திண்டுக்கல் மாவட்டம்

சைபர் கிரைம் காவல் நிலையம்

சைபர் குற்றங்களிலிருந்து தற்காத்துக்கொள்ளும் அறிவுரைகள்

1) வங்கியில் இருந்து பேசுவதாக சொல்லி 1) **A/c** நெம்பர் 2) **ATM DEBIT CARD** நெம்பர், 3) **PIN** நெம்பர் 4) **CCV** நெம்பர், 5) **OTP** நெம்பர் 6) நெட் பேங்கிங் **PASS WORD** 7) **CREDIT CARD** நெம்பர் விபரங்கள் கேட்டு உங்கள் வங்கி கணக்கு **HACK** செய்யப்படலாம்.
2) சுகாதாரதுறையில் இருந்து பேசுவதாகவும், தடுப்பு ஊசி போடப்பட்டவர்களுக்கு அரசு உதவி வழங்க விபரங்களை **UPDATE** செய்யவேண்டும் என கேட்பது போல் விபரங்களை கேட்டு, உங்களது வங்கி கணக்கை குறிவைத்து 1) **Bank A/c No,** 2) **Aadhar Card No, 3) PAN Card No, etc** பெற்றுக் கொண்டு உங்கள் செல்லுக்கு வந்த **OTP** விபரம் கேட்டு பணத்தை பறிக்க முயற்சி செய்யக்கூடும்.
3) உங்கள் செல்போனுக்கு உங்கள் அக்கவுண்டில் இருந்து பணம் பிடித்தம் செய்யப்பட்டதாகவோ / லோன் தொகை பிடிக்கப்பட்ட தாகவோ **SMS/Link** அனுப்பி அதை தவிர்க்க **CLICK** செய்ய வலியுறுத்தி **a/c**ல் இருந்து கொள்ளை அடிப்பதற்கான முயற்சி என்பதை உணரவும்.
4) **KYC/PAN/AADHAR NO** விபரங்கள் குறித்து கேட்டாலோ, **SMS / LINK** அனுப்பினாலோ **UPDATE** செய்யவேண்டாம்.
5) **BANK Account**-ற்கான செல்போன் **/ATM Card** தொலைந்து போனாலோ / திருட்டு போனாலோ உடனடியாக வங்கிக்கு நேரில் தெரியபடுத்தி விரைந்து **Block** செய்யவும்.
6) வலைதளத்தில் கிடைக்கும் வங்கி கஸ்டமர் கேர் எண்கள் கூட போலியாக இருக்க வாய்ப்பு உள்ளது. **LINK**யை அனுப்பியும், **OTP** விபரங்கள் பெற்றும் **A/C HACK** செய்யபடலாம் எச்சரிக்கையாக செயல்படவும்.
7) வங்கிகள் வாடிக்கையாளர்களை, ஒருபோதும் தொலைபேசி மூலம் தொடர்பு கொண்டு வங்கி விபரங்களை கேட்பதில்லை. ஆகவே மேற்கண்ட விபரங்களை கேட்டு போன் செய்தால், எச்சரிக்கையாக இருக்கவும். மேற்படி அழைப்பை தவிர்ப்பது சிறந்தது.
8) உங்களது தனிபட்ட புகைபடங்களை ஒரு போதும் யாரிடமும் பகிரவேண்டாம். அதை **MORPHING** செய்துபணம் பறிக்கவும் / வேறுவகையில் உங்களை மிரட்டவும் நேரிடலாம்.
9) **Face book**-ல் உங்களுக்கு தெரிந்தவர் போல் போலி கணக்கு துவங்கி பண உதவி கேட்க வாய்ப்புண்டு, எனவே அனுப்பும் முன் அவரிடம் நேரிலோ, தொலை பேசியிலோ உறுதி செய்யவும்.
10) **SOCIAL MEDIA**-களில் உங்கள் தனிப்பட்ட விபரங்களை யார்யாரெல்லாம் பார்க்கவேண்டும்/ பார்க்க கூடாது என்பதை **Privacy settings**ல் தெளிவாக குறிப்பிடவும்.
11) **SOCIAL MEDIA**-வில் உங்களது அன்றாட இருப்பிடம் மற்றும் வடிக்கைகளை பற்றிய **LIVE UPDATE** பதிவுகள் குற்றவாளிகளால் கவனிக்கப்படுகிறது என்பதை உணருங்கள்.
12) **SOCIAL MEDIA** வில் வரும் **LINK**- ஐ,**CLICK** செய்தால்,**Bank a/c HACK** ஆக வாய்ப்புள்ளது.
13) பொது இடங்களில் வைக்கப்பட்ட USB சார்ஜர்களில் சார்ஜ் போடுவதை தவிர்க்கவும், உங்களது தகவல்கள் **(Juice Jacking)** முறையில் திருட்டு போகவாய்ப்புள்ளது.
14) பொது இடங்களில் உள்ள **WI-FI** பயன் படுத்தும் போது உங்கள் மொபைல் **HACK** செய்யப்படலாம்.
15) குறைந்த விலையில் பொருட்கள் விற்பனை செய்யப்படுவதாக **SOCIAL MEDIA** தகவலின் அடிப்படையில் பொருள் வாங்கும் போது மிக கவனமாக செயல்படவும். **(Fake website** ஆக இருக்கலாம்)
16) செல்போன் **Tower** அமைக்க இடம் தேவை, மாதம் ரூ 30,000/- வாடகை, 30 லட்சம் முன்பணம் வழங்கப்படும் என வரும் செய்திகளை நம்பி பணம் செலுத்தி ஏமாற வேண்டாம்.
17) **APP**-களின் விபரங்களை முழுவதும் அறியாமல் **Download** செய்ய வேண்டாம். உங்களது தகவல்/ வங்கி கணக்கு திருட்டுபோக இதுவே மூலகாரணமாக அமையும்.
18) ஆர்வத்தை தூண்டும் தலைப்புகளில் வரும் செய்தி **LINK**- களுக்கு பின்னால் தகவல்/பணம் பறிக்கும் கும்பல் மறைந்து இருக்கிறார்கள் என்பதை உணர்வீர்.
19) உங்கள் தொலைபேசி எண்ணுக்கு விலை மதிப்பு மிக்க பரிசு விழுந்துள்ளது என வரும் தகவலை நம்பி அதை பெற அவர்களால் சொல்லப்படும் எந்த கட்டணத்தையும் செலுத்தாதீர்கள்.
20) லோன் பெற்றுதரப்படும் / வழங்கப்படும் என வரும் விளம்பரத்தை நம்பாதீர்கள். லோனுக்காக செலுத்தும் சேவை கட்டணகள் லோனுடன் திருப்பி செலுத்தப்படும் என நம்பவைத்து பணம் பறிக்கப்படும். ஏமாற வேண்டாம்.
21) அறிமுகம் இல்லாதவர்களிடம் **WHATAPP CALL**-ல் பேச வேண்டாம். உங்கள் செல்போனில் உள்ள **FRONT CAMERA** வினால் எதிர் தரப்பில் உள்ளவர்களால், உங்களின் நடவடிக்கைகள் பதிவு செய்யப்பட்டு, அந்த பதிவுகளை உங்கள் உறவினர்களுக்கோ / **SOCIAL MEDIA**-விலோ போட்டு விடுவோம் என உங்களை மிரட்டி பணம் பறிக்க வாய்ப்புள்ளது.
22) **ONLINE**-ல் வேலை தரப்படும் என ஆசையை துண்டும் விளம்பரங்கள் மூலம் உங்களை நம்பவைத்து உங்களிடம் சேவை கட்டணம் என்ற பெயரில் பணம் பறிக்க வாய்ப்புள்ளது. பணம் செலுத்தும் முன், அந்த நிறுவனத்தை பற்றியும், அவர்களால் வேலை பெற்றவர்கள் விபரங்களை கேட்டு பெற்று வேலை பெற்றவர்கள் இல்லத்துக்கே சென்று உறுதி செய்யுங்கள்.
23) **PASSWORD** விபரங்களை எவ்வளவு நம்பிக்கைக்கு உரியவராக இருந்தாலும் ஒருபோதும் கொடுக்க வேண்டாம். அடிக்கடி **Password**ஐ **Change** பண்ணவும். பல வங்கிகணக்கு வைத்துள்ளவர் எனில் அனைத்துக்கும் ஒரே **Password**ஐ கொடுக்காதீர். தங்களது ஒரு வங்கி கணக்கு பாதிக்கப்பட்டால் மற்ற எல்லா கணக்கும் பாதிக்கப்படும்.
24) **SOCIAL MEDIA** வில் தனிப்பட்ட தகவல்கள் (முகவரி, தொலைபேசி எண். படித்த பள்ளி பெயர், நிரந்திர மற்றும் தற்காலிக இருப்பிடம்) போன்றவற்றை வெளிபடையாக தெரியாமல் பார்த்து கொள்ளுங்கள்.
25) பெற்றோர் மேற்பார்வை இல்லாமல், அறிமுகம் இல்லாத நபர்களிடம் ஆன்லைனில் பழகிய யாருடனும் நேரில் சந்திக்க ஒப்புக்கொள்ள கூடாது.
26) பயமுறுத்தும் அல்லது புண்படுத்தும் வகையிலான தகவல் தொடர்பு உரையாடல்களை பெற்றோர் அல்லது நம்பகமான பெரியவர்களிடம் உடனே தெரிவிக்கவேண்டும். அருகில் உள்ளசைபர் கிரைம் காவல் நிலையத்தை தொடர்பு கொள்ளவும்.
27) தவறான பரிவர்த்தனை நடைபெற்றதை அறிந்தவுடன் உடனடியாக **NATIONAL HELPLINE TOLL FREE NO- 1930** எண்ணுக்கு தொடர்பு கொண்டு தகவல் தெரிவித்தால் சைபர் குற்றவாளிகள் கைகளுக்கு செல்லாமல், பணம் பரிவர்த்தனையை தடுத்து நிறுத்த இயலும்.
28) பெரும் சேமிப்பு உள்ள வங்கி கணக்கிற்கு **CELL NO / DEBIT/CREDIT CARD/ NET BANKING** இணைக்காமல் இருப்பது சிறந்தது.
29) தினசரி பணபரிமாற்றத்துக்கு தனி வங்கி கணக்கு குறைந்த இருப்பில் வைத்து பத்திரமாககையாள வேண்டும். தவறு நடைபெற்றாலும், பெரும் நஷ்டம் ஏற்படாமல் தவிர்க்க உதவும்.
30) **OLX APP**ல் விற்கப்படும் பொருளை வாங்க முடிவு செய்தால் அந்த பொருள் இருக்கும் இடத்துக்கு நேரில் சென்று அதன் தரத்தை உறுதி செய்து வாங்கவும். விற்பவர் ஆதாரமாக காட்டும் அடையாள அட்டைகளை நம்பி பணத்தை கட்டி ஏமாற வேண்டாம்.
31) அறிமுகம் இல்லாத புது நட்புவட்டத்தில் இருப்பவர்கள் வெளிநாட்டில் இருந்து உங்களுக்கு விலை உயர்ந்த பரிசு அனுப்புவதாக நம்பவைத்து அதைபெற **CUSTOMES CHARGE, COURIER CHARGE** என பலகாரணங்களை சொல்லி உங்கள் பணத்தை பறிக்ககூடும்.

வங்கி சம்பந்தமான பண இழப்புக்கு **1930** என்ற எண்ணை உடனடியாக தொடர்புகொள்ளவும்.

மேலும் வேறு ஏதேனும் சைபர் கிரைம் குற்றங்கள் சம்பந்தமாக காவல் நிலையத்திற்கு நேரில் வராமலேயே

www.cyber crime.gov.in என்ற வலை தளத்தில் புகார் அளிக்கலாம்.