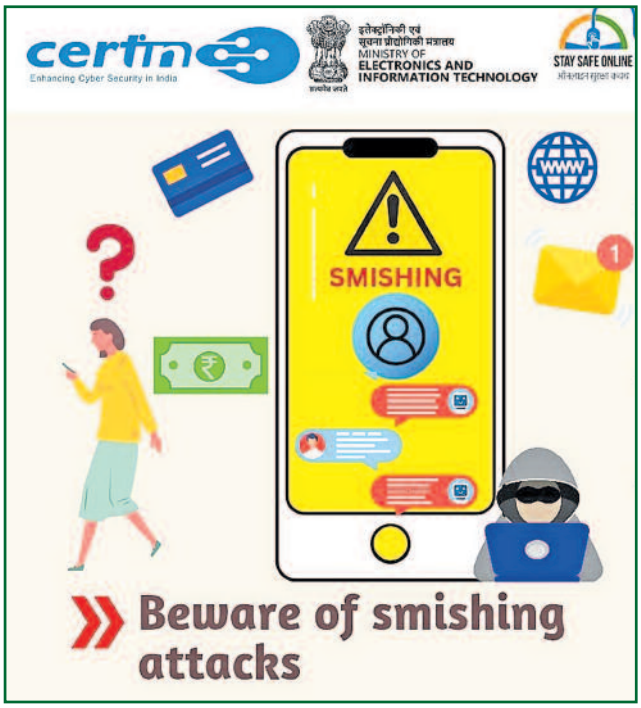
ಫಿಶಿಂಗ್ ರೂಪಾಂತರಿ 'ಸ್ಮಿಶಿಂಗ್'

ಫಿಶಿಂಗ್ ರೂಪಾಂತರ ತಳಿ 'ಸ್ಮಿಶಿಂಗ್' ಸಕ್ರಿಯವಾಗಿದೆ. ಇದು ಸೈಬರ್ ಕೃತ್ಯದ ಹೊಸ ರೂಪವಾಗಿ ಎಲ್ಲೆಡೆ ಕಾಣಿಸಿಕೊಳ್ಳುತ್ತಿದ್ದು, ಈ ಬಗ್ಗೆ ಜಾಗೃತಿ ವಹಿಸುವಂತೆ ಸರ್ಟ್-ಇನ್ ಜನರಿಗೆ ಎಚ್ಚರಿಸಿದೆ.



■ ಶಶಿಕುಮಾರ್ ಸಿ.

ಸಾಮಾಜಿಕ ಜಾಲತಾಣಗಳು, ಸ್ಮಾರ್ಟ್‌ಫೋನ್, ಇಮೇಲ್ ಸೇರಿದಂತೆ ಭಿನ್ನ ಮಾರ್ಗಗಳ ಮೂಲಕ ಟೆಕ್ಸ್ಟ್ ಮೆಸೇಜ್‌ಗಳನ್ನು ಹಾಗೂ ಲಿಂಕ್‌ಗಳನ್ನು ರವಾನಿಸಿ ಜನರನ್ನು ವಂಚನೆಯ ಜಾಲವೊಂದು ಸದ್ಯ ದೇಶದೆಲ್ಲೆಡೆ ಸಕ್ರಿಯವಾಗಿದ್ದು, ಈ ಕೃತ್ಯವನ್ನು 'ಸ್ಮಿಶಿಂಗ್' ಎಂದು ಕರೆಯಲಾಗುತ್ತಿದೆ. ಈ ಬಗ್ಗೆ ಎಚ್ಚರವಹಿಸುವಂತೆ ಕೇಂದ್ರ ಸರ್ಕಾರದ ಅಧೀನದಲ್ಲಿರುವ 'ಸರ್ಟ್-ಇನ್' ಸೂಚಿಸಿದೆ.

ಸ್ಮಿಶಿಂಗ್ ಹೆಸರು ಹೊಸದಾದರೂ ಈ ವಂಚನೆಯ ಜಾಲವು ಅನುಸರಿಸುತ್ತಿರುವ ವಿಧಾನ ಮಾತ್ರ ಹಳೆಯದು. ದೋಷಪೂರಿತ ಅಥವಾ ಮಾಲ್‌ವೇರ್ ಒಳಗೊಂಡ ಲಿಂಕ್‌ಗಳನ್ನು ಎಲ್ಲೆಡೆ ಹರಿಬಿಟ್ಟು, ಅದನ್ನು ಕ್ಲಿಕ್ಕಿಸಿದವರನ್ನು ವಂಚನೆಯ ಬಲೆಗೆ ಬೀಳಿಸುವ ಪ್ರಕ್ರಿಯೆ ಹಿಂದಿನಿಂದಲೂ ನಡೆಯುತ್ತಲೇ ಇದೆ. ಸ್ಮಿಶಿಂಗ್ ಹೆಸರಿನಲ್ಲಿ ಇದು ಮತ್ತೆ ಮುನ್ನೆಲೆಗೆ ಬಂದಿದೆ. ಇದನ್ನು ಫಿಶಿಂಗ್‌ನ ರೂಪಾಂತರವೆನ್ನಬಹುದು.

ಡಿಜಿಟಲ್ ಬಳಕೆದಾರರ ಯೂಸರ್‌ನೇಮ್, ಪಾಸ್‌ವರ್ಡ್, ಕ್ರೆಡಿಟ್ ಕಾರ್ಡ್ ಸಂಖ್ಯೆ ಮತ್ತು ಬ್ಯಾಂಕ್ ಖಾತೆ ಸಂಖ್ಯೆಯಂತಹ ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿ ಕದ್ದು, ಅದನ್ನು ದುರುಪಯೋಗಪಡಿಸಿಕೊಳ್ಳುವ ಹಾಗೂ ಮಾರಾಟ ಮಾಡುವ ಪ್ರಕ್ರಿಯೆಗೆ ಫಿಶಿಂಗ್ ಎನ್ನಬಹುದು. ಸ್ಮಿಶಿಂಗ್-ಫಿಶಿಂಗ್ ಎರಡರ ಉದ್ದೇಶ ಸೈಬರ್ ಅಪರಾಧವೆಸಗುವುದು.

ಡಿಜಿಟಲೀಕರಣದ ನಂತರ ಸೈಬರ್ ಕ್ರೈಮ್ ಪ್ರಕರಣಗಳು ದಿನದಿಂದ ದಿನಕ್ಕೆ ಹೆಚ್ಚಾಗುತ್ತಲೇ ಇವೆ. ಡಿಜಿಟಲ್ ಬಳಕೆದಾರರನ್ನು ನಾನಾ ಬಗೆಯಲ್ಲಿ ವಂಚನೆಗೊಳಿಸಲಾಗುತ್ತಿದೆ. ಈ ಬಗ್ಗೆ ಜನರು ಎಚ್ಚೆತ್ತುಕೊಂಡ ಬಳಿಕವೂ ಹೊಸ ರೀತಿಯಲ್ಲಿ ಹೇಗೆಲ್ಲಾ ಮೋಸಗೊಳಿಸಬಹುದು, ಹೇಗೆಲ್ಲಾ ಹಣ ಎಗರಿಸಬಹುದು ಎಂಬುದರ ಬಗ್ಗೆ ಸೈಬರ್ ಖದೀಮರು ಹೊಂಚುಹಾಕುತ್ತಿದ್ದಾರೆ. ಒಟಿಪಿ ಸ್ಕ್ಯಾಮ್, ಫಿಶಿಂಗ್, ನಕಲಿ ಅಪ್ಲಿಕೇಷನ್‌ಗಳು, ಕ್ಯೂಆರ್ ಕೋಡ್ ಸ್ಕ್ಯಾಮ್‌ಗಳು, ಹನಿ ಟ್ರ್ಯಾಪ್, ಬ್ಯಾಂಕ್ ವಂಚನೆ ಹೀಗೆ ಅನೇಕ ರೀತಿಯಲ್ಲಿ ಮೋಸ ಎಸಗುತ್ತಿದ್ದಾರೆ.

ಸ್ಮಿಶಿಂಗ್ ಟೆಕ್ಸ್ಟ್ ಅಥವಾ ಲಿಂಕ್‌ಗಳು 'ನಂಬಲರ್ಹ' ಮೂಲದ ಸೋಗಿನಲ್ಲಿರುತ್ತವೆ. ಆದರೆ ಅವು ನಂಬಲರ್ಹವಲ್ಲ. ಮೋಸಗೊಳಿಸುವ ಉದ್ದೇಶವುಳ್ಳ ಸಂದೇಶಗಳನ್ನು ಕಳುಹಿಸುವುದು ಇವುಗಳ ಕಾರ್ಯ. ಹೀಗೆ ಕಳುಹಿಸಿದ ದುರುದ್ದೇಶಪೂರಿತ ಲಿಂಕ್‌ಗಳು ಹಾಗೂ ಟೆಕ್ಸ್ಟ್ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡಿದರೆ ತಾನಾಗಿಯೇ ಮಾಹಿತಿಯನ್ನು ಕಳ್ಳರ ಕೈಗಿಟ್ಟಂತಾಗುತ್ತದೆ. ಲಿಂಕ್ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡಿದರೆ ಕೆಲವೊಮ್ಮೆ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಒದಗಿಸುವಂತೆ ಅಮಾಯಕರನ್ನು ಪುಸಲಾಯಿಸಿ ತಕ್ಷಣವೇ ವಂಚನೆಗೊಳಪಡಿಸುತ್ತಾರೆ.

ಸ್ಮಿಶಿಂಗ್ ಪ್ರಕರಣಗಳು ಹಲವೆಡೆ ವರದಿಯಾದ ಬೆನ್ನಲ್ಲೇ ಸರ್ಟ್-ಇನ್ ತನ್ನ ಎಕ್ಸ್ (ಟ್ವಿಟರ್) ಖಾತೆಯಲ್ಲಿ ಎಚ್ಚರಿಕೆಯ ಪೋಸ್ಟರ್ ಹಂಚಿಕೊಂಡಿದ್ದು, ಎಚ್ಚರದಿಂದಿರುವಂತೆ ಜನರಿಗೆ ಸಲಹೆ ನೀಡಿದೆ. 'ಹಣಕಾಸು ವಂಚನೆ ಮಾಡುವ ಸಲುವಾಗಿ, ಬಳಕೆದಾರರ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಸಂಗ್ರಹಿಸಲು ಪಠ್ಯ ಸಂದೇಶಗಳನ್ನು ಕಳುಹಿಸುವ ಮೂಲಕ ವಂಚಕರು ಈ ಸ್ಮಿಶಿಂಗ್ ತಂತ್ರ ಬಳಸುತ್ತಿದ್ದಾರೆ' ಎಂದಿದೆ ಸರ್ಟ್-ಇನ್.

ಇರುವುದೊಂದೆ ಮಾರ್ಗ...

ಸ್ಮಿಶಿಂಗ್ ದಾಳಿಗೆ ಬಲಿಯಾಗುವುದನ್ನು ತಪ್ಪಿಸಲು, ಅನಧಿಕೃತ ಮೂಲದ ಟೆಕ್ಸ್ಟ್ ಹಾಗೂ ಲಿಂಕ್‌ಗಳ ಮೇಲೆ ಕ್ಲಿಕ್ ಮಾಡದೆ ಇರುವುದೊಂದೇ ಆಯ್ಕೆ ಜನರಿಗಿರುವುದು. ಈ ಬಗ್ಗೆ ಜನರು ವೈಯಕ್ತಿಕವಾಗಿ ಜಾಗರೂಕರಾಗಬೇಕು. ಮುಖ್ಯವಾಗಿ ಅಪರಿಚಿತ ಅಥವಾ ಪರಿಶೀಲಿಸದ ಮೂಲಗಳಿಂದ ಲಿಂಕ್‌ಗಳನ್ನು ಕ್ಲಿಕ್ ಮಾಡುವುದನ್ನು ತಪ್ಪಿಸಬೇಕು.

ಸರ್ಟ್-ಇನ್ ಸಲಹೆಗಳು

- ಎಸ್ಎಂಎಸ್ / ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮ ಚಾರ್ಟ್‌ಗಳು ಅಥವಾ ಪೋಸ್ಟ್‌ಗಳಲ್ಲಿನ ಯಾವುದೇ ಅನುಮಾನಾಸ್ಪದ ಲಿಂಕ್ ಕ್ಲಿಕ್ ಮಾಡಬೇಡಿ.
- ಸಂಕ್ಷಿಪ್ತ URLಗಳನ್ನು ಮೌಲ್ಯೀಕರಿಸಲು ಆನ್‌ಲೈನ್ ಸಂಪನ್ಮೂಲಗಳನ್ನು ಬಳಸಿ.
- ಫೋನ್, ಲ್ಯಾಪ್‌ಟಾಪ್‌ಗೆ ಬಂದ ಲಿಂಕ್ ಕ್ಲಿಕ್ ಮಾಡುವ ಮೊದಲು, ಅದರ ಮೂಲದ ಬಗ್ಗೆ ಪರಿಶೀಲಿಸಿ.
- ನವೀಕರಿಸಿದ ಆ್ಯಂಟಿವೈರಸ್ ಮತ್ತು ಆ್ಯಂಟಿಮಾಲ್ವೇರ್ ಉಪಕರಣಗಳನ್ನು ಬಳಸಿ.
- ಬ್ಯಾಂಕ್ ಅಥವಾ ಸಂಸ್ಥೆಯಿಂದ ಅನುಮಾನಾಸ್ಪದ ಸಂದೇಶ ಸ್ವೀಕರಿಸಿದರೆ, ತಕ್ಷಣವೇ ಸಂಬಂಧಿಸಿದವರನ್ನು ಸಂಪರ್ಕಿಸಿ.
- ವೈಯಕ್ತಿಕ ಆನ್‌ಲೈನ್ ವಹಿವಾಟುಗಳಿಗಾಗಿ ಪ್ರತ್ಯೇಕ ಇಮೇಲ್ ಖಾತೆ ಬಳಸಿ.
- ಇಮೇಲ್‌ಗಳು ಮತ್ತು ಬ್ಯಾಂಕ್ ಖಾತೆಗಳಿಗಾಗಿ ಬಹು ಅಂಶದ ದೃಢೀಕರಣ (MFA) ಅಳವಡಿಸಿಕೊಳ್ಳಿ.
- ಇತ್ತೀಚಿನ ಅಪ್‌ಡೇಟ್‌ಗಳೊಂದಿಗೆ ಆಪರೇಟಿಂಗ್ ಸಿಸ್ಟಮ್ ಮತ್ತು ಸಾಫ್ಟ್‌ವೇರ್ ನವೀಕರಿಸಿ. ■