽ കീബോർഡുകൾ ഉപയോഗിക്കുന്നത് ഒഴിവാക്കുക, നിങ്ങളുടെ ലാപ് ടോപ്പിലോ മൊബൈലിലോ നിങ്ങളുടെ വിവരങ്ങൾ നൽകുന്നതിന് വെർച്വൽ കീപാഡ് (ചിത്രം കാണിക്കുക) ഉപയോഗിക്കുക.

- ATM, കാർഡ് മെഷീനുകൾ മുതലായവ - എവിടെയും നിങ്ങളുടെ PIN നൽകുമ്പോൾ ശ്രദ്ധിക്കുക.
- ഏതെങ്കിലും കാർഡ് പ്രവർത്തനത്തെക്കുറിച്ചുള്ള നിരന്തരമായ അലേർട്ടുകൾക്കായി നിങ്ങളുടെ ഇമെയിലും ഫോൺ നമ്പറും അപ്ഡേറ്റ് ചെയ്യുക. നിങ്ങളുടെ ഇടപാടുകളും വാങ്ങലുകളും നിരീക്ഷിക്കുകയും അസാധാരണമായ എന്തെങ്കിലും ഇടപാടുകൾ ഉണ്ടായാൽ ഉടൻ ബാങ്കിനെ അറിയിക്കുകയും ചെയ്യുക.
- വെരിഫൈഡ് ബൈ വിസ (VbV) അല്ലെങ്കിൽ മാസ്റ്റർകാർഡ് സെക്യൂർ കോഡ് (MCSC) രൂപത്തിൽ നിങ്ങളുടെ കാർഡുകൾക്ക് 3D സുരക്ഷിതത്വം ഉണ്ടെന്ന് ഉറപ്പാക്കുക. ഇത് ഇപ്പോൾ ഓൺലൈൻ ഇടപാടുകൾക്ക് ഒരു നിർബന്ധമാണ്, എല്ലാ ESFB കാർഡുകളിലും ഇത് ഉണ്ട്.
- പേയ്മെൻറ് നടത്തുന്നതിന് മുമ്പ് വെബ്സൈറ്റ് സുരക്ഷിതമാണെന്ന് ഉറപ്പാക്കാൻ അതിൻറെ url എപ്പോഴും പരിശോധിക്കുക. ദ്രുത പരിശോധന: നിങ്ങളുടെ ബ്രൗസറിൽ ഒരു ലോക്ക് ഐക്കൺ (https:// show lock symbol) ഉണ്ടെന്ന് ഉറപ്പാക്കുക, അത് സെൻസിറ്റീവ് ഡാറ്റ കൈമാറുമ്പോൾ വെബ്സൈറ്റ് ഒരു എൻക്രിപ്ഷൻ സാങ്കേതികവിദ്യയാണ് ഉപയോഗിക്കുന്നതെന്ന് സൂചിപ്പിക്കുന്നു. ലോക്കിൽ ക്ലിക്ക് ചെയ്യുമ്പോൾ നിങ്ങൾക്ക് ഡിജിറ്റൽ സർട്ടിഫിക്കറ്റും വെബ്സൈറ്റുമായി ബന്ധപ്പെട്ട മറ്റ് വിശദാംശങ്ങളും കാണാൻ കഴിയും. അത്തരം പരിശോധന ലഭ്യമാണെങ്കിൽ മാത്രം തുടരുക.
- ഡൊമെയ്ൻ നാമത്തിനുപകരം IP വിലാസമോ സംഖ്യാ വിലാസമോ പ്രദർശിപ്പിക്കുകയാണെങ്കിൽ സൈറ്റുകളുടെ url പരിശോധിക്കുക, കാരണം അത്തരം സൈറ്റുകൾ ഒരു യഥാർത്ഥ സൈറ്റായിരിക്കില്ല.

ചെയ്യരുതാത്തവ

- ഇകഫിറ്റാസ് സ്മോൾ ഫിനാൻസ് ബാങ്ക് ഒരിക്കലും നിങ്ങളുടെ കാർഡിൻറെ മുൻഭാഗത്തിൻറെയും പിൻഭാഗത്തിൻറെയും പകർപ്പ് പോലുള്ള വിശദാംശങ്ങൾ നിങ്ങളോട് ആവശ്യപ്പെടില്ലെന്ന് ഓർക്കുക.
- ആരെങ്കിലും ബാങ്ക് പ്രതിനിധിയാണെന്ന് അവകാശപ്പെടുകയും നിങ്ങളുടെ കാർഡ് ആവശ്യപ്പെടുകയും ചെയ്താൽ, അത് കൈമാറരുത്.
- കാർഡ് നമ്പർ, കാലഹരണപ്പെടൽ, CVV, PIN അല്ലെങ്കില് OTPപോലുള്ള നിങ്ങളുടെ കാർഡ് വിശദാംശങ്ങൾ ആരുമായും, അവർ ബാങ്ക് ഉദ്യോഗസ്ഥരാണെന്ന് അവകാശപ്പെട്ടാൽ പോലും പങ്കിടരുത്.
- ഓൺലൈൻ വ്യാപാര വെബ്സൈറ്റുകളിൽ നിങ്ങളുടെ കാർഡ് വിശദാംശങ്ങൾ സേവ് ചെയ്യരുത്.
- നിങ്ങളുടെ കാർഡുകളുടെ വിശദാംശങ്ങൾ, ATM PIN, CVV, UPI PIN മുതലായവ ആവശ്യപ്പെടുന്ന ഇൻപുട്ട് ഫീൽഡുകളുള്ള ഇമെയിലുകളിൽ നിങ്ങളുടെ വിശദാംശങ്ങൾ ഒരിക്കലും നൽകരുത്.
- ഗെയിമിംഗ് വെബ്സൈറ്റുകൾ, പോണോഗ്രാഫി വെബ്സൈറ്റുകൾ, ലോട്ടറി, ചൂതാട്ടം എന്നിവയും അതിലേറെയും പോലുള്ള അനധികൃത പേയ്മെൻറ് ഗേറ്റ്വേകളിൽ നിങ്ങളുടെ കാർഡുകൾ ഉപയോഗിക്കുന്നത് ഒഴിവാക്കുക.
- ശൂന്യമായ അപേക്ഷാ ഫോമിൽ ബാങ്ക് പ്രതിനിധി പിന്നീട് പൂരിപ്പിക്കുമെന്ന് വാഗ്ദാനത്തോടെ ഒരിക്കലും ഒപ്പിടരുത്.

3. UPI

ചെയ്യേണ്ടവ:

- സാധുവായ പ്ലാറ്റ്ഫോമുകളിലൂടെ UPI ആപ്ലിക്കേഷൻ ഡൗൺലോഡ് ചെയ്യുക. അതായത് ഗൂഗിൾ പ്ലേ സ്റ്റോർ മുതലായവ
- നിങ്ങളുടെ അടിസ്ഥാന ബ്രാഞ്ച്/നെറ്റ് ബാങ്കിംഗ്/UPI വഴി മൊബൈൽ ബാങ്കിംഗിനായി രജിസ്റ്റർ ചെയ്യുക.
- നിങ്ങൾ ലോഗിൻ ചെയ്ത് പൂർണ്ണമായ സ്വകാര്യതയിൽ UPI ഇടപാട് ആരംഭിക്കുന്നുവെന്ന് ഉറപ്പാക്കുക.
- ഇടപാട് പൂർത്തിയാക്കിയ ശേഷം, നിങ്ങൾ ആപ്ലിക്കേഷനിൽ നിന്ന് ലോഗ് ഔട്ട് ചെയ്തുവെന്ന് ഉറപ്പാക്കുക.
- ഓരോ ഇടപാടിനും, നിങ്ങളുടെ രജിസ്റ്റർ ചെയ്ത മൊബൈൽ നമ്പറിലേക്ക് SMS അലേർട്ട് ലഭിക്കും. നിങ്ങളുടെ അക്കൗണ്ടിൽ ഏതെങ്കിലും അനധികൃത UPI ഇടപാട് കണ്ടെത്തിയാൽ, ഉടൻ തന്നെ നിങ്ങളുടെ ശാഖയിൽ ബന്ധപ്പെടുക.
- ഏതെങ്കിലും ഇടപാടുകൾ പരാജയപ്പെട്ടാൽ, വെബ്സൈറ്റിലും ആപ്ലിക്കേഷനിലും നൽകിയിരിക്കുന്ന എസ്കലേഷൻ മാട്രിക്സ് സ്വീകരിക്കുക.
- നിങ്ങളുടെ UPI ആപ്ലിക്കേഷൻ പാസ്വേഡും UPI PIN / MPIN ഇടയ്ക്കിടെ മാറ്റുക.
- നിങ്ങളുടെ മൊബൈൽ ബാങ്കിംഗ്/UPIയുടെ അനധികൃത ആക്സസ് ഉണ്ടെങ്കിൽ, ATM / ഇൻറർനെറ്റ് ബാങ്കിംഗ് / ബേസ് ബ്രാഞ്ച് (അല്ലെങ്കിൽ ഞങ്ങളുടെ കോൺടാക്റ്റ് സെൻറിറുമായി ബന്ധപ്പെടുക) വഴി ഉടൻ ഡീ-രജിസ്റ്റർ ചെയ്യുക.

- നിങ്ങളുടെ മൊബൈൽ ഫോൺ നഷ്ടപ്പെടുകയോ മോഷ്ടിക്കപ്പെടുകയോ ചെയ്താൽ, ദയവായി ബേസ് ബ്രാഞ്ച് / നെറ്റ് ബാങ്കിംഗ് / ATM / കോൺടാക്റ്റ് സെൻറിർ വഴി നിങ്ങളുടെ മൊബൈൽ ബാങ്കിംഗ് ഉടൻ ഡീ-രജിസ്റ്റർ ചെയ്യുക.
- നിങ്ങളുടെ മൊബൈൽ ബാങ്കിംഗ് / മൊബൈൽ നമ്പർ നിങ്ങളുടെ അഭ്യർത്ഥന കൂടാതെ രജിസ്റ്റർ ചെയ്തിരിക്കുകയോ നിർജ്ജീവമാക്കുകയോ ചെയ്യുകയോ അല്ലെങ്കിൽ ഇതുമായി ബന്ധപ്പെട്ട് നിങ്ങൾക്ക് ഒരു ഫോണ്കോൾ ലഭിക്കുകയോ ചെയ്താൽ, ആരെങ്കിലും ഡ്യൂപ്ലിക്കേറ്റ് SIM എടുക്കാൻ ശ്രമിക്കുന്നു / MPIN / OTP (വൺ ടൈം പാസ്വേഡ്) പോലുള്ള നിങ്ങളുടെ വിവരങ്ങൾ മോഷ്ടിച്ചേക്കാം. ഈ സാഹചര്യത്തിൽ, ദയവായി നിങ്ങളുടെ അടിസ്ഥാന ശാഖയുമായി ഉടൻ ബന്ധപ്പെടുക.

ചെയ്യരുതാത്തവ:

- ദയവായി നിങ്ങളുടെ പാസ്വേഡുകൾ പങ്കിടരുത് / നിങ്ങളുടെ മൊബൈൽ ഹാൻഡ്സെറ്റിൽ സൂക്ഷിക്കരുത്.
- നിങ്ങളുടെ ആപ്ലിക്കേഷൻ പാസ്വേഡോ UPI PIN / MPIN എന്റര് ചെയ്യുന്നത് ആരെയും കാണുവാന് അനുവദിക്കരുത്.
- എളുപ്പത്തിൽ ഊഹിക്കാൻ കഴിയുന്ന ആപ്ലിക്കേഷൻ/ UPI PIN/ MPIN ഒരിക്കലും ഉപയോഗിക്കരുത് ഉദാ: 1111/2222/1234/ ജനന വർഷം, മൊബൈൽ നമ്പർ/ടെലിഫോൺ നമ്പർ.
- മറ്റാരുടെയെങ്കിലും ഉപകരണത്തിൽ UPI ആപ്ലിക്കേഷൻ ഇൻസ്റ്റാൾ ചെയ്ത് ഉപയോഗിക്കരുത്.
- ഇകഫിറ്റാസ് ബാങ്ക് നിങ്ങളുടെ UPI / മൊബൈൽ ബാങ്കിംഗ് പാസ്വേഡുകൾ ആവശ്യപ്പെട്ട് ഫോണ്കോളുകൾ / ഇമെയിലുകൾ ചെയ്യുന്നില്ല. ഏതെങ്കിലും വ്യക്തി ഞങ്ങളുടെ ബാങ്ക് / കോൺടാക്റ്റ് സെൻറിറിൽ നിന്നാണെന്ന് നടിക്കുന്നുവെങ്കിൽ, അത്തരം അഭ്യർത്ഥനകൾ വഞ്ചനാപരമായ സ്ഥാപനങ്ങളില് നിന്നാ യതിനാൽ ദയവായി സ്വീകരിക്കരുത്.
- നിങ്ങളുടെ രജിസ്റ്റർ ചെയ്ത SIM കാർഡും ഡെബിറ്റ് കാർഡും ഒരുമിച്ച് കൊണ്ടുപോകരുത്, കാരണം അവ രണ്ടും നഷ്ടപ്പെടാൻ സാധ്യതയുണ്ട്, ഇത് നിങ്ങളുടെ അക്കൗണ്ടിലേക്ക് ആക്സസ് നേടാൻ ആർക്കും സഹായകമായേക്കാം.

सुरक्षित और जिम्मेदार बैंकिंग उपयोग के लिए दिशानिर्देश

चाहे वह मोबाइल बैंकिंग हो या इंटरनेट बैंकिंग, शाखा या ATM से निकासी हो, सुरक्षित बैंकिंग अनुभव सुनिश्चित करने के लिए कुछ बुनियादी सावधानियों का ध्यान रखना और पालन करना होगा। इक्विटास स्मॉल फाइनेंस बैंक (ESFB) में हम सुरक्षित बैंकिंग की कार्य-प्रणाली को अपनाने में विश्वास करते हैं। इसकी शुरुआत यह सुनिश्चित करने से होती है कि आपके संपर्क विवरण हमारे डेटाबेस में अपडेट रहें ताकि अलर्ट अनपेक्षित प्राप्तकर्ताओं तक न पहुँचें। यदि आप विदेश की यात्रा पर हैं, तो सुनिश्चित करें कि आपका ईमेल ID बैंक के साथ पंजीकृत है।

करने-योग्य और न करने योग्य बातों की सूची:

धोखाधड़ी करने वालों से सावधान रहें, जो कॉल/SMS/ईमेल के माध्यम से आपसे संपर्क करते हैं एवं आपका खाता/कार्ड ब्लॉक होने, KYC विवरण अपडेट करने, क्रेडिट कार्ड की सीमा बढ़ाने, कैशबैक प्वाइंट/रिवॉर्ड कमाने या ऋण/टॉप-अप ऋण लेने के बहाने आपको निशाना बनाते हैं। ऐसी धोखाधड़ी का शिकार न बनें।

ऐसी धोखाधड़ी का शिकार न बनें।

यहाँ ऑनलाइन सुरक्षित रहने और खुद को सुरक्षित रखने के लिए कुछ करने-योग्य और न करने योग्य बातों की सूची दी गई है:

क्या करें

- बैंक के संपर्क विवरण के लिए हमेशा आधिकारिक वेबसाइट पर जाएँ
- बैंक के साथ अपने संपर्क विवरण हमेशा अपडेट रखें और लेन-देन अलर्ट प्राप्त करने के लिए सदस्यता लें
- अपने कंप्यूटर/मोबाइल पर असली एंटी-वायरस तथा एंटी-मैलवेयर सॉफ़्टवेयर इंस्टॉल करें एवं उसे अपडेट रखें
- अपना पासवर्ड मज़बूत और अनोखा रखें
- अपने कार्ड नंबर, पासवर्ड या किसी अन्य व्यक्तिगत/संवेदनशील जानकारी को संग्रहीत करने से बचने के लिए अपने ब्राउज़र की ऑटोकम्प्लीट सेटिंग बंद करें
- प्ले स्टोर या ऐप स्टोर से कोई भी ऐप डाउनलोड करने से पहले सावधान रहें
- लेन-देन करते समय अपने वेब ब्राउज़र के स्टेटस बार में पैडलॉक साइन या https देखें
- संवेदनशील जानकारी साझा करने के लिए कहने वाले संदेशों में वर्तनी की त्रुटियों पर हमेशा ध्यान दें, क्योंकि वे आपको नकली संदेशों की पहचान करने में मदद करेंगे।

क्या न करें

- कभी भी किसी के साथ PIN, पासवर्ड, OTP या कार्ड विवरण जैसी संवेदनशील जानकारी साझा न करें
- अपने बैंक खाते तक पहुँचने के दौरान सार्वजनिक वाई-फाई या मुफ़्त VPN/सार्वजनिक कंप्यूटर का उपयोग करने से बचें
- अज्ञात स्रोतों/प्रेषक ID से प्राप्त लिंक पर क्लिक न करें
- 123456, नाम, जन्मदिन आदि जैसे आम तौर पर इस्तेमाल किए जाने वाले पासवर्ड से दूर रहें
- अपने बैंकिंग पासवर्ड को कहीं भी लिखने और ब्राउज़र पर सहेजने से बचें
- रिमोट शेयरिंग ऐप जैसे कि एनीडेस्क डाउनलोड न करें
- UPI के ज़रिए पैसे प्राप्त करने के लिए QR कोड स्कैन न करें या PIN या OTP दर्ज न करें
- ATM पर अजनबियों की मदद न लें

ध्यान रखें:

ESFB या उसके कर्मचारी/प्रतिनिधि कभी भी आपकी व्यक्तिगत खाता जानकारी नहीं मांगेंगे।

1. पासवर्ड की सुरक्षा

हैकर्स इस बात से अवगत हैं कि लोग अक्सर एक जैसे या मिलते-जुलते पासवर्ड का उपयोग कई अकाउंट्स के लिए करते हैं। यदि आपका बैंकिंग पासवर्ड, अमेज़न पासवर्ड और ईमेल पासवर्ड एक समान है, तो किसी एक साइट की सुरक्षा में खामी अन्य अकाउंट्स को भी खतरे में डाल सकती है।

पासवर्ड का अनुमान लगाना आसान क्यों होता है?

एक बार जब हैकर्स को डेटा ब्रीच से ईमेल पतों की सूची मिल जाती है, तो वे पहले से ही एक अच्छी शुरुआत कर लेते हैं। वहां से, उन्हें बस अपनी पसंद की वेबसाइट चुननी होती है और सबसे लोकप्रिय पासवर्ड के साथ सूचीबद्ध ईमेल आज़माना होता है। कई खातों में सेंध लगने की संभावना है।

अपने खाते को हैक होने से बचाने के लिए, यहां कुछ सबसे खराब पासवर्डों की सूची दी गई है, जिनसे आपको बचना चाहिए:

- 123456 का उपयोग करने से बचें, जो सभी पासवर्डों में सबसे आम है।
- p@ssw0rd! जैसे किसी अक्षर को प्रतीक में बदलना भी एक स्पष्ट चाल है जिसे हैकर्स जानते हैं। पासवर्ड क्रैकिंग प्रोग्राम में हर भाषा में इन सभी प्रकार के संयोजन होते हैं।
- कुछ अस्पष्ट उपयोग करें और अपनी पसंदीदा खेल टीम या पॉप संस्कृति संदर्भों के नामों का उपयोग करने से बचें।
- सनशाइन या मंकी जैसे एकल शब्दों का उपयोग करना और अंत में कोई संख्या या विराम चिह्न जोड़ना, एक मजबूत पासवर्ड नहीं होता है। इसके बजाए, अपने पासवर्ड को मजबूत बनाने के लिए एक वाक्यांश या वाक्य का उपयोग करें।
- 111111, abc123 या 654321 जैसे सामान्य पैटर्न का उपयोग करने से बचें।

एक मजबूत पासवर्ड कैसे बनता हैं?

- असंबंधित शब्दों के संयोजन का उपयोग करना।
- एक संपूर्ण वाक्यांश का उपयोग करना और कुछ अक्षरों को विशेष अक्षरों और संख्याओं में बदलना।
- बड़े और छोटे अक्षरों, प्रतीकों और संख्याओं के संयोजन का उपयोग करना।
- आपका पासवर्ड जितना लंबा होगा, वह उतना ही मजबूत होगा।
- हर खाते के लिए अलग-अलग पासवर्ड का उपयोग करें।

2. डेबिट काड्र्स

यहाँ कुछ 'करें और न करें' दिए गए हैं, जो आपको डेबिट और क्रेडिट कार्ड धोखाधड़ी से बचने में मदद करेंगे और एक सुरक्षित और परेशानी मुक्त बैंकिंग अनुभव प्रदान करेंगे।

क्या करें

- वेलकम किट प्राप्त करने के बाद, सुनिश्चित करें कि लिफाफा सीलबंद है। यदि लिफाफे से छेड़छाड़ का कोई संकेत मिलता है, तो बैंक से तुरंत संपर्क करें।
- कार्ड के पीछे तुरंत हस्ताक्षर करें।
- कार्ड प्राप्त करने के बाद उसका PIN बदलें। आदर्श रूप से, पूर्ण सुरक्षा के लिए हर छह महीने में ऐसा करें।
- अपने कार्ड सुरक्षित रखें। खोने या चोरी होने पर, बैंक को तुरंत सूचित करें।
- नया या अपग्रेडेड कार्ड प्राप्त करने के बाद, पुराने कार्ड को तिरछे काटकर फेंक दें।
- विदेश यात्रा के बाद PIN बदलना उचित है।
- अपने PIN को कहीं भी लिखने के बजाय याद रखने की कोशिश करें।
- अपने लैपटॉप या मोबाइल में अपने क्रेडेंशियल दर्ज करने के लिए भौतिक कीबोर्ड का उपयोग करने से बचें और अधिमानतः वर्चुअल कीपैड (छवि दिखाएं) का उपयोग करें।
- ATM, कार्ड मशीन आदि कहीं भी अपना PIN दर्ज करते समय सावधान रहें।
- किसी भी कार्ड गतिविधि पर लगातार अलर्ट के लिए अपना ईमेल और फ़ोन नंबर अपडेट करें। अपने लेन-देन और खरीदारी पर नज़र रखें और किसी भी असामान्य लेन-देन की तुरंत बैंक को रिपोर्ट करें।

- सुनिश्चित करें कि आपके कार्ड के लिए वेरिफाइड बाय वीज़ा (VbV) या मास्टरकार्ड सिक्योर कोड (MCSC) के रूप में 3D सुरक्षित है। यह अब ऑनलाइन लेनदेन के लिए अनिवार्य है और सभी ESFB कार्ड में यह है।
- भुगतान करने से पहले हमेशा वेबसाइट का url जाँच लें ताकि यह सुनिश्चित हो सके कि यह सुरक्षित है। त्वरित जाँच: सुनिश्चित करें कि आपके ब्राउज़र पर एक लॉक आइकन (https://show lock symbol) है, जो दर्शाता है कि वेबसाइट संवेदनशील डेटा संचारित करते समय एन्क्रिप्शन तकनीक का उपयोग कर रही है। लॉक पर क्लिक करने पर आप डिजिटल प्रमाणपत्र और वेबसाइट से संबंधित अन्य विवरण देख सकते हैं। केवल तभी आगे बढ़ें जब ऐसा सत्यापन उपलब्ध हो
- यदि साइट का url डोमेन नाम के बजाय IP पता या संख्यात्मक पता प्रदर्शित करता है तो जाँच करें क्योंकि ऐसी साइटें वास्तविक साइट नहीं हो सकती हैं।

क्या न करें:

- याद रखें कि इक्विटास स्मॉल फाइनेंस बैंक आपसे कभी भी आपके कार्ड के आगे और पीछे की कॉपी जैसी जानकारी नहीं मांगेगा।
- अगर कोई व्यक्ति बैंक प्रतिनिधि होने का दावा करता है और आपका कार्ड मांगता है, तो उसे न दें।
- कभी भी अपने कार्ड की जानकारी जैसे कार्ड नंबर, एक्सपायरी, CVV, PIN या OTP किसी के साथ साझा न करें, भले ही वे बैंक अधिकारी होने का दावा करें।
- ऑनलाइन मर्चेंट वेबसाइट पर अपने कार्ड की जानकारी सेव न करें।
- कभी भी अपने कार्ड की जानकारी ऐसे ईमेल पर न डालें जिसमें आपके कार्ड की जानकारी, ATM PIN, CVV, UPI PIN आदि के लिए इनपुट फ़ील्ड हों।
- गेमिंग वेबसाइट, पोर्नोग्राफ़ी वेबसाइट, लॉटरी, जुआ आदि जैसे अनधिकृत भुगतान गेटवे पर अपने कार्ड का उपयोग करने से बचें।
- कभी भी खाली आवेदन प्रपत्र पर हस्ताक्षर न करें और वादा करें कि इसे बाद में बैंक प्रतिनिधि द्वारा भरा जाएगा।

3. UPI

क्या करें:

- वैध प्लेटफ़ॉर्म यानी गूगल प्ले स्टोर आदि के माध्यम से UPI एप्लिकेशन डाउनलोड करें।
- अपनी बेस शाखा/नेट बैंकिंग/UPI के माध्यम से मोबाइल बैंकिंग के लिए पंजीकरण करें।
- सुनिश्चित करें कि आप लॉगिन करें और पूरी गोपनीयता के साथ UPI लेनदेन आरंभ करें।
- लेनदेन पूरा करने के बाद, सुनिश्चित करें कि आपने एप्लिकेशन से सफलतापूर्वक लॉग आउट कर लिया है।
- हर लेनदेन के लिए, आपको अपने पंजीकृत मोबाइल नंबर पर SMS अलर्ट प्राप्त होगा। यदि आपको अपने खाते में कोई अनधिकृत UPI लेनदेन दिखाई देता है, तो कृपया तुरंत अपनी शाखा से संपर्क करें।
- किसी भी असफल लेनदेन के मामले में, कृपया वेबसाइट एवं एप्लिकेशन पर दिए गए एस्केलेशन मैट्रिक्स का पालन करें।
- अपना UPI एप्लीकेशन पासवर्ड और UPI PIN / MPIN अक्सर बदलते रहें।
- यदि आपके मोबाइल बैंकिंग/UPI तक कोई व्यक्ति अनधिकृत रूप से पहुँच रखता हो, तो कृपया ATM / इंटरनेट बैंकिंग/आधार शाखा के माध्यम से तुरंत पंजीकरण रद्द करें (या कृपया हमारे संपर्क केंद्र से संपर्क करें)।
- यदि आपका मोबाइल फ़ोन खो जाता है/चोरी हो जाता है, तो कृपया आधार शाखा/नेट बैंकिंग/ ATM / संपर्क केंद्र के माध्यम से तुरंत अपना मोबाइल बैंकिंग पंजीकरण रद्द करें।
- यदि आपके अनुरोध के बिना आपका मोबाइल बैंकिंग/मोबाइल नंबर पंजीकृत/निष्क्रिय कर दिया जाता है या आपको इस संबंध में कोई कॉल आती है, तो हो सकता है कि कोई व्यक्ति डुप्लीकेट SIM प्राप्त करने/आपके mPIN /OTP (वन टाइम पासवर्ड) जैसे क्रेडेंशियल्स चुराने का प्रयास कर रहा हो। इस मामले में, कृपया तुरंत अपनी आधार शाखा से संपर्क करें।

क्या न करें:

- कृपया अपने पासवर्ड साझा न करें/अपने मोबाइल हैंडसेट में संग्रहीत न करें।
- कभी भी किसी को यह न देखने दें कि आप अपना एप्लिकेशन पासवर्ड या UPI PIN /MPIN दर्ज कर रहे हैं।
- कभी भी ऐसा एप्लिकेशन/ UPI PIN /MPIN उपयोग न करें जिसका आसानी से अनुमान लगाया जा सके जैसे: 1111/2222/1234/जन्म वर्ष, मोबाइल नंबर/टेलीफ़ोन नंबर।
- किसी और के डिवाइस में UPI एप्लीकेशन इंस्टॉल करके इस्तेमाल न करें।
- इक्विटास बैंक कॉल/ईमेल करके आपसे UPI / मोबाइल बैंकिंग पासवर्ड नहीं मांगता। अगर कोई कॉलर हमारे बैंक/संपर्क केंद्र से होने का दिखावा करता है, तो कृपया ऐसे अनुरोधों पर ध्यान न दें क्योंकि वे धोखाधड़ी करने वाली संस्थाएँ हैं।
- कभी भी अपना रजिस्टर्ड SIM कार्ड एवं डेबिट कार्ड एक साथ न रखें, क्योंकि दोनों के खोने का जोखिम रहता है, जिससे कोई भी आपके खाते तक पहुँच सकता है।

सुरक्षित आणि जबाबदार बँकिंगच्या वापराची मार्गदर्शक तत्त्वे

मोबाईल बँकिंग असो किंवा इंटरनेट बँकिंग असो, एखाद्या शाखेतून किंवा ATM मधून पैसे काढणे असो, सुरक्षित बँकिंगच्या अनुभवाची खात्री करण्यासाठी तुम्ही काळजी आणि काही मूलभूत खबरदारी घेणे आवश्यक आहे. आम्ही, इक्विटास स्मॉल फायनान्स बँक (ESFB) मध्ये सुरक्षित बँकिंगच्या पद्धतीवर विश्वास ठेवतो. याची सुरुवात, तुमचा संपर्क तपशील आमच्या डेटाबेसमध्ये अद्ययावत केला गेला आहे याची खात्री करून होते, जेणेकरून अलर्ट अनपेक्षित प्राप्तकर्त्यांकडे जाऊ नयेत. जर तुम्ही परदेशात प्रवास करत असाल, तर तुमच्या ईमेल ID बँकेत नोंद केली असल्याची खात्री करा.

'काय केले पाहिजे' आणि 'काय नाही केले पाहिजे' या बाबींची यादी:

तुमचे खाते/कार्ड ब्लॉक केले गेले असल्याने तुमचा KYC तपशील अपडेट करा, क्रेडिट कार्डची वाढीव मर्यादा मिळवा, कॅशबॅक पॉइंट/बक्षिसे मिळवा किंवा कर्ज/कर्जावर टॉप-अप घ्या या सबबीखाली तुम्हाला कॉल/SMS/ईमेलद्वारे लक्ष्य करून फसवणूक करणाऱ्यांपासून सावध रहा. अशा घोटाळ्यांना बळी पडू नका.

अशा घोटाळ्यांना बळी पडू नका.

स्वत:चे रक्षण करण्यासाठी आणि ऑनलाइन सुरक्षित राहण्यासाठी खाली 'काय केले पाहिजे' आणि 'काय करून नये' या बाबी देण्यात आल्या आहेत:

काय केले पाहिजे

- बँकेच्या संपर्क तपशीलासाठी नेहमी अधिकृत वेबसाइटला भेट द्या
- बँकेकडे तुमचा संपर्क तपशील नेहमी अद्ययावत ठेवा आणि व्यवहारांचे अलर्ट मिळवण्यासाठी सदस्यता घ्या
- तुमच्या संगणक/मोबाईलवर अस्सल अँटी-व्हायरस आणि अँटी-मालवेअर सॉफ्टवेअर स्थापित करा आणि त्यांना अद्ययावत ठेवा
- तुमचा पासवर्ड अभेद्य आणि अद्वितीय ठेवा
- तुमचा कार्ड नंबर, पासवर्ड किंवा इतर कोणतीही वैयक्तिक/संवेदनशील माहिती संचयित करणे टाळण्यासाठी तुमच्या ब्राउझरची ऑटोकम्प्लीट सेटिंग्ज बंद करा
- प्ले स्टोअर किंवा ॲप स्टोअरवरून कोणतेही ॲप डाउनलोड करण्यापूर्वी काळजी घ्या
- व्यवहार करताना तुमच्या वेब ब्राउझरच्या स्टेटस बारमध्ये पॅडलॉक चिन्ह किंवा https पहा
- संवेदनशील तपशील शेअर करण्यास सांगणाऱ्या संदेशांमधील शुद्धलेखनाच्या चुका नेहमी पहा, कारण त्यामुळे तुम्हाला बनावट ओळखण्यात मदत होईल.

काय नाही केले पाहिजे

- PIN, पासवर्ड, OTP किंवा कार्ड तपशील यासारखे संवेदनशील तपशील कधीही कोणाशीही शेअर करू नका
- तुमच्या बँक खात्यात प्रवेश करताना सार्वजनिक वाय-फाय किंवा मोफत VPN/सार्वजनिक संगणक वापरणे टाळा
- अज्ञात स्त्रोतांकडून/प्रेषक IDs कडून प्राप्त झालेल्या लिंकवर क्लिक करू नका
- 123456, नावे, वाढदिवस इत्यादी सामान्यपणे वापरल्या जाणाऱ्या पासवर्डपासून दूर रहा.
- तुमचा बँकिंग पासवर्ड कुठेही लिहून ठेवणे आणि ब्राउझरवर सेव्ह करणे टाळा
- रिमोट शेअरिंग ॲप्स डाउनलोड करू नका उदा. एनिडेस्क
- UPI माध्यामतून पैसे मिळवण्यासाठी QR कोड स्कॅन करू नका किंवा PIN किंवा OTP टाकू नका
- ATM मध्ये अनोळखी व्यक्तीची मदत घेऊ नका

या बाबी लक्षात ठेवा:

ESFB किंवा तिचे कर्मचारी/प्रतिनिधी कधीही तुमच्या वैयक्तिक खात्याची माहिती विचारणार नाहीत.

1. पासवर्डचे संरक्षण

हॅकर्सना याची जाणीव असते की, लोक एकापेक्षा जास्त खात्यांसाठी तोच किंवा मिळताजुळता पासवर्ड वापरतात. तुमचा बँकिंग पासवर्ड, ऍमेझॉन पासवर्ड आणि ईमेल पासवर्ड सारखाच असल्यास, एका साइटमधील असुरक्षितता इतरांना धोक्यात आणू शकते.

पासवर्डचा अंदाज लावणे सोपे कशामुळे होते?

एकदा का हॅकर्सने डेटाच्या उल्लंघनातून ईमेल पत्त्यांची यादी मिळवली की, त्यांची एक आधीच चांगली सुरुवात होते. तेथून, त्यांना फक्त त्यांच्या आवडीची वेबसाइट निवडावी लागते आणि सर्वात लोकप्रिय पासवर्डसह यादीतील ईमेल वापरून पहावे लागतात. मग बऱ्याच खात्यांमध्ये प्रवेश प्राप्त होण्याची शक्यता निर्माण होते.

तुमचे खाते हॅक होण्यापासून टाळण्यासाठी, येथे सर्वात वाईट पासवर्डची यादी दिली आहे जी तुम्ही टाळावी:

- 123456 वापरणे टाळा, जो सर्व पासवर्डपैकी सर्वात सामान्य पासवर्ड आहे.
- अक्षराच्या जागी चिन्ह वापरणे, जसे की, p@ssw0rd ही सुद्धा हॅकर्सना माहित असलेली ही एक स्पष्ट युक्ती आहे. पासवर्ड क्रॅकिंग प्रोग्राममध्ये प्रत्येक भाषेत या संयोगांचा प्रत्येक प्रकार असतो.
- काहीतरी अस्पष्ट वापरा आणि तुमच्या आवडत्या क्रीडा संघाची नावे किंवा पॉप संस्कृतीचा संदर्भ वापरणे टाळा.
- सूर्यप्रकाश किंवा माकड यासारखे एकच शब्द वापरल्याने आणि शेवटी एक संख्या किंवा विरामचिन्ह जोडल्याने, एक अभेद्य पासवर्ड बनत नाही. त्याऐवजी, तुमचा पासवर्ड अभेद्य करण्यासाठी एखादा वाक्यांश किंवा वाक्य वापरा.
- 111111, abc123 किंवा 654321 सारखे सामान्य पॅटर्न्स वापरणे टाळा.

पासवर्ड कशामुळे अभेद्य होतो?

- असंबंधित शब्द एकत्र केल्याने.
- एखादा संपूर्ण वाक्यांश वापरल्याने आणि काही अक्षरांना विशेष अक्षरांमध्ये आणि संख्यांमध्ये बदलल्याने.
- अप्पर आणि लोअर केसमधील अक्षरे, चिन्हे आणि संख्या यांच्या संयोगाचा वापर करा.
- तुमचा पासवर्ड जितका मोठा असेल तितका तो अभेद्य होईल.
- प्रत्येक खात्यासाठी वेगवेगळे पासवर्ड वापरा.

2. डेबिट कार्ड

येथे काही 'काय केले पाहिजे आणि काय नाही केले पाहिजे' अशा बाबी देण्यात आल्या आहेत, ज्या तुम्हाला डेबिट आणि क्रेडिट कार्डची फसवणूक टाळण्यास आणि सुरक्षित आणि त्रासमुक्त बँकिंग अनुभवाचा आनंद घेण्यास मदत करतील.

काय केले पाहिजे

- वेलकम किट मिळाल्यावर, लिफाफा सीलबंद असल्याची खात्री करा. छेडछाडीचा कोणताही संकेत असल्यास, ताबडतोब बँकेशी संपर्क साधा.
- ताबडतोब कार्डच्या मागील बाजूवर स्वाक्षरी करा.
- कार्ड मिळाल्यानंतर त्याचा PIN बदला. संपूर्ण संरक्षणासाठी दर सहा महिन्यांनी असे करणे, ही एक चांगली बाब आहे.
- तुमचे कार्ड सुरक्षित प्रकारे ठेवा. कार्डचे नुकसान किंवा चोरी झाल्यास ताबडतोब बँकेला कळवा.
- नवीन किंवा अपग्रेड केलेले कार्ड मिळाल्यानंतर, जुने कार्ड तिरपे कापून टाकून द्या.
- परदेश दौऱ्यानंतर PIN बदलण्याचा सल्ला दिला जातो.
- तुमचा PIN कुठेही लिहिण्याऐवजी तो लक्षात ठेवण्याचा प्रयत्न करा.
- तुमच्या ओळखपत्रांची (क्रेडेन्शियल्स) तुमच्या लॅपटॉप किंवा मोबाइलमध्ये माहिती देण्यासाठी, खराखुरा कीबोर्ड वापरणे टाळा आणि शक्यतो व्हर्च्युअल कीपॅड वापरा (प्रतिमा दाखवा).
- तुमचा PIN कुठेही म्हणजे, ATM, कार्ड मशीन इ. मध्ये टाकताना काळजी घ्या
- कोणत्याही कार्डद्वारे व्यवहारांसाठी सतत सूचना प्राप्त करण्यासाठी तुमचा ईमेल आणि फोन नंबर अद्ययावत करा. तुमच्या व्यवहारांवर आणि खरेदीवर लक्ष ठेवा आणि कोणत्याही असामान्य व्यवहाराची त्वरित बँकेला तक्रार करा.

- तुमच्या कार्डांसाठी, व्हेरिफाईड बाय व्हिसा (VbV) किंवा मास्टरकार्ड सिक्युअर कोड (MCSC) स्वरूपात तुमच्याकडे 3D सिक्युअर असल्याची खात्री करा. हे आता ऑनलाइन व्यवहारांसाठी अनिवार्य आहे आणि ते, सर्व ESFB कार्डांवर असते.
- पेमेंट करण्यापूर्वी वेबसाइट सुरक्षित असल्याची खात्री करण्यासाठी नेहमी वेबसाइटचचा url तपासा. जलद तपासणी: तुमच्या ब्राउझरवर लॉकचे चिन्ह (https://show lock symbol) असल्याची खात्री करा, जे संकेत देते की वेबसाइट संवेदनशील डेटा प्रसारित करताना एनक्रिप्शन तंत्रज्ञान वापरत आहे. लॉकवर क्लिक केल्यावर तुम्ही डिजिटल प्रमाणपत्र आणि वेबसाइटशी संबंधित इतर तपशील पाहू शकता. असे सत्यापन उपलब्ध असल्यासच पुढे जा
- जर एखादी साइट, डोमेन नावाऐवजी IP पत्ता किंवा संख्यात्मक पत्ता दर्शवित असेल, तर अशा साइटचा url तपासा, कारण अशी साइट अस्सल साइट नसण्याची शक्यता असते.

काय नाही केले पाहिजे

- लक्षात ठेवा की, इक्विटास स्मॉल फायनान्स बँक, तुम्हाला तुमच्या कार्डच्या पुढील आणि मागील भागाची प्रत यासारख्या तपशीलासाठी कधीही विचारणार नाही.
- जर कोणतीही व्यक्ती, बँकेची प्रतिनिधी असल्याचा दावा करत असेल आणि तिने, तुमचे कार्ड मागितले तर ते देऊ नका.
- कार्ड नंबर, मुदत समाप्ती, CVV, PIN किंवा OTP यासारखा कार्डचा तपशील कोणत्याही व्यक्तीशी शेअर करू नका, जरी ती व्यक्ती, बँक अधिकारी असल्याचा दावा करत असले तरीही.
- ऑनलाइन व्यापारी वेबसाइटवर तुमच्या कार्डचा तपशील सेव्ह करू नका.
- कार्डचे तपशील, ATM PIN, CVV, UPI PIN इ. विचारणाऱ्या इनपुट फील्ड असलेल्या ईमेलवर तुमचा तपशील कधीही पाठवू नका.
- गेमिंग वेबसाइट, पोर्नोग्राफी वेबसाइट, लॉटरी, जुगार आणि बरेच काही यासारख्या अनधिकृत पेमेंट गेटवेवर तुमची कार्डे वापरणे टाळा.
- बँकेच्या प्रतिनिधीद्वारे त्यास नंतर भरले जाईल असे आश्वासन असलेल्या रिकाम्या अर्जावर कधीही स्वाक्षरी करू नका.

3. UPI

काय केले पाहिजे:

- UPI ॲप्लिकेशन वैध प्लॅटफॉर्मवरून डाउनलोड करा, म्हणजेच गुगल प्ले स्टोअर इ.
- तुमच्या बेस ब्रांच / नेट बँकिंग / UPI माध्यमातून मोबाईल बँकिंगसाठी नोंदणी करा.
- तुम्ही संपूर्ण गोपनीयतेमध्ये लॉग इन करून UPI व्यवहार सुरू करता या बाबीची खात्री करा.
- व्यवहार पूर्ण केल्यानंतर, तुम्ही अर्जातून यशस्वीरित्या लॉग आउट केल्याची खात्री करा.
- प्रत्येक व्यवहारासाठी, तुमच्या नोंदणीकृत मोबाईल नंबरवर SMS अलर्ट मिळेल. तुम्हाला तुमच्या खात्यात कोणताही अनधिकृत UPI व्यवहार आढळल्यास, कृपया ताबडतोब तुमच्या शाखेशी संपर्क साधा.
- कोणत्याही अयशस्वी व्यवहाराच्या बाबतीत, कृपया वेबसाइट आणि ॲप्लिकेशनवर प्रदान केलेले एस्केलेशन मॅट्रिक्स वापरा.
- तुमचा UPI ॲप्लिकेशन पासवर्ड आणि UPI PIN / MPIN वारंवार बदला.
- तुमच्या मोबाइल बँकिंग/UPI मध्ये अनधिकृत प्रवेश झाल्यास, कृपया ATM / इंटरनेट बँकिंग / बेस ब्रांचच्या माध्यमातून (किंवा कृपया आमच्या संपर्क केंद्राशी संपर्क साधा) ताबडतोब नोंदणी रद्द करा.
- तुमचा मोबाईल फोन हरवल्यास / चोरी झाल्यास, कृपया बेस ब्रांच / नेट बँकिंग / ATM / संपर्क केंद्राच्या माध्यमातून ताबडतोब तुमच्या मोबाईल बँकिंगची नोंदणी करा.
- जर तुमचा मोबाईल बँकिंग / मोबाईल नंबर तुमच्या विनंतीशिवाय नोंदणी रहित / निष्क्रिय झाला असेल किंवा तुम्हाला या संदर्भात कॉल आला तर, कोणीतरी डुप्लिकेट SIM मिळवण्याचा / तुमची क्रेडेन्शियल्स जसे की mPIN / OTP (वन टाइम पासवर्ड) चोरण्याचा प्रयत्न करत असेल. या प्रकरणात, कृपया तुमच्या मूळ शाखेशी त्वरित संपर्क साधा.

काय नाही केले पाहिजे:

- कृपया तुमचे पासवर्ड शेअर करू नका / त्यांना तुमच्या मोबाईल हँडसेटमध्ये साठवू नका.
- तुमचा ॲप्लिकेशन पासवर्ड किंवा UPI PIN / MPIN टाकताना कोणालाही कधीही पाहू देऊ नका.
- कधीही सहज अंदाज लावता येईल असा ॲप्लिकेशन / UPI PIN / MPIN वापरू नका उदा: 1111/2222/1234/ जन्म वर्ष, मोबाईल नंबर/टेलिफोन नंबर.
- UPI ॲप्लिकेशन दुसऱ्या कोणाच्या तरी उपकरणामध्ये इंस्टॉल करू नका आणि वापरू नका.
- इक्विटास बँक, तुमचे UPI / मोबाइल बँकिंग पासवर्ड विचारण्यासाठी कॉल करत नाही / ईमेल पाठवत नाही. जर कोणी कॉलर आमच्या बँक / संपर्क केंद्राकडून असल्याचे भासवत असेल, तर कृपया अशा विनंत्या लक्षात घेऊ नका कारण त्या फसव्या संस्था असतात.
- तुमचे नोंदणीकृत SIM कार्ड आणि डेबिट कार्ड कधीही सोबत ठेवू नका, कारण ते दोन्ही गमावण्याचा धोका असतो आणि त्यामुळे तुमच्या खात्यात कोणालाही प्रवेश मिळू शकतो.

ਸੁਰੱਖਿਅਤ ਅਤੇ ਜ਼ਿੰਮੇਵਾਰੀ ਨਾਲ ਬੈਂਕਿੰਗ ਦੀ ਵਰਤੋਂ ਕਰਨ ਦੇ ਦਿਸ਼ਾ-ਨਿਰਦੇਸ਼

ਭਾਵੇਂ ਇਹ ਮੋਬਾਈਲ ਬੈਂਕਿੰਗ ਹੋਵੇ ਜਾਂ ਇੰਟਰਨੈਟ ਬੈਂਕਿੰਗ, ਭਾਵੇਂ ਕਿਸੇ ਬੈਂਕ ਦੀ ਬ੍ਰਾਂਚ ਜਾਂ ATM ਤੋਂ ਪੈਸੇ ਕਢਵਾਉਣਾ ਹੋਵੇ, ਇੱਕ ਬੈਂਕਿੰਗ ਦੇ ਅਨੁਭਵ ਨੂੰ ਸੁਰੱਖਿਅਤ ਬਣਾਉਣ ਲਈ ਹਰੇਕ ਨੂੰ ਕੁਝ ਬੁਨਿਆਦੀ ਸਾਵਧਾਨੀਆਂ ਵਰਤਣ ਦੀ ਲੋੜ ਹੁੰਦੀ ਹੈ। ਅਸੀਂ, ਇਕੁਇਟਾਸ ਸਮਾਲ ਫਾਈਨੈਂਸ ਬੈਂਕ (ESFB) ਵਿਖੇ ਸੁਰੱਖਿਅਤ ਨੂੰ ਵਰਤਦੇ ਹੋਏ ਬੈਂਕਿੰਗ ਕਰਨ ਵਿੱਚ ਵਿਸ਼ਵਾਸ ਕਰਦੇ ਹਾਂ। ਇਸ ਦੀ ਸ਼ੁਰੂਆਤ ਲਈ ਇਹ ਪੱਕਾ ਕੀਤਾ ਜਾਂਦਾ ਹੈ ਕਿ ਤੁਹਾਡੇ ਸੰਪਰਕ ਵੇਰਵੇ ਸਾਡੇ ਡੇਟਾਬੇਸ ਵਿੱਚ ਅੱਪਡੇਟ ਹੋ ਰਹੇ ਹਨ ਤਾਂ ਜੋ ਚੇਤਾਵਨੀਆਂ ਵਾਲੇ ਕੋਈ ਵੀ ਮੈਸੇਜ ਕਿਸੇ ਅਣਜਾਣ ਵਿਅਕਤੀ ਕੋਲ ਨਾ ਜਾਣ। ਜੇਕਰ ਤੁਸੀਂ ਵਿਦੇਸ਼ ਯਾਤਰਾ ਕਰ ਰਹੇ ਹੋ, ਤਾਂ ਇਹ ਯਕੀਨੀ ਬਣਾਓ ਕਿ ਤੁਹਾਡੀ ਈਮੇਲ ID ਬੈਂਕ ਵਿੱਚ ਰਜਿਸਟਰਡ ਹੈ।

ਕੀ ਕਰਨਾ ਹੈ ਅਤੇ ਕੀ ਨਹੀਂ ਕਰਨਾ, ਉਸ ਦੀ ਸੂਚੀ:

ਧੋਖੇਬਾਜ਼ਾਂ ਤੋਂ ਸਾਵਧਾਨ ਰਹੋ ਜੋ ਤੁਹਾਡੇ KYC ਵੇਰਵਿਆਂ ਨੂੰ ਅੱਪਡੇਟ ਕਰਨ ਦੇ ਬਹਾਨੇ ਤੁਹਾਨੂੰ ਕਾਲ/SMS/ਈਮੇਲ ਕਰਦੇ ਹਨ ਅਤੇ ਇਹ ਕਹਿੰਦੇ ਹਨ ਕਿ ਤੁਹਾਡਾ ਖਾਤਾ/ਕਾਰਡ ਬਲੌਕ ਹੈ, ਇੱਕ ਵਧੀ ਹੋਈ ਕ੍ਰੈਡਿਟ ਕਾਰਡ ਸੀਮਾ ਪ੍ਰਾਪਤ ਕਰਨਾ, ਕੈਸ਼ਬੈਕ ਪੁਆਇੰਟ/ਇਨਾਮ ਕਮਾਉਣਾ ਜਾਂ ਇੱਕ 'ਤੇ ਲੋਨ/ਟੌਪ-ਅੱਪ ਪ੍ਰਾਪਤ ਕਰਨਾ। ਅਜਿਹੇ ਧੋਖਿਆਂ ਦਾ ਸ਼ਿਕਾਰ ਨਾ ਹੋਵੋ।

ਅਜਿਹੇ ਧੋਖਿਆਂ ਦਾ ਸ਼ਿਕਾਰ ਨਾ ਹੋਵੋ।

ਆਪਣੇ ਆਪ ਨੂੰ ਸੁਰੱਖਿਅਤ ਰੱਖਣ ਅਤੇ ਔਨਲਾਈਨ ਸੁਰੱਖਿਅਤ ਰਹਿਣ ਲਈ ਇੱਥੇ ਕੀ ਕਰਨਾ ਹੈ ਅਤੇ ਨਾ ਕਰਨਾ ਹੈ, ਉਸ ਬਾਰੇ ਦੱਸਿਆ ਗਿਆ ਹੈ:

ਕੀ ਕਰਨਾ ਹੈ

- ਬੈਂਕ ਦੇ ਸੰਪਰਕ ਵੇਰਵਿਆਂ ਲਈ ਹਮੇਸ਼ਾ ਅਧਿਕਾਰਤ ਵੈੱਬਸਾਈਟ 'ਤੇ ਜਾਓ
- ਬੈਂਕ ਨਾਲ ਆਪਣੇ ਸੰਪਰਕ ਵੇਰਵਿਆਂ ਨੂੰ ਹਮੇਸ਼ਾ ਅੱਪਡੇਟ ਰੱਖੋ ਅਤੇ ਲੈਣ-ਦੇਣ ਸੰਬੰਧੀ ਅਲਰਟ ਲਈ ਮੈਸੇਜ ਕਰੋ
- ਆਪਣੇ ਕੰਪਿਊਟਰ/ਮੋਬਾਈਲ 'ਤੇ ਅਸਲ ਐਂਟੀ-ਵਾਇਰਸ ਅਤੇ ਐਂਟੀ-ਮਾਲਵੇਅਰ ਸੌਫਟਵੇਅਰ ਇੰਸਟਾਲ ਕਰੋ ਅਤੇ ਇਸਨੂੰ ਅਪ-ਟੂ-ਡੇਟ ਰੱਖੋ
- ਆਪਣਾ ਪਾਸਵਰਡ ਮਜ਼ਬੂਤ ਅਤੇ ਸੱਭ ਤੋਂ ਵੱਖ ਰੱਖੋ
- ਆਪਣੇ ਕਾਰਡ ਦੇ ਨੰਬਰ, ਪਾਸਵਰਡ ਜਾਂ ਕਿਸੇ ਹੋਰ ਨਿੱਜੀ/ਸੰਵੇਦਨਸ਼ੀਲ ਜਾਣਕਾਰੀ ਨੂੰ ਸਟੋਰ ਕਰਨ ਤੋਂ ਬਚਣ ਲਈ ਆਪਣੇ ਬ੍ਰਾਊਜ਼ਰ ਦੀਆਂ ਸਵੈ-ਸੰਪੂਰਨ ਸੈਟਿੰਗਾਂ ਨੂੰ ਬੰਦ ਕਰੋ
- ਪਲੇ ਸਟੋਰ ਜਾਂ ਐਪ ਸਟੋਰ ਤੋਂ ਕੋਈ ਵੀ ਐਪ ਡਾਊਨਲੋਡ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਸਾਵਧਾਨ ਰਹੋ
- ਲੈਣ-ਦੇਣ ਕਰਦੇ ਸਮੇਂ ਆਪਣੇ ਵੈੱਬ ਬ੍ਰਾਊਜ਼ਰ ਦੇ ਸਟੇਟਸ ਬਾਰ ਵਿੱਚ ਪੈਡਲੌਕ ਸਾਈਨ ਜਾਂ https ਦੇਖੋ
- ਸੰਵੇਦਨਸ਼ੀਲ ਵੇਰਵਿਆਂ ਨੂੰ ਸਾਂਝਾ ਕਰਨ ਲਈ ਕਹਿਣ ਵਾਲੇ ਮੈਸੇਜ ਵਿੱਚ ਸਪੈਲਿੰਗ ਦੀਆਂ ਗਲਤੀਆਂ 'ਤੇ ਹਮੇਸ਼ਾ ਧਿਆਨ ਰੱਖੋ, ਕਿਉਂਕਿ ਉਹ ਨਕਲੀ ਹੈ ਇਸ ਦੀ ਪਛਾਣ ਕਰਨ ਵਿੱਚ ਤੁਹਾਨੂੰ ਮਦਦ ਮਿਲੇਗੀ।

ਕੀ ਨਹੀਂ ਕਰਨਾ ਹੈ

- PIN, ਪਾਸਵਰਡ, OTP ਜਾਂ ਕਾਰਡ ਦੇ ਵੇਰਵਿਆਂ ਵਰਗੇ ਸੰਵੇਦਨਸ਼ੀਲ ਵੇਰਵਿਆਂ ਨੂੰ ਕਦੇ ਵੀ ਕਿਸੇ ਨਾਲ ਸਾਂਝਾ ਨਾ ਕਰੋ
- ਆਪਣੇ ਬੈਂਕ ਖਾਤੇ ਨੂੰ ਖੋਲਣ ਲਈ ਪਬਲਿਕ ਵਾਈ-ਫਾਈ ਜਾਂ ਮੁਫਤ VPN/ਪਬਲਿਕ ਕੰਪਿਊਟਰਾਂ ਦੀ ਵਰਤੋਂ ਨਾ ਕਰੋ
- ਅਣਜਾਣ ਸਰੋਤਾਂ/ਭੇਜਣ ਵਾਲੇ ਦੀ ID ਤੋਂ ਪ੍ਰਾਪਤ ਲਿੰਕਾਂ 'ਤੇ ਕਲਿੱਕ ਨਾ ਕਰੋ
- ਆਮ ਤੌਰ 'ਤੇ ਸੋਖੇ ਵਰਤੇ ਜਾਣ ਵਾਲੇ ਪਾਸਵਰਡ ਜਿਵੇਂ ਕਿ 123456, ਨਾਮ, ਜਨਮਦਿਨ ਆਦਿ ਨਾ ਵਰਤੋਂ
- ਆਪਣਾ ਬੈਂਕਿੰਗ ਪਾਸਵਰਡ ਕਿਤੇ ਵੀ ਲਿਖਣ ਅਤੇ ਇਸਨੂੰ ਬ੍ਰਾਊਜ਼ਰ 'ਤੇ ਸੇਵ ਕਰਨ ਦੀ ਗਲਤੀ ਨਾ ਕਰੋ
- ਰਿਮੋਟ ਸ਼ੇਅਰਿੰਗ ਐਪਸ ਨੂੰ ਡਾਊਨਲੋਡ ਨਾ ਕਰੋ ਜਿਵੇਂ ਕਿ ਏਨੀਡੈਸਕ
- UPI ਰਾਹੀਂ ਪੈਸੇ ਪ੍ਰਾਪਤ ਕਰਨ ਲਈ QR ਕੋਡ ਨੂੰ ਸਕੈਨ ਨਾ ਕਰੋ ਜਾਂ PIN ਜਾਂ OTP ਨਾ ਭਰੋ
- ATM ਦੀ ਵਰਤੋਂ ਕਰਨ ਲਈ ਅਜਨਬੀਆਂ ਦੀ ਮਦਦ ਨਾ ਲਓ

ਯਾਦ ਰੱਖੋ:

ESFB ਜਾਂ ਇਸਦੇ ਕਰਮਚਾਰੀ/ਪ੍ਰਤੀਨਿਧੀ ਕਦੇ ਵੀ ਤੁਹਾਡੀ ਨਿੱਜੀ ਖਾਤਾ ਜਾਣਕਾਰੀ ਨਹੀਂ ਮੰਗਣਗੇ।

1. **ਪਾਸਵਰਡ ਸੁਰੱਖਿਆ**

ਹੈਕਰਾਂ ਨੂੰ ਪਤਾ ਹੈ ਕਿ ਲੋਕ ਇੱਕ ਤੋਂ ਵੱਧ ਖਾਤਿਆਂ ਲਈ ਇੱਕੋ ਜਾਂ ਸਮਾਨ ਪਾਸਵਰਡ ਦੀ ਵਰਤੋਂ ਕਰਦੇ ਹਨ। ਜੇਕਰ ਤੁਹਾਡਾ ਬੈਂਕਿੰਗ ਪਾਸਵਰਡ, ਐਮਾਜ਼ਾਨ ਪਾਸਵਰਡ, ਅਤੇ ਈਮੇਲ ਪਾਸਵਰਡ ਇੱਕੋ ਜਿਹੇ ਹਨ, ਤਾਂ ਇੱਕ ਸਾਈਟ ਦੇ ਨਾਲ-ਨਾਲ ਦੂਜਿਆਂ ਸਾਇਟਸ ਨੂੰ ਵੀ ਖਤਰਾ ਹੋ ਸਕਦਾ ਹੈ।

ਐਸਾ ਕੀ ਹੈ ਜਿਸ ਨਾਲ ਇੱਕ ਪਾਸਵਰਡ ਦਾ ਅੰਦਾਜ਼ਾ ਲਗਾਉਣਾ ਆਸਾਨ ਹੁੰਦਾ ਹੈ?

ਇੱਕ ਵਾਰ ਹੈਕਰ ਇੱਕ ਡੇਟਾ ਤੋਂ ਈਮੇਲ ਪਤਿਆਂ ਦੀ ਇੱਕ ਸੂਚੀ ਪ੍ਰਾਪਤ ਕਰ ਲੈਂਦੇ ਹਨ, ਉਹਨਾਂ ਕੋਲ ਪਹਿਲਾਂ ਹੀ ਇੱਕ ਚੰਗੀ ਸ਼ੁਰੂਆਤ ਹੁੰਦੀ ਹੈ। ਉੱਥੋਂ, ਉਹਨਾਂ ਨੂੰ ਬਸ ਆਪਣੀ ਪਸੰਦ ਦੀ ਇੱਕ ਵੈਬਸਾਈਟ ਚੁਣਨੀ ਪੈਂਦੀ ਹੈ ਅਤੇ ਸਭ ਤੋਂ ਪ੍ਰਸਿੱਧ ਪਾਸਵਰਡਾਂ ਨਾਲ ਸੂਚੀਬੱਧ ਈਮੇਲਾਂ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰਨੀ ਪੈਂਦੀ ਹੈ। ਕਿਸੇ ਨਾ ਕਿਸੇ ਖਾਤੇ 'ਤੇ ਇਹਨਾਂ ਪਾਸਵਰਡ ਦੇ ਲੱਗਣ ਦੀ ਸੰਭਾਵਨਾ ਹੁੰਦੀ ਹੈ।

ਆਪਣੇ ਖਾਤੇ ਨੂੰ ਹੈਕ ਹੋਣ ਤੋਂ ਬਚਾਉਣ ਲਈ, ਇੱਥੇ ਸਭ ਤੋਂ ਭੈੜੇ ਪਾਸਵਰਡਾਂ ਦੀ ਸੂਚੀ ਦਿੱਤੀ ਗਈ ਹੈ ਜਿਨ੍ਹਾਂ ਨੂੰ ਤੁਹਾਨੂੰ ਨਹੀਂ ਰੱਖਣਾ ਚਾਹੀਦਾ ਹੈ:

- 123456 ਦੀ ਵਰਤੋਂ ਕਰਨ ਤੋਂ ਬਚੋ, ਜੋ ਸਾਰੇ ਪਾਸਵਰਡਾਂ ਵਿੱਚੋਂ ਸਭ ਤੋਂ ਆਮ ਹੈ।
- ਇੱਕ ਅੱਖਰ ਨੂੰ p@ssw0rd! ਵਰਗੇ ਚਿੰਨ੍ਹ ਵਿੱਚ ਬਦਲਣਾ! ਇਹ ਵੀ ਇੱਕ ਸਪੱਸ਼ਟ ਚਾਲ ਹੈ ਜੋ ਹੈਕਰ ਜਾਣਦੇ ਹਨ। ਪਾਸਵਰਡ ਕ੍ਰੈਕਿੰਗ ਪ੍ਰੋਗਰਾਮਾਂ ਵਿੱਚ ਹਰ ਭਾਸ਼ਾ ਵਿੱਚ ਇਹਨਾਂ ਦੇ ਕਮਬੀਨੇਸ਼ਨ ਦੀ ਹਰ ਕਿਸਮ ਹੁੰਦੀ ਹੈ।
- ਕੁਝ ਅਸਪਸ਼ਟ ਵਰਤੋ ਅਤੇ ਆਪਣੀ ਮਨਪਸੰਦ ਸਪੋਰਟਸ ਟੀਮ ਦੇ ਨਾਂ ਜਾਂ ਪੌਪ ਕਲਚਰ ਦੇ ਹਵਾਲੇ ਵਰਤਣ ਤੋਂ ਬਚੋ।
- ਸਨਸ਼ਾਈਨ ਜਾਂ ਮੌਂਕੀ ਵਰਗੇ ਇੱਕਲੇ ਸ਼ਬਦਾਂ ਦੀ ਵਰਤੋਂ ਕਰਨਾ ਅਤੇ ਅੰਤ ਵਿੱਚ ਇੱਕ ਨੰਬਰ ਜਾਂ ਵਿਰਾਮ ਚਿੰਨ੍ਹ ਜੋੜਨਾ, ਇੱਕ ਮਜ਼ਬੂਤ ਪਾਸਵਰਡ ਨਹੀਂ ਬਣਾਉਂਦਾ। ਇਸਦੀ ਬਜਾਏ, ਆਪਣੇ ਪਾਸਵਰਡ ਨੂੰ ਮਜ਼ਬੂਤ ਬਣਾਉਣ ਲਈ ਇੱਕ ਵਾਕਾਂਸ਼ ਜਾਂ ਵਾਕ ਦੀ ਵਰਤੋਂ ਕਰੋ।
- 111111, abc123 ਜਾਂ 654321 ਵਰਗੇ ਆਮ ਪੈਟਰਨ ਦੀ ਵਰਤੋਂ ਕਰਨ ਤੋਂ ਬਚੋ।

ਕਿਹੜੀ ਚੀਜ਼ ਪਾਸਵਰਡ ਨੂੰ ਮਜ਼ਬੂਤ ਬਣਾਉਂਦੀ ਹੈ?

- ਅਸੰਬੰਧਿਤ ਸ਼ਬਦਾਂ ਨੂੰ ਜੋੜਨਾ।
- ਇੱਕ ਪੂਰੇ ਵਾਕਾਂਸ਼ ਦੀ ਵਰਤੋਂ ਕਰਨਾ ਅਤੇ ਕੁਝ ਅੱਖਰਾਂ ਨੂੰ ਵਿਸ਼ੇਸ਼ ਅੱਖਰਾਂ ਅਤੇ ਸੰਖਿਆਵਾਂ ਵਿੱਚ ਬਦਲਣਾ।
- ਵੱਡੇ ਅਤੇ ਛੋਟੇ ਅੱਖਰਾਂ, ਚਿੰਨ੍ਹਾਂ ਅਤੇ ਸੰਖਿਆਵਾਂ ਦੇ ਕਮਬੀਨੇਸ਼ਨ ਦੀ ਵਰਤੋਂ ਕਰਨਾ।
- ਤੁਹਾਡਾ ਪਾਸਵਰਡ ਜਿੰਨਾ ਲੰਬਾ ਹੋਵੇਗਾ, ਇਹ ਓਨਾ ਹੀ ਮਜ਼ਬੂਤ ਹੋਵੇਗਾ।
- ਹਰ ਖਾਤੇ ਲਈ ਵੱਖ-ਵੱਖ ਪਾਸਵਰਡ ਵਰਤਣਾ।

2. **ਡੈਬਿਟ ਕਾਰਡ**

ਇੱਥੇ ਕੁਝ 'ਕਰੋ ਅਤੇ ਨਾ ਕਰੋ' ਦਿੱਤੇ ਗਏ ਹਨ, ਜੋ ਤੁਹਾਨੂੰ ਡੈਬਿਟ ਅਤੇ ਕ੍ਰੈਡਿਟ ਕਾਰਡਾਂ ਦੀ ਧੋਖਾਧੜੀ ਤੋਂ ਬਚਣ ਅਤੇ ਇੱਕ ਸੁਰੱਖਿਅਤ ਅਤੇ ਮੁਸ਼ਕਲ ਰਹਿਤ ਬੈਂਕਿੰਗ ਦੇ ਅਨੁਭਵ ਦਾ ਆਨੰਦ ਲੈਣ ਵਿੱਚ ਮਦਦ ਕਰਨਗੇ।

ਕੀ ਕਰਨਾ ਹੈ

- ਸਵਾਗਤ ਕਿੱਟ ਪ੍ਰਾਪਤ ਕਰਨ 'ਤੇ, ਇਹ ਯਕੀਨੀ ਬਣਾਓ ਕਿ ਲਿਫ਼ਾਫ਼ਾ ਸੀਲ ਕੀਤਾ ਗਿਆ ਹੈ। ਜੇਕਰ ਤੁਹਾਨੂੰ ਲਗਦਾ ਹੈ ਕਿ ਇਸ ਨਾਲ ਛੇੜਛਾੜ ਕੀਤੀ ਗਈ ਹੈ, ਤਾਂ ਤੁਰੰਤ ਬੈਂਕ ਨਾਲ ਸੰਪਰਕ ਕਰੋ।
- ਕਾਰਡ ਦੇ ਉਲਟੇ ਪਾਸੇ ਤੁਰੰਤ ਦਸਤਖਤ ਕਰੋ।
- ਕਾਰਡ ਪ੍ਰਾਪਤ ਕਰਨ ਤੋਂ ਬਾਅਦ ਉਸ ਦਾ PIN ਬਦਲੋ। ਆਦਰਸ਼ਕ ਤੌਰ 'ਤੇ, ਪੂਰੀ ਸੁਰੱਖਿਆ ਲਈ ਹਰ ਛੇ ਮਹੀਨਿਆਂ ਬਾਅਦ ਅਜਿਹਾ ਕਰੋ।
- ਆਪਣੇ ਕਾਰਡ ਸੁਰੱਖਿਅਤ ਰੱਖੋ। ਨੁਕਸਾਨ ਜਾਂ ਚੋਰੀ ਦੀ ਸਥਿਤੀ ਵਿੱਚ, ਤੁਰੰਤ ਬੈਂਕ ਨੂੰ ਸੂਚਿਤ ਕਰੋ।
- ਨਵਾਂ ਜਾਂ ਅੱਪਗਰੇਡ ਕਾਰਡ ਪ੍ਰਾਪਤ ਕਰਨ ਤੋਂ ਬਾਅਦ, ਪੁਰਾਣੇ ਕਾਰਡ ਨੂੰ ਤਿਰਛੇ ਰੂਪ ਵਿੱਚ ਕੱਟ ਕੇ ਰੱਦ ਕਰੋ।
- ਵਿਦੇਸ਼ ਯਾਤਰਾ ਤੋਂ ਬਾਅਦ PIN ਨੂੰ ਬਦਲਣ ਦੀ ਸਲਾਹ ਦਿੱਤੀ ਜਾਂਦੀ ਹੈ।
- ਆਪਣੇ PIN ਨੂੰ ਕਿਤੇ ਵੀ ਲਿਖਣ ਦੀ ਬਜਾਏ ਇਸਨੂੰ ਯਾਦ ਕਰਨ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰੋ।
- ਭੌਤਿਕ ਕੀਬੋਰਡਾਂ ਦੀ ਵਰਤੋਂ ਕਰਨ ਤੋਂ ਬਚੋ ਅਤੇ ਆਪਣੇ ਲੈਪ ਟਾਪ ਜਾਂ ਮੋਬਾਈਲ ਵਿੱਚ ਆਪਣੇ ਪ੍ਰਮਾਣ ਪੱਤਰਾਂ ਨੂੰ ਇਨਪੁਟ ਕਰਨ ਲਈ ਤਰਜੀਹੀ ਤੌਰ 'ਤੇ ਵਰਚੁਅਲ ਕੀਪੈਡ (ਚਿੱਤਰ ਦਿਖਾਓ) ਦੀ ਵਰਤੋਂ ਕਰੋ।
- ਕਿਤੇ ਵੀ ਆਪਣਾ PIN ਦਾਖਲ ਕਰਦੇ ਸਮੇਂ ਸਾਵਧਾਨ ਰਹੋ - ਜਿਵੇਂ ਕਿ ATM, ਕਾਰਡ ਮਸ਼ੀਨਾਂ, ਆਦਿ।

- ਕਿਸੇ ਵੀ ਕਾਰਡ ਗਤੀਵਿਧੀ 'ਤੇ ਲਗਾਤਾਰ ਚੇਤਾਵਨੀਆਂ ਲਈ ਆਪਣਾ ਈਮੇਲ ਅਤੇ ਫ਼ੋਨ ਨੰਬਰ ਅੱਪਡੇਟ ਕਰੋ। ਆਪਣੇ ਲੈਣ-ਦੇਣ ਅਤੇ ਖਰੀਦਦਾਰੀ 'ਤੇ ਨਜ਼ਰ ਰੱਖੋ ਅਤੇ ਕਿਸੇ ਵੀ ਅਸਾਧਾਰਨ ਲੈਣ-ਦੇਣ ਦੀ ਤੁਰੰਤ ਬੈਂਕ ਨੂੰ ਰਿਪੋਰਟ ਕਰੋ।
- ਇਹ ਯਕੀਨੀ ਬਣਾਓ ਕਿ ਤੁਹਾਡੇ ਕੋਲ ਤੁਹਾਡੇ ਕਾਰਡਾਂ ਲਈ ਵੇਰੀਫਾਇਡ ਬਾਈ ਵੀਜ਼ਾ (VbV) ਜਾਂ ਮਾਸਟਰਕਾਰਡ ਸੁਰੱਖਿਅਤ ਕੋਡ (MCSC) ਦੇ ਰੂਪ ਵਿੱਚ 3D ਸੁਰੱਖਿਅਤ ਹੈ। ਇਹ ਹੁਣ ਔਨਲਾਈਨ ਲੈਣ-ਦੇਣ ਲਈ ਜਰੂਰੀ ਹੈ ਅਤੇ ਸਾਰੇ ESFB ਕਾਰਡਾਂ ਕੋਲ ਇਹ ਹੈ।
- ਹਮੇਸ਼ਾ ਭੁਗਤਾਨ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਵੈੱਬਸਾਈਟ ਦੇ url ਨੂੰ ਚੈਕ ਕਰੋ ਕਿ ਇਹ ਇੱਕ ਸੁਰੱਖਿਅਤ ਹੈ। ਉਸੇ ਵੇਲੇ ਚੈਕ ਕਰੋ: ਇਹ ਯਕੀਨੀ ਬਣਾਓ ਕਿ ਤੁਹਾਡੇ ਬ੍ਰਾਊਜ਼ਰ 'ਤੇ ਲਾਕ ਆਈਕਨ (https://show lock symbol) ਹੈ, ਜੋ ਇਹ ਦਰਸਾਉਂਦਾ ਹੈ ਕਿ ਵੈੱਬਸਾਈਟ ਸੰਵੇਦਨਸ਼ੀਲ ਡਾਟਾ ਸੰਚਾਰਿਤ ਕਰਦੇ ਸਮੇਂ ਇੱਕ ਐਨਕ੍ਰਿਪਸ਼ਨ ਤਕਨਾਲੋਜੀ ਦੀ ਵਰਤੋਂ ਕਰ ਰਹੀ ਹੈ। ਲਾਕ 'ਤੇ ਕਲਿੱਕ ਕਰਨ 'ਤੇ ਤੁਸੀਂ ਡਿਜੀਟਲ ਸਰਟੀਫਿਕੇਟ ਅਤੇ ਵੈੱਬਸਾਈਟ ਨਾਲ ਸਬੰਧਤ ਹੋਰ ਵੇਰਵੇ ਦੇਖ ਸਕਦੇ ਹੋ। ਜੇਕਰ ਅਜਿਹੀ ਪੁਸ਼ਟੀ ਉਪਲਬਧ ਹੋਵੇ ਤਾਂ ਹੀ ਅੱਗੇ ਵਧੋ।
- ਸਾਈਟਾਂ ਦੇ url ਨੂੰ ਚੈਕ ਕਰੋ ਕਿ ਕੀ ਇਹ ਡੋਮੇਨ ਨਾਮ ਦੀ ਬਜਾਏ IP ਐਡਰੈੱਸ ਜਾਂ ਸੰਖਿਆਤਮਿਕ ਪਤਾ ਦਰਸਾਉਂਦਾ ਹੈ ਕਿਉਂਕਿ ਅਜਿਹੀਆਂ ਸਾਈਟਾਂ ਦਾ ਅਸਲ ਸਾਈਟ ਨਾ ਹੋਣ ਦੀ ਸੰਭਾਵਨਾ ਹੁੰਦੀ ਹੈ।

ਕੀ ਨਹੀਂ ਕਰਨਾ ਹੈ

- ਯਾਦ ਰੱਖੋ ਕਿ ਇਕੁਇਟਾਸ ਸਮਾਲ ਫਾਈਨੈਂਸ ਬੈਂਕ ਕਦੇ ਵੀ ਤੁਹਾਡੇ ਤੋਂ ਵੇਰਵਿਆਂ ਲਈ ਨਹੀਂ ਪੁੱਛੇਗਾ ਜਿਵੇਂ ਕਿ ਤੁਹਾਡੇ ਕਾਰਡ ਦੇ ਅੱਗੇ ਅਤੇ ਪਿੱਛੇ ਦੀ ਕਾਪੀ।
- ਜੇਕਰ ਕੋਈ ਬੈਂਕ ਦਾ ਪ੍ਰਤੀਨਿਧੀ ਹੋਣ ਦਾ ਦਾਅਵਾ ਕਰਦਾ ਹੈ ਅਤੇ ਤੁਹਾਡੇ ਕਾਰਡ ਦੀ ਮੰਗ ਕਰਦਾ ਹੈ, ਤਾਂ ਇਸਨੂੰ ਨਾ ਦਵੋ।
- ਆਪਣੇ ਕਾਰਡ ਦੇ ਵੇਰਵੇ ਜਿਵੇਂ ਕਿ ਕਾਰਡ ਨੰਬਰ, ਮਿਆਦ, CVV, PIN ਜਾਂ OTP ਕਦੇ ਵੀ ਕਿਸੇ ਨਾਲ ਸਾਂਝਾ ਨਾ ਕਰੋ, ਭਾਵੇਂ ਉਹ ਬੈਂਕ ਅਧਿਕਾਰੀ ਹੋਣ ਦਾ ਦਾਅਵਾ ਕਰਦਾ ਹੋਵੇ।
- ਔਨਲਾਈਨ ਵਪਾਰੀ ਵੈੱਬਸਾਈਟਾਂ 'ਤੇ ਆਪਣੇ ਕਾਰਡ ਦੇ ਵੇਰਵਿਆਂ ਨੂੰ ਸੇਵ ਨਾ ਕਰੋ।
- ਆਪਣੇ ਕਾਰਡਾਂ ਦੇ ਵੇਰਵਿਆਂ, ATM PIN, CVV, UPI PIN ਆਦਿ ਬਾਰੇ ਪੁੱਛਣ ਵਾਲੇ ਇਨਪੁਟ ਖੇਤਰਾਂ ਵਾਲੇ ਈਮੇਲਾਂ 'ਤੇ ਕਦੇ ਵੀ ਆਪਣਾ ਵੇਰਵਾ ਨਾ ਦਿਓ।
- ਗੈਰ-ਅਧਿਕਾਰਤ ਭੁਗਤਾਨ ਗੇਟਵੇ ਜਿਵੇਂ ਕਿ ਗੇਮਿੰਗ ਵੈੱਬਸਾਈਟਾਂ, ਪੋਰਨੋਗ੍ਰਾਫੀ ਵੈੱਬਸਾਈਟਾਂ, ਲਾਟਰੀ, ਜੂਏਬਾਜ਼ੀ ਅਤੇ ਹੋਰ ਬਹੁਤ ਕੁਝ 'ਤੇ ਆਪਣੇ ਕਾਰਡਾਂ ਦੀ ਵਰਤੋਂ ਕਰਨ ਤੋਂ ਬਚੋ।
- ਬੈਂਕ ਦੇ ਪ੍ਰਤੀਨਿਧੀ ਦੁਆਰਾ ਬਾਅਦ ਵਿੱਚ ਭਰੇ ਜਾਣ ਦੇ ਵਾਅਦੇ ਨਾਲ ਕਦੇ ਵੀ ਖਾਲੀ ਅਰਜ਼ੀ ਫਾਰਮ 'ਤੇ ਦਸਤਖਤ ਨਾ ਕਰੋ।

3. UPI

ਕੀ ਕਰਨਾ ਹੈ:

- ਵੈਧ ਪਲੇਟਫਾਰਮਾਂ ਜਿਵੇਂ ਕਿ ਗੂਗਲ ਪਲੇ ਸਟੋਰ ਆਦਿ ਰਾਹੀਂ UPI ਐਪਲੀਕੇਸ਼ਨ ਡਾਊਨਲੋਡ ਕਰੋ।
- ਆਪਣੀ ਖਾਸ ਬ੍ਰਾਂਚ/ਨੈੱਟ ਬੈਂਕਿੰਗ/UPI ਰਾਹੀਂ ਮੋਬਾਈਲ ਬੈਂਕਿੰਗ ਲਈ ਰਜਿਸਟਰ ਕਰੋ।
- ਇਹ ਯਕੀਨੀ ਬਣਾਓ ਕਿ ਤੁਸੀਂ ਪੂਰੀ ਗੋਪਨੀਯਤਾ ਨਾਲ ਲੈਂਗਇਨ ਕੀਤਾ ਹੈ ਅਤੇ UPI ਟ੍ਰਾਂਜੈਕਸ਼ਨ ਸ਼ੁਰੂ ਕੀਤਾ ਹੈ।
- ਲੈਣ-ਦੇਣ ਨੂੰ ਪੂਰਾ ਕਰਨ ਤੋਂ ਬਾਅਦ, ਯਕੀਨੀ ਬਣਾਓ ਕਿ ਤੁਸੀਂ ਐਪਲੀਕੇਸ਼ਨ ਤੋਂ ਸਫਲਤਾਪੂਰਵਕ ਲੈਂਗ ਆਊਟ ਹੋ ਗਏ ਹੋ।
- ਹਰੇਕ ਲੈਣ-ਦੇਣ ਲਈ, ਤੁਹਾਨੂੰ ਆਪਣੇ ਰਜਿਸਟਰਡ ਮੋਬਾਈਲ ਨੰਬਰ 'ਤੇ ਅਲਰਟ sms ਆਵੇਗਾ। ਜੇਕਰ ਤੁਹਾਨੂੰ ਆਪਣੇ ਖਾਤੇ ਵਿੱਚ ਕੋਈ ਅਣਅਧਿਕਾਰਤ UPI ਦਾ ਲੈਣ-ਦੇਣ ਮਿਲਦਾ ਹੈ, ਤਾਂ ਕਿਰਪਾ ਕਰਕੇ ਤੁਰੰਤ ਆਪਣੀ ਬ੍ਰਾਂਚ ਨਾਲ ਸੰਪਰਕ ਕਰੋ।
- ਕਿਸੇ ਵੀ ਅਸਫਲ ਲੈਣ-ਦੇਣ ਦੇ ਮਾਮਲੇ ਵਿੱਚ, ਕਿਰਪਾ ਕਰਕੇ ਵੈਬਸਾਈਟ ਅਤੇ ਐਪਲੀਕੇਸ਼ਨ 'ਤੇ ਦਿੱਤੇ ਗਏ ਏਸਕੇਲੇਸ਼ਨ ਮੈਟਰਿਕਸ ਨਾਲ ਸੰਪਰਕ ਕਰੋ।
- ਆਪਣਾ UPI ਐਪਲੀਕੇਸ਼ਨ ਪਾਸਵਰਡ ਅਤੇ UPI PIN / MPIN ਵਾਰ-ਵਾਰ ਬਦਲੋ।
- ਤੁਹਾਡੀ ਮੋਬਾਈਲ ਬੈਂਕਿੰਗ/UPI ਦੀ ਅਣਅਧਿਕਾਰਤ ਪਹੁੰਚ ਦੇ ਮਾਮਲੇ ਵਿੱਚ, ਕਿਰਪਾ ਕਰਕੇ ATM / ਇੰਟਰਨੈਟ ਬੈਂਕਿੰਗ / ਖਾਸ ਬ੍ਰਾਂਚ (ਜਾਂ ਕਿਰਪਾ ਕਰਕੇ ਸਾਡੇ ਸੰਪਰਕ ਕੇਂਦਰ ਨਾਲ ਸੰਪਰਕ ਕਰੋ) ਰਾਹੀਂ ਤੁਰੰਤ ਰਜਿਸਟਰ ਕਰੋ।
- ਜੇਕਰ ਤੁਹਾਡਾ ਮੋਬਾਈਲ ਫ਼ੋਨ ਗੁੰਮ / ਚੋਰੀ ਹੋ ਜਾਂਦਾ ਹੈ, ਤਾਂ ਕਿਰਪਾ ਕਰਕੇ ਖਾਸ ਬ੍ਰਾਂਚ / ਨੈੱਟ ਬੈਂਕਿੰਗ / ATM / ਸੰਪਰਕ ਕੇਂਦਰ ਰਾਹੀਂ ਤੁਰੰਤ ਆਪਣੀ ਮੋਬਾਈਲ ਬੈਂਕਿੰਗ ਰਜਿਸਟਰ ਕਰੋ।
- ਜੇਕਰ ਤੁਹਾਡਾ ਮੋਬਾਈਲ ਬੈਂਕਿੰਗ / ਮੋਬਾਈਲ ਨੰਬਰ ਤੁਹਾਡੀ ਬੇਨਤੀ ਤੋਂ ਬਿਨਾਂ ਰਜਿਸਟਰਡ/ਡੀਐਕਟੀਵੇਟ ਹੋ ਜਾਂਦਾ ਹੈ ਜਾਂ ਤੁਹਾਨੂੰ ਇਸ ਸਬੰਧ ਵਿੱਚ ਕਾਲ ਆਉਂਦੀ ਹੈ, ਤਾਂ ਹੋ ਸਕਦਾ ਹੈ ਕਿ ਕੋਈ ਡੁਪਲੀਕੇਟ SIM ਪ੍ਰਾਪਤ ਕਰਨ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰ ਰਿਹਾ ਹੋਵੇ/ ਤੁਹਾਡੇ ਪ੍ਰਮਾਣ ਪੱਤਰ ਜਿਵੇਂ ਕਿ mPIN/OTP (ਵਨ ਟਾਈਮ ਪਾਸਵਰਡ), ਆਦਿ ਨੂੰ ਚੋਰੀ ਕਰ ਸਕਦਾ ਹੈ। ਇਸ ਮਾਮਲੇ ਵਿੱਚ, ਕਿਰਪਾ ਕਰਕੇ ਤੁਰੰਤ ਆਪਣੀ ਖਾਸ ਬ੍ਰਾਂਚ ਨਾਲ ਸੰਪਰਕ ਕਰੋ।

ਕੀ ਨਹੀਂ ਕਰਨਾ ਹੈ:

- ਕਿਰਪਾ ਕਰਕੇ ਆਪਣੇ ਪਾਸਵਰਡ ਸਾਂਝੇ ਨਾ ਕਰੋ ਅਤੇ ਇਸਨੂੰ ਆਪਣੇ ਮੋਬਾਈਲ ਹੈਂਡਸੈੱਟ ਵਿੱਚ ਸਟੋਰ ਨਾ ਕਰੋ।
- ਕਦੇ ਵੀ ਕਿਸੇ ਨੂੰ ਤੁਹਾਡਾ ਆਪਣਾ ਐਪਲੀਕੇਸ਼ਨ ਪਾਸਵਰਡ ਜਾਂ UPI PIN / MPIN ਦਾਖਲ ਕਰਦੇ ਹੋਏ ਨਾ ਦੇਖਣ ਦਿਓ।
- ਕਦੇ ਵੀ ਅਜਿਹੀ ਐਪਲੀਕੇਸ਼ਨ / UPI PIN / MPIN ਦੀ ਵਰਤੋਂ ਨਾ ਕਰੋ ਜਿਸਦਾ ਆਸਾਨੀ ਨਾਲ ਅੰਦਾਜ਼ਾ ਲਗਾਇਆ ਜਾ ਸਕਦਾ ਹੋਵੇ ਜਿਵੇਂ: 1111/2222/1234/ ਜਨਮ ਸਾਲ, ਮੋਬਾਈਲ ਨੰਬਰ/ਟੈਲੀਫੋਨ ਨੰਬਰ।
- ਕਿਸੇ ਹੋਰ ਦੇ ਡਿਵਾਈਸ ਵਿੱਚ UPI ਐਪਲੀਕੇਸ਼ਨ ਨੂੰ ਇੰਸਟਾਲ ਨਾ ਕਰੋ ਅਤੇ ਨਾ ਹੀ ਵਰਤੋ।
- ਇਕੁਇਟਾਸ ਬੈਂਕ ਤੁਹਾਡੇ UPI / ਮੋਬਾਈਲ ਬੈਂਕਿੰਗ ਪਾਸਵਰਡਾਂ ਦੀ ਮੰਗ ਕਰਦੇ ਹੋਏ, ਕਾਲਾਂ/ਈਮੇਲਾਂ ਨਹੀਂ ਕਰਦਾ। ਜੇਕਰ ਕੋਈ ਕਾਲਰ ਸਾਡੇ ਬੈਂਕ / ਸੰਪਰਕ ਕੇਂਦਰ ਤੋਂ ਹੋਣ ਦਾ ਢੌਂਗ ਕਰਦਾ ਹੈ, ਤਾਂ ਕਿਰਪਾ ਕਰਕੇ ਅਜਿਹੀਆਂ ਬੇਨਤੀਆਂ ਨੂੰ ਸਵੀਕਾਰ ਨਾ ਕਰੋ ਕਿਉਂਕਿ ਉਹ ਧੋਖਾਧੜੀ ਵਾਲੀਆਂ ਸੰਸਥਾਵਾਂ ਹਨ।
- ਕਦੇ ਵੀ ਆਪਣੇ ਰਜਿਸਟਰਡ SIM ਕਾਰਡ ਅਤੇ ਡੈਬਿਟ ਕਾਰਡ ਨੂੰ ਨਾਲ ਨਾ ਰੱਖੋ, ਕਿਉਂਕਿ ਦੋਵਾਂ ਦੇ ਗੁੰਮ ਹੋਣ ਦਾ ਜੋਖਮ ਹੁੰਦਾ ਹੈ, ਜਿਸ ਨਾਲ ਕੋਈ ਵੀ ਤੁਹਾਡੇ ਖਾਤੇ ਤੱਕ ਪਹੁੰਚ ਪ੍ਰਾਪਤ ਕਰ ਸਕਦਾ ਹੈ।

பாதுகாப்பான மற்றும் பொறுப்பான வங்கிப் பயன்பாட்டுக்கான வழிகாட்டுதல்கள்

இது மொபைல் பேங்கிங் அல்லது இணைய பேங்கிங், கிளை அல்லது ATM மூலம் பணம் எடுக்கும் வகையிலும், நீங்கள் பாதுகாப்பான பேங்கிங் அனுபவத்தை உறுதி செய்ய சில அடிப்படை முன்னெச்சரிக்கைகளை கவனித்து பின்பற்ற வேண்டும். எங்களுக்கு, எக்விடாஸ் ஸ்மால் பைனான்ஸ் பேங்கில் (ESFB) பாதுகாப்பான பேங்கிங் நடைமுறையில் நம்பிக்கை உள்ளது. எச்சரிக்கைகள் எதிர்பாராத பெறுநர்களுக்குச் செல்லாமல் இருக்க, உங்கள் தொடர்பு விவரங்கள் எங்கள் தரவுத்தளத்தில் புதுப்பிக்கப்படுவதை உறுதி செய்வது முக்கியமாகும். நீங்கள் வெளிநாடு செல்வதாக இருந்தால், உங்கள் மின்னஞ்சல் ID வங்கியில் பதிவு செய்யப்பட்டிருப்பதை உறுதி செய்யவும்.

செய்ய வேண்டியவை மற்றும் செய்யக்கூடாதவைகளின் பட்டியல்:

உங்கள் கணக்கு/கார்டு தடுக்கப்பட்டுள்ளதால், உங்கள் KYC விவரங்களைப் புதுப்பித்தல், அதிகரித்த கிரெடிட் கார்டு வரம்பைப் பெறுதல், கேஷ்பேக் புள்ளிகள்/வெகுமதிகளைப் பெறுதல் அல்லது கடன்/டாப்-அப் ஆகியவற்றைப் பெறுதல் போன்ற காரணங்களால் அழைப்புகள்/ SMS/ மின்னஞ்சல்கள் மூலம் உங்களைக் குறிவைக்கும் மோசடி செய்பவர்களிடம் ஜாக்கிரதையாக இருங்கள். இதுபோன்ற ஏமாற்று வேலைகளில் சிக்காதீர்கள்.

இதுபோன்ற ஏமாற்று வேலைகளில் சிக்காதீர்கள்.

உங்களைப் பாதுகாத்துக் கொள்ளவும், ஆன்லைனில் பாதுகாப்பாக இருக்கவும் செய்ய வேண்டியவை மற்றும் செய்யக்கூடாதவை இங்கே:

செய்ய வேண்டியவை:

- வங்கியின் தொடர்பு விவரங்களுக்கு எப்போதும் அதிகாரப்பூர்வ இணையதளத்தைப் பார்க்கவும்
- எப்போதும் உங்கள் தொடர்பு விவரங்களை வங்கியுடன் புதுப்பித்து வைத்திருக்கவும் மற்றும் பரிமாற்ற அறிவிப்புகளை பெற பதிவு செய்யவும்.
- உங்கள் கணினி/மொபைலில் உண்மையான ஆன்டி-வைரஸ் மற்றும் ஆன்டி-மால்வேர் மென்பொருளை நிறுவி அதை புதுப்பித்து வைத்திருங்கள்
- உங்கள் கடவுச்சொல்லை வலுவாகவும் தனித்துவமாகவும் வைத்திருக்கவும்.
- உங்கள் கார்டு எண், கடவுச்சொற்கள் அல்லது பிற தனிப்பட்ட/முக்கியத் தகவல்களைச் சேமிப்பதைத் தவிர்க்க, உங்கள் ப்ரௌசரின் தன்னியக்க அமைப்புகளை முடக்கவும்.
- ப்ளே ஸ்டோர் அல்லது ஆப் ஸ்டோரிலிருந்து எந்தவொரு ஆப்களைப் பதிவிறக்கம் செய்யும் முன் கவனமாக இருங்கள்.
- பரிவர்த்தனை செய்யும் போது உங்கள் இணைய ப்ரௌசரின் ஸ்டேட்டஸ் பாரில் பேட்லாக் அடையாளம் அல்லது https-ஐப் பார்க்கவும்.
- எப்போதும் உங்கள் தனிப்பட்ட தகவல்களை பகிருமாறு கேட்கும் செய்திகளில் சொல் பிழைகள் இருக்கிறதா எனப் பாருங்கள், ஏனெனில் அவை மோசடி செய்திகளை அடையாளம் காண உதவும்.

செய்யக்கூடாதவை

- PIN, கடவுச்சொற்கள், OTP அல்லது அட்டை விவரங்கள் போன்ற முக்கியமான விவரங்களை யாருடனும் பகிர வேண்டாம்
- உங்கள் வங்கிக் கணக்கை அணுகும் போது பொது வை-பை அல்லது இலவச VPN/பொது கணினிகளை தவிர்க்க வேண்டும்.
- அறியப்படாத ஆதாரங்கள்/அனுப்புநர் ID-களில் இருந்து பெறப்பட்ட இணைப்புகளைக் கிளிக் செய்ய வேண்டாம்.
- 123456, பெயர்கள், பிறந்த தேதி போன்ற பொதுவாக பயன்படுத்தப்படும் கடவுச்சொற்களைப் பயன்படுத்துவதை தவிர்க்கவும்
- உங்கள் வங்கிக் கடவுச்சொல்லை எழுதுவதையும் ப்ரௌசரில் சேமிப்பதையும் தவிர்க்கவும்
- எனிடெஸ்க் போன்ற தொலைதூர பகிர்வு ஆப்-களைப் பதிவிறக்க வேண்டாம்
- UPI மூலம் பணத்தைப் பெற QR குறியீட்டை ஸ்கேன் செய்யாதீர்கள் அல்லது PIN அல்லது OTP-ஐ உள்ளிடாதீர்கள்.
- ATM-இல் அறிமுகமில்லாதவர்களின் உதவியைப் பெற வேண்டாம்.

நினைவில் கொள்ளுங்கள்:

ESFB அல்லது அதன் பணியாளர்கள்/பிரதிநிதிகள் உங்கள் தனிப்பட்ட கணக்கு தகவலை ஒருபோதும் கேட்க மாட்டார்கள்.

1. கடவுச்சொல் பாதுகாப்பு

பல கணக்குகளுக்கு ஒரே அல்லது ஒத்த கடவுச்சொற்களை மக்கள் பயன்படுத்துவதை ஹேக்கர்கள் அறிவார்கள். உங்கள் வங்கிக் கடவுச்சொல், அமேசான் கடவுச்சொல் மற்றும் மின்னஞ்சல் கடவுச்சொல் ஆகியவை ஒரே மாதிரியாக இருந்தால், ஒரு தளத்தில் உள்ள பாதிப்பு மற்றவற்றிற்கு ஆபத்தை ஏற்படுத்தும்.

கடவுச்சொல்லை யூகிப்பதை எளிதாக்குவது எது?

தரவு மீறலில் இருந்து மின்னஞ்சல் முகவரிகளின் பட்டியலை ஹேக்கர்கள் பெற்றவுடன், இதன் மூலம் அவர்களுக்கு நல்ல தொடக்கம் ஏற்படுகிறது. அங்கிருந்து, அவர்கள் தங்களுக்கு விருப்பமான இணையதளத்தைத் தேர்ந்தெடுத்து, மிகவும் பிரபலமான கடவுச்சொற்களுடன் பட்டியலிடப்பட்ட மின்னஞ்சல்களை முயற்சிக்கிறார்கள். இவ்வாறு முயற்சிப்பதன் மூலம் ஒரு சில கணக்குகளில் சேர வாய்ப்புகள் உள்ளன.

உங்கள் கணக்கு ஹேக் செய்யப்படுவதைத் தவிர்க்க, நீங்கள் தவிர்க்க வேண்டிய கடவுச்சொற்களின் பட்டியல் இங்கே:

- எல்லா கடவுச்சொற்களிலும் மிகவும் பொதுவான 123456-ஐப் பயன்படுத்துவதைத் தவிர்க்கவும்.
- p@ssw0rd! போன்ற சின்னத்திற்கு பதிலாக ஒரு எழுத்தை மாற்றுவதும் ஹேக்கர்கள் நன்கு அறிந்த ஒரு தந்திரமாகும். கடவுச்சொல் கிராக்கிங் நிரல்கள் ஒவ்வொரு மொழியிலும் இந்த கலவைகளின் ஒவ்வொரு வகையையும் கொண்டிருக்கின்றன.
- அசாதாரணமான ஒன்றைப் பயன்படுத்தவும், உங்களுக்குப் பிடித்த விளையாட்டுக் குழுவின் பெயர்கள் அல்லது பாப் கலாச்சாரக் குறிப்புகளைப் பயன்படுத்துவதைத் தவிர்க்கவும்.
- சன்ஷைன் அல்லது குரங்கு போன்ற ஒற்றைச் சொற்களைப் பயன்படுத்தி இறுதியில் ஒரு எண் அல்லது நிறுத்தற்குறியைச் சேர்ப்பது வலுவான கடவுச்சொல்லை உருவாக்காது. அதற்கு பதிலாக, உங்கள் கடவுச்சொல்லை வலிமையாக்க ஒரு சொற்றொடர் அல்லது வாக்கியத்தைப் பயன்படுத்தவும்.
- 111111, abc123 அல்லது 654321 போன்ற பொதுவான பேட்டர்களைப் பயன்படுத்துவதைத் தவிர்க்கவும்.

கடவுச்சொல்லை வலிமையாக்குவது எது?

- தொடர்பில்லாத சொற்களை இணைத்தல்.
- முழுச் சொற்றொடரைப் பயன்படுத்துதல் மற்றும் சில எழுத்துக்களை சிறப்பு எழுத்துகள் மற்றும் எண்களாக மாற்றுதல்.
- பெரிய மற்றும் சிறிய எழுத்துக்கள், குறியீடுகள் மற்றும் எண்களின் கலவையைப் பயன்படுத்தவும்.
- உங்கள் கடவுச்சொல் எவ்வளவு நீளமாக இருக்கிறதோ, அவ்வளவு வலிமையானது.
- ஒவ்வொரு கணக்கிற்கும் வெவ்வேறு கடவுச்சொற்களைப் பயன்படுத்தவும்.

2. டெபிட் கார்டுகள்

டெபிட் மற்றும் கிரெடிட் கார்டு மோசடிகளைத் தவிர்க்கவும், பாதுகாப்பான மற்றும் தொந்தரவு இல்லாத வங்கி அனுபவத்தைப் பெறவும் உதவும் சில 'செய்ய வேண்டியவை மற்றும் செய்யக்கூடாதவை' இங்கே கொடுக்கப்பட்டுள்ளன.

செய்ய வேண்டியவை:

- வரவேற்பு கிட் கிடைத்ததும், உறை சீல் வைக்கப்பட்டுள்ளதா என்பதை உறுதிசெய்யவும். ஏதேனும் முறைகேடு இருந்தால், உடனடியாக வங்கியைத் தொடர்புகொள்ளவும்.
- அட்டையின் பின்புறத்தில் உடனடியாக கையொப்பமிடுங்கள்.
- கார்டைப் பெற்ற பிறகு அதன் PIN-ஐ மாற்றவும். முழுமையான பாதுகாப்பிற்காக ஆறு மாதங்களுக்கு ஒரு முறை இதைச் செய்வது நல்லது.
- உங்கள் அட்டைகளை பாதுகாப்பாக வைத்திருங்கள். இழப்பு அல்லது திருட்டு ஏற்பட்டால், உடனடியாக வங்கிக்குத் தெரிவிக்கவும்.
- புதிய அல்லது மேம்படுத்தப்பட்ட கார்டைப் பெற்ற பிறகு, பழைய கார்டை குறுக்காக வெட்டி நிராகரிக்கவும்.
- வெளிநாட்டுப் பயணத்திற்குப் பிறகு PIN-ஐ மாற்றுவது நல்லது.
- உங்கள் PIN-ஐ எங்கும் எழுதுவதற்குப் பதிலாக அதை நினைவில் வைத்துக்கொள்ள முயற்சிக்கவும்.
- விசைப்பலகைகளைப் பயன்படுத்துவதைத் தவிர்க்கவும் மற்றும் உங்கள் லேப் டாப் அல்லது மொபைலில் உங்களின் சான்றுகளை உள்ளிட, விர்ச்சுவல் விசைப்பலகையைப் (படத்தைக் காட்டு) பயன்படுத்தவும்.
- உங்கள் PIN-ஐ எந்த இடத்திலும் உள்ளிடும்போது கவனமாக இருங்கள் - ATM, கார்டு இயந்திரங்கள் போன்றவை.
- எந்தவொரு கார்டு நடவடிக்கையிலும் நிலையான விழிப்பூட்டல்களுக்கு உங்கள் மின்னஞ்சல் மற்றும் தொலைபேசி எண்ணைப் புதுப்பிக்கவும். உங்கள் பரிவர்த்தனைகள் மற்றும் வாங்குதல்களைக் கண்காணித்து, ஏதேனும் வழக்கத்திற்கு மாறான பரிவர்த்தனைகள் இருந்தால் உடனடியாக வங்கிக்குத் தெரிவிக்கவும்.

- உங்கள் கார்டுகளுக்கு 3D பாதுகாப்பு வெரி.ஃபைடு பை விசா (VbV) அல்லது மாஸ்டர்கார்டு செக்யூர் கோடு (MCSC) இருப்பதை உறுதி செய்யவும். இப்போது இது ஆன்லைன் பரிமாற்றங்களுக்கு கட்டாயமாக உள்ளது, மேலும் அனைத்து ESFB கார்டுகளிலும் இது உள்ளது.
- பணம் செலுத்துவதற்கு முன்னர், இணையதளத்தின் URL-ஐ எப்பொழுதும் சரிபார்த்து, அது பாதுகாப்பானது என்பதை உறுதி செய்யவும். விரைவான சரிபார்ப்பு: உங்கள் பிரௌசரில் ஒரு லாக் ஐகான் (https://show lock symbol) இருப்பதை உறுதி செய்யவும், இது அந்த இணையதளம் உண்மையான தரவை பரிமாறும்போது குறியாக்க தொழில்நுட்பத்தைப் பயன்படுத்துவதை குறிக்கின்றது. லாக் ஐகான்-ஐ கிளிக் செய்வதன் மூலம், நீங்கள் டிஜிட்டல் சான்றிதழும், இணையதளத்தின் தொடர்புடைய பிற விவரங்களையும் பார்க்க முடியும். இப்படியான சரிபார்ப்பு கிடைத்தவுடன் மட்டுமே தொடரவும்
- டொமைன் பெயருக்குப் பதிலாக IP முகவரி அல்லது எண் முகவரியைக் காட்டினால், தளங்களின் URL-ஐச் சரிபார்க்கவும், ஏனெனில் அத்தகைய தளங்கள் உண்மையான தளமாக இருக்காது.

செய்யக்கூடாதவை

- எக்விடாஸ் ஸ்மால் பைனான்ஸ் பேங்க் உங்கள் கார்டின் முன் மற்றும் பின் நகல் போன்ற விவரங்களை உங்களிடம் கேட்காது என்பதை நினைவில் கொள்ளுங்கள்.
- யாரேனும் வங்கிப் பிரதிநிதி என்று கூறிக்கொண்டு உங்கள் அட்டையைக் கேட்டால், அதை ஒப்படைக்க வேண்டாம்.
- கார்டு எண், காலாவதி, CVV, PIN அல்லது OTP போன்ற உங்களின் கார்டு விவரங்களை அவர்கள் வங்கி அதிகாரிகள் எனக் கூறிக்கொண்டாலும், யாருடனும் பகிர வேண்டாம்.
- ஆன்லைன் வணிக இணையதளங்களில் உங்கள் கார்டு விவரங்களைச் சேமிக்க வேண்டாம்.
- உங்கள் கார்டுகளின் விவரங்கள், ATM PIN, CVV, UPI PIN போன்றவற்றைக் கேட்கும் உள்ளீட்டு புலங்களைக் கொண்ட மின்னஞ்சல்களில் உங்கள் விவரங்களை ஒருபோதும் உள்ளிட வேண்டாம்.
- கேமிங் இணையதளங்கள், ஆபாச இணையதளங்கள், லாட்டரி, சூதாட்டம் மற்றும் பலவற்றின் அங்கீகரிக்கப்படாத கட்டண நுழைவாயில்களில் உங்கள் கார்டுகளைப் பயன்படுத்துவதைத் தவிர்க்கவும்.
- வெற்று விண்ணப்பப் படிவத்தில் வங்கிப் பிரதிநிதியால் பின்னர் நிரப்பப்படும் என்ற வாக்குறுதியுடன் கையெழுத்திட வேண்டாம்.

3. UPI

செய்ய வேண்டியவை:

- சரியான தளங்களில் இருந்து, உதாரணமாக கூகுள் பிளே ஸ்டோரின் மூலம் UPI பயன்பாட்டை பதிவிறக்கம் செய்யவும்
- உங்கள் அடிப்படை கிளை / நெட் பேங்கிங் / UPI வழியாக மொபைல் பேங்கிங்கிற்கு பதிவு செய்யவும்.
- நீங்கள் உள்நுழைந்து UPI பரிவர்த்தனையை முழுத் தனியுரிமையில் தொடங்குவதை உறுதிசெய்து கொள்ளவும்.
- பரிவர்த்தனையை முடித்த பிறகு, நீங்கள் விண்ணப்பத்திலிருந்து வெற்றிகரமாக வெளியேறிவிட்டீர்கள் என்பதை உறுதிப்படுத்திக் கொள்ளுங்கள்.
- ஒவ்வொரு பரிவர்த்தனைக்கும், உங்கள் பதிவு செய்யப்பட்ட மொபைல் எண்ணுக்கு SMS எச்சரிக்கையைப் பெறுவீர்கள். உங்கள் கணக்கில் அங்கீகரிக்கப்படாத UPI பரிவர்த்தனை ஏதேனும் இருந்தால், உடனடியாக உங்கள் கிளையைத் தொடர்புகொள்ளவும்.
- ஏதேனும் தோல்வியுற்ற பரிவர்த்தனைகள் ஏற்பட்டால், இணையதளம் மற்றும் பயன்பாட்டில் கொடுக்கப்பட்டுள்ள விரிவாக்க மேட்ரிக்ஸைப் பயன்படுத்துங்கள்.
- உங்களின் UPI பயன்பாட்டு கடவுச்சொல் மற்றும் UPI PIN / MPIN-ஐ அடிக்கடி மாற்றவும்.
- உங்கள் மொபைல் பேங்கிங் /UPI-இன் அங்கீகரிக்கப்படாத அணுகல் ஏற்பட்டால், தயவுசெய்து ATM / இணைய வங்கி / அடிப்படை கிளை (அல்லது எங்கள் தொடர்பு மையத்தைத் தொடர்பு கொள்ளவும்) மூலம் உடனடியாகப் பதிவு செய்யுங்கள்.
- உங்கள் மொபைல் தொலைந்து போனால் / திருடப்பட்டால், தயவு செய்து உங்கள் மொபைல் பேங்கிங்கை உடனடியாக அடிப்படை கிளை / நெட் பேங்கிங் / ATM / தொடர்பு மையம் மூலம் பதிவு செய்யவும்.
- உங்கள் மொபைல் வங்கி / மொபைல் எண் உங்கள் கோரிக்கையின்றி பதிவுசெய்யப்பட்டாலோ அல்லது செயலிழக்கச் செய்யப்பட்டாலோ அல்லது இது தொடர்பாக உங்களுக்கு அழைப்பு வந்தாலோ, யாரேனும் ஒருவர் டூப்ளிகேட் SIM-ஐப் பெற முயற்சிக்கலாம் / mPIN/OTP (ஒருமுறை கடவுச்சொல்) போன்ற உங்களின் சான்றுகளைத் திருடலாம். இந்த வழக்கில், உடனடியாக உங்கள் அடிப்படை கிளையை தொடர்பு கொள்ளவும்.

செய்யக்கூடாதவை:

- தயவு செய்து உங்கள் கடவுச்சொற்களை பகிர வேண்டாம் / உங்கள் மொபைல் கைபேசியில் சேமிக்க வேண்டாம்.
- உங்கள் பயன்பாட்டு கடவுச்சொல் அல்லது UPI PIN / MPIN-ஐ உள்ளிடுவதை யாரும் பார்க்க அனுமதிக்காதீர்கள்.
- எளிதில் யூகிக்கக்கூடிய பயன்பாடு/ UPI PIN / MPIN-ஐ ஒருபோதும் பயன்படுத்த வேண்டாம் எ.கா: 1111/2222/1234/ பிறந்த ஆண்டு, மொபைல் எண்/தொலைபேசி எண்.
- வேறொருவரின் சாதனத்தில் UPI ஆப்ஸை நிறுவி பயன்படுத்த வேண்டாம்.
- எக்விடாஸ் பேங்க் உங்கள் UPI / மொபைல் பேங்கிங் கடவுச்சொற்களைக் கேட்டு அழைப்புகள் / மின்னஞ்சல்களைச் செய்யாது. எங்கள் வங்கி/தொடர்பு மையத்தில் இருந்து அழைப்பவர் யாரேனும் இருப்பதாகக் காட்டிக் கொண்டால், அத்தகைய கோரிக்கைகள் மோசடி நிறுவனங்களாக இருப்பதால், தயவுசெய்து அதைப் பெற வேண்டாம்.
- உங்கள் பதிவு செய்யப்பட்ட SIM கார்டு மற்றும் டெபிட் கார்டு இரண்டையும் இழக்கும் அபாயம் இருப்பதால், அவற்றை ஒன்றாக எடுத்துச் செல்ல வேண்டாம். உங்கள் கணக்கிற்கான அணுகலைப் பெறுவதற்கு இது உதவும்.

સલામત અને જવાબદારીપૂર્વકની બેંકિંગ ઉપયોગિતા માર્ગદર્શિકા

મોબાઇલ બેંકિંગ હોય કે ઇન્ટરનેટ બેંકિંગ શાખામાંથી ઉપાડવાના હોય કે ATM માંથી ઉપાડવાના હોય કોઈએ પણ કાળજી અને સાવધાની રાખવાની તથા સલામત બેંકિંગ અનુભવાય તેની ખાતરી રાખવા કેટલીક પાયાની સાવધાન કરતી ચેતવણીઓ પાળવાની જરૂર છે. અમે ઇક્વિટાસ સ્મોલ ફાઇનાન્સ બેંક (ESFB) ખાતે સલામત બેંકિંગમાં માનીએ છીએ. આ એ ચોક્કસ બનાવવાથી શરૂ થાય છે કે તમારા સંપર્કની વિગતો અમારા ડેટાબેઝ અપડેટ થયેલો છે જેથી કરીને સાવધાનીની સૂચના (એલર્ટ) અનિચ્છનીય પ્રાપ્તકર્તાને ન જાય. એવા સંજોગોમાં કે તમે વિદેશ મુસાફરી કરી રહ્યા છો ત્યારે ખાતરી રાખો કે તમારો ઇ-મેઈલ ID બેન્ક સાથે રજિસ્ટર્ડ થયેલ છે.

આ કરવું અને આ ન કરવું તેની સૂચિ:

એવા છેતરપિંડી કરનારાઓથી સાવધાન રહો જેઓ તમને કોલ / SMS / ઈમેઈલ મારફત KYC ની વિગતો અપડેટ કરવાના બહાના હેઠળ ટાર્ગેટ બનાવે છે જેમ કે તમારું ખાતું /કાર્ડ બ્લોક થઈ ગયું છે, વધારાની ક્રેડિટ કાર્ડ લિમિટ પ્રાપ્ત કરવી, કેશ બેક પોઈન્ટસ /ઈનામ મેળવો વ્રધ્ધિ કરેલ રકમવાળી લોન પ્રાપ્ત કરવી / લોન ટોપ-અપ કરવી. આવા કૌભાંડનો શિકાર બનશો નહીં.

આવા કૌભાંડનો શિકાર બનશો નહીં.

તમારા જાતને સુરક્ષિત રાખવા અને ઓનલાઈન સલામત રહેવા આ રહ્યું - શું કરવું અને શું ન કરવું:

આટલું કરો

- બેન્કની સંપર્કની વિગતો માટે હંમેશા અધિકૃત હોય તેવી વેબસાઇટની મુલાકાત લો.
- હંમેશા તમારા સંપર્કની વિગતો બેન્ક સાથે અપડેટ થયેલી રાખો અને ટ્રાન્જકશન એલર્ટ મેળવવા માટે સબ્સક્રાઈબ કરો.
- તમારા કોમ્પ્યુટ/મોબાઈલ પર જેન્યૂન એન્ટિ-વાઇરસ અને એન્ટિ-માલવેર સૉફ્ટવેર ઇન્સ્ટોલ કરો અને તેને અપડેટ કરેલા રાખો.
- તમારો પાસવર્ડ સ્ટ્રોંગ અને યુનિક રાખો.
- તમારો કાર્ડ નંબર/પાસવર્ડ કે અન્ય અંગત અને સંવેદનશીલ માહિતી સ્ટોર કરવાનું નિવારવા તમારા બ્રાઉઝરનું ઓટોકંપલેટ સેટિંગ બંધ કરી દો.
- પ્લે સ્ટોર કે એપ સ્ટોરમાંથી કોઈપણ એપ ડાઉનલોડીંગ કરતા પહેલા સાવધાન રહો.
- ટ્રાન્જકશન વખતે તમારી વેબબ્રાઉઝરના સ્ટેટસ બારમાં પેડલોક સાઇન કે http માટે જુઓ.
- મેસેજોમાં હમેશા સ્પેલિંગ ભૂલનું ધ્યાન રાખો કે જેમાં સંવેદનશીલ વિગતો શેર કરવા કહેતું હોય, કારણ કે આ તમને બનાવટી બાબત ઓળખવામાં મદદ કરશે.

આટલું ન કરો

- કોઈ સાથે કદી સંવેદનશીલ વિગતો જેવી કે PIN, પાસવર્ડ, OTP કે કાર્ડની વિગતો શેર ન કરો.
- તમારા બેન્ક અકાઉન્ટને એક્સેસ કરતી વખતે જાહેર ઉપયોગના વાઇ-ફાઈ કે ફ્રી VPN/જાહેર ઉપયોગના કોમ્પ્યુટર્સનો ઉપયોગ કરવાનું નિવારો.
- અજાણ્યા સોર્સ/મોકલનારના ID માંથી મળેલી લિંક પર ક્લિક કરશો નહીં.
- સર્વસામાન્યરીતે વપરાતા પાસવર્ડ, જેવા કે 123456, નામ, બર્થ-ડે થી દૂર રહો.
- તમારા બેંકિંગ પાસવર્ડને ગમે ત્યાં લખવાનું અને બ્રાઉઝર પર સેવ કરવાનું ટાળો.
- રિમોટ શેરિંગ એપ્સ, એટલે કે એનીડેસ્ક ડાઉનલોડ ન કરો.
- QR કોડ સ્કેન ન કરો કે કોઈ PIN કે UPI મારફત પૈસા પ્રાપ્ત કરવા OTP એન્ટર ન કરો.
- ATM ખાતે અજાણ્યાની મદદ ન લો.

યાદ રાખો:

ESFB કે તેના કર્મચારીઓ/પ્રતિનિધિઓ તમારા અંગત ખાતાની માહિતી કદી પૂછશે નહીં.

1. પાસવર્ડની સુરક્ષા

હેકર્સ સાવધાન હોય છે કે લોકો વિવિધ ખાતાઓ માટે એકસરખો કે મળતો આવતો પાસવર્ડ વાપરે છે. જો તમારો બેંકિંગ પાસવર્ડ, અમેઝૉન પાસવર્ડ અને ઈમેઈલ પાસવર્ડ એક જ સરખા હોય તો પછી એક સાઇટની ભેદ્યતા બીજી સાઇટોને જોખમમાં મુકી શકે.

પાસવર્ડનું અનુમાન કરવાનું સરળ શું શું બનાવે છે?

એક વખત હેકર્સ ડેટા બ્રિચમાંથી ઇ-મેઈલ એડ્રેસોની એક સૂચિ મેળવી લે છે તો પછી તેમને શુભ શરૂઆત મળી જ ગઈ છે. ત્યાંથી તેઓને માત્ર તેમની પસંદગીની વેબસાઇટ ઉપાડી લેવાનું રહે છે અને સૂચિ બનાવેલા ઇ-મેઇલ્સના જાણીતા બનેલા પાસવર્ડ દ્વારા ચાદીના ઇ-મેઈલ પર અજમાયશ કરશે. અહીં કેટલાય ખાતાઓમાં દાખલ થવાના મોકા રહેલ છે.

એકાઉન્ટ હેક ન થાય તે નિવારવા, અહી કેટલાક ખરાબમથી ખરાબ પાસવર્ડ ની સૂચિ આપેલી છે જે તમારે ટાળવા જોઈએ:

- 123456, બધા પાસવર્ડ માંથી સૌથી સામાન્ય પાસવર્ડ છે તેનો ઉપયોગ ટાળો.
- એક અક્ષરને સિમ્બોલમાં લઈ જવો, જેમ કે p@ssw0rd! પણ એક સ્વાભાવિક ટ્રિક છે કે જે હેકર્સ જાણે છે.પાસવર્ડ ક્રેકીંગ પ્રોગ્રામ દરેક ભાષામાં આ પ્રકારના કોંબીનેશન્સ (સંયોજનો) ધરાવે છે.
- કઇક અસ્પષ્ટ હોય તેનો ઉપયોગ કરો અને તમારી મનપસંદ રમતોની ટીમના નામનો કે પોપ કલ્ચર રેફરન્સોનો ઉપયોગ નિવારો.
- એકાક્ષરનો ઉપયોગ કરવો જેવા કે સનશાઈન કે મંકી અને અંતમાં કોઈ નંબર કે વિરામચિહ્ન ઉમેરવું તે કોઈ સ્ટ્રોંગ પાસવર્ડ નથી બનાવતો. તેને બદલે, તમારે પાસવર્ડ સ્ટ્રોંગ બનાવવા એક કહેવત કે ફ્રેઝ/માર્મિકવચન વાપરવું.
- સર્વસામાન્ય પેટર્ન જેવી કે 111111, abc123 કે 654321 વાપરવાનું ટાળો.

એક પાસવર્ડને સ્ટ્રોંગ શું શું બનાવે છે?

- અસબંધિત શબ્દો સયોજવા.
- સંપૂર્ણ શબ્દસમૂહનો ઉપયોગ કરવો અને કેટલાક અક્ષરોને વિશિષ્ટ અક્ષરો અને સંખ્યાઓમાં બદલવું.
- અપર અને લોઅર કેસના અક્ષરોના કોંબીનેશન, સિમ્બોલ્સ અને સંખ્યાનો ઉપયોગ કરવો.
- જેટલો લાંબો પાસવર્ડ એટલો મજબૂત પાસવર્ડ.
- દરેક એકાઉન્ટ માટે જુદો પાસવર્ડ વાપરવો.

2. ડેબિટ કાર્ડ્સ

અહીં કેટલીક 'શું કરવું અને શું ન કરવું' ની બાબતો છે, જે તમને ડેબિટ અને ક્રેડિટ કાર્ડની છેતરપિંડીથી બચવામાં અને સલામત અને મુશ્કેલીરહિત બેંકિંગ અનુભવ માણવામાં મદદ કરશે.

આટલું કરો:

- સ્વાગત કીટ પ્રાપ્ત કર્યા પછી, ખાતરી કરો કે પરબિડીયું સીલ થયેલ છે. જો કોઈ છેડછાડનો સંકેત મળે તો તરત જ બેંકનો સંપર્ક કરો.
- કાર્ડના પાછલા ભાગ પર તરત જ સહી કરો.
- કાર્ડ મળ્યા પછી તેનો PIN બદલો. આદર્શ રીતે, સંપૂર્ણ સુરક્ષા માટે દર છ મહિને આવું કરો.
- તમારા કાર્ડ સુરક્ષિત રીતે રાખો. ગુમ કે ચોરીના કિસ્સામાં તરત જ બેંકને જાણ કરો.
- નવું અથવા અપગ્રેડ કરેલું કાર્ડ પ્રાપ્ત કર્યા પછી, જૂના કાર્ડને એક ખુણેથી બીજા ખૂણા સુધી કાપીને નિકાલ કરો.
- વિદેશ પ્રવાસ પછી PIN બદલવાની સલાહ આપવામાં આવે છે.
- તમારો PIN ગમે ત્યાં લખવાને બદલે તેને યાદ રાખવાનો પ્રયાસ કરો.
- ખરીદેલા કી-બોર્ડનો ઉપયોગ કરવાનું ટાળો અને તમારા લેપ ટોપ કે મોબાઈલમાં તમારા ક્રેડેન્શિયલ્સને ઇનપુટ કરવા માટે વર્ચ્યુઅલ (કોમ્પ્યુટરમાં આવતું) કી પેડ (છબી બતાવો) નો ઉપયોગ ઈચ્છવા યોગ્ય છે.
- કોઈ પણ જગ્યાએ-ATM, કાર્ડ મશીનો વિ.-પર PIN દાખલ કરવામાં સાવધાન રહો.
- કોઈપણ કાર્ડ એક્ટિવિટી માટે તમારો ઈમેલ અને ફોન નંબર સતત એલર્ટ્સ માટે અપડેટ કરો. તમારા વ્યવહારો અને ખરીદીઓ પર નજર રાખો અને અસામાન્ય ટ્રાંઝકશન (વ્યવહાર) હોય તો બેંકને તુંરત જ જાણ કરો.

- ચોકસાઇ રાખો કે તમારી પાસે તમારા કાર્ડ માટે 3D સિકયુર કોડ, વિસા (VbV) અથવા માસ્ટકાર્ડ સિકયુર કોડ (MCSC) દ્વારા ખરાઈ કરેલું હોય તેવા રૂપમાં છે. આ હાલ ઓનલાઈન ટ્રાન્જકશન માટે આ આદેશ છે અને આ બધા ESFB પાસે છે.
- હમેશા એક ચૂકવણું કરતાં પહેલા વેબસાઇટનો URL એક કરો કે આ એક સલામત વેબસાઇટ છે તેની ચોક્કસાઈ કરવા .ક્વીક ચેક: ચોક્કસાઈ કરો કે તમારા બ્રાઉઝર પર લોક આઇકોન (https://show lock symbol) છે, જે સૂચવે છે, આ વેબસાઇટ એનક્રીપ્શન ટેક્નોલૉજીનો ઉપયોગ કરે છે. લોક પર ક્લિક કરતાં તમે ડીજીટલ સર્ટિફિકેટ તથા વેબસાઈટ સંબધિત અન્ય વિગતો જોઈ શકશો, આવું વેરિફિકેશન ઉપલબ્ધ હોય તો જ આગળ વધો.
- વેબસાઇટોનું URL ચેક કરો, જો તે ડોમેઈન નેમને બદલે IP એડ્રેસ કે ન્યૂમેંટિકલ એડ્રેસ દર્શાવતુ હોય, તેથી આ સાઇટો સાચી ન હોવા જેવી છે.

આટલું ન કરો

- યાદ રાખો કે ઇક્વિટાસ સ્મોલ ફાઇનાન્સ બેંક કદી તમને વિગતો જેવી કે તમારા કાર્ડના આગળના અને પાછળના ભાગની કોપી/નકલ,માંગતી નથી.
- જો કોઈ બેન્કનો પ્રતિવિધિ હોવાનો દાવો કરે અને તમારું કાર્ડ માંગે તો તે સોપશો નહીં.
- તમારા કાર્ડની વિગત જેવી કે કાર્ડ નંબર એકસ્પાઇરી ડેટ, CVV, PIN કે OTP કોઈ પણ સાથે શેર કરતાં નહીં, જો તે બેન્કનો અધિકારી/કર્મચારી હોવાનો દાવો કરતો હોય, તો પણ.
- તમારા કાર્ડની વિગતો ઓનલાઈન મર્ચન્ટવેબસાઇટો પર સેવ કરતા નહીં.
- તમારી વિગતો ઈન્પુટ ખાનાવાળા ઇ-મેઈલમાં જે તમારા કાર્ડની વિગતો ATM PIN, CVV, UPI PIN માંગતી હોય તેમાં દાખલ કરવી નહીં.
- તમારા કાર્ડનો અનધિકૃત પેમેન્ટ ગેટ-વેઇઝ જેવા કે ગેમિંગ વેબસાઇટ,પોર્નોગ્રાફી વેબસાઇટ, લોટરી,ગેમ્બલિંગ (જુગાર) અને એવી ઘણી બધી સાઇટો પર ઉપયોગ કરવાનું ટાળો.
- લખાણ વગરનું અરજીપત્ર એવા ખોટા વચન સાથે કે આ પછીથી બેન્ક પ્રતિનિધિ દ્વારા ભરવામાં આવે છે, તેમાં કદી સહી ન કરવી.

3. UPI

આટલું કરો:

- UPI અરજીપત્રક માન્ય પ્લેટફોર્મ એટ્લે કે ગૂગલ પ્લે સ્ટોર વિ. મારફત ડાઉનલોડ કરો.
- માબાઈલ બેંકિંગનું રજીસ્ટ્રેશન મૂળ બેન્કની બ્રાન્ચ/નેટ બેંકિંગ/UPI મારફત કરો.
- ચોક્સસાઈ રાખો કે તમે લૉગ-ઇન અને UPI ટ્રાન્જકશન એકદમ ખાનગીમાં કરો છો.
- ટ્રાન્જક્શન પૂર્ણ થયે તમે ચોક્કસાઈ રાખો કે તમે એપ્લિકેશનમાંથી સફળતાપૂર્વક લૉગ-આઉટ થઈ ગયા છો.
- દરેક ટ્રાન્જકશન માટે તમે તમારા રજિસ્ટર્ડ મોબાઈલ નંબર એક SMS એલર્ટ મેળવશો. જો તમને તમારા ખાતામાં અનાધિકૃત UPI ટ્રાન્જકશનજણાય તો તમારી બેન્કનીબ્રાન્ચ સાથે તુરંત જ મળવાનું કામ કરો.
- કોઈપણ નિષ્ફળ ટ્રાન્જકશનના મામલામાં કૃપા કરી એપ્લીકેશન અને વેબસાઇટ ઉપર આપેલ એપ્લીકેશન મેટ્રિકસનું કાર્યાનુંસંધાન કરો.
- તમારી UPI એપ્લીકેશન પાસવર્ડ અને UPI-PIN/MPIN અવાર-નવાર બદલો.
- અનધિકૃત મોબાઈલ બેંકિંગ / UPI એક્સેસના મામલામાં કૃપા કરી ATM / ઇન્ટરનેટ બેંકિંગ/ મૂળ બેન્કની બ્રાન્ચ મારફત તુરત જ રજીસ્ટ્રેશન રદ કરો. (અથવા કૃપા કરી અમારા સંપર્ક કેન્દ્રનો સંપર્ક કરો.)
- જો તમારો મોબાઇલ ફોન ખોવાઈ/ચોરાઇ જાય તો તમારા મોબાઈલ બેંકિંગનું તુરંત જ શાખા / નેટ બેંકિંગ / ATM/સમપર કેન્દ્ર મારફત રજીસ્ટ્રેશન રદ કરો.
- જો તમારું મોબાઈલ બેંકિંગ / મોબાઈલ નંબરનું રજીસ્ટ્રેશન તમારી વિનંતી વિના નીકળી ગયું હોય/ડીએક્ટિવ થઈ ગયું હોય અથવા તમને આ બાબતમાં ફોનકોલ મળે છે તો કોઈક ડુપ્લિકેટ SIM કાર્ડ કાઢવાનો તમારા કેડેન્શિયલ જેવા કે MPIN/OTP (એક વખત નાખવાનો પાસવર્ડ) વીગેરે ચોરવાનો પ્રયત્ન કરી રહ્યું છે .આ મામલામાં કૃપા કરી તમારી મૂળ બેન્ક શાખાનો તુરંત જ સંપર્ક કરો.

આટલું ન કરો:

- કૃપા કરી તમારો પાસવર્ડ શેર ના કરો/ તમારા મોબાઈલ હેન્ડસેટમાં સ્ટોર ના કરો.
- તમે તમારો એપ્લીકેશનનો પાસવર્ડ કે UPI PIN/MPIN દાખલ કરો તે કોઈને પણ જોવા ન દો.
- એપ્લીકેશન UPI PIN / MPIN જેને સહેલાઇથી અનુમાન લગાવી શકાય તેને ઉદાહરણ: 1111/2222/1234, જન્મનું વર્ષ,મોબાઈલ નંબર/ ટેલિફોન નંબરનો કદી ઉપયોગ ન કરવો.
- બીજા કોઈના ડિવાઇસ (સાધન)માં UPI એપ્લીકેશન ડાઉનલોડ ન કરો.
- ઇક્વિટાસ બેંક તમારા UPI/મોબાઇલ બેંકિંગ પાસવર્ડ પૂછવા કોલ/ઈ-મેઈલ કરતી નથી. જો કોઈ ફોન કરનાર અમારી બેન્ક સંપર્ક કેન્દ્રમાંથી બોલતો હોવાનો ઢોંગ કરે છે તો આવી વિનંતી ગ્રાહ્ય રાખવી નહીં કારણ કે તે છેતરપિંડી કરનાર હસ્તી છે.
- કદી તમારા રજિસ્ટર થયેલ SIM કાર્ડ અને ડેબિટ કાર્ડ સાથે રાખવું નહીં, બંનેનું ખોવાઈ જવાનું જોખમ હોય છે, જે કોઈપણને તમારા એકાઉન્ટ સુધી એક્સેસ કરવા સક્ષમ બનાવી શકે છે.