Everyday Technology

నిత్య జీవితంలో సాంకేతికత

పూర్ణిమ తమ్మిరెడ్డి • వ్యాసాలు

ఎలమి

నిత్య జీవితంలో సాంకేతికత

Everyday Technology
నిత్య జీవితంలో సాంకేతికత
పూర్ణిమ తమ్మిరెడ్డి | Purnima Tammireddy

Elami Publications
Flatno GF 003, Sai Venkat Apartment,
Site No: 8, Prestige Enclave, New AirportRoad,
Bettahalasur Cross,Bengaluru-562157
elamibooks@gmail.com
+91-824747541

© **Purnima Tammireddy**

ISBN: xxxx-xxxx-xx

CoverArt
Rahak

Cover & Book Design
Navnudi
https://navanudi.in
team.navanudi@gmail.com
+91-8977040889

Printed at
Trinity Academy for Corporate Training
Bangalore
+91-9341342475

Sole Distribution
Navodaya Book House
Opp.AArya Samaj Street, Kachiguda X-Roads,
Hyderabad-500027
040-2465-2387, +91-9000413413
www.telugubooks.in

For copies, All leading book storesin AP&Telangana, +91-8247474541

1. అంతర్జాలమందు అనుమానించువాడు ధన్యుడు, సుమతీ!

కంప్యూటర్ హార్డ్‌వేర్, సాఫ్ట్‌వేర్ రెండూ అప్పుడప్పుడే ప్రజలకి అందుబాటులోకి వస్తున్న సమయం అది. 1990 దశకంలో 'మైన్‌స్వీపర్' అని ఒక గేమ్ ఉండేది. ఆ ఆట ప్రారంభంలో గదులన్నీ మూసేసి ఉంటాయి. కొన్నింటి వెనుక అంకెలుంటే, కొన్నింటి వెనుక బాంబులు. ఆట గెలవడానికి బాంబులున్న గడి ఒక్కటి కూడా నొక్కకుండా, అంకెలున్న గదులన్నీ తెరవగలగాలి.

ఈ మైన్‌స్వీపర్ ఆట మొదలుకుని నేటి వరకూ – అంటే, గత రెండు దశాబ్దాల్లో – ఒక ఎండ్ యూజర్‌గా మాత్రమే కాక, నా వృత్తిరీత్యా కూడా టెక్నాలజీ విజృంభించిన వైనాన్ని దగ్గరగా చూస్తున్నాను. టెక్నాలజీ ఎంత త్వరిత గతిన, ఎంత విస్తృతంగా మన జీవితాలతో పెనవేసుకుపోయిందో గుర్తుచేసుకోడానికి ఉదాహరణగా తెలుగువారి జీవితంలో విడదీయలేని భాగమైన సినిమాలు–సినిమా టికెట్ బుకింగ్‌లనే తీసుకుందాం.

'తొలి ప్రేమ' (1998) నాటికి లైన్‌లో నిల్చునో, నిల్చోబెట్టో టికెట్లు కొనుక్కోవాల్సిందే. 'బాలు', 'బంగారం' (2005–06) విడుదల అయ్యేనాటికి ఒకట్రెండు టెలీబుకింగ్ సైట్లు ఉండేవి. మనం ఫోన్ చేసి టికెట్లు బ్లాక్ చేసుకోవచ్చు, కానీ దీన్ని ఎవరూ పెద్దగా వాడినట్టు లేరు.

'జల్సా' (2008) నాటికి బుక్‌మైషో.కాం లాంటి సైట్ల ద్వారా ఆన్‌లైన్ టికెట్లు మామూలైపోయాయి. అయితే ఆన్‌లైన్ ద్వారా మనకోసం సీటు కేటాయించినా,

అది టికెట్ కాదు కాబట్టి మళ్లీ కౌంటర్ దగ్గర నిల్చుని మెసేజ్ చూపించి కాగితపు టికెట్ తీసుకోవాల్సి వచ్చేది.

కొన్నాళ్లకు వాటికీ కియాస్క్‌లు పుట్టుకొచ్చాయి. మన ఆన్‌లైన్ టికెట్ మీదున్న ఒక ప్రత్యేకమైన నంబరును టైప్ చేస్తే ఆ మెషీన్ పేపరు టికెట్లని ఇస్తుంది. అంటే మనిషికి, మనిషికి మధ్య వ్యవహారం (హ్యూమన్–హ్యూమన్ ఇంటరాక్షన్), మనిషికి, మెషీన్‌కి మధ్య వ్యవహారం (హ్యూమన్–మెషీన్ ఇంటరాక్షన్)గా మారిపోయింది.

'అజ్ఞాతవాసి' (2018) వచ్చేసరికి ఆ పేపరు టికెట్లు కూడా అవసరం లేకుండా మొబైల్‌లో కనిపించే క్యూఆర్ (QR) కోడ్‌ను స్కానర్‌కి చూపిస్తే, అది గ్రీన్ సిగ్నల్ ఇవ్వగానే లోపలికి వెళ్లిపోవచ్చు. 'వకీల్ సాబ్' (2021) ఓటీటీలలో (నెట్‌ఫ్లిక్స్, అమెజాన్ వగైరా) చూసే అవకాశం వచ్చేసింది, సినిమా హాళ్లకు కోవిడ్ వల్ల వెళ్లలేకపోయినా.

ఇవన్నీ సౌలభ్యాలు. సినిమా చూడ్డానికి ముందు, ఏ థియటర్‌లో చూడబోతున్నామో ఆ థియటర్ దగ్గరే పడిగాపులు పడి, క్యూలో తోసుకుని, కొట్టుకుని టికెట్లు కొనాల్సిన అవసరంలేని సౌలభ్యాలు.

సినిమా షో ఒక అరగంట ఉందనగా ఎక్కడి నుంచైనా టికెట్ బుక్ చేసుకునే వెసులుబాటు, టికెట్ బుక్ చేసుకునే ముందు ఏయే థియటర్లలో ఎన్ని సీట్లు బుక్ అవుతున్నాయి (అంటే, సినిమా హిట్టా, ఫట్టా) కూడా సుమారుగా తెల్సుకునే వీలు, టికెట్ రూపంలో వచ్చే చిన్న కాగితం ముక్కని సినిమా అయ్యేంతవరకూ జాగ్రత్త చేసుకోవాల్సిన అవసరం లేని హాయి.. జీవితం సుఖంగా మారిపోయింది.

బాంబులుంటాయి జాగ్రత్త..

ఇప్పుడు ఇంటర్నెటునే 'మైన్‌స్వీపర్' గేమ్ అనుకుంటే, ఈ సౌలభ్యాలన్నీ అంకెలున్న గడులని అనుకోవచ్చు. వీటిపైన చెంగుచెంగుమంటూ అడుగులేసుకుంటూ మనం అంతర్జాల (ఇంటర్నెట్) అంతరిక్షంలో (స్పేస్)లో దూసుకెళిపోవచ్చు. దూసుకెళ్ళిపోతున్నాం కూడా.

అంతటా ఇలా సౌలభ్యాల గడులే ఉంటే ఆటలోనైనా, బతుకులోనైనా మజా ఏముంటుంది? ప్రపంచంలో నేరస్థులు, అపరాధులు ఉన్నప్పుడు సైబర్ స్పేస్‌లో ఉండకుండా పోతారా? కానీ మనకే ఆ స్పృహ తక్కువగా ఉంటుంది. పని తర్వగా అయిపోవడం, సులువుగా అయిపోవడం ఇచ్చే నిశ్చింత కాస్త ఎక్కువైపోయి ఏమరపాటు మొదలవుతుంది. అనాలోచితంగా ఎప్పుడో మందుపాతర మీద అడుగు వేస్తాం. అంతే, ఢాం!

"ఆ... అలా మాకేం కాదులెండి. మేం మర్యాదస్తులం. పాడు సైట్లకి వెళ్ళిన పాపాన పోలేదెప్పుడూ! మా మీద ఎవరు పగబట్టి ఇలా నష్టం కలిగించాలనుకుంటారూ?" అని సాగదీస్తుంటారు కొందరు. అడల్ట్ కంటెంట్ చూస్తేనో, రమ్మీలూ లాటరీలూ లాంటివి ఆడితేనో మాత్రమే ఆన్‌లైన్ అపాయాలు కలగవచ్చుననే అపోహలుంటాయి కొందరికి.

అలా ఏం ఉండదు. సినిమాకి టికెట్ బుక్ చేసుకోవడంలాంటి సాధారణ పనిలో కూడా బోలెడు తేడాలు రావచ్చు. మన టికెట్ ఐడి, క్యూఆర్ కోడ్ వేరొకరి చేతిలో పడి, మనకన్నా ముందు వాళ్ళు కలెక్ట్ చేసుకుంటే టికెట్లు మాత్రమే గోవింద! ప్రాణం ఉసూరుమన్నా, పోయిన డబ్బు వందల్లోనే కాబట్టి కావాలంటే ఇంకో షో చూడవచ్చు. అదే, టికెట్ బుక్ చేస్తున్న క్రమంలో క్రెడిట్ కార్డ్ వివరాలు ఇవ్వడంలో అజాగ్రత్తగా ఉంటే బ్యాంక్ బాలెన్స్ అంతా ఇంకెవరో స్వాహా చేసేయచ్చు.

డబ్బు నష్టపోతే అంతో ఇంతో అని లెక్క తేలుతుంది. మనం ఎక్కడ సినిమా చూస్తున్నాం, ఎవరితో చూస్తున్నాం (ఇన్ఫో షేరింగ్), హాలుకు ఏ దారిన, ఎంత వేగంతో చేరుకున్నాం (లొకేషన్ ట్రాకింగ్), సినిమా గురించి సోషల్ మీడియాలో తిట్టుకున్నామా, మెచ్చుకున్నామా (సెంటిమెంట్ అనాలసిస్) లాంటివాటికి కావాల్సిన డేటా ఇప్పటి యాప్స్ ఎటూ సేకరిస్తున్నాయి కాబట్టి, వీటన్నింటిని కలిపి రేపు మనకో ఆన్‌లైన్ వ్యక్తిత్వాన్ని (ఆన్‌లైన్ పర్సోనా) తయారుచేసి దాన్ని మనకి ప్రతినిధిగా వాడుకుంటే ఎన్ని సమస్యల్లో ఇరుక్కుంటామో మనకి తెలీదు.

మనమెంత సదాశయంతో అంతర్జాలంలోకి అడుగిడినా, ఎంత సత్ప్రవర్తనతో మెలిగినా మన ప్రతి అడుగు కోసం చుట్టూరా బాంబులు కాచుకునుంటాయని

మర్చిపోతే ఎప్పుడో తప్పటడుగు పడుతుంది, అంతా మటాష్ అయిపోతుంది.

'ఫైండింగ్ మెథడ్ టు ది మేడ్‌నెస్'

మనం మన ఇష్టాయిష్టాలకి సంబంధం లేకుండా ఆడుతున్న ఈ ఆటలో నియామాలేంటో మనకి తెలీవు. ఏది ఓటమో, ఏది గెలుపో తెలీదు. మైన్‌స్వీపర్‌లో ఆట మొదలయ్యేటప్పటికి ఎన్ని గడులుంటాయో, ముగిసేటప్పటికీ అన్నే ఉంటాయి. ఒక గడి వెనుక 1 ఉంటే దానర్థం ఆ గడి చుట్టూ ఉన్న గడులలో ఒక బాంబు ఉందని. ఆ అర్థం మారదు. కానీ మనం ఆడుతున్న ఈ ఆటలో గడులు ఎటు వైపైనా, ఎంతైనా పెరుగుతూ పోవచ్చు. ఇవాళ అంకె అనిపించింది రేపు బాంబుగా మారవచ్చు. (సరదాగా కుటుంబ సభ్యులతో, ఫ్రెండ్స్ తో కబుర్లాడుకోడానికి, ఫోటోలు షేర్ చేయడానికి మొదలైన ఫేస్‌బుక్ మీద ఇవ్వాళ ప్రపంచ అగ్రరాజ్యమైన అమెరికా రాజకీయాలని నిర్దేశిస్తుందనే పూర్తిగా కొట్టిపారేయలేని ఆరోపణలున్నాయి కదా)

అలా అని ఆటని 'క్విట్' చేయనూ లేం. మరెలా?

ఇలాంటివాటికే నా మొట్టమొదటి మానేజర్ చెప్పిన చిట్కా ఒకటి ఉంది.. 'ఫైండింగ్ మెథడ్ టు ది మేడ్‌నెస్'. అంటే, వెర్రెక్కించేంతటి అతలాకుతల పరిస్థితులని కూడా ఏదో విధంగా, చిన్న చిన్న మొత్తాలలోనైనా ఉపాయాలతో, చిట్కాలతో అధిగమించవచ్చు. ఇన్ని మాటలెందుకు గానీ, పవన్ కళ్యాణ్ మాటలనే కాస్త అటు ఇటు సర్దితే... "తిక్కుంటే, దానికో లెక్క కనుక్కోవాలి".

మనం వాడుతున్న టెక్నాలజిలో లోటుపాట్లు మనకి తెలుసు (ఉదా: ఇంట్లో కూర్చుని కాళ్ళు కదపకుండా షాపింగ్ చేయచ్చు. క్రెడిట్ కార్డ్ నంబర్, ఓటీపీలు మన అంతట మనమే వేరేవాళ్ళకి ఇచ్చేస్తే మనల్ని ఎవరూ కాపాడలేరు.)

మనం వాడుతున్న టెక్నాలజీ వల్ల మనకేం జరుగుతుందో తెలిసే అవకాశం లేదు, లేక ఎప్పటికో గానీ తెలీదు. (ఉదా: మనిషి ఎప్పుడూ ఊహించలేనంత సమాచారం ఇప్పుడు ఒక క్లిక్ దూరంలో ఉంది. అలా అందుబాటులో ఉన్న సమాచారం కోసం ఒక లింక్ నుంచి ఇంకో లింక్‌కు దూకడం అలవాటైపోయి, ఏ పని మీదా ఏకాగ్రత నిలవని పరిస్థితి (అటెన్షన్ డెఫిషియన్సీ) ఏర్పడుతుందని

ఇప్పుడిప్పుడే పరిశోధనలు చెప్తున్నాయి. ఇది ముందు తరాల్లో ఎలాంటి బిహేవియరల్ ఎనామలీస్ తీసుకొస్తుందో చెప్పలేం.)

ఇప్పుడు వీటితో కుస్తీ పట్టాలంటే, మొదటిదాని విషయంలో అప్రమత్తంగా ఉండాలి. అంటే, అపరిచిత మనిషిని ఇంట్లోకి రానివ్వడానికో, ఇంట్లోకి రమ్మనాల్సి వచ్చాకో ఎంత అప్రమత్తంగా, ఎలా కనిపెట్టుకుని ఉంటామో, ఎలా అనుమానంతో ఒక కన్ను వేసి ఉంచుతామో, అలా టెక్నాలజీని కనిపెట్టుకుని ఉండాలి.

"క్లిక్ హియర్" అని కనిపించిన చోటల్లా నొక్కకుండా, "మీ క్రెడిట్ కార్డ్ నెంబర్ వెనుక సీవీవీ అని ఒకటుంటుంది సార్, మూడు అంకెలు, అవి చెప్పగానే మీకు గిఫ్ట్ అమౌంట్ క్రెడిట్ అయిపోతుంది సార్, గంటలో" అని అడగ్గానే ఊరిపోయి నంబర్ చెప్పేయకుండా ఉండడం లాంటివి తెలుసుకోవాలి. నేర్చుకోవాలి. అలవాటుగా మార్చుకోవాలి.

అలానే, పర్యవసానాలు మనకింకా తెలీని టెక్నాలజీలపై ఓ కన్నేసి ఉంచితే, అవి మనలో, మనం మసులుకుంటున్న తీరులో కలిగిస్తున్న మార్పులపై మనకు కొంత అవగాహన కలగవచ్చు. మన ముందు తరాల వారికి కనీసం ఓ హెచ్చరిక అందించే అవకాశం ఉంటుంది.

దీని వల్ల ఏం తెలుస్తుంది మనకి? టెక్నాలజీ లోటుపాట్లు మనకి తెలిసినా, తెలియకపోయినా మనం దాన్ని "అనుమానిస్తూ" ఉండడం వల్ల ప్రయోజనాలు ఉన్నాయనిపిస్తుంది. అందుకే, "అంతర్జాలమందు అనుమానించువారు ధన్యులు, సుమతీ" అని నాకు నేను చెప్పుకుంటుంటాను.

అనుమానమే రక్ష

కానీ ఒకటా, అరా, పొద్దస్తమానూ ఆన్‌లైన్‌లోనే ఉంటామే, ఇలా అనుమానిస్తూ కూర్చుంటే అదో జబ్బులా తయారవ్వదా? అని అడిగేవారుంటారు. నేనూ ఆలోచించాను.

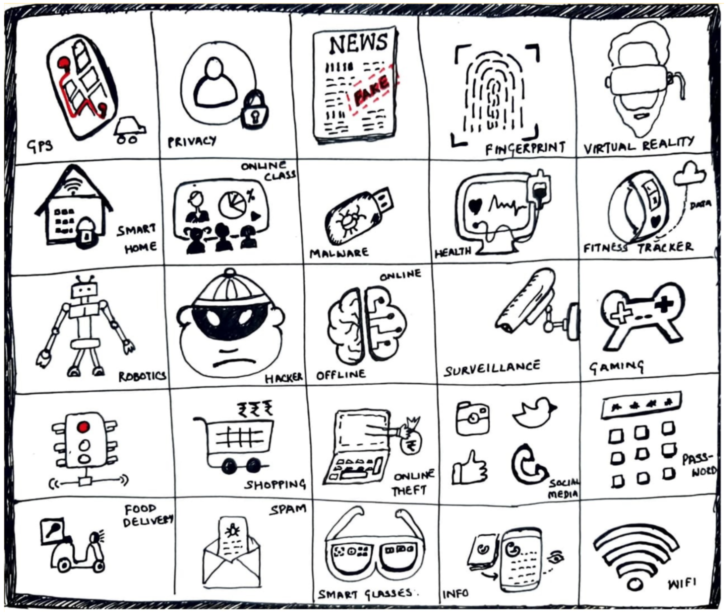
అనుమానంకు బదులుగా “అప్రమత్తంగా ఉండువారు ధన్యులు” అని అందాం అనుకున్నాను. కానీ వర్చువల్ ప్రపంచాన్ని పక్కనపెట్టేసి కాసేపు వాస్తవ ప్రపంచంలోకి వస్తే, కోవిడ్ సమయంలో మనం అచ్చంగా ఇరవై నాలుగు గంటలూ ఇళ్ళల్లో ఉన్నాం. ఇంటి విషయంలో అజాగ్రత్తగానీ, అశ్రద్ధగానీ చేస్తామా? గేట్లకి, తలుపులకీ తాళాలూ, గొళ్ళాలు పకడ్బందీగా వేసుకోమూ? ఎందుకని? ఏ మాత్రం అటూ ఇటూ చేసినా ఆస్తి నష్టమో, ప్రాణ నష్టమో జరుగుతుందని భయం, ఆందోళన. అంతకన్నా ఎక్కువ అనుమానం.

అనుమానమే లేకపోతే ఆటోవాడో, కొట్టువాడో చిల్లర ఇవ్వగానే చూసుకుంటామా? టూరిస్ట్ ప్లేసుల్లో బ్యాక్‌ప్యాక్‌ను కూడా ముందుకేసుకుని చంటిపిల్లాడిలా జాగ్రత్తగా హత్తుకుంటామా? కొంచెం రద్దీగా ఉందనిపిస్తే చాలు పదేపదే జేబుల మీద చేతులుపెట్టో, హ్యాండ్ బ్యాగ్ మొత్తం చంకలో దూర్చేసే నడుస్తామా? ఇవన్నీ ఎందుకు చేస్తాం? అనుమానం, యువర్ ఆనర్, అనుమానం.

ఇంటర్నెట్ మనకి తెలిసిన ప్రపంచానికన్నా పెద్దగా వేరు కాదు. మనుషులు, మమతలు, భావావేశాలూ, కక్షలూ కుట్రలూ, అన్నీ అవే. నిరాకారమైన, నిర్గుణమైన ఒక ‘ఐడి’ వెనుక కూర్చుని ఏమైనా చేయొచ్చు, ఏమన్నా అనొచ్చు. ఇక్కడ పట్టుబడేవరకూ అందరూ దొరలే.

అయితే, నిజజీవితంలో అనుమానం మనలో భాగమైనంతగా ఆన్‌లైన్‌లో కాలేదు. సెకండ్ నేచర్‌గా మారలేదు. ఆన్‌లైన్‌లో అప్రమత్తంగా ఉండాలంటే ముందు ప్రతీది అనుమానించాలని మనం మళ్ళీ మళ్ళీ గుర్తుచేసుకోవాలి.

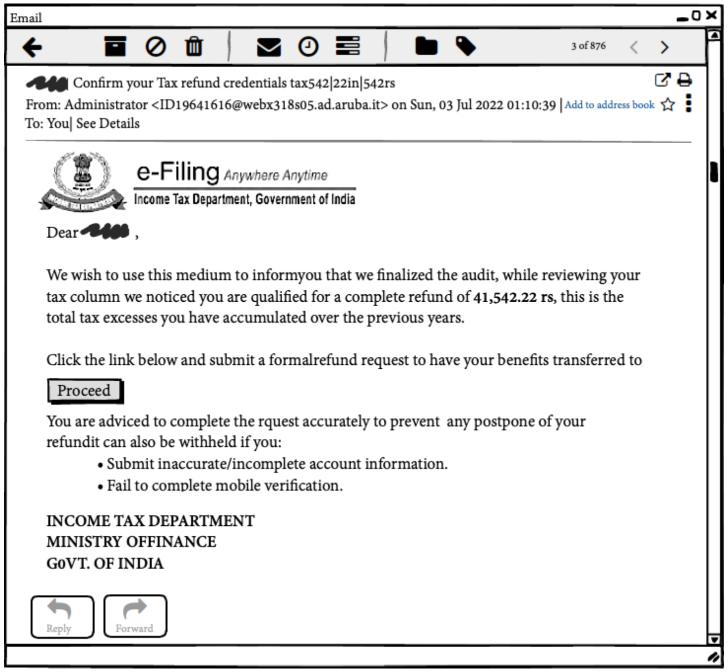
ఇది ఇంటర్నెట్ కాబట్టి, కంప్యూటేషన్ మీద నడుస్తుంది కాబట్టి, దీని తిక్కకీ ఓ లెక్కనెలా కనిపెట్టాలో, ఏ లాజిక్‌తో కొట్టాలో, ఆ వివరాలు కొన్ని ఈ పుస్తకంలో, మీ కోసం.



0-0.

2. ఐటీ రిఫండ్స్ పేరిట కొత్త ఆన్‌లైన్ స్కాములు

☞ ఈ కింది ఈమెయిల్‌ని చూడండి. ఒక ఐదు క్షణాలకన్నా ఎక్కువ వెచ్చించకుండా పైపైన చదవండి.



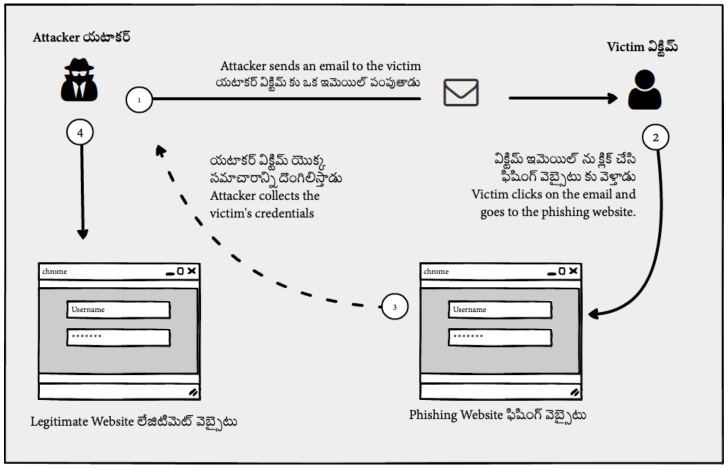
0-0.

మీకేమనిపించింది? ఇది నిజంగానే ఇన్‌కమ్ టాక్స్ డిపార్ట్మెంట్ వారి నుంచి వచ్చిన మెయిల్‌గా కనిపిస్తుందా? అందులో వాడిన భాష, సమాచారం సబబుగా

అనిపిస్తుందా? ఈ ఈమెయిల్ గనుక మీ ఇన్‌బాక్స్ లోకి వస్తే "ప్రొసీడ్" బటన్ పై మీరు క్లిక్ చేసే అవకాశాలెంత?

ఇప్పుడు ఆ స్క్రీన్‌షాట్‌ను మరింత శ్రద్ధగా చూడండి. జాగ్రత్తగా చదవండి. ఏదో తేడాగా ఉందని అనిపించాలి. ఐటీ డిపార్ట్మెంట్ నుంచి మీకు ఇదివరకు వచ్చినవాటితో పోల్చి చూడండి. మీకు తేడాలు స్పష్టంగా తెలియడం మొదలెడతాయి.

ఇదో కొత్త రకం ఫిషింగ్ అటాక్. నమ్మదగినవారి పేరు అడ్డం పెట్టుకుని, వారు పంపినట్టు ఈమెయిల్ పంపి చేసే మోసాన్నే ఫిషింగ్ అంటారు. ఇందులో ఉన్న "ప్రొసీడ్" బటన్ నొక్కితే అది అసలైన ఇన్‌కమ్ టాక్స్ సైటుకు వెళ్ళకుండా స్కామర్ల వెబ్‌సైట్‌కు వెళ్తుంది. అక్కడ గానీ వారు అడిగినట్టు బ్యాంక్ వివరాలు (పాస్‌వర్డ్, ఓటిపీతో సహా) ఇస్తే, వాటిని రికార్డ్ చేసుకుని, అకౌంట్ నుంచి డబ్బును కాజేస్తారు.



0-0.

ఇలాంటి ఈమెయిల్స్ ని కనిపెట్టడం ఎలా? ఎలా వీటిని బారిన పడకుండా ఉండడం? పొరపాటున క్లిక్ చేసేస్తే ఏం చేయాలి? అలాంటి విషయాలన్నీ ఈ

వ్యాసంలో తెలుసుకుందాం.

ఫిషింగ్ అటాక్స్ – ట్రెండ్స్

దేశంలోని అత్యధికులకు ఆదాయ పన్ను రిటర్న్స్ ఫైల్ చేయడానికి 31 జూలై ఆఖరి గడువు. ఆ నెలలోనే అందరూ ఫైల్ చేయడానికి ప్లాన్ చేసుకుంటుంటారు. ఏడాది కాలంగా కట్టాల్సినదానికన్నా ఎక్కువ ఆదాయ పన్ను కట్టినవాళ్ళకి ఐటీ వారు డబ్బులు రిఫండ్ చేస్తుంటారు. దాన్నే ఆసరాగా చేసుకుని ఈ స్కామర్లు కొత్త అటాక్‌ను సృష్టించారు.

ఐటీ డిపార్ట్మెంట్ వారి బానర్, సిగ్నేచర్ వాడుకుని, “మా లెక్కల ప్రకారం మీకు డబ్బు వచ్చేదుంది, వీలైన వెంటనే మీ వివరాలన్నీ పంపిస్తే మీ డబ్బు మీకు వేసేస్తాం” అని రాశారు.

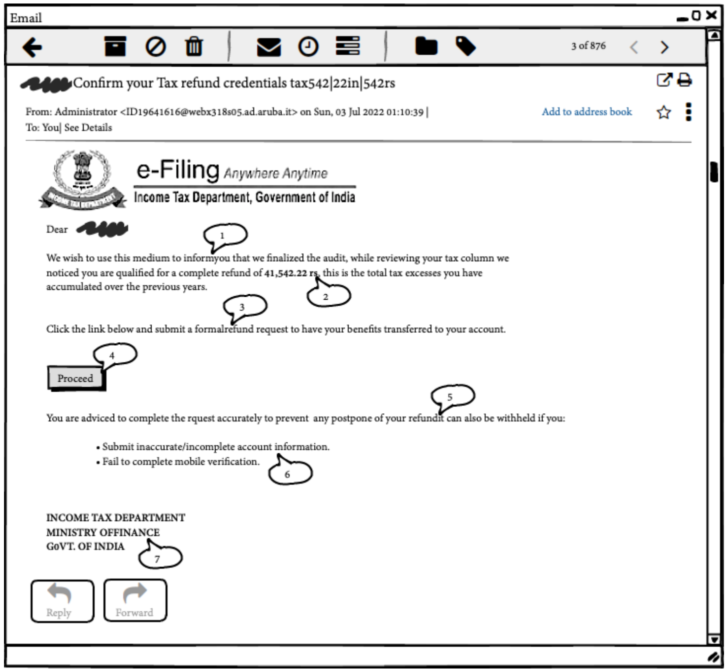
వస్తువులు అమ్మే కంపెనీలు ఎలా అయితే సమయం, సందర్భం వాడుకుని తమ వస్తువులని మార్కెటింగ్ చేస్తారో, స్కామర్లు కూడా ప్రస్తుతం దేని మీద హడావిడి నడుస్తుంటే దాన్నే వాడుకుంటూ హాని కలిగించడానికి ప్రయత్నిస్తుంటారు. జూలై నెలలో ఆదాయపన్నుల లావాదేవీలు తేల్చుకోవాల్సిన సమయం కాబట్టి, అందరూ ఆ పనుల్లో హడావిడిగా ఉంటారు కాబట్టి, అలాంటి ఒక మెయిల్ పంపిస్తే, నిజమైన మెయిల్ అనుకుని వారి బుట్టలో పడేవారు ఉంటారని వారి అంచనా.

ఆ అంచనా తప్పయ్యే పరిస్థితులు, ముఖ్యంగా మన దేశంలో, చాలా తక్కువ. మనం అన్ని రకాల డిజిటిల్ ట్రాన్సాక్షన్స్ చేస్తున్నాం కానీ మనకి డిజిటల్ లిటరసీ పెద్దగా లేదు. కాస్తో కూస్తో అవగాహన ఉన్నా కూడా అనేకానేక పనులు ఒత్తిళ్ళ మధ్య సతమతమయ్యే సగటు మనిషి ఆలోచించకుండా ఇలాంటి మాయలకు లొంగిపోయే అవకాశాలూ ఎక్కువే.

ఫిషింగ్ ఈమెయిల్ అని ఎలా కనిపెట్టడం?

ఎంత తెలివైన నేరస్థుడైనా ఏదో ఒక క్లూ వదిలేసినట్టే సైబర్ క్రిమినల్స్ కూడా కొన్ని క్లూస్ వదిలిపెడుతుంటారు ఇలాంటి ఫేక్ మెసేజుల్లో. మనం వాటిని

గమనించుకుంటే ఇవి కనిపెట్టడం పెద్ద కష్టమైన పని కాదు.



0-0.

పై ఈమెయిల్‌లో ఉన్న ప్రమాద ఘంటికలు కొన్ని పరిశీలిద్దాం:

సబ్జక్ట్ లైన్:

1. సబ్జెక్ట్ లైనులోనే వాళ్ళకి కావాల్సింది క్రెడెన్షియల్స్ (అంటే, పాస్‌వర్డ్ తదితర వివరాలు) అని స్పష్టం చేశారు. ఏ ప్రభుత్వ, ప్రభుత్వేతర సంస్థలు (బాంకింగ్, టాక్స్ లాంటి డబ్బు సంబంధిత ఆప్స్ నుంచి సరదాకి వాడే సోషల్ మీడియా, గేమింగ్ వరకూ) ఎవరూ మన పాస్‌వర్డ్లు చెప్పమని, పంచుకోమని అడగరు. ఆయా వెబ్‌సైట్స్, ఆప్స్ లాగిన్ అప్పుడు మాత్రమే పాస్‌వర్డ్ ఇవ్వాలి తప్పించి మరెక్కడా, మరెవ్వరికీ ఇవ్వకూడదు. ఇక్కడీ మెయిల్‌లో అలా అడగడమే మొదటి హెచ్చరికగా పరిగణించాలి.

2. అలానే ఇంకమ్ టాక్స్ వారి మెయిల్స్ లో మన పాన్ కార్డ్ మాస్క్ చేసిన వివరాలు ఉండవచ్చు. లేదా, మన యూజర్ నేమ్. అంతే కానీ, tax54t|22in|542rs లాంటి అర్థంలేని సంఖ్యలు ఉండవు. ఇవి పెట్టడంలో వాళ్ళ ఉద్దేశ్యం, అర్థం కానిదేదో కనిపిస్తే మనం ఇంకాస్త తికమక పడి, ఆ గందరగోళంలో తొందరపడతామనే ఆశ మాత్రమే.

ఈమెయిల్ పంపినవారి అడ్రస్:

1. నిజంగా ఐటీ డిపార్ట్మెంట్ వారు పంపినదైతే ఈమెయిల్ ఐడి, gov.in అన్న డొమేన్‌తో ముగియాలి. కానీ ఇక్కడ aruba.it తో ముగిసింది. ఆ డొమేన్ వేరెవరికో చెందినది అయ్యుండచ్చు, లేదా కొత్తగా సృష్టించి ఉండచ్చు. కానీ భారత ప్రభుత్వ సంస్థలు gov.in డొమేన్ తప్ప ఇంకేవీ వాడవు.
2. webxc3180... అన్న భాగం కూడా అనుమానాలకు తావిచ్చేది. ఫేక్ ఈమెయిల్ ఐడీలు క్రియేట్ చేయడానికి ఇలాంటి రాండమ్ నెంబర్లు జెనరేట్ చేస్తుంటారు.

ఈమెయిల్ మెసేజ్:

1. ఇందులో కూడా అండర్‌లైన్ చేసిన పదాలను గమనించండి. సరైన ఇంగ్లీషు కాదు. భారత దేశం మొత్తం ఆదాయపన్నులు లెక్కించే సంస్థ అలా అవకతవకలతో కూడిన మెసేజీలు పంపించదు.
2. ఇంకోటి, ఏ ఏడాదికా ఏడాది పన్నులు కట్టి, రిటర్న్స్ ఫైల్ చేస్తే, ఆ ఏడాదిలోనే రావాల్సిన రిఫెండ్ వచ్చేస్తుంది. ఏళ్ళ కొద్దీ జమ అయ్యేది కాదది. పోనీ, ఏ కారణాలవల్లో అలా అయ్యిందే అనుకున్నా ఆ వివరాలు మనం ఫైల్ చేసేటప్పుడో, చేసేశాకో చూపిస్తుంది. కానీ, "రా...రా, నీ డబ్బు నా దగ్గర ఉండిపోయింది" అని ఆత్రంగా అయితే పిలవదు. **ఇక్కడ టోన్‌ని గమనించుకోవడం ముఖ్యం.**

ప్రొసీడ్ బటన్:

ఇదే అసలు వల. తక్కిన ఈమెయిల్ అంతా ఈ వలలో చిక్కోడానికి వేసిన ఎర. ఇక్కడ క్లిక్ చేస్తే అది ఒక మారు వెబ్‌సైటుకి వెళ్ళి మన వివరాలన్నీ కాజేస్తుంది.

అడిగిన సమాచారం:

1. **అకౌంట్ ఇన్ఫర్మేషన్:** నిజంగానే డబ్బులు రావాల్సి ఉంటే, సైటులోకి లాగిన్ అయ్యి, ఫలానా సెక్షన్‌కి వెళ్ళి రిక్వెస్ట్ పెట్టుకోండి అన్న సందేశం ఉండాలి. **అలా కాకుండా ఇక్కడ అకౌంట్ ఇన్ఫో అడుగుతున్నారు.** అంటే, యూజర్ నేమ్, పాస్‌వర్డ్ లు. ఐటీ వెబ్‌సైట్ లో యూజర్‌నేమ్ పాన్ కార్డ్ కూడా అవ్వచ్చు. ఇవ్వన్నీ వాళ్ళ దొంగ సైటులో మనం టైపు చేస్తే, వాటిని సేవ్ చేసుకుని మన డబ్బు కాజేసే విధంగా వాడతారు.

మొబైల్ వెరిఫికేషన్:

ఇలాంటి దారుణాలను అరికట్టాలనే ఒన్ టైమ్ పాస్‌వర్డ్ (ఓ.టీ.పీ)లు వచ్చాయి. మిగితా అన్ని వివరాలు దుండగుల చేతిల్లోకి వెళ్ళినా ఓ.టీ.పీ లేకపోతే వాళ్ళు దొంగ లావాదేవీలు చేయలేరు. అందుకే ఇక్కడ "మొబైల్ వెరిఫికేషన్" కూడా పూర్తి చేయాలని నొక్కి వక్కాణించారు. ఆ వెరిఫికేషన్ కూడా చేస్తే మీరిచ్చిన ఓటిపి(OTP)ని అప్పటికప్పుడు మీ అకౌంట్ నుంచి డబ్బు కాజేయడానికి వాడచ్చు. లేదా, మొబైల్ మీద ఏదో మాల్‌వేర్ ప్రవేశపెట్టి టైప్ చేసే ప్రతీ పదాన్ని మానిటర్ చేయవచ్చు. లేదా, వచ్చిన ఎస్.ఎం.ఎస్‌లు చదవచ్చు.

అడిగిన సమాచారం ఇవ్వకపోతే పరిణామాలు:

వాళ్ళు అడిగిన సమాచారం సరిగ్గా ఇవ్వమని, ఏ మాత్రం అటు ఇటు అయినా రావాల్సిన డబ్బు రాదని ఒక బెదిరింపు ఉంది ఇక్కడ. బెదిరింపులు/కంగారు పెట్టడం/తోచనివ్వకపోవడం/భారీ నష్టం జరిగిపోతుందని భయపెట్టడం/ వ్యవధి లేదు, వెంటనే స్పందించాలనడం – ఇవ్వన్నీ స్కామర్లు వాడే జిమ్మిక్కులు.

తీసుకోవాల్సిన జాగ్రత్తలు

ఇక్కడ పంచుకున్న ఈమెయిల్ ఒక ఉదాహరణ మాత్రమే. ఇలాంటివే ఇంకెన్నో ఫిషింగ్ అటాక్స్ క్రిమినల్స్ చేస్తూనే ఉంటారు. నిజమైన ఈమెయిల్ కి మరింత దగ్గరగా ఉండే విధంగా ఇంకా హంగులు ఏర్పాటు చేయవచ్చు. అలాంటి వలల్లో పడకుండా ఉండేందుకు తీసుకోవాల్సిన జాగ్రత్తలు కొన్ని:

- **సావధానం వహించడం:** మెసేజ్‌లో చాలా పెద్ద అమౌంట్ పోతుందని చెప్పినా కూడా గాభరా పడకుండా కాస్త సావధానం వహించడం. ఇది ఎందుకు ముఖ్యమంటే, ఏ ప్రభుత్వ సంస్థలు, బ్యాంకులు నిముషాలు, గంటల వ్యవధి ఇచ్చి పనులు చేయమనరు. నిజంగా రావాల్సిన డబ్బు ఉంటే రెండు రోజులు పోయాక అయినా అప్లై చేసుకోవచ్చు. దుండగులు మాత్రమే కంగారు పెట్టేసి అదిలిస్తారు. మరో ఆలోచన రానివ్వకుండా వ్యవహరిస్తారు.
- **క్లిక్/డౌన్లోడ్ చేసుకోకుండా ఉండడం:** వెంటనే అక్కడున్న లింకులను క్లిక్ చేయకుండా ఉండడం, అటాచ్‌మెంట్స్ ఏమన్నా ఉంటే డౌన్లోడ్ చేసుకోకుండా ఉండడం. ఎందుకంటే, ప్రమాదం గలిగించే సామాగ్రి అంతా వీటిల్లోనే ఉంటుంది.
- **నిజమని అనుమానమొస్తే అసలు సైటుకే వెళ్ళడం:** ఒకవేళ మీకు రావాల్సిన డబ్బు ఉండి, ఇలాంటి మెసేజ్ కనిపించినా కూడా వెంటనే ఏం క్లిక్ చేయొద్దు. ఈమెయిల్, ఎస్.ఎం.ఎస్ ఇవ్వనీ మాధ్యమాలు మాత్రమే. అసలు సమాచారం ఉన్నది ఆయా సంస్థల (నిఖార్సైన) వెబ్‌సైటుల్లో. అందుకని మనం ఆ సైటు ఓపెన్ చేసి, అక్కడ మన లాగిన్ వివరాలు ఇచ్చి, లోపలికి వెళ్ళాక ఈ సమాచారం కోసం వెతుక్కోవచ్చు. నిజంగానే అంత కీలకమైన సమాచారమే అయితే లాగిన్ అవ్వగానే మీకు ఇదే మెసేజ్ కనిపించేట్టు కూడా పెడతారు, ఆయా వెబ్‌సైట్లవారు.
- **మోసం అని తెలిస్తే "స్పామ్" అని మార్క్ చేయడం:** కేవలం మాయ చేయడమే ఈ మెయిల్ ఉద్దేశ్యం అని తేలిపోయాక దాన్ని స్పామ్ అని మార్క్ చేస్తే, అదే స్కామ్ పార్టీల నుంచి మరిన్ని మెయిల్స్ రాకుండా మెయిల్ సర్వీస్ ప్రొవైడర్ ఆపగలుగుతారు. ఎక్కువ మంది స్పామ్‌గా మార్క్ చేస్తే, ఆ మెసేజీలు వస్తున్న ఐపి అడ్రస్, లొకేషన్ ఆధారంగా, బాడీలో ఉన్న మెసేజ్ ఆధారంగా కూడా వాటిని ఆటోమేటిగ్గా స్పామ్ అని గుర్తించగలుగుతారు. ఇలాంటి మాయలకు తొందరగా పడిపోయేవాళ్ళని (టెక్ విషయాలు తెలీనివారిని, ఇంగ్లీషు బాగా రానివారిని) కాపాడగలుగుతారు.

ఒకవేళ పొరపాటున క్లిక్/డౌన్లోడ్ చేస్తే...

- వెంటనే వివరాలు ఇచ్చేసిన అకౌంట్‌కు సంబంధించిన పాస్‌వర్డ్స్ రీసెట్ చేయడం.
- అకౌంట్ పరంగా అనధికారిక లావాదేవీలేవైనా జరుగుతున్నాయేమోనని చూసుకుంటూ ఉండడం. ఇక్కడ బ్యాంక్ అకౌంట్ వివరాలు ఇస్తున్నాం కాబట్టి వెంటనే బ్యాంక్ వారిని సంప్రదించి వారికి జరిగిన విషయాన్ని తెలియజేస్తే వాళ్ళూ తగిన చర్యలు తీసుకుంటారు.

మీరు గ్రహించే లోపే డబ్బు నష్టపోతే వెంటనే సైబర్ క్రైమ్ బ్రాంచ్‌ని సంప్రదించాలి.

||||||||||||||||||/•|

3. మెటాడేటాలోనే ఉంది మతలబంతా - స్మిషింగ్!

అనగనగా ఒక సైబరు కొలను. అందులో బోలెడన్ని చేపలు హాయిగా ఉంటూ వచ్చాయి. వాటిల్లో మూడు చేపల పేర్లు: సుమతి, కాలమతి, మందమతి. మంచి స్నేహితులు. ఒకరి దగ్గర ఉన్నది మిగితా ఇద్దరితో "లైకు. షేరు. సబ్‌స్క్రైబ్" చేసుకుంటుండేవారు.

సైబరు కొలను ఏమంత సురక్షితమైంది కాదని, హాకర్లు-ఫ్రాడ్‌స్టర్లు ఎప్పుడన్నా వలేసి పట్టుకోవచ్చునని, ఎల్లప్పుడూ అప్రమత్తంగా ఉండాలని ఆ నోటా ఈ నోటా వినిపిస్తూనే ఉన్నా వాళ్ళెవ్వరూ పెద్ద పట్టించుకోలేదు. ఓ పూట మందమతి వచ్చింది. "లింకు మీద నొక్కకపోతే నా బాంక్ అకౌంట్ బ్లాకు చేసేస్తారని SMS వచ్చింది. అందుకని గాభరా పడి నొక్కేశాను. ఇప్పుడు నా డబ్బులన్నీ కట్ అయిపోతున్నాయి" అని లబోదిబోమంది. సుమతి ఎప్పటికప్పుడు సైబరు సెక్యురిటి సంగతులు తెలుసుకుంటూ ఉంటుంది కాబట్టి, జరిగిన మోసం పసిగట్టి, మందమతి చేత క్రెడిట్ కార్డులు బ్లాక్ (block) చేయించి, బాంక్ అకౌంట్ పాస్‌వర్డులు మార్పించింది.

"మెసేజి రాగానే ముందూ వెనుకా ఆలోచించాలి. వెంటనే లింకులు నొక్కేయకూడదు" సుమతి నీరసంతో కూడిన విసుగుతో అంది.

కాలమతి ఏదో గుర్తొచ్చినట్టుంది, "నేను అమెజాన్‌లో ఆర్డర్ చేశానా, స్పీకర్స్, అవి వచ్చాయి. భలే ఉన్నాయి. ఒక గిఫ్ట్ కూడా వస్తుందట! కానీ అమెజాను సైటులోకి వెళ్ళి చూస్తే దాని ప్రస్తావనే లేదు!" అంటూ ఒక SMS తెరిచి చూపించింది. దాన్ని చూసీచూడగానే మందమతి కళ్ళల్లో మెరుపు. సుమతేమో తలపట్టుకుంది.

"ఇది ఫ్రాడ్ మెసేజి. మెసేజిలో ఏముందో చూడ్డం కాదు. ముందు, మెటాడేటా చూడండోసారి" అంది సుమతి. ఇద్దరూ తెల్లమొహాలేశారు.

"డాక్టర్ దగ్గరకి జ్వరం ఉందని వెళ్తే ఆవిడ థర్మామీటరులో జ్వరం ఎంతుందో చూస్తారు. అలానే కళ్ళని, నాలుకని, ఊపిరి తీసుకునే విధానాన్ని, బి.పిని అన్నింటిని కూడా చూస్తారా లేదా? ఎందుకని? జ్వరం ఎంతుందో అన్న విషయంతో పాటు ఇవ్వన్నీ కూడా తెలిస్తే అందుకు తగ్గ వైద్యం చేసే వీలవుతుంది కనుక. ***అలానే మనకి వచ్చిన మెసేజిలో ఏముంది అనేదానితో పాటుగా ఎవరు-ఎందుకు-ఎలా అనేది కూడా చూసుకోవాలి.***"

ఫిషింగ్-స్మిషింగ్

ఇంటర్నెటులో ఉనికికి మూలం ఐడెంటిటి. ఒకరిని ఒకరు గుర్తుపట్టడానికి ఉన్న ఏకైక ఆధారం. వ్యక్తులైతే ప్రొఫైల్ పేర్లు, ఈమెయిల్ ఐడిలు, డిస్‌ప్లే పిక్చర్లు. సంస్థలైతే వీటితో పాటు వెబ్‌సైట్లు, లోగోలు వగైరాలు కీలకం. అయితే కొందరు సైబర్ నేరగాళ్ళు ఈ సమాచారాన్ని వాడుకుంటూ అసలు, సిసలైన వ్యక్తులుగా/ సంస్థలుగా ఫోజు కొడుతూ మన కీలక సమాచారాన్ని మనకి తెలీకుండా లాక్కునే అవకాశాలు ఉన్నాయి. వీటి వెనుక ఎక్కువగా డబ్బు కాజేయడమే ఉద్దేశ్యంగా ఉంటుంది కానీ అప్పుడప్పుడూ బ్లాక్‌మేల్ లాంటి ఉద్దేశ్యాలూ ఉండచ్చు. ఇలా ఒకరి ఐడెంటిటి అడ్డం పెట్టుకుని ఈమెయిల్ ద్వారా మోసం చేస్తే దాన్ని phishing (ఫిషింగ్) అంటారు. ఒకవేళ SMS ద్వారా చేస్తే smishing (SMS-phishing, స్మిషింగ్) అంటారు.

ఆ పేర్లల్లోనే అంతరార్థం ఉంది. కొలను ఏదైనా – ఈమెయిల్, SMS, వాట్సాప్, మెసెంజర్ – మనల్ని చేపలుగా భావించి ఎర వేసేవాళ్ళు ఉంటారు. ఎన్ని సెక్యూరిటి సాఫ్ట్‌వేర్లున్నా అవి "ఇదేదో తేడా కొడుతుంది, ఆశ పడి నోరు తెరిస్తే కష్టం" అని చూచాయిగా హెచ్చరించగలవే తప్ప, మన పేరాశలకి, దురాశలకి, అమాయకత్వాలకి అడ్డుకట్ట వేయవు, వేయలేవు. మనుషులుగా మనకుండే భావోద్వేగాల మీద దెబ్బకొట్టి మన చేత మన గొయ్యే తవ్వించడంలో హాకర్లు, సైబర్ నేరగాళ్ళు నిష్ణాతులు. దాన్నే social engineering (సోషల్ ఇంజనీరింగ్) అని అంటారు. పకడ్బందీగా ఎన్ని బీకాలు, తాళాలూ వేసినా

తాళం చెవులున్నవాడి నుంచి వాటిని నయానో, భయానో లాక్కుంటే చాలునన్నది వాళ్ళ ధీమా.

నిజజీవితంలోలానే ఇలాంటి మోసాల్లో కూడా కొన్ని కొట్టొచ్చిన లక్షణాలుంటాయి.

- మనకి బాగా తెలిసిన, నమ్మకమున్న సంస్థలు, మనుషుల పేర్లు, ఫోటోలు వాడడం
- 'ఆలసించిన ఆశాభంగం'/ 'చెప్పింది చేయకపోతే చచ్చినంత పని" అని తోచనివ్వకపోవడం
- ఈ ఆశని, భయాన్ని వాడుకుని మన చేత వాళ్ళకి కావాల్సిన పనులు చేయించుకోవడం

వాళ్ళకి కావాల్సినవి ఏమై ఉండచ్చు?

- నేరుగా వాళ్ళ ఖాతాలోకి మనం డబ్బులు వేసేలా చేయడం
- వాళ్ళిచ్చిన లింకు నొక్కడం వల్ల మన మొబైళ్ళల్లో మాల్‌వేరుని (హానికారకమైన సాఫ్ట్వేరు) దొడ్డిదారిన ఇన్‌స్టాలు చేసి మన కీలకమైన సమాచారం (యూజర్ నేమ్, పాస్‌వర్డ్, క్రెడిట్ కార్డు నెంబర్లు) తెలుసుకుని, వాటి ద్వారా ఆర్థిక నష్టం కలిగించడం
- మన అకౌంట్లు బ్లాక్ చేసి, వాటిని తిరిగి ఇవ్వడానికి డబ్బుని డిమాండ్ చేయడం, మానసికంగా క్షోభ పెట్టడం

వీటికి చిక్కకుండా ఉండడానికి మనమేం చేయచ్చు?

1. మనకి తెలీని నెంబరుని ఏ మెసేజి వచ్చినా అనుమానంగా చూడడం
2. అసలు మెసేజి కన్నా ఎవరు పంపారు, ఎలాంటి టోన్ వాడారు, ఏం చేయమంటున్నారు వగైరా గమనించుకోవడం

కొన్ని SMSలను పరిశీలించి పైన చెప్పుకున్న థియరీని ప్రాక్టికల్సులో చూద్దాం.

0-0.

ఈ మెసేజిని (SMS1) పరిశీలిస్తే:

1. **నెంబర్:**
   a. తెలియని నెంబర్ నుంచి వచ్చింది.

   b. ఒకవేళ ఒక బాంకింగ్/డిజిటల్ పేమెంట్/ఈకామెర్స్ సంస్థ ఇలాంటివి పంపదల్చుకుంటే ఇలా పది అంకెల నెంబర్లని వాడరు. వాళ్ళ ఆడ్స్, మెసేజింగ్ కోసం ప్రత్యేకమైన ఐడిలని వాడతారు. (ఉదా: AD-AxisBk, AX-HDBKPL)

2. **మెసేజి:**

మెసేజిలో ఏ మాత్రం పనికొచ్చే విషయంగానీ, వివరాలుగానీ లేవు.

b. ఇది మనకి ప్రత్యేకించిన మెసేజి అనిపించే వివరాలు (పేరు, బాంకు/సంస్థ, ఏ కార్డు, ఎప్పుడు అప్లై చేశాం) ఏవీ లేకుండా ఉంది. ఇలాంటివి గుంపులుగా (bulk)గా పంపదల్చుకుంటే, వాళ్ళ దగ్గర ఫోను నెంబర్ల చిట్టా ఉంటే చాలు, పది లైన్లకి మించని కోడ్ కూడా వాటిన్నింటికి నిమిషాల్లో పంపించేయగలదు.

c. లింకు ఎందుకు నొక్కాలో (కార్డు స్టేటసు కోసమా, లేదూ మరిన్ని వివరాల కోసమా, ఏదైనా కంప్లైంటు చేయడానికా) అన్నది చెప్పలేదు.

3. **లింకు:**

a. epq9.com అన్నది అనుమానాలకి తావిచ్చే డొమేను పేరు.

b. లింకు నొక్కేముందు పరిశీలించాల్సినవి:

i. అసలు మీరు ఏదైనా కార్డ్ కి అప్లై చేసున్నారా? ఒకవేళ చేసుంటే, ఇలాంటి లింకులు తెరవనసరం లేదు. ఆ బాంక్ సైటుకో, ఆ సంస్థకున్న ఆప్ (app), వెబ్సైటుకెళ్ళి, లాగినై అక్కడే వివరాలు చూసుకోవచ్చు.

ii. కార్డ్‌కి అప్లై చేయకపోతే: కుతూహలం కొద్దీ లింకు నొక్కకూడదు. చీకట్లో రాయేసి చూద్దామనుకుని ప్రయత్నిస్తే త్వరాత చాలా కంపు కంపు అయ్యే అవకాశముంటుంది.

ఈ మెసేజిని ఏం చేయచ్చు?

స్పామ్ అని గుర్తించాలి. తీరికుంటే నెంబర్ బ్లాక్, డిలీట్ చేయండి. లేకపోతే దాని మానాన దాన్ని

ఉండనివ్వండి.