Adopt "zero trust model" on Internet to save ourself from any fraud.

Play list of podcast of Shri Amit Dubey, Cyber Security Expert –
https://www.youtube.com/watch?v=J8qvn_HZb_A&list=PLqhVpp_JBawktbYZaJBn9qMaE1dG6kLJu

1st Episode Link: Here's How Hackers Are Targeting You,... https://www.youtube.com/watch?v=J8qvn_HZb_A
2nd Episode Link: Mobile Phone Hack Trick से ऐसे बचें |... https://www.youtube.com/watch?v=JtPiRdj04IU
3rd Episode Link: Mobile Phone Hack, OTP Fraud, WhatsAp... https://www.youtube.com/watch?v=48VNZ1FpkBY
4th Episode Link: Mobile से आपको HACK किया जा रहा | Wha... https://www.youtube.com/watch?v=8RM4W_mWjTc
5th Episode Link: Mobile Phone Hack, OTP Fraud, WhatsAp... https://www.youtube.com/watch?v=WSJZh3cZuM0
6th Episode Link: How Hackers Hack Mobile Phone, Bank A... https://www.youtube.com/watch?v=shiTy3kAvoo
7th Episode Link: Hackers Hacking Mobile Phone, OTP, Ba... https://www.youtube.com/watch?v=bn4nc78AxEo
8th Episode Link: Podcast with Cyber Expert Amit Dubey ... https://www.youtube.com/watch?v=1HmmTwnfXyo
9th Episode Link: Podcast Cyber Expert Amit Dubey | Sha... https://www.youtube.com/watch?v=x_dOL6Ma8iw
10th Episode Link: Hacker Hacks Hotel, Steals Diamonds W... https://www.youtube.com/watch?v=2pSz_PnG-Bw
11th Episode Link: Hacker Steals iPhones Worth 10 Crore ... https://www.youtube.com/watch?v=Ic3hsZOvUcY
12th Episode Link: What is Dark Web? How To Access Dark ... https://www.youtube.com/watch?v=mtbn2R1zMpo
13th Episode Link: How Hackers Hack Mobile Phone Using A... https://www.youtube.com/watch?v=6q603E5w8zc
14th Episode Link: How AI Solved 19 Yr Old Murder Case |... https://www.youtube.com/watch?v=jpJ4d7zdlSU
15th Episode Link: Mobile Phone Listens To You Even When... https://www.youtube.com/watch?v=ZTIw6cgrwmA
16th Episode Link: How China is Preparing Cyber Army | C... https://www.youtube.com/watch?v=bnpNNAkTX_w
17th Episode Link: Mobile Phone Hacked by Downloading Image... https://www.youtube.com/watch?v=OaMmuUzmEhA
18th Episode Link:

हैकर्स की नई ट्रिक, बचने का एक तरीका
Cyber crime exposed: Digital arrest, OTP scams, password leak

SMS, Call and Email spoofing – https://www.youtube.com/watch?v=shiTy3kAvoo&t=2501s
E-sim fraud – How to prevent – https://www.youtube.com/watch?v=shiTy3kAvoo&t=2432s

Digital Arrest से कैसे बाहर निकलें? Hacking Expert Amit Dubey से जानिए
https://www.youtube.com/watch?v=f_tSA2OAmSU

How to activate or deactivate call forwarding on Jio, Airtel, Vi, and BSNL
https://www.91mobiles.com/hub/call-forwarding-codes-jio-airtel-vi-bsnl-how-to-activate/

MobiArmour: Mobi Armour by MobiArmour
https://play.google.com/store/apps/details?id=com.prosthetik.supernova

About this app: Introducing "MobiArmour (Mobi Armour): Your Guardian in the Digital Realm" — the all-inclusive solution dedicated to fortifying your digital existence against an array of potential hazards. In a time where technology assumes an integral role in our everyday lives, guaranteeing your online security has never held more significance.

ओटीपी कैसे हैक होता है? सावधान रहें, बचें और दूसरों को भी बचाएँ।

1. ओटीपी आने पर मोबाइल के स्क्रीन पर फ्लैश होता है – मोबाइल कहीं भी नहीं छोड़ना है।
2. ओटीपी कॉल पर भी आता है – मोबाइल कहीं भी नहीं छोड़ना है।
3. ओटीपी कॉल मर्जिंग टेक्निक से – दो अननोन नंबर से कॉल आ रहे हैं तो आपको कॉल मर्ज नहीं करना है।
4. ओटीपी कॉल फॉरवर्डिंग टेक्निक से – आपके नंबर से कॉल डायल करवा दें, तो आपके कॉल अनकंडीशनली क्रिमिनल को फॉरवर्ड होने लगेंगे, तो आपके ओटीपी भी फॉरवर्ड हो जाएँगे।
5. ओटीपी वॉइस मेलिंग टेक्निक से – ओटीपी आपके वॉइस मेल में रिकॉर्ड हो जाएगा। क्योंकि आप फोन उठा नहीं पा रहे हो, फोन आपका बिजी हो या व आपको बिजी कर देगा एक नए दूसरे नंबर से फोन लगा के जानबूझकर । वॉइस मेल डिऐक्टिव करें।
6. ओटीपी ई सिम ऐक्टीवेट कर लेने से – ई सिम ऐक्टीवेट कोड को कभी भी अपने फोन से सर्वर को ना भेजें।
7. ओटीपी स्क्रीन शेयरिंग टेक्निक से – क्विक सपोर्ट / एनी डेस्क या टीम व्यूअर इंस्टॉल कराके आपके फोन की स्क्रीन शेयर कर देता है। (गूगल मीट / माइक्रोसॉफ्ट टीम / जूम etc) अवॉइड वेब कॉल्स ऑन मोबाइल फोन क्योंकि कम्प्यूटर पर ओटीपी नहीं आएगा।
8. ओटीपी क्यूआर कोड स्कैन से – अप्रामाणिक क्यूआर कोड स्कैन करने से कोई वाइरस तरीके का ऐप फोन में इंस्टाल हो जाएगा जो आपके फोन को पूरा ऐक्सेस कर लेगा।
9. ईमेल आईडी का पासवर्ड – ईमेल पर बैंक का भी ओटीपी आता है । ईमेल आईडी का पासवर्ड किसी को नहीं बतायें।
10. इमेज या वीडियो के माध्यम से कोई वाइरस का ऐप फोन में इंस्टाल हो जाएगा जो आपके फोन को पूरा ऐक्सेस कर लेगा।
11.
12.

"इस दुनिया में दो ही तरह के लोग होते हैं एक जिनको पता है कि व हैक हो गए और दूसरे जिनको पता नहीं कि वो हैक हो गए दरअसल हम सब हैक हो चुके हैं और हमारा डाटा ऑलरेडी बाहर है।" – **अमित दूबे** Cyber Security Expert

साभार: हैकर्स की नई ट्रिक, बचने का एक तरीका | Cyber Crime Investigator Amit Dubey | Whatsapp Hacked https://www.youtube.com/watch?v=1cyVP7AZoZs

Essence in Hindi –

1st Episode Link: https://www.youtube.com/watch?v=J8qvn__HZb__A

1. गेम के थ्रू घर की करीब 150 इमेजेस क्रिमिनल के सर्वर पर अपलोड हुई थी. जब वो पिक्चर्स कैप्चर हुई तो उस दीवार पर कितना सिग्नल लेवल है वो भी कैप्चर हो गया .
2. इनोवेशन दुनिया में होता है उसका जो पहला यूजर है वो एक क्रिमिनल होता है
3. पिक्चर भेज कर ब्लैकमल करना.
4. इंटरनेट पर जब आप काम करते हैं तो आपकी लोकेशन तो जाती है.
5. हम कोई कंटेंट देख रहे हो चाहे हम फ्री में कुछ चीजें लेने की कोशिश कर रहे.
6. इनकी पूरी ट्रेनिंग होती है ओके और बड़े प्रोफेशनल तरीके से होती है इनको बताया जाता है कि ह्यूमन साइकोलॉजी कैसे काम करती है. यह बहुत ज्यादा कूल और काम होकर हमेशा बात करते हैं क्योंकि उनको पता है कि यदि आप शांत होकर बात करेंगे तो आप लोग जल्दी भरोसा कर लेते हैं. इसके अलावा जो टेक्निकल चीजें हैं – बिहेवियरल एस्पेक्ट्स है फिशिंग लिंक कैसे क्रिएट करना है, एप्स कैसे क्रिएट करना है, हर चीज की ट्रेनिंग होती है और उसके बाद टारगेटेड जॉब दी जाती है कि आपको इतना इतने लोगों को टारगेट करना है. उनको पहले से डाटा दिया जाता है. जो इनको ये प्रोवाइड कराता है कोई तो बॉडी है, जो इसके पीछे ऑर्गेनाइज तरीके से काम करती है. तो ये सारी चीजें इनको प्रोवाइड कराई जाती हैं. अपने घर से बैठ के फोन करते नहीं है ये हमेशा बॉर्डर एरिया में रहते हैं ऐसे एरिया में कि आज यहां से कॉल करेंगे कल यूपी से परसों यहां मथुरा में है फिर नूह में चले गए फिर फरीदाबाद चले गए फिर दिल्ली आ गए तो ये लोकेशन बड़ी तेजी से मूव करती है तो हमेशा आप देखोगे जो हॉटस्पॉट है ये बॉर्डर एरियाज में ज्यादा पनपते हैं. इंडिया के लोगों के बच्चों को पकड़ लिया वहां पे लेके चले गए और वहां पे उनसे साइबर क्राइम करवा रहे. उनको ट्रेन कर रहे .
7. लोगों को लालच भी दिया जाता है कि आपके बैंक अकाउंट में पैसा आ जाएगा. एक मनी ट्रेल बन जाती है अंतत क्या होता है कि सारे अकाउंट ब्लॉक कर दिए जाते हैं. लालच में फस गए होते हैं सफर करना होता है
8. एप्लीकेशन होगी जिससे वह एसएमएस पढ़ती होगी बाहर भेजती होगी और फिर एसएमएस डिलीट करती होगी
9. बच्चे एनोनिमस चैट – पूरी दुनिया से बातचीत कर सकते हैं और वो आपको एक एनोनिमिटी दे देता है. क्रिमिनल था उसने इसको कुछ भेजा कि यह एप्लीकेशन अपने फादर के फोन में इंस्टॉल कर दो तो मैं 200 रोक्स पॉइंट्स मिलेंगे सो 200 रोक्स पॉइंट के चक्कर में इस बच्चे ने वो एप्लीकेशन अपने फादर के फोन में इंस्टॉल कर दी और उसके बाद उसने कहा अन इंस्टॉल कर दो क्योंकि थोड़ी दिनों बाद फिर करोगे तो फिर मिलेंगे उसने अन इंस्टॉल भी कर दि जस्ट गेम खेलता था.
10. सिर्फ लिंक क्लिक करने से आपकी बहुत सारी इंफॉर्मेशन बिना परमिशन के निकल जाती है आप चाहे तो चेक कर सकते हैं एक लिंक है https://privacy.net/analyzer/
11. ब्राउजर सबसे ज्यादा टारगेट होता है. किसी को एक्सप्लोइट करके डाटा चुरा सकता है ऑटो फिल भी चुरा सकता है पासवर्ड भी चुरा सकता है ऑटो फिल में आपके बैंक अकाउंट डिटेल भी हो सकते हैं आपके पर्सनल आधार कार्ड बैंक और ये सारे सोशल सिक्योरिटी नंबर हो सकते हैं
12. मैं कहता हूं कोई भी अन लोन लिंक क्लिक कर रहे हैं या कोई भी हम अननोन एप्लीकेशन इंस्टॉल कर रहे हैं जिसकी वजह से हमारा डाटा बाहर जाएगा, यह रोकना बहुत जरूरी है क्योंकि जैसे यह हो जाएगा आपके संग क्रिमिनल्स के अटैक बढ़ जाएंगे
13. स्क्रीनशॉट भेजने से OTP share. ब्यूटीफुली माइंड प्ले किया जाता है
14. कंडीशनल कॉल फॉरवर्डिंग या ऑल कॉल फॉरवर्डिंग कर सकता. OTP काल पर भी आता है
15. टू फैक्टर ऑथेंटिकेटेड Whatsapp को कर लें. आपसे वो सिक्स डिजिट का कोड, उसके संग एक ईमेल आईडी भी मांगेगा वो भी दे दें.
16. फिर दूसरा जो तरीका है ओटीपी चुराने का वो है कॉल मर्जिंग टेक्निक. कॉल मर्जिंग में क्या है – जैसे आप मेरे बहुत अच्छे मित्र हैं आपको एक कॉल आता है – अयाज भाई अमित जी ने आपका नंबर दिया .है ओके, तो अयाज भाई ट्रस्ट करेंगे ही. .....और मीठी मीठी बातें और अयाज भाई खुश हो गए. थोड़ी देर में नंबर से कॉल आ रहा होगा, अयाज भाई कहे ये अमित का नंबर नहीं है. नहीं, नहीं उनका वीआईपी नंबर है. आप मर्ज कीजिए ना, मर्ज कीजिए. थोड़ा सा अर्जेंसी दिखाई, प्रेशर दिखाया, आपने मर्ज कर दिया. जैसे ही आप मर्ज करेंगे आपके अकाउंट से पैसे निकल जाएंगे या आपका हैक हो जाएगा. आपने दो इनकमिंग कॉल मर्ज कर दी, एगजैक्टली. और अपने पैरों पर कुल्हाड़ी मार ली . आपको वो आपके ओटीपी का कॉल था. आपने मर्ज किया आपने उसको ओटीपी सुनवा दिया. वो तो रेडी था सुनने को
17. यह दूसरा तरीका है जो बहुत चल रहा है. ऐसे वॉइस मेल के थ्रू निकल जाते हैं
18. जूम कॉल के थ्रू निकल जाता है आपकी स्क्रीन शेयर करा ली किसी बहाने से या कोई भी वेब मीटिंग. मैं आपको एक मीट का लिंक भेजता हूं आप अपनी स्क्रीन शेयर कीजिए और वही देखते हम क्या इशू है जो एरर आ रही होगी ना उस हिसाब से

फिक्स कर देंगे ठीक है साब. उन्होने मीट का लिंक भेजा. लिंक क्लिक किया, मीटिंग जवाइन कर ली, स्क्रीन शेयर कर दिया, बोला आप एक रुप ट्रांसफर करो, आप एक रुपए ट्रांसफर करो, फिर ओटीपी भी आएगा वो भी दिखेगा उसको स्क्रीन पर, तब तक तो 10000, 15000, 15000 निकल जाता है.

19. हमारे घर के बुजुर्ग उनको स्पेसिफिकली टारगेट करते हैं.

20. डिजिटली अरेस्टेड – इसको कॉल आया आपका एक कुरियर आया हुआ है. आपके नाम से कुरियर भेजा जा रहा था थाईलैंड और व वापस आ गया है और उसमें कुछ पासपोर्ट है कुछ करें है कुछ ड्रग्स है एमडीए में और इलीगल चीजें पाई गई है तो इसलिए इंक्वायरी शुरू हो गई है और आपके खिलाफ एफआईआर हो गई है तो मुंबई क्राइम ब्रांच इसको देख रही है तो हम आपका कनेक्ट कर देते हैं. आप एक वीडियो कॉल पे स्टेटमेंट दे दो ओके और उसके लिए आपको एक अमाउंट देना पड़ेगा 50000 दोगे तो वीडियो कॉल स्टेटमेंट हम रिकॉर्ड कर लेंगे. उसके बाद कहेगा कि भाई साहब अब आप इस कैमरे को ऑफ नहीं कर सकते आप डिजिटली अरेस्टेड हैं. अब इस कैमरे को ऑन रखना, मोबाइल चार्ज रखना और आप कैमरे के सामने रहना, हिलना नहीं क्योंकि अभी इंक्वायरी चल रही है. यदि आपने बंद किया आपको तुरंत अरेस्ट कर लिया जाएगा. आप अपना पैसा खुद ही उनके अकाउंट में डालते जाएंगे

21. यूपी पुलिस की जो ये 1090 हेल्पलाइन है उसका जो रेजोल्यूशन रेट है वो 95% से ऊपर है. ये बताना चाह रहा हूं मैं लोगों को कि जितनी ये हेल्पलाइन है प्लीज उनको यूज कीजिए ट्रस्ट कीजिए वो वर्क करती है और बहुत अच्छा काम कर रही हैं

2nd Episode Link: https://www.youtube.com/watch?v=JtPiRdj04IU

1. आपको समझ में आएगा कि अरे ये डाटा जा रहा है हमारा वॉइस सुनते हैं आपकी सराउंडिंग्स की, आपके ओटीपी सारे उनके पास जाते हैं आपके कॉल रिकॉर्डिंग जितना डाटा आप देखोगे ना ये सब जा रहा है

2. हैकर आपसे पैसा लेना चाहता है. आपने पैसा दिया वो आपको परेशान करता रहेगा. आप पैसा नहीं देंगे वो आपको छोड़ के किसी और जगह एनर्जी लगाएगा .

3. क्रिमिनल्स डू नॉट हैक योर डिवाइस टू रीच टू यू, क्रिमिनल्स हैक यू टु रीच योर डिवाइस

4. रिकॉर्ड कर लिया, शेयर कर दिया, पोस्ट कर दिया, तीनों इक्वली सीवियर क्राइम है और उसके लिए रिस्पांसिबिलिटी आपकी होगी. UK में आप किसी बच्चे की फोटो बिना अनुमति के नहीं ले सकते.

5. फेक बना के ब्लैकमेलिंग शुरू हो जाती है सेक्सटॉर्शन के केसेस जो आपने सुने हैं कि आप ही का फेस लेकर आपकी कुछ पिक्चर बनाई और ब्लैकमेलिंग शुरू हो गई और आप डर गए उसको भी रिपोर्ट नहीं कर रहे. तो रिपोर्ट तो कीजिए क्योंकि यदि आप रिपोर्ट नहीं कर रहे तो आप एक तरीके से क्रिमिनल को एडवांटेज दे रहे हैं

6. हमारा जो ब्रेन है ना – प्रोडक्ट ऑफ द डेटा है. हम डाटा से इन्फ्लुएंस होते हैं डाटा पर ट्रस्ट करते हैं. हम कॉन्शसनेस को यूज कम करते हैं

7. आप आपके अकाउंट में पैसे आने के लिए आपको कुछ नहीं करना है आपको सिर्फ तब करना है जब पैसे देने है किसी को इतनी चीज कैसे इग्नोर कर सकता है.

8. लिंक क्लिक मत करना (क्योंकि क्यू आर कोड भी लिंक होता). मैंने लिंक क्लिक नहीं किया, ठीक है. तो मेरे पैसे कैसे गए? बोले यार उसने क्यूआर कोड भेजा था, मैंने स्कैन कर दिया.

9. ये जो हमारा बिलीव सिस्टम कई बार हमारे लिए प्रॉब्लम क्रिएट करता है तो मैं कह रहा हूं कि आप क्वेश्चन करें

10. क्यूआर कोड आजकल बहुत ज्यादा यूज होने लगा है लेकिन उसको थोड़ा मैनिपुलेट करके आपके सा प्रॉब्लम क्रिएट की जा सकती है. एक पोस्टर लगा दूं फ्री वाईफाई और एक क्यूआर कोड. थोड़ी देर में 25–30 लोगों को हैक कर निकल लेंगे इतनी सी चीज है इसमें कोई मुझे रॉकेट साइंस नहीं करनी है क्योंकि मैं फोर्सेबल आपसे कुछ इंस्टॉल करवा दूंगा आपके फोन में और उसके बाद आप गए. उसको चेक कैसे करना उसका एक तरीका है एक एप्लीकेशन है मोबी आर्मर करके. वो आप इंस्टॉल कर ले अपने फोन में व आपका कोई डाटा नहीं लेते और उसमें एक ऑप्शन है क्यूआर कोड स्कैन का, लिंक स्कैन का, ओटीपी सिक्योरिटी का तो आप यदि क्यूआर कोड उसके थ्रू स्कैन करेंगे तो वो उसको क्यूआर कोड को पहले सैंड बॉक्सिंग एनवायरमेंट में ले जाएगा वहा रन करेगा. देखेगा कि अनसेफ है कोई आपका ऑटो फिल डिटेल तो नहीं चुरा रहा, आपके अकाउंट से पेमेंट तो नहीं कर रहा क्योंकि पेमेंट भी होता है क्यूआर कोड से और उसके बाद ग्रीन रेड करके बता देगा कि यह सेफ है. आप इसको आगे कंटिन्यू कर सकते हो

11. दूसरा लिंक बेस फ्रॉड होते हैं जिसमें आपको ई–कॉमर्स का लिंक आ गया. फोन आए साब आ बुक किया था वो डिलीवरी नहीं हुआ, कौन सी वेबसाइट थी. ये था. हां सर बहुत सारे ऐसी 40% पर डिस्काउंट था, 30% पर डिस्काउंट था और त्यौहारों के टाइम पर तो बहुत आते हैं. आपको पता नहीं होता कि इस पर ट्रस्ट करूं ना करूं. तो वो लिंक आप स्कैन करें. उस वेबसाइट

के अंदर कोई वायरस तो नहीं है कोई मैलवेयर जो आप खोलो तो आपका डटा चुरा ले या आपकी डिटेल्स निकाल ले वो हर तरीके से स्कैन करके आपको एक आईडिया देगा रेड ग्रीन कि आप इसमें कंटिन्यू करो या ना करो

12. तीसरा उसम एक ऑप्शन है वाईफाई सिक्योरिटी क्योंकि वाईफाई के थ्रू भी बहुत चांसेस होते हैं आपने पब्लिक वाईफाई कर लिया. अच्छा वाईफाई क्या है यदि आप और मैं एक ही वाईफाई में कनेक्टेड है तो मैं आपके खिलाफ एक मैन इन द मिडल अटैक कर सकता हूं. मैं आपके ट्रैफिक को देख सकता हूं. क्या आप मोबाइल पर खोल रहे हो वेबसाइट और यह एक थ्रेट हो सकता है आपको. इसलिए हम कहते हैं कि पब्लिक वाईफाई में कमर्शियल ट्रांजैक्शन ना करें. अवॉइड करें. लेकिन आप चेक कैसे करेंगे कि वाईफाई सेफ है या नहीं है तो उसमें एक ऑप्शन है व वाईफाई बता देगा सेफ है अनसेफ है

13. ओटीपी सिक्योरिटी का ऑप्शन है कि जितने भी ओटीपी चुराने के तरीके हैं वह सारे ब्लॉक कर देगा आपके फोन में जैसे कॉल मर्जिंग नहीं होगी, कॉल फॉरवर्डिंग नहीं होगी, वॉइस मेल फीचर डिसेबल कर देगा, स्क्रीन शेयरिंग ऑप्शन ऑफ होगी

14. फिर चौथा इसमें है कि जितने एप्लीकेशन आप इंस्टॉल करते हो सबको स्कैन करेगा और यह देखेगा कि इस एप्लीकेशन मिसयूज तो नहीं हो सकती क्रिमिनल द्वारा ऐसे कई सारी एप्लीकेशन ऐसी है जो ऑथेंटिक है लेजिटलक्वेस्ट नहीं करने देगा क्योंकि खास तौर से ऐसे लोग जो सीनियर सिटीजन है या बच्चे उनको आईडिया नहीं होता कि हम जो भी इंस्टॉल कर रहे हैं ये ठीक है. गेम इंस्टॉल कर रहे हो अब गेम से लोग लुट जाते हैं उन गेम्स को ब्लॉक कर देती है. गेम में मल्टीप्लेयर चैट फैसिलिटी होती है. अब बच्चों को लगता है कि साने वाला मेरा उमर का है, बिल्कुल उसमें आधे क्रिमिनल हैं और वो बच्चों के थ्रू आपके फोन को हैक करना चाह रहे हैं. वो बच्चों को डरा के, लालच देकर के मान लो एक लिंक भेजा उनकी डिटेल बच्चे की लीक हो गई

15. अपने फोन बेच देते हैं और उनके अंदर से लोग डाटा रिकवर कर लेते हैं बिल्कुल. और फिर वो उनके अगेंस्ट यूज होता है

16. यदि आपका प्रॉपर्ली क्लीन फोन नहीं है, फॉर्मेट भी करेंगे तब भी रिकवर हो जाता है. अच्छे अच्छे रिलेशन में कॉन्फ्लेक्ट आ जाता है तो इसलिए ऐसी चीजें ना ही करें अवॉइड करें फोन फॉर्मेट हो गया डिलीट हो गया तब भी सर्फेस होते हैं. सामने वाले का फोन चोरी करवा दिया और फिर डिलीटेड डाटा रिकवर कराया, उसकी चैट निकलवाई या जो भी कंटेंट मिला और उसको फिर उसके खिलाफ यूज़ किया ये भी करते हैं लोग तो आप प्लीज रखें ही ना ऐसा कोई कंटेंट तो ज्यादा अच्छे हैं. और खास तौर से यदि फोन डिस्कार्ड कर रहे हैं तो उसको प्रॉपर्ली फॉर्मेट करें, मल्टीपल टाइम्स फॉर्मेट करें, क्लीन अप प्रोसेस यूज़ करें और उसके बाद ही छोड़ें.

17. इस दुनिया में कोई चीज फ्री नहीं होती तो हवा पानी भी फ्री नहीं है तो हम जब भी कोई चीज फ्री यूज कर रहे हैं तो कहीं ना कहीं कोई ना कोई तरीका है जिससे वो पैसा कमाए. आज नहीं कमाए तो कल कमाए, आज किसी और तरीके से कमा रहा होगा, कल सीधे–सीधे भी कमा सकता है.

18. आप का जो फोन का जीमेल है आप जगह जगह लाग इन कर करके रखते हैं, वह आपके घर के लैपटॉप में भी लगा हुआ है, वो ऑफिस के पीसी में भी होगा, आईपैड में भी है, जो चार लोग शेयर भी कर रहे हैं या कई बार किसी और के भी लैपटॉप में कर दिया लॉगइन और भूल गए. यदि वह जीमेल का एक्सेस मुझे 10 सेकंड के लिए मिल गया 20 सेकंड के लिए मिल गया तो मैं आपकी जिंदगी में कल हंगामा क्रिएट कर सकता हूं. बिलकुल क्या कर सकता हूं सोचिए. ऐसी बहुत सारी चीजें हैं जो आप फोन से ऑथेंटिकेट कर लें. ईमेल ओटीपी या एसएमएस ओटीपी

19. सर मेरा फोन हैक हो गया फोन एक्चुअली हैक नहीं होता. **जो फीचर्स है ये मिस यूज हो रहे होते हैं.** आपके आसपास ही जिसको वो एक्सेस मिल गया या तो लाग इन मिल गया, कुछ तो मिसयूज करेंगे.

20. कोई दूसरों से शेयर ना करें पासवर्ड

21. पहले अपने डाटा की वैल्यू समझ लें आप अपने अराउंड देखें तो जितने भी टॉप 10 रिचेस्ट कंपनीज हैं, वो वो हैं जो आपको फ्री प्रोडक्ट देती हैं. जो आपसे पैसा लेते हैं अपने प्रोडक्ट या सर्विस का वो गरीब हैं. फ्री वाली सब रिचेस्ट हैं और इनके पास जो पैसा है, जो इनकी वैल्युएशन है ना, वो जो पैसा ले रही हैं उनसे इतना आगे है कि वो टच भी नहीं कर सकते. आप चेक कर सकते हो प्ले स्टोर पर जाकर कि कितना डाटा लेते हैं. एंड दैट इंक्लूड्स एवरीथिंग. लोकेशन तो एक बहुत बेसिक चीज है. आपकी हेल्थ फिटनेस, आपके फाइनेंशियल रिकॉर्ड्स, आपके पॉलिटिकल आइडिया, आपके रिलीजियस आइडल, आपकी सेक्सुअल ओरिएंटेशन, आपके एक्जेक्ट एड्रेस ऑफ योर हाउस, एवरीथिंग दे टेक एंड ऑल ईमेल्स वॉइस सुनते हैं, आपकी सराउंडिंग्स की, आपके ओटीपी सारे उनके पास जाते हैं. आपके कॉल रिकॉर्डिंग्स एंड ऑल. सो जितना डटा आप देखोगे ना, यह सब जा रहा है तब आपको समझ आएगा कि इस डेटा का होने क्या वाला है और क्यों जा रहा? सो दैट दे कैन ड्राइव योर लाइफ. आप क्या पहनोगे, क्या खाओगे, क्या खरीदोगे, क्या देखोगे, किसको वोट दोगे, क्या लाइक करोगे, क्या डिसलाइक करोगे, एवरीथिंग विल बी डिसाइडेड बाय सम बडी एल्स. आपके नेटवर्क में कौन–कौन है, बिल्कुल कांटेक्ट लिस्ट जा रहा ,है सबके पास जा रहा. आपके क्लोजेस्ट कौन–कौन है, वो भी पता कर लेते हैं. किससे आप ज्यादा बात करते हैं, किससे आप कभी–कभी, बहुत ज्यादा कनेक्टेड हैं किससे आप बहुत ज्यादा मिलते हैं

22. आपकी प्राइवेसी आपका फंडामेंटल राइट है. यदि आपको ब्लैकमेल कर रहे हैं तो तो क्राइम है

23. आप वीपीएन यूज कर ले पर वीपीएन आप क्यों यूज कर रहे हैं. प्राइवेसी के लिए. देयर नथिंग फ्री इन दिस वर्ल्ड. आप यह ना सोचें कि आप वीपीएन यूज कर रहे हैं और उससे बचे रहेंगे, तो ये बहुत बड़ी गलती है आपकी.

3rd Episode Link: https://www.youtube.com/watch?v=48VNZ1FpkBY

1. सबसे ज्यादा बैंक ही हैक होते हैं पर यह खबर लोगों को बताई नहीं जाती
2. आरबीआई की जो गाइडलाइन है वो क्लियर है. उसमें कहा है कि तीन दिन के अंदर आप बैंक को इफॉर्म करते हैं कि आपके अकाउंट से पैसा निकल गया है तो बैंक इज लायबल टू पे यू 100% मनी बट आपकी गलती नहीं होनी चाहिए.
3. एक पैकेज दिया जाता है क्रिमिनल्स को कि ये फादर है यह बेटा है. बेटे को वो कॉल करते हैं पहले उसकी आवाज क्लोन करते हैं फिर वो फादर को कॉल करते हैं और जब वो फादर को कॉल कर रहे होते हैं तो बेटे को बिजी कर देते हैं
4. 4–5 हजार की डिवाइसेज आती हैं और वो किसी भी जो यूएसबी चार्जर है उसके पीछे प्लग इन कर सकते हो आप. वो आपका डाटा सक कर सकती है. आपका डाटा कॉपी कर सकते हैं और इस चीज को अवॉइड करने के लिए तरीका यही है कि आप पावर प्लग यूज करें, यूएसबी के थ्रू चार्ज ना करें . कई बार लोग लोगों के लैपटॉप से भी चार्ज कर करते तो वो भी कॉपी कर सकते हैं
5. 12 हजार की डिवाइस आपके क्रेडिट कार्ड को रिमोट कॉपी कर सकते हैं. अरे क्लोन कर सकते हैं. मैं आपके बगल से निकलूं और वो डिवाइस ऐसे लगाके निकल जाऊँ तो आपका क्रेडिट कार्ड या डेबिट कार्ड की क्लोनिंग मेरे पास आ जाएगी
6. कोई सर्वर होता है ना उसको ट्रिपल ए सर्वर बोला जाता है. **ट्रिपल ए क्या होता है – ऑथेंटिकेशन, ऑथराइजेशन, अकाउंटिंग.** ये तीन चीजें उसमें जरूर होनी चाहिए. यदि नहीं है तो फिर आपका काम पूरा नहीं हुआ है. ऑथेंटिकेशन का मतलब है कि मैंने पहचाना कि आप कौन है जिसने लॉगइन किया. ऑथराइजेशन का मतलब है कि इनको किस–किस चीज का एक्सेस देना है इनको सिर्फ इन्हीं का डाटा दिखाना है, या इनको अमित का भी डाटा दिखा देना है, इनको किसी और का भी डाटा दिखा देना है ये ऑथराइजेशन है. और अकाउंटिंग का मतलब है कि इन्होंने जब लॉगइन किया उसके बाद किया क्या है इस सर्वर पर. डाटा तो नहीं डाउनलोड कर लिया 1 टेराबाइट का. ऐसा तो नहीं है कुछ और करने ऐसा जा रहे तो इसकी अकाउंटिंग भी की जाए लॉग भी रखा जाए
7. मेरा पैसा किस अकाउंट में गया था उसके बाद कहां गया उसका मनी ट्रेल क्या था, बैंक पैसे को किसी अकाउंट में तो रोक सकते थे तो कितना रोका, जिसका जानने का आपको हक है. आपको अपनी पावर समझनी होगी. अब आपको पुश करना पड़ेगा बैंक को और यदि आपको ऐसा लगता है कि बैंक आपको सपोर्ट नहीं कर रहा है, रिस्पांस नहीं कर रहा है तो आप आरबीआई ओंबड्समैन भी जा सकते हो. आप जितनी जल्दी एक्शन लेंगे जिस अकाउंट में पैसा गया उस अकाउंट को फ्रीज करवाना है यदि वो अकाउंट आपने फ्रीज करवा दिया किसी भी तरीके से.
8. **अकाउंटफ्रीज करवाने के लिए तीन ऑप्शन हैं –**

पहला **1930 जो गृह मंत्रालय के 24 घंटे का पोर्टल है** आप उस पर तुरन्त कॉल करें. उसको अपना ट्रांजैक्शन आईडी बताएं कि यूपीआई से गया, आपने खुद आरटीजीएस किया या जो भी ट्रांसफर हुआ है और उसको बोलें कि भाई ये पैसा आप इस अकाउंट में फ्रीज करा दीजिए. उनके पास पावर्स हैं, वो करा सकते हैं .

दूसरा है कि आप **अपने बैंक को बोलें** कि मैंने डिस्प्यूट रेज कर दिया है और उसमें रिक्वेस्ट करें कि इस अकाउंट में जो पैसा गया उसको आप फ्रीज कराइए. बैंक करा सकता है बैंक के पास ये पावर है क्योंकि उसी ने ट्रांसफर किया है वो तुरंत दूसरे बैंक को रिक्वेस्ट कर सकता है.

तीसरा है कि आप **खुद भी एक कंप्लेन उस बैंक को भेज सकते हैं**. हर बैंक के नोडल ऑफिसर्स होते हैं. आप उसको एक कंप्लेन कर दें कि भाई इस अकाउंट में मेरे इस अकाउंट से पैसा आया है. आई एम रेजिंग दिस रिक्वेस्ट टू प्लीज फ्रीज इट तो उसका नोडल ऑफिसर एक्शन ले सकता है

9. कार से ही मीटिंग ज्वाइन करना. फेक वीडियो कॉल मीटिंग ऑडियो क्लोन करके. **स्पूफ ईमेल** क्योंकि कंपनी का ईमेल सर्वर डीमार्क कम्प्लाएंस नहीं था. वॉइस क्लोनिंग तो बहुत सारे टूल आ गए हैं
10. **चार ही तरीके हैं** जिससे आपका फोन हैक हो सकता है – **एक** तो है ईमेल, **दूसरा** आपने कोई ऐप इंस्टॉल कर ली, **तीसरा** आपने कोई वेबसाइट ऐसी खोल ली और उसने कोई प्लगइन इंस्टॉल कर दिया और **चौथा** है कि आपने किसी तरीके से ओटीपी दे दिया या अपना कोई क्रेडेंशियल शेयर कर दिया. तो यही चार अटैक वेक्टर्स हैं जो अभी मेजर्ली चल रहे हैं.
11. फोन यहां पड़ा हुआ है अब ओटीपी आया किसी ने देख लिया क्योंकि आपने वो फीचर डिसेबल नहीं किया हुआ है कि जब लॉक मोड में भी ओटीपी आए तब भी ऊपर दिखता है. ऐसे भी फीचर्स बिल्कुल रहते हैं तो इसमें आपको अंदर से जाके डिसेबल कर देना है तो वो नहीं दिखेगा
12. दूसरा है कि कॉल तो उठा ही लेता है. बिल्कुल मेरा फोन लॉक भी है और कॉल आता है तो कोई उठा के ओटीपी सुन सकता है. तो आप फोन छोड़ के वहाँ चले गए और उस समय ओटीपी कॉल पे मँगाया और सुन लिया. तो इस तरह की चीजें जो गलती से हम लोग इग्नोर कर देते हैं. यदि हम इस बारे में कॉन्शियस हो जाए तो आपके संग हैकिंग वाली सिचुएशन नहीं होगी.
13. इस एप्लीकेशन का नाम है – हु टच माय फोन. हु टच माय फोन फ्री है

14. ओवरऑल इंटरनेट का हम 3 परसेंट से ज्यादा कभी एक्सेस कर नहीं सकते. 90 परसेंट जो इंटरनेट है वो डीप वेब – डीप वेब – क्लासिफाइड सर्वर जैसे बैंक के सर्वर हैं, गवर्नमेंट के सर्वर्स, कॉलेज के सर्वर हैं, आरोग्य सेतु आधार कार्ड पासपोर्ट इन सबके सर्वर डीप वेब में आते हैं. जो इंटरनेट पर हैं, क्रेडेंशियल के थ्रू एक्सेस होते हैं. उसके बाद है 7 परसेंट डार्क वेब जो सबसे ज्यादा इंटरेस्टिंग है. इसमें दुनिया की हर इलीगल, इंसानियत की दृष्टि से सही नहीं समझोगे हैवानियत वाली चीजें होती हैं
15. हमें कहानियां बताने की जरूरत है. इस वक्त जिस तरीके के इंसीडेंट हो रहे हैं अवेयरनेस उन स्टोरीज के फॉर्म में फैलाई जाए, जो हम बड़े आराम से कर सकते हैं
16. वो फ्री में क्लाउड सर्विसेस देते हैं क्यों देते हैं क्योंकि वो डाटा को कंट्रोल कर सकते हैं. एक बार आपकी लत लग गई और आपका डाटा हमारे पास है तो आप कहां जाओगे. आपकी 10 साल की हिस्ट्री मेरे पास है. आज अगर आपके पास मेरे 20 साल की हिस्ट्री है अब मैं उसको स्विच कर ही नहीं सकता. इट्स ऑल डेटा ड्रिवन बिकॉज डेटा इज सेंट्रलाइज एंड सम बडी इज यूजिंग दिस डटा टू मेक मनी. और आसानी से पैसा तभी बनता है जब वो डाटा नेगेटिवली यूज हो रहा हो.
17. आपने केसेस सुने होंगे कि प्रेसिडेंट्स तक के फोन हैक हुए हैं. जीरो डेज वलनरबिलिटी.

4th Episode Link: https://www.youtube.com/watch?v=8RM4W_mWjTc