



టెక్ టాక్

ఎన్క్రిప్షన్ ఈజ్

సూపర్ ప్రైవేసీ

ఒకప్పుడు డైరీ రాయడం చాలామంది అలవాటుగా ఉండేది. యూజర్ ఐడీలు, పాస్ వర్డులు లేకపోయినా.. ఒకరి డైరీ చదవొద్దన్న నైతికత దానికి రక్షణ కల్పించేది. ఇప్పుడు ఫంగర్ప్రింటింగ్ లాక్, ప్యాటర్న్ పాస్వర్డ్ ఎన్ని ఉన్నా.. డేటా భద్రత 2జీ సిగ్నల్ కన్నా బలహీనంగా ఉంటున్నది. మెసేజ్ రూపంలోనే ఫోన్లోకి చొరబడి వ్యక్తిగత సమాచారాన్ని కొల్లగొట్టేస్తున్నారు స్కామర్లు. అయితే, ఆన్లైన్ అకౌంట్లను ఎన్క్రిప్ట్ చేయడం ద్వారా స్టార్ట్ దునియాలో సేఫ్గా ఉండొచ్చు.

ఎన్క్రిప్షన్ అంటే మన డేటాను ఇతరులు యాక్సెస్ చేయకుండా కల్పించే రక్షణ. ఉదాహరణకు వాట్సాప్ లో మనం ఒక మెసేజ్ పంపాం అనుకోండి. వాట్సాప్ ఎన్క్రిప్ట్ చేయడం ద్వారా మనం పంపే సందేశాలు జంబుల్ గా మారిపోతాయి. దీనిని క్రిప్టోగ్రఫీ అంటారు. మీరు ఎవరికి పంపారో ఆ వ్యక్తికి మాత్రం డిస్క్రిప్ట్ మెసేజ్ చేరుతుంది. అలా రిసెప్టర్ మాత్రమే మనం పంపిన మెసేజ్ను చదవగలడు.

ఎన్క్రిప్షన్ చేయడం ఎలాగంటే..

మారిన కాలమాన పరిస్థితుల్లో మన జీవన విధానం అంతా మెయిల్ బాక్స్ లో నిక్షిప్తమైంది. స్కామర్లుగానీ మెయిల్ అకౌంట్ లోకి చొరబడ్డారా.. దానికి లింక్ అయి ఉన్న సామాజిక మాధ్యమాల అకౌంట్లూ ప్రమాదంలో పడ్డాయి. వ్యక్తిగత సమాచారం లూటీ కావొచ్చు. మెయిల్ లోని వివరాల ఆధారంగా మీ బ్యాంకు ఖాతానూ ఇక్కట్లకు గురిచేయొచ్చు. మీ ఇ-మె

యిల్ అకౌంట్ భద్రంగా ఉండాలంటే మెయిల్ బాక్స్ లో టూ-ఫ్యాక్టర్ (2ఎఫ్ఎ) ఆఫ్ టీకేషన్ ఎనేబుల్ చేయాలి. సులభతరమైన పాస్ వర్డ్ కాకుండా కఠినమైనదాన్ని సెటప్ చేయడం ద్వారా అదనపు భద్రత లభిస్తుంది. టూ ఫ్యాక్టర్ ఆఫ్ టీకేషన్ ఎలా ఎనేబుల్ చేసుకోవాలంటే..

- గూగుల్: <https://www.google.com/landing/2step/>
 - ఫేస్ బుక్: <https://www.facebook.com/help/148233965247823>
 - ఇన్ స్టాగ్రామ్: <https://help.instagram.com/566810106808145>
 - ట్విట్టర్: <https://help.twitter.com/en/managing-your-account/two-factor-authentication>
 - లింకీన్: <https://www.linkedin.com/help/linkedin/answer/544/turn-two-step-verification-on-and-off?lang=en>
- హార్డ్ డ్రైవ్ ఎన్క్రిప్షన్**
డెస్క్ టాప్, ల్యాప్ టాప్ లోని డేటా సేఫ్ గా ఉండాలంటే హార్డ్ డ్రైవ్ ఎన్క్రిప్షన్ మంచి మార్గం. డేటాను పూర్తిస్థాయిలో ఎన్క్రిప్ట్ చేయడం ద్వారా మన డివైజ్ లోకి స్కామర్లు తొంగిచూసినా వారికేం బోధపడదు. సిస్టమ్ మీరు ఓపెన్ చేసి, పాస్ వర్డ్ ఎంటర్ చేయగానే డేటా అంతా డిస్క్రిప్ట్ అవుతుంది. ఇండివిడ్యువల్ ఫైల్స్ ను కూడా ఎన్క్రిప్ట్ చేసుకోవచ్చు.

ఒకప్పుడు కేవలం సందేశాలకు, సంభాషణలకు మాత్రమే పరిమితమైన ఫోన్ తో ఇప్పుడు అపరిమితమైన సేవలు పొందుతున్నాం. స్మార్ట్ ఫోన్ వచ్చాక కీలక విషయాలు, బ్యాంకు వివరాలు అన్నీ అందులోనే పొందుపరుస్తున్నాం. ఆర్థిక లావాదేవీలకు బెస్ట్ ఆప్షన్ గా ఫోన్ నే ఎంచుకుంటున్నాం. అయితే, మన అలవాటును స్కామర్లు తమ వెసులుబాటుగా మార్చుకుంటున్నారు. చిటికెలో ఏమార్చి మోసాలకు పాల్పడుతున్నారు. ఫ్రాడ్ స్టర్ల బారిన పడొద్దంటే ఎన్క్రిప్షన్ కు మించిన ప్రైవేసీ లేదంటున్నారు నిపుణులు.

కానీ, ప్రతిసారి పాస్ కోడ్ వాటిని డిస్క్రిప్ట్ చేసుకోవాల్సి వస్తుంది. దానికన్నా.. హార్డ్ డ్రైవ్ ను ఎన్క్రిప్ట్ చేసుకోవడం మేలైన మార్గం. మీ డివైజ్ కు కఠినమైన పాస్ వర్డ్ ఉండటం ముఖ్యమని మరచొద్దు.

యాపిల్ మ్యూజ్ కంప్యూటర్స్ లో హార్డ్ డ్రైవ్ ఎన్క్రిప్షన్ వివరాలు <https://support.apple.com/en-in/guide/disk-utility/dskutl135612/mac> లింక్ ద్వారా తెలుసుకోండి.

విండోస్ ఆపరేటింగ్ సిస్టమ్ అయితే .. <https://support.microsoft.com/en-us/windows/turn-on-device-encryption-0c453637-bc88-5f74-5105-741561aae838> లింక్ ను ఉపయోగించండి.

పాస్ వర్డ్ ప్రాటిక్స్

ఇప్పటికీ మన దేశంలో చాలామంది పాస్ వర్డ్ గా 1234, 0000, 4321 తరహా సాదాసీదా కీ సంబర్ధను ఎంచుకుంటున్నారని సర్వేలు చెబుతున్నాయి. ఫోన్ భద్రతలో పాస్ వర్డ్ కీలకం. పాస్ వర్డ్ ఎంత కఠినంగా ఉంటే.. మీ ఫోన్ అంత సురక్షితంగా ఉంటుంది. ఎవరు పడితేవారు దానిని యాక్సెస్ చేయలేరు. స్కామర్ల చేతికి చిక్కినా మీ ఫోన్ ను అంత తేలిగ్గా ఓపెన్ చేయకుండా ఉండాలంటే పద్మవ్యూహం కన్నా పడునైన పాస్ వర్డ్ ను ఎంపిక చేసుకోవాలి. ఇప్పటివరకు ఉన్న పాస్ వర్డ్ ను కింద సూచించిన లింక్ ల ద్వారా మార్చుకోండి.

- ఆండ్రాయిడ్: <https://support.google.com/android/answer/9079129?hl=en>
- ఐ ఫోన్: <https://support.apple.com/en-in/guide/iphone/iph14a867ae/ios>

సమాచారం ఇలా భద్రం..

వాట్సాప్, సిగ్నల్, టెలిగ్రామ్ తదితర మెసేజింగ్ యాప్స్ లో ఫ్రైవేసీ సెట్టింగ్స్ పకడ్బందీగా ఉండేలా చూసుకోండి.

- టూ స్టెప్ వెరిఫికేషన్ యాక్టివేట్ చేయండి.
- ఫ్రైవేసీ సెట్టింగ్స్ మార్చుకోండి.
- లాక్ కోడ్ ఉండేలా చూసుకోండి.
- అకౌంట్ యాక్టివిటీని ఎప్పటికప్పుడూ గమనిస్తూ ఉండండి.
- ఆటో మెటిక్ బ్యాకప్ ఆప్షన్ ను ఎనేబుల్ చేయండి.



అనిల్ రాచమల్ల
వ్యవస్థాపకులు
ఎండ్ నో ఫౌండేషన్