அவர்கள் சேர்த்து வைத்திருக்கும் வீடு, நிலம், பணம், தங்கம் என வெவ்வேறு பதில்களைத் தேடி நாம் யோசித்தால். "அதெல்லாம் கிடையாது. 490 ரூபாய் / ஐந்தே டாலர்" என முடித்துவிடுகிறது இணைய சமூகம். ''நிலம், தங்கம், எண்ணெய் ஆகிய பொருள்களுக்காக அடித்துக்கொண்ட மனித உயிர்கள், இனி டேட்டாவுக்காக மல்லுக்கட்டும்" என்றார் கிளைவ் ஹம்பி என்ற அறிஞர். இப்போது உலகெங்கிலும் தொடர்ந்து நடந்து வரும் தகவல் திருட்டுச் சம்பவங்கள் அந்த வாசகத்தை நிதர்சனமாக்கிவருகின்றன.

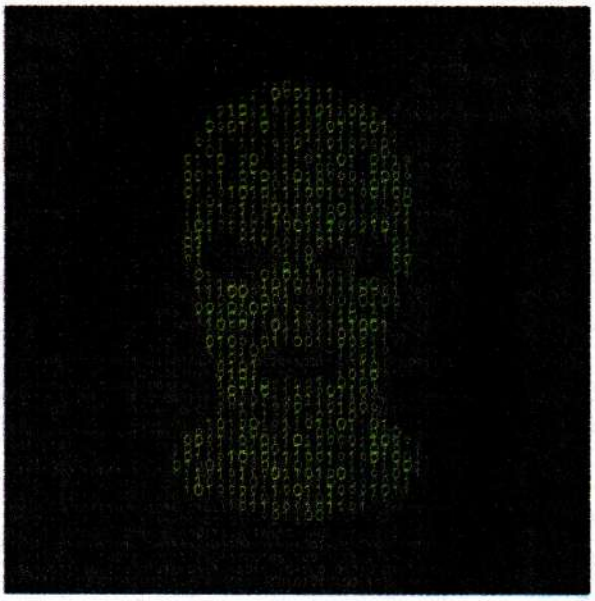
67 கோடி இந்தியர்களின் தகவல்களைத் திருடி விற்றதாக, சமீபத்தில் சைபராபாத் போலீஸாரால் வினய் பரத்வாஜ் என்பவர் கைது செய்யப்பட்டார். இந்தியாவின் 24 மாநிலங்களிலுள்ள பல்வேறு நிறுவனங்களின் வாடிக்கையாளர்களின் தனிப்பட்ட தகவல்களை சட்டவிரோதமாகப் பெற்று, InspireWebz என்ற இணையதளம் மூலமாக 2000, 3000 ரூபாய்க்கு விற்பனை செய்துள்ளார் வினய் பரத்வாஜ். ஹரியானாவின் ஃபரீதாபாத் நகரில் அலுவலகம் வைத்திருக்கும் இவரால் திருடப்பட்ட தரவுகளில் பெரும்பாலானவை ஜி.எஸ்.டி, போக்குவரத்துத் துறை போன்ற அரசு அலுவலகங்களில் இருந்த தகவல்கள். இதுதவிர அமேசான், நெட்ப்ளிக்ஸ், யூடியூப், புக் மை ஷோ, ஸொமேட்டோ, ஃபேஸ்புக் என்று மக்கள் அதிகம் பயன்படுத்தும் இணையதளங்களில் தனிநபர்கள் தங்களைக் குறித்துத் தெரிவித்து வைத்திருந்த விவரங்கள்.

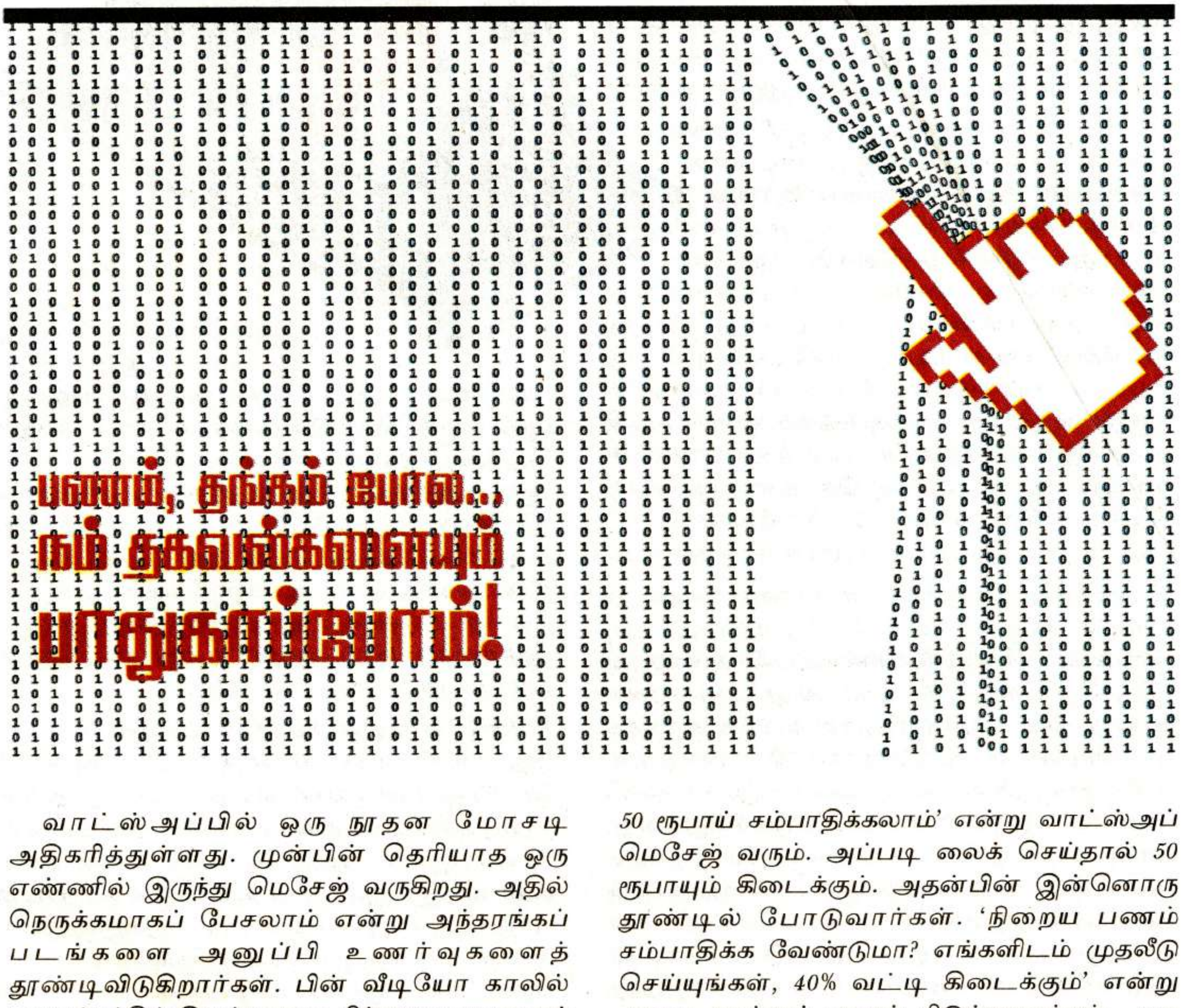
கிரெடிட் கார்டு வைத்திருப்பவர்கள், அடிக்கடி விமானப்பயணம் செய்பவர்கள், பங்குச்சந்தை முதலீட்டாளர்கள், நீட் தேர்வு எழுதிய மாணவர்கள், அதிகம் சம்பாதிக்கும் பணக்காரர்கள் என்று காய்கறிகளைக் கூறு போட்டு விற்பது போல 104 பிரிவுகளாக இந்தியர்களைப் பிரித்து, ஒவ்வொரு பிரிவினர் குறித்த தகவல்களுக்கும் ஒவ்வொரு விலை வைத்து விற்றிருக்கிறார்கள். ஒவ்வொருவரின் வருமான தகவல்கள், முகவரி, மொபைல் எண், பிறந்த தேதி, இமெயில் ஐடி போன்ற விவரங்கள் இவர்கள் வசம் உள்ளன. இதில் என், உங்களின் விவரங்களும் உண்டா என்பது யாருக்குமே தெரியாது.

எந்தெந்த நிறுவனங்களிலிருந்து இவர்கள் தகவல்களைத் திருடினார்களோ, சம்பந்தப்பட்ட 21 நிறுவனங்களுக்கு சைபராபாத் காவல்துறை நோட்டீஸ் அனுப்பியது. விசாரணைக்கு வந்த நிறுவனங்கள் தங்கள் சேவையகங்களில் இருந்து தரவுக் கசிவு ஏற்பட்டதைக்கூட அறிந்திருக்கவில்லை. சிலர் தரவு திருடப்படுவதை மறுத்தாலும், சேகரிக்கப்பட்ட தரவு அவர்களின் தளத்தின் அதே வடிவத்தில் இருப்பதைக் கண்டு அதிர்ச்சியடைந்தனர். சமீபத்தில் இதே போல பிக் பாஸ்கெட் நிறுவனத்தில் இருந்து 20மில்லியன் தரவுகள் திருடு போயின. இந்தப் பட்டியல் நீண்டு கொண்டே போகிறது.

பணத்திற்கு ஆசைப்பட்டு டேட்டா விற்பனை செய்யும் இவர்கள் குற்றத்தின் வீரியத்தைக்கூட புரிந்துகொள்வதில்லை என்கிறார்கள் காவலர்கள். 'தகவலை வெளியிட்டது குற்றமா' என்றே கேட்கிறார்கள். இவர்களிடம் தகவல் எங்கிருந்து வந்தது என்று கேள்வி கேட்க ஆரம்பித்தால் மற்றொரு இருள் உலகம் நம் தலையைச் சுற்றவைக்கிறது.

"ஒரு விஷயம் உண்மையாக இருப்பது போல, மிகவும் உண்மை போல தோன்றினால், ஒருவேளை அது அப்படியில்லாமல் இருக்கலாம்" என்று சந்தேகிக்கச் சொல்கிறார்கள் சைபர் நிபுணர்கள். இந்த டிஜிட்டல் உலகத்தில் பணத்தைத் தொலைத்துவிட்டாலும் அதை நீங்கள் சம்பாதித்துவிடலாம். ஒரு பாஸ்வேர்டு இல்லாத போனைத் தொலைத்தால், திரும்பவும் மீட்கவே முடியாத பல விஷயங்களை இழக்க நேரிடும் என்கிறார்கள் அவர்கள்.





பணம், தங்கம் போல... நம் தகவல்களையும் பாதுகாப்போம்!

வாட்ஸ்அப்பில் ஒரு நூதன மோசடி அதிகரித்துள்ளது. முன்பின் தெரியாத ஒரு எண்ணில் இருந்து மெசேஜ் வருகிறது. அதில் நெருக்கமாகப் பேசலாம் என்று அந்தரங்கப் படங்களை அனுப்பி உணர்வுகளைத் தூண்டிவிடுகிறார்கள். பின் வீடியோ காலில் மறுபக்கத்தில் இருப்பவரை நிர்வாணமாக வரச் சொல்லி வருபவர்களைப் படம் எடுத்துவிட்டு, சிறிது நேரம் கழித்து அந்த நபரின் தொலைபேசித் தொடர்புகளில் இருக்கும் நபர்களுக்கும், பேஸ்புக் நண்பர்களுக்கும் வீடியோவை அனுப்பி விடுவேன் என்று கூறி மிரட்டிப் பணம் பறிப்பது தான் அது. பாதிக்கப்பட்ட ஒருவர் கூறிய தகவலின்படி 15 லட்சம் ரூபாய் வரை அவரிடம் மோசடி நடந்துள்ளது. இன்றைய நிலையில் வழக்குப்பதிவு செய்யப்படாமல் இருக்கும் அதிக குற்ற நிகழ்வு இது.

'கஷ்டமில்லாமல் சம்பாதிக்கலாம். எங்கள் யூடியூப் வீடியோவுக்கு ஒரு லைக் போட்டால் 50 ரூபாய் சம்பாதிக்கலாம்' என்று வாட்ஸ்அப் மெசேஜ் வரும். அப்படி லைக் செய்தால் 50 ரூபாயும் கிடைக்கும். அதன்பின் இன்னொரு தூண்டில் போடுவார்கள். 'நிறைய பணம் சம்பாதிக்க வேண்டுமா? எங்களிடம் முதலீடு செய்யுங்கள், 40% வட்டி கிடைக்கும்' என்று ஆசை காட்டிப் பணம் பிடுங்குவார்கள். அது வட்டியுடன் சேர்ந்து பெருகியிருப்பதாக அடிக்கடி மெசேஜ் வரும். ஆனால், கடைசிவரை பணம் வராது. இந்த மோசடியிலும் பலர் கோடிக்கணக்கில் ஏமாந்திருக்கிறார்கள்.

தகவல் திருட்டு மூலமாகவே நமது எண் அவர்களுக்குக் கிடைக்கும். இதில் குறிப்பிடத்தகுந்த விஷயம் என்னவென்றால் வயதான, ஓரளவு வசதியான நபர்களைக் குறி வைத்தே இது நடக்கிறது என்பதுதான்.

அடுத்த மோசடி 'நீங்கள் இந்த டிகிரிதானே முடித்துள்ளீர்கள். உங்களுக்கு இது முதல் வேலை என்றாலும் சம்பளம் மாதம் 60,000 ரூபாய்,

உணவு, தங்குமிடம், கேப் வசதி என அனைத்தும் இலவசம்' என்று ஆசையைத் தூண்டிவிட்ட பின்னர், 'வேலையில் சேர ஒரே ஒரு முறை மூன்று லட்சம் பணம் செலுத்த வேண்டும்' என்பது. பெற்றோரின் நகையை, நிலத்தை அடமானம் வைத்துப் பணத்தைக் காட்டினால், அடுத்து நிகழும் சம்பவங்கள் கண்ணீர்க் கதைகளே. முதல் தலைமுறைப்பட்டதாரிகளையும், *fresher*-களையும் குறி வைத்தே இது நடக்கிறது.

அடுத்து வெறும் பத்தே நிமிடங்களில் லோன் வசதி. எந்த டாக்குமெண்ட்ஸும் தேவை இல்லை. மொபைல் எண், பான் கார்டு, ஈமெயில் முகவரி இருந்தால் போதும் என்கிற லோன் ஆப்கள். இதுமாதிரியான செயலிகள் போடும் வட்டித் தொகை சமாளிக்க முடியாத பெரிய ஆப்பாகவே மாறிவிடுகிறது. கட்ட முடியாத நிலை வரும்போது அந்த நபரின் தொலைபேசித் தொடர்புகளில் இருக்கும் நண்பர்களுக்கு 'உங்கள் நண்பர் கடன் வாங்கித் திருப்பித் தரவில்லை. உங்களைத்தான் *co applicant*-ஆகப் பதிவு செய்துள்ளார்' என்று மெசேஜ் செய்து மிரட்டுவது. இவ்வாறு 600 கோடி ரூபாய்க்கு மேல் மோசடி நடந்துள்ளது.

மனித மனத்தின் உணர்வுகளை வைத்தே சைபர் குற்றவாளிகள் விளையாடுகிறார்கள். *Data breach* செய்யும் ஹேக்கர்களின் செயலில்தான் இது தொடங்குகிறது. யார் அந்த ஹேக்கர்கள் என்று தேட ஆரம்பித்தால் உரிக்க உரிக்கக் காணாமல்போகும் வெங்காயத்தின் கதைதான். ஒரே நிமிடத்தில் பல நாடுகளில் இருப்பதாகக் காட்டும் இருட்டு உலகமாயிருக்கிறது அது. அதற்குப் பெயர் டார்க் வெப். அதில் இருக்கும் மார்க்கெட்டில் வெறும் 5 டாலருக்கு ஒரு மனிதனின் தனிப்பட்ட தகவலை நீங்கள் பெற்றுவிடலாம். முதலீடு, வர்த்தகம், கடன் மற்றும் மேட்ரிமோனியல் பயன்பாடுகள் இந்தத் தரவுத் திருடலின் வழக்கமான இலக்குகளாக இருக்கின்றன. இதில், ஒரு நபரின் கடவுச்சொல், தனிப்பட்ட தகவல்கள், வங்கி அல்லது நிதித் தகவல்கள் திருடப்படும் அச்சுறுத்தல் உள்ளது. நெதர்லாந்தை மையமாகக் கொண்டு செயல்படும் நிறுவனத்தின் ஆய்வறிக்கை, இந்தியாவிலுள்ள 100 நபர்களில் 18 நபர்களின் தரவுகள் பாதுகாப்பு இல்லாமல் இருப்பதாக அதிர்ச்சியை ஏற்படுத்தியுள்ளது.

ஒரு தரவு என்ன செய்துவிட முடியும் என்று கேட்டால். ''உங்களை ஒண்ணுமில்லாம ஆக்கிவிட முடியும்'' என்று பேசத் தொடங்கினார் சைபர் க்ரைம் வழக்குகளைக் கையாளும் வழக்கறிஞர் சத்யநாராயணன்.

"டேட்டா திருட்டை ரெண்டு விதமா பாக்கலாம். ஒன்னு ஆன்லைன், இன்னொன்னு ஆஃப்லைன். ஆஃப்லைன் திருட்டு வெளிய நாம நகல் எடுத்துக் குடுக்குற ஆவணங்கள் மூலமா நடக்கலாம். ஆனா அதிகமா திருடப்படுறதும், மோசமான விளைவுகள ஏற்படுத்துறதும் *'Data Breach'*ன்னு சொல்லப்படுற ஆன்லைன் டேட்டா திருட்டுக்கள்தான். உங்கள் மெயில் அல்லது போன் தகவல்கள் எத்தனை முறை *breach* ஆகியிருக்கு பார்ப்போமா?" என்று அவர் கேட்க, பயத்துடன் "எப்படி?" என்றேன்.

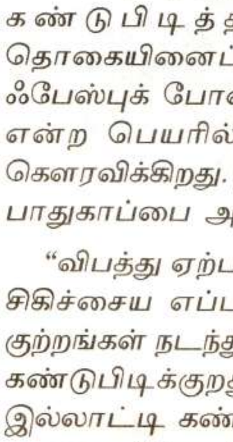
Have i been pwned என்ற லிங்கினை அனுப்பி இதற்குள் சென்று உங்கள் இமெயில் ஐடி-யைக் கொடுத்துப் பாருங்கள் என்றார். கொடுத்த சில நொடிகளில் 5 நிறுவனங்களில் எனது தரவுகள் *breach* ஆகியிருப்பதாக தகவல் வந்தது. நான் உணவு ஆர்டர் செய்யும் செயலி, படம் பார்ப்பதற்கு சப்-டைட்டில் எடுக்கும் தளம் உட்பட 5 பிரபல தளங்களின் பெயர்கள் வரவே, பதறினேன். இது எப்படி நடக்கிறது என்று கேட்க, "ஹேக்கர்லேயே ரெண்டு வகை உண்டு *bad hackers* மற்றும் *White hat hackers*. ஒரு நிறுவனம் தன் வாடிக்கையாளரோட பாதுகாப்ப கண்டிப்பா உறுதிப்படுத்தியே ஆகணும். *Penetration testing* மூலமா அதைச் செய்வாங்க. உதாரணத்துக்கு வீடு பூட்டுன அப்புறம் அது சரியாப் பூட்டி இருக்கான்னு பாக்குற மாதிரி, இணையத்துல தகவல எடுக்கக்கூடிய வாய்ப்பு இருக்கான்னு பார்க்குறது.

இந்த வேலையைச் செய்யக்கூடியவர்கள *White hat hackers*-னு சொல்லுவோம். ஒவ்வொரு நிறுவனத்திலும் *Cyber Security*-ல இருக்கிறவங்க இதுல வேலை செய்வாங்க. இதே வேலைய *bad*

hackers செய்தால் உங்கள் தகவல் திருடு போகலாம். அதுதான் *data breach*. இப்படித்தான் ஐந்து முறை உங்க டேட்டா பிரீச் ஆகியிருக்கு. ஆனா அதுக்கப்பறம் நீங்கள் பாஸ்வேர்ட மாற்றியிருந்து, சம்பந்தப்பட்ட நிறுவனம் சைபர் பாதுகாப்பை அதிகரித்திருந்தா எந்த பயமும் இல்ல. இதுல இருந்து தப்பிக்க மாசத்துக்கு ஒரு முறையாவது நம்ம பாஸ்வேர்ட மாத்திட்டே இருக்கணும்" என்கிறார் சத்ய நாராயணன்.

வாடிக்கையாளர்களின் தகவல்கள் பிரீச் ஆகியிருந்தால் சம்பந்தப்பட்ட நிறுவனம் நம்மைத் தொடர்பு கொண்டு அதனை அறிவிக்க வேண்டும். சமீபத்தில் ஐ.சி.ஐ.சி.ஐ வங்கி அவ்வாறு செய்திருந்தது. ஆனால் பெரும்பாலான நிறுவனங்கள் அவ்வாறு செய்வதில்லை. அமெரிக்கா போன்ற நாடுகளில் *Data breach* ஏற்பட்டால் சம்பந்தப்பட்ட நிறுவனம் வாடிக்கையாளருக்கு நஷ்டஈடு வழங்க வேண்டுமென சட்டமிருக்கிறது. இந்தியாவில் அவ்வாறான சட்டங்கள் கிடையாது. அதே போல அங்கே இருக்கும் நிறுவனங்கள் *bug bounty programme* நடத்துகின்றன. அது நிறுவனத்திற்கு வெளியே இருக்கும் *White hat hackers*-களுக்குப் போட்டி நடத்தி, பிரீச் நடந்திருப்பதைக் கண்டுபிடித்தால் அவர்களுக்கு ஒரு தொகையினைப் பரிசாக வழங்குகிறது. இதை ஃபேஸ்புக் போன்ற நிறுவனங்கள் *'Wall of fame'* என்ற பெயரில் செய்து *White hacker*-களை கௌரவிக்கிறது. இதுமேலும் வாடிக்கையாளரின் பாதுகாப்பை அதிகரிக்கும் முறையாகும்.

"விபத்து ஏற்பட்டால் 2 மணி நேரத்துக்குள்ள சிகிச்சைய எப்படி ஆரம்பிக்கணுமோ, சைபர் குற்றங்கள் நடந்து ஒரு நாளுக்குள்ள குற்றவாளிய கண்டுபிடிக்குறதுக்கான முயற்சி செய்யணும். இல்லாட்டி கண்டுபிடிக்குறது ரொம்ப கஷ்டம். ஆனா தமிழ்நாட்டைப் பொறுத்தவரை இப்போ தான் எல்லா மாவட்டங்களுக்கும் சைபர் செல்லே ஆரம்பிக்கப்பட்டிருக்கு. அதுக்கு முன்னாடி சென்னை, கோவைல மட்டும்தான் இருந்துச்சு. இப்போதான் கணினித்துறை சார்ந்த நிபுணர்கள் அதுல இயங்கி வராங்க. முன்னாடி சாதாரணக் காவலர்கள்தான் இருந்தாங்க. ஏராளமான வழக்குகள் பதிவு செய்யப்படும் போது மனிதவளப் பற்றாக்குறையும் நடவடிக்கை எடுக்க முடியாமப்போறதுக்குப் பெரிய காரணமா இருக்கு" என்கிறார் சத்யநாராயணன்.



சத்யநாராயணன்

எதையும் மிக அதிகமாகப் பகிர்வதே ஆபத்தானதுதான். இது சமூக வலைதளங்களுக்குப் பொருந்தும். *Google* உட்பட அனைத்துத் தளங்களிலும் *Two factor authentication*-ஐ செய்து வைத்திருக்க வேண்டும். *Secondary* போன் நம்பர் கொடுத்து வைத்திருக்க வேண்டும். பழைய டாக்குமென்ட்களை வருட இறுதியில் *PURGE* செய்துவிட வேண்டும். முக்கியமான ஆவணங்களின் தகவலை கணினியில் சேகரித்து வைக்காமல் தனியாக ஹார்டு டிஸ்கில் சேகரித்து வைக்க வேண்டும். ஆண்ட்ராய்டு மொபைல்களில் புதிதாகச் செயலிகளைப் பதிவிறக்கம் செய்தால் அது *permission* என்று கேட்கும் அனைத்திற்கும் *'Allow'* கொடுக்கக்கூடாது. *Browser*-களில் *password*-ஐ சேமித்து வைத்தாலும் *Settings*-ல் சென்று *Security option*-ல் *data breach notification*-ஐ *on* செய்ய வேண்டும். எக்காரணம் கொண்டும் *Sensitive personalised information* எனச் சொல்லக்கூடிய *OTP, ATM PIN* போன்ற எண்களை யார் கேட்டாலும் கொடுத்துவிடக் கூடாது. *End to End encrypted* சேவை என்றும் *incognito* என்றும் எதுவுமே கிடையாது. இணையதளத்தில் *Privacy* என்ற வார்த்தைக்கு இடமே இல்லை. ஆக அனைத்திலும் கவனம் வேண்டும்.

கடந்த ஆண்டு மட்டும் அரசாங்கத்திற்குச் சொந்தமான 50 வெப்சைட்களில் இருந்து தகவல் திருட்டு நடைபெற்றுள்ளது. ஒட்டுமொத்தமாக மூன்று லட்சத்திற்கும் அதிகமான வகைகளில் இணையதள மோசடிகள் இன்றும் நடைபெற்று வருகின்றன. ஆனால், இன்னமும் தகவல் திருட்டு சிவில் வழக்காகவே பார்க்கப்படுகிறது. இதன் விளைவுகள் பெரிதாக இருப்பதால் கிரிமினல் வழக்காக மாற்றப்பட வேண்டும். இந்தியாவில் தரவுப் பாதுகாப்பு சட்டம் இல்லை. டிஜிட்டல் தனிநபர் தரவுப் பாதுகாப்பு மசோதா, நாடாளுமன்றத்தில் நிலுவையில் உள்ளது. வரும் கூட்டத்தொடரில் அது செயல்படுத்தப்படலாம். அப்படி நிறைவேறினாலும், அதனால் என்னென்ன பாதுகாப்புகள் கிடைக்கும் என்பதில் இதுவரை தெளிவு இல்லை.

இன்று அனைவரின் அத்தியாவசியமாக இணையம் மாறிவிட்டது. பல மாற்றங்களும் நன்மைகளும் அதனால் உள்ளன. இருப்பினும் ஒளி நிறைந்த பகுதிக்கு மட்டும் முக்கியத்துவம் அளித்து, இருண்ட பகுதியை அலட்சியம் செய்தால், அந்த இருண்ட பகுதி கும்மிருட்டாக மாறக்கூடிய அபாயமுள்ளது. விழிப்புடன் செயல்படுவோம். இணைய இருளிலிருந்து விலகிடுவோம்! வி