ಮೋಸದ ವಹಿವಾಟುಗಳ ವಿರುದ್ಧ ಬ್ಯಾಂಕುಗಳು ತೆಗೆದುಕೊಳ್ಳಬೇಕಾದ ಮುನ್ನಚ್ಚರಿಕೆಗಳ ಕಾರ್ಯ ವಿಧಾನ

ಫಿಶಿಂಗ್ ಲಿಂಕ್‌ಗಳು(Phishing links) : -

- ವಂಚಕರು ಮೂರನೇ ವ್ಯಕ್ತಿಯ ಫಿಶಿಂಗ್ ವೆಬ್‌ಸೈಟ್ ಅನ್ನು ರಚಿಸುತ್ತಾರೆ, ಅದು ಅಸ್ತಿತ್ವದಲ್ಲಿರುವ ನಿಜವಾದ ವೆಬ್‌ಸೈಟ್‌ನಂತೆ ಕಾಣುತ್ತದೆ, ಉದಾಹರಣೆಗೆ – ಬ್ಯಾಂಕ್‌ನ ವೆಬ್‌ಸೈಟ್ ಅಥವಾ ಇ–ಕಾಮರ್ಸ್ ವೆಬ್‌ಸೈಟ್ ಅಥವಾ ಹುಡುಕಾಟ ಎಂಜಿನ್, ಇತ್ಯಾದಿ.
- ಈ ವೆಬ್‌ಸೈಟ್‌ಗಳಿಗೆ ಲಿಂಕ್‌ಗಳನ್ನು ವಂಚಕರು ಕಿರು ಸಂದೇಶ ಸೇವೆ (SMS) / ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮ / ಇಮೇಲ್ / ತ್ವರಿತ ಸಂದೇಶವಾಹಕ, ಇತ್ಯಾದಿಗಳ ಮೂಲಕ ಪ್ರಸಾರ ಮಾಡುತ್ತಾರೆ.
- ಅನೇಕ ಗ್ರಾಹಕರು ವಿವರವಾದ ಯೂನಿಫಾರ್ಮ್ ರಿಸೋರ್ಸ್ ಲೊಕೇಟರ್ (URL) ಅನ್ನು ಪರಿಶೀಲಿಸದೆ ಲಿಂಕ್ ಅನ್ನು ಕ್ಲಿಕ್ ಮಾಡುತ್ತಾರೆ ಮತ್ತು ವಂಚಕರು ಸೆರೆಹಿಡಿದು ಬಳಸಿರುವ ವೈಯಕ್ತಿಕ ಗುರುತಿನ ಸಂಖ್ಯೆ (PIN), ಒಂದು ಬಾರಿಯ ಪಾಸ್‌ವರ್ಡ್ (OTP), ಪಾಸ್‌ವರ್ಡ್, ಇತ್ಯಾದಿಗಳಂತಹ ಸುರಕ್ಷಿತ ರುಜುವಾತುಗಳನ್ನು ನಮೂದಿಸಿ.

ಮುನ್ನಚ್ಚರಿಕೆಗಳು : –

- ಅಜ್ಞಾತ / ಪರಿಶೀಲಿಸದ ಲಿಂಕ್‌ಗಳನ್ನು ಕ್ಲಿಕ್ ಮಾಡಬೇಡಿ ಮತ್ತು ಭವಿಷ್ಯದಲ್ಲಿ ತಪ್ಪಾಗಿ ಪ್ರವೇಶಿಸುವುದನ್ನು ತಪ್ಪಿಸಲು ಅಜ್ಞಾತ ಕಳುಹಿಸುವವರು ಕಳುಹಿಸಿದ ಅಂತಹ SMS / ಇಮೇಲ್ ಅನ್ನು ತಕ್ಷಣವೇ ಅಳಿಸಬೇಡಿ.
- ಬ್ಯಾಂಕ್ / ಇ–ಕಾಮರ್ಸ್ / ಹುಡುಕಾಟ ಎಂಜಿನ್ ವೆಬ್‌ಸೈಟ್‌ಗೆ ಲಿಂಕ್‌ಗಳನ್ನು ಒದಗಿಸುವ ಮೇಲ್‌ಗಳನ್ನು ಅನ್‌ಸಬ್‌ಸ್ಕ್ರೈಬ್ ಮಾಡಿ ಮತ್ತು ಅಂತಹ ಇಮೇಲ್‌ಗಳನ್ನು ಅಳಿಸುವ ಮೊದಲು ಕಳುಹಿಸುವವರ ಇಮೇಲ್ ಐಡಿಯನ್ನು ನಿರ್ಬಂಧಿಸಿ.
- ಯಾವಾಗಲೂ ನಿಮ್ಮ ಬ್ಯಾಂಕ್ / ಸೇವಾ ಪೂರೈಕೆದಾರರ ಅಧಿಕೃತ ವೆಬ್‌ಸೈಟ್‌ಗೆ ಹೋಗಿ. ವಿಶೇಷವಾಗಿ ಹಣಕಾಸಿನ ರುಜುವಾತುಗಳನ್ನು ನಮೂದಿಸುವ ಅಗತ್ಯವಿರುವಲ್ಲಿ ವೆಬ್‌ಸೈಟ್ ವಿವರಗಳನ್ನು ಎಚ್ಚರಿಕೆಯಿಂದ ಪರಿಶೀಲಿಸಿ. ಸುರಕ್ಷಿತ ರುಜುವಾತುಗಳನ್ನು ನಮೂದಿಸುವ ಮೊದಲು ವೆಬ್‌ಸೈಟ್‌ನಲ್ಲಿ ಸುರಕ್ಷಿತ ಚಿಹ್ನೆಯನ್ನು (ಪ್ಯಾಡ್‌ಲಾಕ್ ಚಿಹ್ನೆಯೊಂದಿಗೆ http) ಪರಿಶೀಲಿಸಿ.
- ಸ್ಪೆಲಿಂಗ್ ದೋಷಗಳಿಗಾಗಿ ಇಮೇಲ್‌ಗಳಲ್ಲಿ ಸ್ವೀಕರಿಸಿದ URL ಗಳು ಮತ್ತು ಡೊಮೇನ್ ಹೆಸರುಗಳನ್ನು ಪರಿಶೀಲಿಸಿ. ಅನುಮಾನವಿದ್ದಲ್ಲಿ ಮಾಹಿತಿ ನೀಡಿ.

ವಿಶಿಂಗ್ ಕಾಲ್ಸ್(Vishing calls) :-

- ವಂಚಕರು ದೂರವಾಣಿ ಕರೆ/ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮಗಳ ಮೂಲಕ ಬ್ಯಾಂಕರ್‌ಗಳು/ಕಂಪನಿಯ ಕಾರ್ಯನಿರ್ವಾಹಕರು/ವಿಮಾ ಏಜೆಂಟ್‌ಗಳು/ಸರ್ಕಾರಿ ಅಧಿಕಾರಿಗಳು ಇತ್ಯಾದಿಯಾಗಿ ಗ್ರಾಹಕರಿಗೆ ಕರೆ ಮಾಡುತ್ತಾರೆ ಅಥವಾ ಸಂಪರ್ಕಿಸುತ್ತಾರೆ. ವಿಶ್ವಾಸವನ್ನು ಪಡೆಯಲು, ವಂಚಕರು ಗ್ರಾಹಕರ ಹೆಸರು ಅಥವಾ ಹುಟ್ಟಿದ ದಿನಾಂಕದಂತಹ ಕೆಲವು ಗ್ರಾಹಕರ ವಿವರಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳುತ್ತಾರೆ.
- ಕೆಲವು ಸಂದರ್ಭಗಳಲ್ಲಿ, ವಂಚಕರು ಪಾಸ್‌ವರ್ಡ್‌ಗಳು / OTP / PIN / ಕಾರ್ಡ್ ಪರಿಶೀಲನೆ ಮೌಲ್ಯ (CVV) ಇತ್ಯಾದಿಗಳಂತಹ ಗೌಪ್ಯ ವಿವರಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳಲು ಗ್ರಾಹಕರ ಮೇಲೆ ಒತ್ತಡ / ಮೋಸ ಮಾಡುತ್ತಾರೆ. ಕೆಲವು ದಂಡವನ್ನು ನಿಲ್ಲಿಸಿ, ಆಕರ್ಷಕ ರಿಯಾಯಿತಿ, ಇತ್ಯಾದಿ. ಈ ರುಜುವಾತುಗಳನ್ನು ನಂತರ ಗ್ರಾಹಕರನ್ನು ವಂಚಿಸಲು ಬಳಸಲಾಗುತ್ತದೆ.

ಮುನ್ನಚ್ಚರಿಕೆಗಳು : –

- ಬ್ಯಾಂಕ್ ಅಧಿಕಾರಿಗಳು / ಹಣಕಾಸು ಸಂಸ್ಥೆಗಳು / RBI / ಯಾವುದೇ ನಿಜವಾದ ಘಟಕವು ಬಳಕೆದಾರರ ಹೆಸರು / ಪಾಸ್‌ವರ್ಡ್ / ಕಾರ್ಡ್ ವಿವರಗಳು / CVV / OTP ಯಂತಹ ಗೌಪ್ಯ ಮಾಹಿತಿಯನ್ನು ಹಂಚಿಕೊಳ್ಳಲು ಎಂದಿಗೂ ಗ್ರಾಹಕರನ್ನು ಕೇಳುವುದಿಲ್ಲ.
- ಈ ಗೌಪ್ಯ ವಿವರಗಳನ್ನು ಯಾರೊಂದಿಗೂ, ನಿಮ್ಮ ಸ್ವಂತ ಕುಟುಂಬದ ಸದಸ್ಯರು ಮತ್ತು ಸ್ನೇಹಿತರೊಂದಿಗೆ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.

ಆನ್‌ಲೈನ್ ಮಾರಾಟ ವೇದಿಕೆಗಳನ್ನು ಬಳಸಿಕೊಂಡು ವಂಚನೆಗಳು : –

- ವಂಚಕರು ಆನ್‌ಲೈನ್ ಮಾರಾಟ ವೇದಿಕೆಗಳಲ್ಲಿ ಖರೀದಿದಾರರಂತೆ ನಟಿಸುತ್ತಾರೆ ಮತ್ತು ಮಾರಾಟಗಾರರ ಉತ್ಪನ್ನ/ಗಳಲ್ಲಿ ಆಸಕ್ತಿಯನ್ನು ತೋರಿಸುತ್ತಾರೆ. ಅನೇಕ ವಂಚಕರು ಆತ್ಮವಿಶ್ವಾಸವನ್ನು ಪಡೆಯಲು ದೂರದ ಸ್ಥಳಗಳಲ್ಲಿ ನಿಯೋಜಿಸಲಾದ ರಕ್ಷಣಾ ಸಿಬ್ಬಂದಿ ಎಂದು ನಟಿಸುತ್ತಾರೆ.
- ಮಾರಾಟಗಾರರಿಗೆ ಹಣವನ್ನು ಪಾವತಿಸುವ ಬದಲು, ಅವರು ಯುನಿಫೈಡ್ ಪೇಮೆಂಟ್ಸ್ ಇಂಟರ್ಫೇಸ್ (UPI) ಅಪ್ಲಿಕೇಶನ್ ಮೂಲಕ "ಹಣವನ್ನು ವಿನಂತಿಸಿ" ಆಯ್ಕೆಯನ್ನು ಬಳಸುತ್ತಾರೆ ಮತ್ತು UPI PIN ಅನ್ನು ನಮೂದಿಸುವ ಮೂಲಕ ಮಾರಾಟಗಾರನು ವಿನಂತಿಯನ್ನು ಅನುಮೋದಿಸಬೇಕೆಂದು ಒತ್ತಾಯಿಸುತ್ತಾರೆ. ಮಾರಾಟಗಾರನು ಪಿನ್ ನಮೂದಿಸಿದ ನಂತರ, ಹಣವನ್ನು ವಂಚಕನ ಖಾತೆಗೆ ವರ್ಗಾಯಿಸಲಾಗುತ್ತದೆ.

ಮುನ್ನಚ್ಚರಿಕೆಗಳು : –

- ನೀವು ಆನ್‌ಲೈನ್ ಮಾರಾಟ ವೇದಿಕೆಗಳನ್ನು ಬಳಸಿಕೊಂಡು ಉತ್ಪನ್ನಗಳನ್ನು ಖರೀದಿಸುವಾಗ ಅಥವಾ ಮಾರಾಟ ಮಾಡುವಾಗ ಯಾವಾಗಲೂ ಜಾಗರೂಕರಾಗಿರಿ.
- ಹಣವನ್ನು ಸ್ವೀಕರಿಸಲು ಎಲ್ಲಿಯೂ ಪಿನ್ / ಪಾಸ್‌ವರ್ಡ್ ಅನ್ನು ನಮೂದಿಸುವ ಅಗತ್ಯವಿಲ್ಲ ಎಂದು ಯಾವಾಗಲೂ ನೆನಪಿಡಿ.
- UPI ಅಥವಾ ಯಾವುದೇ ಇತರ ಅಪ್ಲಿಕೇಶನ್‌ಗೆ ನೀವು ವಹಿವಾಟನ್ನು ಪೂರ್ಣಗೊಳಿಸಲು PIN ಅನ್ನು ನಮೂದಿಸುವ ಅಗತ್ಯವಿದ್ದರೆ, ನೀವು ಅದನ್ನು ಸ್ವೀಕರಿಸುವ ಬದಲು ಹಣವನ್ನು ಕಳುಹಿಸುತ್ತೀರಿ ಎಂದರ್ಥ.

ಅಪರಿಚಿತ / ಪರಿಶೀಲಿಸದ ಮೊಬೈಲ್ ಅಪ್ಲಿಕೇಶನ್‌ಗಳ ಬಳಕೆಯಿಂದಾಗಿ ವಂಚನೆಗಳು :–

- ವಂಚಕರು SMS / ಇಮೇಲ್ / ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮ / ತತ್‌ಕ್ಷಣ ಮೆಸೆಂಜರ್, ಇತ್ಯಾದಿಗಳ ಮೂಲಕ ಪ್ರಸಾರ ಮಾಡುತ್ತಾರೆ, ಕೆಲವು ಅಪ್ಲಿಕೇಶನ್ ಲಿಂಕ್‌ಗಳು, ಅಧಿಕೃತ ಘಟಕಗಳ ಅಸ್ತಿತ್ವದಲ್ಲಿರುವ ಅಪ್ಲಿಕೇಶನ್‌ಗಳಂತೆಯೇ ಕಾಣಿಸಿಕೊಳ್ಳುವಂತೆ ಮರೆಮಾಚುತ್ತಾರೆ.
- ವಂಚಕರು ಅಂತಹ ಲಿಂಕ್‌ಗಳ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡಲು ಗ್ರಾಹಕರನ್ನು ಮೋಸಗೊಳಿಸುತ್ತಾರೆ, ಇದು ಗ್ರಾಹಕರ ಮೊಬೈಲ್ / ಲ್ಯಾಪ್‌ಟಾಪ್ / ಡೆಸ್ಕ್‌ಟಾಪ್ ಇತ್ಯಾದಿಗಳಲ್ಲಿ ಅಪರಿಚಿತ / ಪರಿಶೀಲಿಸದ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡಲು ಕಾರಣವಾಗುತ್ತದೆ.
- ದುರುದ್ದೇಶಪೂರಿತ ಅಪ್ಲಿಕೇಶನ್ ಅನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡಿದ ನಂತರ, ವಂಚಕನು ಗ್ರಾಹಕರ ಸಾಧನಕ್ಕೆ ಸಂಪೂರ್ಣ ಪ್ರವೇಶವನ್ನು ಪಡೆಯುತ್ತಾನೆ. ಇವುಗಳು ಸಾಧನದಲ್ಲಿ ಸಂಗ್ರಹಿಸಲಾದ ಗೌಪ್ಯ

ವಿವರಗಳು ಮತ್ತು ಅಂತಹ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಸ್ಥಾಪಿಸುವ ಮೊದಲು / ನಂತರ ಸ್ವೀಕರಿಸಿದ ಸಂದೇಶಗಳು / OTP ಗಳನ್ನು ಒಳಗೊಂಡಿರುತ್ತವೆ.

ಮುನ್ನಚ್ಚರಿಕೆಗಳು : –

- ಯಾವುದೇ ಪರಿಶೀಲಿಸದ / ಅಪರಿಚಿತ ಮೂಲಗಳಿಂದ ಅಥವಾ ಅಪರಿಚಿತ ವ್ಯಕ್ತಿಯಿಂದ ಕೇಳಲ್ಪಟ್ಟ / ಮಾರ್ಗದರ್ಶನದಲ್ಲಿ ಅಪ್ಲಿಕೇಶನ್ ಅನ್ನು ಎಂದಿಗೂ ಡೌನ್‌ಲೋಡ್ ಮಾಡಬೇಡಿ.
- ಡೌನ್‌ಲೋಡ್ ಮಾಡುವ ಮೊದಲು ವಿವೇಕಯುತ ಅಭ್ಯಾಸವಾಗಿ, ಡೌನ್‌ಲೋಡ್ ಆಗುತ್ತಿರುವ ಅಪ್ಲಿಕೇಶನ್‌ನ ಪ್ರಕಾಶಕರು / ಮಾಲೀಕರು ಮತ್ತು ಅದರ ಬಳಕೆದಾರರ ರೇಟಿಂಗ್‌ಗಳು ಇತ್ಯಾದಿಗಳನ್ನು ಪರಿಶೀಲಿಸಿ.
- ಅಪ್ಲಿಕೇಶನ್ ಅನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡುವಾಗ, ಅನುಮತಿ/ಗಳು ಮತ್ತು ಸಂಪರ್ಕಗಳು, ಛಾಯಾಚಿತ್ರಗಳು ಇತ್ಯಾದಿಗಳಂತಹ ನಿಮ್ಮ ಡೇಟಾಗೆ ಪ್ರವೇಶವನ್ನು ಪರಿಶೀಲಿಸಿ. ಬಯಸಿದ ಅಪ್ಲಿಕೇಶನ್ ಅನ್ನು ಬಳಸಲು ಸಂಪೂರ್ಣವಾಗಿ ಅಗತ್ಯವಿರುವ ಅನುಮತಿಗಳನ್ನು ಮಾತ್ರ ನೀಡಿ.

ಎಟಿಎಂ ಕಾರ್ಡ್ ಸ್ಕಿಮ್ಮಿಂಗ್(ATM card skimming):-

- ವಂಚಕರು ಎಟಿಎಂ ಯಂತ್ರಗಳಲ್ಲಿ ಸ್ಕಿಮ್ಮಿಂಗ್ ಸಾಧನಗಳನ್ನು ಸ್ಥಾಪಿಸುತ್ತಾರೆ ಮತ್ತು ಡೇಟಾವನ್ನು ಕದಿಯುತ್ತಾರೆ
- ಗ್ರಾಹಕರ ಕಾರ್ಡ್.
- ವಂಚಕರು ಡಮ್ಮಿ ಕೀಪ್ಯಾಡ್ ಅಥವಾ ಸಣ್ಣ / ಪಿನ್‌ಹೋಲ್ ಕ್ಯಾಮೆರಾವನ್ನು ಸಹ ಸ್ಥಾಪಿಸಬಹುದು, ಎಟಿಎಂ ಪಿನ್ ಅನ್ನು ಸೆರೆಹಿಡಿಯಲು ಸರಳ ದೃಷ್ಟಿಯಿಂದ ಚೆನ್ನಾಗಿ ಮರೆಮಾಡಲಾಗಿದೆ.
- ಕೆಲವೊಮ್ಮೆ, ಗ್ರಾಹಕರು ಎಟಿಎಂ ಯಂತ್ರದಲ್ಲಿ ಪಿನ್ ಅನ್ನು ನಮೂದಿಸಿದಾಗ ಹತ್ತಿರದಲ್ಲಿ ನಿಂತಿರುವ ಇತರ ಗ್ರಾಹಕರಂತೆ ನಟಿಸುವ ವಂಚಕರು ಪಿನ್‌ಗೆ ಪ್ರವೇಶವನ್ನು ಪಡೆಯುತ್ತಾರೆ.
- ಈ ಡೇಟಾವನ್ನು ನಂತರ ನಕಲಿ ಕಾರ್ಡ್ ರಚಿಸಲು ಬಳಸಲಾಗುತ್ತದೆ ಮತ್ತು
- ಗ್ರಾಹಕರ ಖಾತೆಯಿಂದ ಹಣವನ್ನು ಹಿಂಪಡೆಯಿರಿ.

ಮುನ್ನಚ್ಚರಿಕೆಗಳು : –

- ವಹಿವಾಟು ಮಾಡುವ ಮೊದಲು ಕಾರ್ಡ್ ಅಳವಡಿಕೆ ಸ್ಲಾಟ್ ಅಥವಾ ಎಟಿಎಂ ಯಂತ್ರದ ಕೀಪ್ಯಾಡ್ ಬಳಿ ಯಾವುದೇ ಹೆಚ್ಚುವರಿ ಸಾಧನವನ್ನು ಲಗತ್ತಿಸಲಾಗಿಲ್ಲ ಎಂಬುದನ್ನು ಯಾವಾಗಲೂ ಪರಿಶೀಲಿಸಿ.
- ಪಿನ್ ನಮೂದಿಸುವಾಗ ನಿಮ್ಮ ಇನ್ನೊಂದು ಕೈಯಿಂದ ಕೀಪ್ಯಾಡ್ ಅನ್ನು ಕವರ್ ಮಾಡಿ.
- ನಿಮ್ಮ ಎಟಿಎಂ ಕಾರ್ಡ್‌ನಲ್ಲಿ ಪಿನ್ ಅನ್ನು ಎಂದಿಗೂ ಬರೆಯಬೇಡಿ.
- ನಿಮ್ಮ ಹತ್ತಿರ ನಿಂತಿರುವ ಯಾವುದೇ ಇತರ / ಅಪರಿಚಿತ ವ್ಯಕ್ತಿಯ ಉಪಸ್ಥಿತಿಯಲ್ಲಿ ಪಿನ್ ಅನ್ನು ನಮೂದಿಸಬೇಡಿ.
- ನಗದು ಹಿಂಪಡೆಯಲು ನಿಮ್ಮ ATM ಕಾರ್ಡ್ ಅನ್ನು ಯಾರಿಗೂ ನೀಡಬೇಡಿ.
- ಯಾವುದೇ ಅಪರಿಚಿತ ವ್ಯಕ್ತಿ ನೀಡಿದ ಸೂಚನೆಗಳನ್ನು ಅನುಸರಿಸಬೇಡಿ ಅಥವಾ ATM ಗಳಲ್ಲಿ ಅಪರಿಚಿತರು / ಅಪರಿಚಿತ ವ್ಯಕ್ತಿಗಳಿಂದ ಸಹಾಯ / ಮಾರ್ಗದರ್ಶನವನ್ನು ತೆಗೆದುಕೊಳ್ಳಬೇಡಿ.

- ಎಟಿಎಂನಲ್ಲಿ ಹಣವನ್ನು ವಿತರಿಸಲಾಗದಿದ್ದರೆ, ಎಟಿಎಂನಿಂದ ಹೊರಡುವ ಮೊದಲು 'ರದ್ದುಮಾಡು' ಬಟನ್ ಅನ್ನು ಒತ್ತಿ ಮತ್ತು ಮುಖಪುಟ ಪರದೆಯು ಕಾಣಿಸಿಕೊಳ್ಳುವವರೆಗೆ ಕಾಯಿರಿ.

ಸ್ಕ್ರೀನ್ ಹಂಚಿಕೆ ಅಪ್ಲಿಕೇಶನ್ / ರಿಮೋಟ್ ಪ್ರವೇಶವನ್ನು ಬಳಸಿಕೊಂಡು ವಂಚನೆಗಳು(Frauds using screen sharing app / Remote access) :–

- ವಂಚಕರು ಸ್ಕ್ರೀನ್ ಶೇರಿಂಗ್ ಆ್ಯಪ್ ಡೌನ್‌ಲೋಡ್ ಮಾಡಲು ಗ್ರಾಹಕರನ್ನು ಮೋಸಗೊಳಿಸುತ್ತಾರೆ.
- ಅಂತಹ ಅಪ್ಲಿಕೇಶನ್ ಅನ್ನು ಬಳಸಿಕೊಂಡು, ವಂಚಕರು ಗ್ರಾಹಕರ ಮೊಬೈಲ್ / ಲ್ಯಾಪ್‌ಟಾಪ್ ಅನ್ನು ವೀಕ್ಷಿಸಬಹುದು / ನಿಯಂತ್ರಿಸಬಹುದು ಮತ್ತು ಗ್ರಾಹಕರ ಆರ್ಥಿಕ ರುಜುವಾತುಗಳಿಗೆ ಪ್ರವೇಶವನ್ನು ಪಡೆಯಬಹುದು.
- ವಂಚಕರು ಈ ಮಾಹಿತಿಯನ್ನು ಅನಧಿಕೃತವಾಗಿ ಹಣ ವರ್ಗಾವಣೆ ಮಾಡಲು ಅಥವಾ ಗ್ರಾಹಕರ ಇಂಟರ್ನೆಟ್ ಬ್ಯಾಂಕಿಂಗ್ / ಪಾವತಿ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಬಳಸಿಕೊಂಡು ಪಾವತಿಗಳನ್ನು ಮಾಡಲು ಬಳಸುತ್ತಾರೆ.

ಮುನ್ನಚ್ಚರಿಕೆಗಳು : –

- ನಿಮ್ಮ ಸಾಧನವು ಯಾವುದೇ ತಾಂತ್ರಿಕ ದೋಷವನ್ನು ಎದುರಿಸಿದರೆ ಮತ್ತು ನೀವು ಯಾವುದೇ ಸ್ಕ್ರೀನ್ ಹಂಚಿಕೆ ಅಪ್ಲಿಕೇಶನ್ ಅನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡಬೇಕಾದರೆ, ನಿಮ್ಮ ಸಾಧನದಿಂದ ಎಲ್ಲಾ ಪಾವತಿ ಸಂಬಂಧಿತ ಅಪ್ಲಿಕೇಶನ್‌ಗಳಿಂದ ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಿ / ಲಾಗ್ ಔಟ್ ಮಾಡಿ.
- ಕಂಪನಿಯ ಅಧಿಕೃತ ವೆಬ್‌ಸೈಟ್‌ನಲ್ಲಿ ಗೋಚರಿಸುವಂತೆ ಕಂಪನಿಯ ಅಧಿಕೃತ ಟೋಲ್–ಫ್ರೀ ಸಂಖ್ಯೆಯ ಮೂಲಕ ನಿಮಗೆ ಸಲಹೆ ನೀಡಿದಾಗ ಮಾತ್ರ ಅಂತಹ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡಿ. ಕಂಪನಿಯ ಕಾರ್ಯನಿರ್ವಾಹಕರು ಆತನ/ಅವಳ ವೈಯಕ್ತಿಕ ಸಂಪರ್ಕ ಸಂಖ್ಯೆಯ ಮೂಲಕ ನಿಮ್ಮನ್ನು ಸಂಪರ್ಕಿಸಿದರೆ ಅಂತಹ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಡೌನ್‌ಲೋಡ್ ಮಾಡಬೇಡಿ.
- ಕೆಲಸ ಪೂರ್ಣಗೊಂಡ ತಕ್ಷಣ, ನಿಮ್ಮ ಸಾಧನದಿಂದ ಸ್ಕ್ರೀನ್ ಹಂಚಿಕೆ ಅಪ್ಲಿಕೇಶನ್ ಅನ್ನು ತೆಗೆದುಹಾಕಲಾಗಿದೆ ಎಂದು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಿ.

ಸಿಮ್ ಸ್ವಾಪ್ / ಸಿಮ್ ಕ್ಲೋನಿಂಗ್(SIM swap / SIM cloning):-

- ವಂಚಕರು ಗ್ರಾಹಕರ ಚಂದಾದಾರರ ಗುರುತಿನ ಮಾಡ್ಯೂಲ್ (SIM) ಕಾರ್ಡ್‌ಗೆ ಪ್ರವೇಶವನ್ನು ಪಡೆಯುತ್ತಾರೆ ಅಥವಾ
- ಗ್ರಾಹಕರ ಬ್ಯಾಂಕ್ ಖಾತೆಗೆ ಸಂಪರ್ಕಗೊಂಡಿರುವ ನೋಂದಾಯಿತ ಮೊಬೈಲ್ ಸಂಖ್ಯೆಗೆ ನಕಲಿ ಸಿಮ್ ಕಾರ್ಡ್ (ಎಲೆಕ್ಟ್ರಾನಿಕ್–ಸಿಮ್ ಸೇರಿದಂತೆ) ಪಡೆಯಬಹುದು.
- ವಂಚಕರು ಅನಧಿಕೃತ ವಹಿವಾಟುಗಳನ್ನು ನಡೆಸಲು ಇಂತಹ ನಕಲಿ ಸಿಮ್‌ನಲ್ಲಿ ಪಡೆದ OTP ಅನ್ನು ಬಳಸುತ್ತಾರೆ.
- ವಂಚಕರು ಸಾಮಾನ್ಯವಾಗಿ ಟೆಲಿಫೋನ್/ಮೊಬೈಲ್ ನೆಟ್‌ವರ್ಕ್ ಸಿಬ್ಬಂದಿಯಂತೆ ನಟಿಸುವ ಮೂಲಕ ಗ್ರಾಹಕರಿಂದ ವೈಯಕ್ತಿಕ/ಗುರುತಿನ ವಿವರಗಳನ್ನು ಸಂಗ್ರಹಿಸುತ್ತಾರೆ ಮತ್ತು ಆಫರ್‌ಗಳ ಹೆಸರಿನಲ್ಲಿ ಗ್ರಾಹಕರ ವಿವರಗಳನ್ನು ವಿನಂತಿಸುತ್ತಾರೆ – 3G ಯಿಂದ 4G ಗೆ ಸಿಮ್ ಕಾರ್ಡ್

ಅನ್ನು ಉಚಿತವಾಗಿ ಅಪ್‌ಗ್ರೇಡ್ ಮಾಡಲು ಅಥವಾ ಹೆಚ್ಚುವರಿ ಪ್ರಯೋಜನಗಳನ್ನು ಒದಗಿಸಲು ಸಿಮ್ ಕಾರ್ಡ್‌ನಲ್ಲಿ.

ಮುನ್ನಚ್ಚರಿಕೆಗಳು : –

- ನಿಮ್ಮ ಸಿಮ್ ಕಾರ್ಡ್‌ಗೆ ಸಂಬಂಧಿಸಿದ ಗುರುತಿನ ರುಜುವಾತುಗಳನ್ನು ಎಂದಿಗೂ ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.
- ನಿಮ್ಮ ಫೋನ್‌ನಲ್ಲಿ ಮೊಬೈಲ್ ನೆಟ್‌ವರ್ಕ್ ಪ್ರವೇಶದ ಬಗ್ಗೆ ಜಾಗರೂಕರಾಗಿರಿ. ನಿಯಮಿತ ಪರಿಸರದಲ್ಲಿ ಸಾಕಷ್ಟು ಸಮಯದವರೆಗೆ ನಿಮ್ಮ ಫೋನ್‌ನಲ್ಲಿ ಯಾವುದೇ ಮೊಬೈಲ್ ನೆಟ್‌ವರ್ಕ್ ಇಲ್ಲದಿದ್ದರೆ, ನಿಮ್ಮ ಮೊಬೈಲ್ ಸಂಖ್ಯೆಗೆ ಯಾವುದೇ ನಕಲಿ ಸಿಮ್ ನೀಡಲಾಗುತ್ತಿಲ್ಲ / ನೀಡಲಾಗಿಲ್ಲ ಎಂದು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಲು ತಕ್ಷಣವೇ ಮೊಬೈಲ್ ಆಪರೇಟರ್ ಅನ್ನು ಸಂಪರ್ಕಿಸಿ.

ಸರ್ಚ್ ಇಂಜಿನ್‌ಗಳ ಮೂಲಕ ಫಲಿತಾಂಶಗಳಲ್ಲಿ ರುಜುವಾತುಗಳನ್ನು ರಾಜಿ ಮಾಡಿಕೊಳ್ಳುವ ಮೂಲಕ ವಂಚನೆಗಳು(Frauds by compromising credentials on results through search engines):-

- ಗ್ರಾಹಕರು ತಮ್ಮ ಬ್ಯಾಂಕ್, ವಿಮಾ ಕಂಪನಿ, ಆಧಾರ್ ಅಪ್‌ಡೇಟ್ ಸೆಂಟರ್ ಇತ್ಯಾದಿಗಳ ಸಂಪರ್ಕ ವಿವರಗಳು / ಗ್ರಾಹಕ ಆರೈಕೆ ಸಂಖ್ಯೆಗಳನ್ನು ಪಡೆಯಲು ಸರ್ಚ್ ಇಂಜಿನ್‌ಗಳನ್ನು ಬಳಸುತ್ತಾರೆ. ಸರ್ಚ್ ಇಂಜಿನ್‌ಗಳಲ್ಲಿನ ಈ ಸಂಪರ್ಕ ವಿವರಗಳು ಸಾಮಾನ್ಯವಾಗಿ ಆಯಾ ಘಟಕಕ್ಕೆ ಸೇರಿರುವುದಿಲ್ಲ ಆದರೆ ಕಾಣಿಸಿಕೊಳ್ಳುವಂತೆ ಮಾಡಲಾಗುತ್ತದೆ. ವಂಚಕರಿಂದ ಅದರಂತೆ.
- ಗ್ರಾಹಕರು ಸರ್ಚ್ ಇಂಜಿನ್‌ನಲ್ಲಿ ಬ್ಯಾಂಕ್ / ಕಂಪನಿಯ ಸಂಪರ್ಕ ಸಂಖ್ಯೆಗಳಂತೆ ಪ್ರದರ್ಶಿಸಲಾದ ವಂಚಕರ ಅಪರಿಚಿತ / ಪರಿಶೀಲಿಸದ ಸಂಪರ್ಕ ಸಂಖ್ಯೆಗಳನ್ನು ಸಂಪರ್ಕಿಸಬಹುದು.
- ಗ್ರಾಹಕರು ಒಮ್ಮೆ ಈ ಸಂಪರ್ಕ ಸಂಖ್ಯೆಗಳಿಗೆ ಕರೆ ಮಾಡಿದರೆ, ವಂಚಕರು ತಮ್ಮ ಕಾರ್ಡ್ ರುಜುವಾತುಗಳನ್ನು / ವಿವರಗಳನ್ನು ಪರಿಶೀಲನೆಗಾಗಿ ಹಂಚಿಕೊಳ್ಳಲು ಗ್ರಾಹಕರನ್ನು ಕೇಳುತ್ತಾರೆ.
- ವಂಚಕನು RE ಯ ನಿಜವಾದ ಪ್ರತಿನಿಧಿ ಎಂದು ಭಾವಿಸಿದರೆ, ಗ್ರಾಹಕರು ತಮ್ಮ ಸುರಕ್ಷಿತ ವಿವರಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳುತ್ತಾರೆ ಮತ್ತು ಹೀಗಾಗಿ ವಂಚನೆಗಳಿಗೆ ಬಲಿಯಾಗುತ್ತಾರೆ.

ಮುನ್ನಚ್ಚರಿಕೆಗಳು : –

- ಬ್ಯಾಂಕ್‌ಗಳು/ಕಂಪನಿಗಳ ಅಧಿಕೃತ ವೆಬ್‌ಸೈಟ್‌ಗಳಿಂದ ಗ್ರಾಹಕ ಆರೈಕೆ ಸಂಪರ್ಕ ವಿವರಗಳನ್ನು ಯಾವಾಗಲೂ ಪಡೆದುಕೊಳ್ಳಿ.
- ಸರ್ಚ್ ಇಂಜಿನ್ ಫಲಿತಾಂಶಗಳ ಪುಟದಲ್ಲಿ ನೇರವಾಗಿ ಪ್ರದರ್ಶಿಸಲಾದ ಸಂಖ್ಯೆಗಳಿಗೆ ಕರೆ ಮಾಡಬೇಡಿ ಏಕೆಂದರೆ ಇವುಗಳು ಸಾಮಾನ್ಯವಾಗಿ ವಂಚಕರಿಂದ ಮರೆಮಾಚಲ್ಪಡುತ್ತವೆ.
- ಗ್ರಾಹಕ ಆರೈಕೆ ಸಂಖ್ಯೆಗಳು ಎಂದಿಗೂ ಮೊಬೈಲ್ ಸಂಖ್ಯೆಗಳ ರೂಪದಲ್ಲಿಲ್ಲ ಎಂಬುದನ್ನು ದಯವಿಟ್ಟು ಗಮನಿಸಿ.

QR ಕೋಡ್ ಸ್ಕ್ಯಾನ್ ಮೂಲಕ ಹಗರಣ(Scam through QR code scan):-

- ವಂಚಕರು ಸಾಮಾನ್ಯವಾಗಿ ವಿವಿಧ ನೆಪಗಳ ಅಡಿಯಲ್ಲಿ ಗ್ರಾಹಕರನ್ನು ಸಂಪರ್ಕಿಸುತ್ತಾರೆ ಮತ್ತು ಗ್ರಾಹಕರ ಫೋನ್‌ನಲ್ಲಿರುವ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಬಳಸಿಕೊಂಡು ತ್ವರಿತ ಪ್ರತಿಕ್ರಿಯೆ (QR) ಕೋಡ್‌ಗಳನ್ನು ಸ್ಕ್ಯಾನ್ ಮಾಡಲು ಅವರನ್ನು ಮೋಸಗೊಳಿಸುತ್ತಾರೆ.

- ಅಂತಹ ಕಿಖ ಕೋಡ್‌ಗಳನ್ನು ಸ್ಕ್ಯಾನ್ ಮಾಡುವ ಮೂಲಕ, ಗ್ರಾಹಕರು ತಮ್ಮ ಖಾತೆಯಿಂದ ಹಣವನ್ನು ಹಿಂಪಡೆಯಲು ವಂಚಕರಿಗೆ ತಿಳಿಯದೆ ಅಧಿಕಾರ ನೀಡಬಹುದು.

ಮುನ್ನಚ್ಚರಿಕೆಗಳು : –

- ಯಾವುದೇ ಪಾವತಿ ಅಪ್ಲಿಕೇಶನ್ ಬಳಸಿ QR ಕೋಡ್/ಗಳನ್ನು ಸ್ಕ್ಯಾನ್ ಮಾಡುವಾಗ ಜಾಗರೂಕರಾಗಿರಿ. QR ಕೋಡ್‌ಗಳು ನಿರ್ದಿಷ್ಟ ಖಾತೆಗೆ ಹಣವನ್ನು ವರ್ಗಾಯಿಸಲು ಖಾತೆಯ ವಿವರಗಳನ್ನು ಒಳಗೊಂಡಿರುತ್ತವೆ.
- ಹಣವನ್ನು ಸ್ವೀಕರಿಸಲು ಯಾವುದೇ QR ಕೋಡ್ ಅನ್ನು ಸ್ಕ್ಯಾನ್ ಮಾಡಬೇಡಿ. ಹಣದ ಸ್ವೀಕೃತಿಯನ್ನು ಒಳಗೊಂಡಿರುವ ವಹಿವಾಟುಗಳಿಗೆ ಬಾರ್‌ಕೋಡ್‌ಗಳು / ಕ್ಯೂಆರ್ ಕೋಡ್‌ಗಳನ್ನು ಸ್ಕ್ಯಾನ್ ಮಾಡುವ ಅಗತ್ಯವಿಲ್ಲ ಅಥವಾ ಮೊಬೈಲ್ ಬ್ಯಾಂಕಿಂಗ್ ಪಿನ್ (ಎಂ–ಪಿನ್), ಪಾಸ್‌ವರ್ಡ್‌ಗಳು ಇತ್ಯಾದಿಗಳನ್ನು ನಮೂದಿಸುವ ಅಗತ್ಯವಿಲ್ಲ.

ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮದಲ್ಲಿ ಸೋಗು ಹಾಕುವುದು(Impersonation on social media):-

- ವಂಚಕರು ಫೇಸ್‌ಬುಕ್, ಇನ್‌ಸ್ಟಾಗ್ರಾಮ್, ಟ್ವಿಟರ್ ಇತ್ಯಾದಿ ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮಗಳ ಬಳಕೆದಾರರ ವಿವರಗಳನ್ನು ಬಳಸಿಕೊಂಡು ನಕಲಿ ಖಾತೆಗಳನ್ನು ರಚಿಸುತ್ತಾರೆ.
- ವಂಚಕರು ನಂತರ ತುರ್ತು ವೈದ್ಯಕೀಯ ಉದ್ದೇಶಗಳು, ಪಾವತಿಗಳು ಇತ್ಯಾದಿಗಳಿಗಾಗಿ ಹಣವನ್ನು ಕೇಳುವ ವಿನಂತಿಯನ್ನು ಬಳಕೆದಾರರ ಸ್ನೇಹಿತರಿಗೆ ಕಳುಹಿಸುತ್ತಾರೆ.
- ವಂಚಕರು, ನಕಲಿ ವಿವರಗಳನ್ನು ಬಳಸಿ, ಬಳಕೆದಾರರನ್ನು ಸಂಪರ್ಕಿಸಿ ಮತ್ತು ಸಮಯದ ಅವಧಿಯಲ್ಲಿ ಬಳಕೆದಾರರ ವಿಶ್ವಾಸವನ್ನು ಗಳಿಸುತ್ತಾರೆ. ಬಳಕೆದಾರರು ತಮ್ಮ ವೈಯಕ್ತಿಕ ಅಥವಾ ಖಾಸಗಿ ಮಾಹಿತಿಯನ್ನು ಹಂಚಿಕೊಂಡಾಗ, ವಂಚಕರು ಅಂತಹ ಮಾಹಿತಿಯನ್ನು ಬ್ಲ್ಯಾಕ್‌ಮೇಲ್ ಮಾಡಲು ಅಥವಾ ಬಳಕೆದಾರರಿಂದ ಹಣವನ್ನು ಸುಲಿಗೆ ಮಾಡಲು ಬಳಸುತ್ತಾರೆ.

ಮುನ್ನಚ್ಚರಿಕೆಗಳು : –

- ಪ್ರೊಫೈಲ್ ಸೋಗು ಹಾಕಿಲ್ಲ ಎಂಬುದನ್ನು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಲು ಫೋನ್ ಕರೆ/ಭೌತಿಕ ಸಭೆಯ ಮೂಲಕ ದೃಢೀಕರಿಸುವ ಮೂಲಕ ಯಾವಾಗಲೂ ಸ್ನೇಹಿತ/ಸಂಬಂಧಿಯಿಂದ ಬಂದ ನಿಧಿಯ ವಿನಂತಿಯ ನೈಜತೆಯನ್ನು ಪರಿಶೀಲಿಸಿ.
- ಅಪರಿಚಿತ ವ್ಯಕ್ತಿಗಳಿಗೆ ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಪಾವತಿಗಳನ್ನು ಮಾಡಬೇಡಿ.
- ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮ ವೇದಿಕೆಗಳಲ್ಲಿ ವೈಯಕ್ತಿಕ ಮತ್ತು ಗೌಪ್ಯ ಮಾಹಿತಿಯನ್ನು ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.

ಜ್ಯೂಸ್ ಜಾಕಿಂಗ್(Juice jacking) :-

- ಮೊಬೈಲ್‌ನ ಚಾರ್ಜಿಂಗ್ ಪೋರ್ಟ್ ಅನ್ನು ಫೈಲ್‌ಗಳು / ಡೇಟಾವನ್ನು ವರ್ಗಾಯಿಸಲು ಸಹ ಬಳಸಬಹುದು.
- ವಂಚಕರು ಸಾರ್ವಜನಿಕ ಚಾರ್ಜಿಂಗ್ ಪೋರ್ಟ್‌ಗಳನ್ನು ಮಾಲ್‌ವೇರ್ ಅನ್ನು ಅಲ್ಲಿ ಸಂಪರ್ಕಗೊಂಡಿರುವ ಗ್ರಾಹಕರ ಫೋನ್‌ಗಳಿಗೆ ವರ್ಗಾಯಿಸಲು ಬಳಸುತ್ತಾರೆ ಮತ್ತು ಗ್ರಾಹಕರ ಮೊಬೈಲ್ ಫೋನ್‌ಗಳಿಂದ ಇಮೇಲ್‌ಗಳು, ಖಿಒಖಿ, ಉಳಿಸಿದ ಪಾಸ್‌ವರ್ಡ್‌ಗಳು ಇತ್ಯಾದಿಗಳಂತಹ ಸೂಕ್ಷ್ಮ ಡೇಟಾವನ್ನು ನಿಯಂತ್ರಣ / ಪ್ರವೇಶ / ಕದಿಯುತ್ತಾರೆ (ಜ್ಯೂಸ್ ಜಾಕಿಂಗ್).

ಮುನ್ನಚ್ಚರಿಕೆಗಳು : –

- ಸಾರ್ವಜನಿಕ / ಅಪರಿಚಿತ ಚಾರ್ಜಿಂಗ್ ಪೋರ್ಟ್‌ಗಳು / ಕೇಬಲ್‌ಗಳನ್ನು ಬಳಸುವುದನ್ನು ತಪ್ಪಿಸಿ.

ಲಾಟರಿ ವಂಚನೆ(Lottery fraud):-

- ಗ್ರಾಹಕರು ದೊಡ್ಡ ಲಾಟರಿ ಗೆದ್ದಿದ್ದಾರೆ ಎಂದು ವಂಚಕರು ಇಮೇಲ್‌ಗಳನ್ನು ಕಳುಹಿಸುತ್ತಾರೆ ಅಥವಾ ಫೋನ್ ಕರೆಗಳನ್ನು ಮಾಡುತ್ತಾರೆ. ಆದಾಗ್ಯೂ, ಹಣವನ್ನು ಸ್ವೀಕರಿಸಲು, ವಂಚಕರು ತಮ್ಮ ಬ್ಯಾಂಕ್ ಖಾತೆ / ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ವಿವರಗಳನ್ನು ವಂಚಕರು ವಂಚನೆ ಮಾಡುವವರು ವಶಪಡಿಸಿಕೊಂಡಿರುವ ವೆಬ್‌ಸೈಟ್‌ನಲ್ಲಿ ನಮೂದಿಸುವ ಮೂಲಕ ತಮ್ಮ ಗುರುತನ್ನು ದೃಢೀಕರಿಸಲು ಗ್ರಾಹಕರನ್ನು ಕೇಳುತ್ತಾರೆ.
- ವಂಚಕರು ಗ್ರಾಹಕರನ್ನು ತೆರಿಗೆಗಳು/ಫಾರೆಕ್ಸ್ ಶುಲ್ಕಗಳು/ಮುಂಗಡವಾಗಿ ಪಾವತಿಸಲು ಅಥವಾ ಶಿಪ್ಪಿಂಗ್ ಅನ್ನು ಪಾವತಿಸಲು ಕೇಳುತ್ತಾರೆ
- ಲಾಟರಿ / ಉತ್ಪನ್ನವನ್ನು ಸ್ವೀಕರಿಸಲು ಶುಲ್ಕಗಳು, ಸಂಸ್ಕರಣೆ / ನಿರ್ವಹಣೆ ಶುಲ್ಕ ಇತ್ಯಾದಿ.
- ಕೆಲವು ಸಂದರ್ಭಗಳಲ್ಲಿ ವಂಚಕರು, RBI ಅಥವಾ ವಿದೇಶಿ ಬ್ಯಾಂಕ್/ಕಂಪನಿ/ಅಂತರರಾಷ್ಟ್ರೀಯ ಹಣಕಾಸು ಸಂಸ್ಥೆಯ ಪ್ರತಿನಿಧಿಯಾಗಿ ಪೋಸ್ ನೀಡಬಹುದು ಮತ್ತು ಆ ಸಂಸ್ಥೆಯಿಂದ ವಿದೇಶಿ ಕರೆನ್ಸಿಯಲ್ಲಿ ದೊಡ್ಡ ಮೊತ್ತವನ್ನು ಸ್ವೀಕರಿಸಲು ತುಲನಾತ್ಮಕವಾಗಿ ಸಣ್ಣ ಮೊತ್ತವನ್ನು ವರ್ಗಾಯಿಸಲು ಗ್ರಾಹಕರನ್ನು ಕೇಳಿಕೊಳ್ಳಬಹುದು.
- ವಿನಂತಿಸಿದ ಹಣವು ಸಾಮಾನ್ಯವಾಗಿ ಭರವಸೆ ನೀಡಿದ ಲಾಟರಿ / ಬಹುಮಾನದ ಅತ್ಯಂತ ಕಡಿಮೆ ಶೇಕಡಾವಾರು ಆಗಿರುವುದರಿಂದ, ಗ್ರಾಹಕನು ವಂಚಕನ ಬಲೆಗೆ ಬೀಳಬಹುದು ಮತ್ತು ಪಾವತಿ.

ಮುನ್ನಚ್ಚರಿಕೆಗಳು : –

- ಅಂತಹ ನಂಬಲಾಗದ ಲಾಟರಿ ಅಥವಾ ಕೊಡುಗೆಗಳ ಬಗ್ಗೆ ಎಚ್ಚರದಿಂದಿರಿ – ಯಾರೂ ಉಚಿತ ಹಣವನ್ನು ನೀಡುವುದಿಲ್ಲ, ವಿಶೇಷವಾಗಿ ಅಂತಹ ದೊಡ್ಡ ಮೊತ್ತದ ಹಣವನ್ನು.
- ಯಾವುದೇ ಲಾಟರಿ ಕರೆಗಳು / ಇಮೇಲ್‌ಗಳಿಗೆ ಪ್ರತಿಕ್ರಿಯೆಯಾಗಿ ಪಾವತಿಗಳನ್ನು ಮಾಡಬೇಡಿ ಅಥವಾ ಸುರಕ್ಷಿತ ರುಜುವಾತುಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳಬೇಡಿ.
- RBI ಎಂದಿಗೂ ಸಾರ್ವಜನಿಕರ ಖಾತೆಗಳನ್ನು ತೆರೆಯುವುದಿಲ್ಲ ಅಥವಾ ಅವರಿಂದ ಠೇವಣಿಗಳನ್ನು ತೆಗೆದುಕೊಳ್ಳುವುದಿಲ್ಲ. ಇಂತಹ ಸಂದೇಶಗಳು ಮೋಸದಿಂದ ಕೂಡಿರುತ್ತವೆ.
- RBI ಎಂದಿಗೂ ಸಾರ್ವಜನಿಕರ ವೈಯಕ್ತಿಕ / ಬ್ಯಾಂಕ್ ವಿವರಗಳನ್ನು ಕೇಳುವುದಿಲ್ಲ. ನಕಲಿ RBI ಲೋಗೋಗಳು ಮತ್ತು ಸಂದೇಶಗಳ ಬಗ್ಗೆ ಎಚ್ಚರದಿಂದಿರಿ.
- ಬಹುಮಾನದ ಹಣ, ಸರ್ಕಾರಿ ನೆರವು ಮತ್ತು ಬ್ಯಾಂಕ್‌ಗಳು, ಸಂಸ್ಥೆಗಳು ಇತ್ಯಾದಿಗಳಿಂದ ಬಹುಮಾನದ ಹಣವನ್ನು ಸ್ವೀಕರಿಸಲು ನಿಮ್ಮ ಗ್ರಾಹಕರನ್ನು ತಿಳಿದುಕೊಳ್ಳಿ (KYC) ಅಪ್‌ಡೇಟ್ ನೀಡುವ/ ಭರವಸೆ ನೀಡುವ ಸಂದೇಶಗಳಿಗೆ ಎಂದಿಗೂ ಪ್ರತಿಕ್ರಿಯಿಸಬೇಡಿ.

ಆನ್‌ಲೈನ್ ಉದ್ಯೋಗ ವಂಚನೆ(Online job fraud):-

- ವಂಚಕರು ನಕಲಿ ಉದ್ಯೋಗ ಹುಡುಕಾಟ ವೆಬ್‌ಸೈಟ್‌ಗಳನ್ನು ರಚಿಸುತ್ತಾರೆ ಮತ್ತು ಉದ್ಯೋಗಾಕಾಂಕ್ಷಿಗಳು ನೋಂದಣಿ ಸಮಯದಲ್ಲಿ ಈ ವೆಬ್‌ಸೈಟ್‌ಗಳಲ್ಲಿ ತಮ್ಮ ಬ್ಯಾಂಕ್ ಖಾತೆ /

ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ / ಡೆಬಿಟ್ ಕಾರ್ಡ್‌ನ ಸುರಕ್ಷಿತ ರುಜುವಾತುಗಳನ್ನು ಹಂಚಿಕೊಂಡಾಗ, ಅವರ ಖಾತೆಗಳು ರಾಜಿ ಮಾಡಿಕೊಳ್ಳುತ್ತವೆ.

- ವಂಚಕರು ಪ್ರತಿಷ್ಠಿತ ಕಂಪನಿ(ಗಳ) ಅಧಿಕಾರಿಗಳಂತೆ ನಟಿಸುತ್ತಾರೆ ಮತ್ತು ನಕಲಿ ಸಂದರ್ಶನಗಳನ್ನು ನಡೆಸಿದ ನಂತರ ಉದ್ಯೋಗವನ್ನು ನೀಡುತ್ತಾರೆ. ಉದ್ಯೋಗಾಕಾಂಕ್ಷಿ ನಂತರ ನೋಂದಣಿ, ಕಡ್ಡಾಯ ತರಬೇತಿ ಕಾರ್ಯಕ್ರಮ, ಲ್ಯಾಪ್‌ಟಾಪ್ ಇತ್ಯಾದಿಗಳಿಗೆ ಹಣವನ್ನು ವರ್ಗಾಯಿಸಲು ಪ್ರೇರೇಪಿಸಲ್ಪಡುತ್ತಾನೆ.

ಮುನ್ನಚ್ಚರಿಕೆಗಳು : –

- ಸಾಗರೋತ್ತರ ಘಟಕಗಳು ಸೇರಿದಂತೆ ಯಾವುದೇ ಉದ್ಯೋಗ ಆಫರ್‌ಗಾಗಿ, ಮೊದಲು ಉದ್ಯೋಗಿ ಕಂಪನಿ/ಅದರ ಪ್ರತಿನಿಧಿಯ ಗುರುತು ಮತ್ತು ಸಂಪರ್ಕ ವಿವರಗಳನ್ನು ದೃಢೀಕರಿಸಿ.
- ಉದ್ಯೋಗವನ್ನು ನೀಡುವ ನಿಜವಾದ ಕಂಪನಿಯು ಉದ್ಯೋಗವನ್ನು ನೀಡಲು ಎಂದಿಗೂ ಹಣವನ್ನು ಕೇಳುವುದಿಲ್ಲ ಎಂಬುದನ್ನು ಯಾವಾಗಲೂ ನೆನಪಿನಲ್ಲಿಡಿ.
- ಅಜ್ಞಾತ ಉದ್ಯೋಗ ಹುಡುಕಾಟ ವೆಬ್‌ಸೈಟ್‌ಗಳಲ್ಲಿ ಪಾವತಿಗಳನ್ನು ಮಾಡಬೇಡಿ.

ಹಣದ ಹೇಸರಗತ್ತೆಗಳು(Money mules):-

- ಮನಿ ಮ್ಯೂಲ್ ಎನ್ನುವುದು ತಮ್ಮ ಬ್ಯಾಂಕ್ ಖಾತೆಗಳ ಮೂಲಕ ಕದ್ದ / ಅಕ್ರಮ ಹಣವನ್ನು ಲಾಂಡರಿಂಗ್ ಮಾಡಲು ವಂಚಕರಿಂದ ವಂಚಿತರಾದ ಅಮಾಯಕ ಬಲಿಪಶುಗಳನ್ನು ವಿವರಿಸಲು ಬಳಸಲಾಗುವ ಪದವಾಗಿದೆ.
- ವಂಚಕರು ಇಮೇಲ್‌ಗಳು, ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮ ಇತ್ಯಾದಿಗಳ ಮೂಲಕ ಗ್ರಾಹಕರನ್ನು ಸಂಪರ್ಕಿಸುತ್ತಾರೆ ಮತ್ತು ಆಕರ್ಷಕ ಕಮಿಷನ್‌ಗಳಿಗೆ ಬದಲಾಗಿ ತಮ್ಮ ಬ್ಯಾಂಕ್ ಖಾತೆಗಳಿಗೆ (ಹಣ ಹೇಸರಗತ್ತೆ) ಹಣವನ್ನು ಸ್ವೀಕರಿಸಲು ಅವರಿಗೆ ಮನವರಿಕೆ ಮಾಡುತ್ತಾರೆ.
- ಹಣದ ಹೇಸರಗತ್ತೆಯು ಹಣವನ್ನು ಮತ್ತೊಂದು ಹಣದ ಹೇಸರಗತ್ತೆಯ ಖಾತೆಗೆ ವರ್ಗಾಯಿಸಲು ನಿರ್ದೇಶಿಸಲ್ಪಡುತ್ತದೆ, ಇದು ಸರಪಳಿಯನ್ನು ಪ್ರಾರಂಭಿಸುತ್ತದೆ, ಅದು ಅಂತಿಮವಾಗಿ ಹಣವನ್ನು ವಂಚಕನ ಖಾತೆಗೆ ವರ್ಗಾಯಿಸುತ್ತದೆ.
- ಪರ್ಯಾಯವಾಗಿ, ವಂಚಕನು ಹಣವನ್ನು ಹಿಂಪಡೆಯಲು ಮತ್ತು ಯಾರಿಗಾದರೂ ಹಸ್ತಾಂತರಿಸಲು ಹಣದ ಹೇಸರಗತ್ತೆಗೆ ನಿರ್ದೇಶಿಸಬಹುದು.
- ಇಂತಹ ವಂಚನೆಗಳು ವರದಿಯಾದಾಗ, ಹಣದ ಹೇಸರಗತ್ತೆಯು ಮನಿ ಲಾಂಡರಿಂಗ್‌ಗಾಗಿ ಪೋಲೀಸರ ತನಿಖೆಯ ಗುರಿಯಾಗುತ್ತದೆ.

ಮುನ್ನಚ್ಚರಿಕೆಗಳು : –

- ಶುಲ್ಕ / ಪಾವತಿಗಾಗಿ ಹಣವನ್ನು ಸ್ವೀಕರಿಸಲು ಅಥವಾ ವರ್ಗಾಯಿಸಲು ನಿಮ್ಮ ಖಾತೆಯನ್ನು ಬಳಸಲು ಇತರರಿಗೆ ಅನುಮತಿಸಬೇಡಿ.
- ನಿಮ್ಮ ಬ್ಯಾಂಕ್ ಖಾತೆ ವಿವರಗಳನ್ನು ಕೇಳುವ ಇಮೇಲ್‌ಗಳಿಗೆ ಪ್ರತಿಕ್ರಿಯಿಸಬೇಡಿ.
- ಆಕರ್ಷಕ ಕೊಡುಗೆಗಳು / ಕಮಿಷನ್‌ಗಳಿಗೆ ಒಳಗಾಗಬೇಡಿ ಮತ್ತು ಅನಧಿಕೃತ ಹಣವನ್ನು ಸ್ವೀಕರಿಸಲು ಮತ್ತು ಇತರರಿಗೆ ವರ್ಗಾಯಿಸಲು ಅಥವಾ ಹಣವನ್ನು ಹಿಂಪಡೆಯಲು ಮತ್ತು ಅದನ್ನು ಉತ್ತಮ ಶುಲ್ಕಕ್ಕೆ ನೀಡಲು ಒಪ್ಪಿಗೆ ನೀಡಬೇಡಿ.

- ನಿಧಿಯ ಮೂಲವು ನಿಜವಾಗಿಲ್ಲದಿದ್ದರೆ ಅಥವಾ ಆಧಾರವಾಗಿರುವ ವ್ಯವಹಾರದ ತಾರ್ಕಿಕತೆಯನ್ನು ಅಧಿಕಾರಿಗಳಿಗೆ ಸಾಬೀತುಪಡಿಸದಿದ್ದರೆ, ಹಣವನ್ನು ಸ್ವೀಕರಿಸುವವರು ಪೊಲೀಸ್ ಮತ್ತು ಇತರ ಕಾನೂನು ಜಾರಿ ಸಂಸ್ಥೆಗಳೊಂದಿಗೆ ಗಂಭೀರ ತೊಂದರೆಗೆ ಸಿಲುಕುವ ಸಾಧ್ಯತೆಯಿದೆ.

****