Twitter Thread by Nafs

Nafs
@NafsSays

I'll touch upon few different types of cyber frauds and few possible ways in which we can avoid ourselves to be duped of money, time & energy.

Will also attach few real registered FIRs showing that most of the times such crimes happen with educated & learned people.

1/16

Cyber Fraud type 1 - Facebook/Instagram

Profile cloning -Fraudster will make exact same profile like yours - using pictures from your own profile. They will then message to your contacts asking for money immediately for the surgery of mother or similar emotional lie

2/16

सेवा में एसएचओ साइबर पुलिस स्टेशन विषय:-फेसबूक मसेंजर से दोस्त की फेसबूक मसेंजर से मैसेज भेजकर पैसा रुपये 20,000 लेने हेतु श्रीमान जी मैं कुमार सिंह स्थाई पता, ग्राम ज पुर पोस्ट प पुर का रहने वाला हूँ।दिनांक-17/ /2020 को मेरे दोस्त तिवारी के फेसबूक मसेंजर से मेरे पास मैसेज आया कि मेरे दीदी की तबीयत खराब है। हमे रुपये की शक्त जरूरत है जिस पर मैंने अपने फोन पे 96 42 से बताए गए नंबर फोन पे 96706525508 पर कुल बीस हजार रुपये "दस हजार प्लस दस हजार " दे दी जो बाद में मैंने अपने दोस्त रमेश तिवारी से फोन पे पूछने पर पता चला की उसने ऐसा कोई पैसा नहीं मंगवाया था, मेरे पास फेसबूक मसेंजर से भेजे गए मैसेज का फेसबूक अकाउंट यूआरएल । www.facebook.com/Rameshtiwari.tiwari.359 कृपया उचित कानूनी कार्यावाही की जाये।

Always verify before sending money.
Don't verify by calling that person, instead, call a common friend or family member of that person. Don't think you can't be fooled - I know at least 20 people working in Top IT MNCs becoming victim of this fraud. Lock your FB/Insta.

3/16

First Information contents (प्रथम सूचना तथ्य):

a male person called up my father on his mobile from 6371758854.The caller impersonated as a friend in distress due to relatives in hospital and in need of money for a couple of hours. My father Mr PC I ,(80 years old, Retired senior government officer) asked me and my wife to transfer the money on paytm account given by caller as 7797568910. We transferred a sum of 1.2 lakh in various tranches. As later the caller said to my father that the relatives have died and another amount was needed urgently.(the transactions are in the attached file) later in the evening the caller called my father to return the money and asked my phone numbers to return the money by sending a QR code on whatspp from 9813885227 on the pretext of merchant swipe account and asked me to press the payment button. I did that and another 10000 was transferred to Malati Mahato.(the QR code picture in the attached file) Then he insisted again to pay, I told him to transfer directly on the UPI id, I shared that and then asked father to check with his friend and it turned out that the fried had never been to the hospital … and we were cheated for a sum of 1.3 Lakh.

Cyber Fraud type 2 -OLX/Quikr

This generally happens while selling something on OLX/Quikr & similar platforms. In such cases, people will fraud in the name of paying money by asking to scan the QR code or click a link.

NEVER scan the QR code to receive money, give your UPI

4/16

12. **First Information contents (प्रथम सूचना तथ्य):**

To the SHO Cyber Police Station Sub: fraudulent transaction in the name of purchasing item from olx Respected sir, I , Paul, resident of Haryana have given an advertisement in OLX to sell my sofa cum bed for Rs. 6500 on 01.03.2020. On 02.03.2020, I received a call from 9812928226, stating that this person would purchase the sofa. He will transfer 3000 Rs. through paytm and handover 6500 in cash to me. So he sent a QR code of re 1 as a test transaction and credited Rs. 2 on my account. Like this he started doing transaction of Rs 2999, Rs. 6000, Rs. 6000, Rs. 9000, Rs. 9000, Rs. 10000, Rs. 6000, Rs. 5000, Rs. 5000 total of Rs. 49000. The person always told that the money will get credited but it did not and the entire amount got debited. The second number from where I received a call was 7988472218. Request you to look into the matter and urge you to help me in the recovery of the said amount thanking you

Cyber Fraud type 3 - Fake SMS & Call from unknown numbers

Fraudster will send fake SMS showing amount credited to the account - with correct account number in SMS. Then they will call from unknown numbers asking for money.

ALWAYS check your bank account first via bank app.

5/16

सेवा में, श्रीमानजी, (चौकी इन्चार्ज जी) निमोठ निवेदन है कि में पुत्र चन्द निवासी गाँव तहसील जिला का रहने वाला हु दिनाक 2020 को 12.54 PM बजे मेरे मोबाइल फ़ोन न 9 9 पर एक अनजान न 9983054652 से फ़ोन आया और मेरा नाम बोलकर कहा की तेरे खाता मेने 110000 रु डाले है I मैंने मैसेज चेक किया तो उस पर 50000 रु 60000रु के दो मेसिज थे मेने विश्वास करके अपना जानकार अमित समझा कि वह बोल रहा है मेने उससे पूछा की अमित बोल रहा है तो उसने हाँ कहा ओर मैंने उसके कहे अनुसार 10000-10000 हज़ार करके फ़ोन से (PHONE PAY UPI) द्वारा ऑनलाइन 46000 रु O.B.C बैंक के खाता न से भेज दिए तथा 48000 हजार रु अपने भाई दीपक से कहकर उसके फ़ोन न0 से फ़ोन पे UPI द्वारा(S.B.I) खाता न: 3 2 से उसके बताए गए फ़ोन नo 9 5(UPI) द्वारा पैसे कुल टोटल 94000 रु हजार ट्रान्सफर कर दिए उसके बाद मेने अपना खाता चेक किया तो उसमे 500 रु बकाया था और कोई भी पैसा मेरे खाते में नहीं आया तो मुझे शक हुआ और अपने जानकार अमित से पूछा तो उसने कहा कि मैंने ना तो आपसे बात की और ना पैसे डाले और ना डलवाए जो नाम पता ना मालूम व्यक्ति न मेरे साथ धोखा धडी करके 94000 रु हजार ठग लिए उसके खिलाफ क़ानूनी कार्येवाही करके मेरे

Cyber Fraud type 4- Courier/package frauds

Read the attached FIRs to understand - fraudster will befriend on social media by sharing watsapp number for authenticity. These numbers are generally foreign numbers because watsapp phone calls can't be recorded.

6/16

12. First Information contents (प्रथम सूचना तथ्य):

To The S.H.O. cyber police station Respected sir, I am . Singh from house no 14 (Current Add) Permanent Add- House no 6 Dist-Azamgarh- 276204 U.P. Respected sir, A girl (Annabella more) has send me friend request on facebook after that she has given me her whatsapp number 447935373401 and she started chat with me after one weak I told her that I am going to my home town because my mother is not well after that she has send few gift and 30000 pound, after 2 day I received a call from (8796775460) this number and he told me that I have curiar in your name and you have to pay receiving amount 27999 Rs, and I have payed amount 27999 Rs. A/C no.-10502413000499 Benificiary Name- Mujahir Beg IFSC Code –ORBC0101050 IMPS ref no.- 005513801999 After that he called me and told me to pay 65000 more for your 30000 pound(which has sent by girl) after that he told me to pay and I have payed him 65000 in A/c no.- 0062000100391730 (43000 payed in this A/C no) Beneficiary Name – Sagar Mohammad zohir IFSC code PUNB0006200 PAN NO.- JBWPK3998F and (220000rs payed in this account- A/C no- 10502413000499 Benificiary Name – Mujahir Beg IFSC code-ORBC0101050 IMPS Reference no-005610868096 After that he told me that you gave to pay currency conversion amount to RBI 127999 Rs and I payed this amount in this account- 49000 in this A/ no 50100330733642 IFSC code HDFC0000043 PAN NO- JEIPK2855A IMPS ref No-005709883759 and I have payed 49000 in this A/C no 1387101068759 IFSC code CNRB0001387 PAN no-JEIPK2855A IMPS Ref Cod -005709891102 and I have payed 29999 Rs in this A/C no -50100339554102 IFSC code HDFC0005956 PAN No-CKIPA9475R IMPS Ref No-005710895099 after that he asked me to pay 379999 Rs income tax amount to pay RBI and I have payed him 140000 RS only in this A/C-0188000108716699 IFSC code-PUNB0018800 PAN No-GAJMJ9856A I have payed this amount by PNB ATM and I have payed him 40000 by PNB ATM and one Lakh by PNB ATM after that he told me to pay 179999 Rs but I have deney to pay because I do not have to pay they are using duplicate server name of RBI. So dear sir please help me to get back my money in my account

Cyber Fraud type 5 - Fake insurance policies or online purchase

Please see attached FIRs.

Don't buy an insurance/scheme/bitcoin etc. that is way below the normal rates and always check the email ID & website

twice for authenticity. Any official ID on gmail is MOSTLY FRAUD.

7/16

IFFCO Tokio General Insurance Company and its innocent customers.3. Some unknown persons impersonating themselves as representatives of IFFCO-TOKIO have been misrepresenting and inducing unsuspecting persons (both existing customers and customers showing interest in IFFCO Tokio) to part with their money by taking fictitious insurance policies and misappropriating the premium received by diverting the deposits into bank accounts not belonging to IFFCO-TOKIO. These imposters have created and used fake and forged email id "sales@iffcotokio.org.in", they have forged letterhead and logo of IFFCO-TOKIO to project authenticity they have redirected the request to their bank accounts and have received the amount from the customers in order to misappropriate the money, deceive and cheat the customers and the Company. After receiving the money they stopped responding to the calls of the innocent customers.
4.Modus operandi adopted by these imposters is that by falsely claiming themselves to be representatives of IFFCO-Tokio they have contacted existing customers for renewal of their policy at discounted rates. They also contacted some unsuspecting persons and induced them to buy insurance policies of IFFCO Tokio at discounted rates. Impersonators have used phone calls and whatsapp messages to contact and connect with the unsuspecting customers. Imposters have also shared fabricated quotations having logo and other details purported to be of IFFCO Tokio General Insurance Company Ltd. The fabricated quotations had account details, over which the customers made payments through different online payment options.. After receipt of payment into the fictitious accounts, customers' phone calls or whatsapp messages were not entertained. It is pertinent to mention here that

Cyber Fraud type 6 - Asking to install app for doing KYC, asking to deposit money for granting loan

Never install any app on anyone's suggestion - fraudster will be able to see all the activity done on mobile including password.

Visit branch for loans and check in-person.

8/16

सेवा में, SHO महोदय, Cyber Crime Police Station, Subject: Complaint against Fraudulent transfer of Money from my a/c° महोदय, मैं मुझे 19/ /2019, को SMS द्वारा सूचित किया गया कि PAYTM KI KYC अगर ना करवाई, तो मेरा PAYTM A/C बंद हो जाएगा। मैंने उसे फोन किया तो RAHUL नाम के लड़के ने 06291549974 से मुझसे बात करके एक app download करने को कहा। मैंने उसकी instructions follow करी एंव कोई OTP या password उसे नहीं दिया। फिर भी उसने मुझे Paytm App. Logout करवा के login करवाया एंव 10/ मेरे SBI CREDIT CARD NO- 4 1 डलवाए । इतनी ही देर में मेरे A/Cs से पैसे निकलने शुरू हो गए। मेरे SBI Credit Card no-437 91 से Rs 56,748/ एंव Rs 27000/ पे Snap deal पे कुछ खरीदा गया SBI के Saving A/C no-1('7 से कुल Rs 4,11,000/- निकल गए। Paytm से 1565/- निकल गए । मैंने यह सब 19/ /2019 को शाम 04:30 -05:15 बजे के बीच में हुआ है।

Cyber Fraud type 7- Identity Theft

This is most common & most emotionally traumatic for girls. Fraudsters take the pics from social media, use that to morph into pornography & then blackmail.

Lock your FB/Insta profiles; Add watermark or grey-out pics to use as profile pic

9/16

To, The Commissioner Of Poice, . Subject: Complain Regarding identity theft/Cyber Crime, Respected Sir, This is regarding a profile that was created on www.seeking .com with the name of in my name using my photographs. I have never created a profi9le on the website and in fact had no idea until I started receiving calls from random phone numbers. The caller have been enquiring if I stay in the society I am currently residing in (i.e. Apartments, Sector – , Gurgaon). The different callers have been asking inappropriate and explicit questions. Since, they have my phone numbers and address I am not feeling safe. A list of phone numbers that I've received call from has been enclosed. Along with the screenshot of the profile that was created in my name. Also, attached is the complain made to the website to bring down the profile.Yours sincerely,

If one finds misuse of their pics, they should complaint immediately nearby Cyber cell via both email & physical complaint.
Take screenshots.
Also report complaint on https://t.co/ScaXbENBZz

State-wise email IDs & phone numbers can be found on - https://t.co/kpwiHvxvD9

10/16

Cyber Fraud type 8 - Social networking business fraud

Fraudster will show the dreams to become rich quickly in the name of clicking ads, writing reviews, creating fake profiles for corporates/political parties on social media etc etc.

GREED = STUPIDITY = PAIN

11/16

मेरा न्यु सब्जी मंडी, में आढ़त का काम है। मुझे पेयवेय सोल्यूशंस कंपनी के बारे मे दोस्तो से पता लगा और उसके बाद मैं और मेरा दोस्त गाजियाबाद बी-233, पैसिफिक बिज़नस पार्क ,साहिबाबाद,गाजियाबाद,यू पी-201010 ऑफिस पर गए और ऑफिस मैं हमारी मुलाक़ात रिसिप्शन पर बैठी हुई मैडम से हुई और हमने उनसे इस कंपनी के बारे जानना चाहा,तो उन्होने हमे इस कम्पनी सीनियर अधिकारी,अमर गोयल से मिलवाया। अमर गोयल द्वारा हमे चंद दिनों मे अमीर बनने का सपना दिखाया गया। अमर गोयल ने यह भी विश्वास दिलाया कि कंपनी आपको रोजाना काम करने के पैसे आपके खाते मे ट्रान्सफर करेगी इन सभी बातों से उत्साहित होकर हमने यह जानना चाहा कि आखिर कंपनी क्या काम करवाती है और क्या यह काम करने से सरकारी कानून का ऊल्लघन तो नहीं होगा। तो यह सुनकर अमर गोयल ने हमे फिर से विश्वास दिलाया कि यह एक सरकारी मान्यता प्राप्त कंपनी है जो कि और बड़ी-बड़ी कम्पनियों के एड़वरटीजमेंट के लिए काम करती है और इस प्रकार अमर गोयल ने हमे इस कंपनी के बारे बताया व समझाया कि आपको प्रतिदिन चंद वैबसाइट पर सिर्फ क्लिक करने से 8 रु. प्रति क्लिक के हिसाब से एक साल तक दिया जाएगा जिसकी कीमत हमारी कंपनी आपसे मात्र एक लाख पन्द्रह हज्जार रूपए एक आइ.डी. कि होगी और जिसमे प्रतिदिन आप 250 क्लिक कर सकते है और आप को 365 दिनों तक प्रतिदिन 250 क्लिक मिलेंगे। इसी प्रकार अगर आप किसी अन्य व्यक्ति को इसमे शामिल करेंगे तो कंपनी आपको कुछ अन्य उपहार और बोनस भी देगी।. अमर गोयल की इन बातों मे आकर हमने pay way solutions कंपनी के खाते axis bank account no.916020062119755 IFSC code UTIB0000095 मे 3,45,000/-रूपए की आर.टी.जी.एस. मेरे पंजाब नेसनल बैक 4 8 से 2016 को किया और 2017 को 28,75,000/- रुपए की आर.टी.जी.एस उपरोक्त पीएनबी से करवाई और (.2017 को ही 3,45,000/- रुपए का आर.टी.जी.एस मेरे बुआ जी के लड़के ने केनरा बैंक, से करवाई और ये सारी पेमेंट करने के बाद कंपनी की तरफ से मुझे कोई रसीद नहीं मिली और मुझे 31 आइ.डी. दी गयी। यह कि मै .2016 से लगातार बताये गये अनुसार दिन रात 18 से 20 घंटे तक रोजाना काम करता रहा और उसके बाद कंपनी ने मुझे 6,56,200/- रुपये पांच अलग-अलग अकाउंट मे मुझे दिये और इसके बाद कभी काम आना बंद हुआ तो कभी पैसा आना बंद हुआ तो कभी साइट का चलना बंद हुआ और पूछने पर ये बताया कि कंपनी की साइट पर कुछ काम चल रहा है। आप क्लिक करते रहिए बकाया पैसा आपको जरूर मिलेगा। जैसे ही साइट ठीक होगी और इस प्रकार मैं रात को 12:00 बजे उठकर साइट पर रोजाना 18 से 20 घंटे तक कम करता रहा पर मुझे रोजाना काम करने का पैसा नहीं मिला और मेरे द्वारा दोबारा पूछने पर बताया गया कि कंपनी का ज्यादा ट्राजॅकसन होने की वजह से कंपनी अपना खाता और बैंको मे खुलवा रही है जिसके कारण मुझे इन सभी परेशानियों का सामना करना पड़ा,जो उन्होने मेरे किया हुआ काम का विवरण मेल करने को कहा और इस प्रकार दो महीने निकल चुके थे। इन सब बातों से मेरी मानसिक व शारीरिक हालत बहुत खराब हो चुकी थी। कुछ और ना सूझने पर मैं कंपनी के बताये गये कम्पनी के औफिस पर पहुचा तो औफिस मे कम्पनी के

Cyber Fraud type 9 - Honey Trap

Read the FIRs attached - thousands of such frauds happening on daily basis but seldom get reported due to guilt & fake morality.

MADEVER.COM गत 05/ /2018 को MADEVER.COM के साइट पर आनलाइन रजिस्टर किया जिसका REPLY मुझे MADEVER कम्पनी के कर्मचारी पूजा का फोन आया और उन्होने मुझे अपने कम्पनी के (आनलाई दोस्ती) के प्लान के हिसाब से मुझसे अपनी कम्पनी के पेटीएम मे रुपए 3700 अदा करने को कहा जोकि मैने किया उसके बाद उन्होने अपना whatsapp न0 पर पेटीएम का रसीद माँगा मैने दिया फिर उन्होने मेरे whatsapp पर दो लडकियो का फोटो भेजा और आनलाइन दोस्ती के लिए सेलेक्ट करने को कहा मैने किया उनका नाम शालिनी बताया और उनका मोबाइल नम्बर एंव whatsapp नम्बर दिया उसके बाद शालिनी ने मुझे शाम 5 बजे 06/ /2018 शनिवार को सदर अस्पताल के पास मिलने को कहा और उस दौरान उन्होने मुझसे रुपए 22500 का वाडी मसाज क्रीम के लिए पूजा से बात करने को कहा और सदर अस्पताल मिल कर वापस देने को कहा फिर मैने POOJA से बात किया फिर पूजा ने अपनी कम्पनी के हेड ब्रान्च का अकाउन्ट नम्बर और IFSC कोड दिया और रुपये डालने के बाद शालिनी का फोन आया कि मै सदर अस्पताल मे नही मिल सकती हू आप पूजा से बात करो फिर पूजा ने मुझे कहा कि उनके मम्मी पापा आ गए है वो आपसे वहाँ नही मिल सकती आप ऐसा करो कि होटल बुक करवा लो फिर उन्होने मुझसे रुपए 18600 अपने हेड ब्रान्च के अकाउन्ट मे डलवाया उस्के बाद उन लोगो ने अपना मोबाइल बन्द कर लिया और जब मैने उनसे दुसरे दिन बात किया तो उन्होने मुझे रुपए वापस देने का बादा किया जो कि आज तक नही दिया आपका प्रार्थी

Cyber Fraud type 10 - Online matrimony

Most gullible in such type of cases are girls especially widows/divorcees. Common modus operandi is good looks, to pose as rich NRI or a person with stable earnings

Few articles:

https://t.co/6eMvPJHvxO

https://t.co/6O7TLkrbkE

13/16

Few tips to avoid Online matrimony frauds:
a)cut-off communication as soon as they ask for money.
b)don't meet secretly
c)keep a third person in loop
d) ask for address & get that verified
e) do video chats, take screenshots and tell them about it - genuine ones will be ok

14/16

12. First Information contents (प्रथम सूचना तथ्य):

To, SHO Cyber Police Station, . Sir, I am here to register a complain against a person, Hasseen Chaudhary. Whom I met through Shaadi.com Regarding matrimony. Hasseen, approached me through Shaadi.com on 23rd of sep and then he texted me on whatsapp through his UK number 044-7588757631. After few discussion over whatsapp, we decided to meet and then on 14th October. This guy texted me asking money to fund his ticket. Hasseen is basically from UK, Leicester as mentioned in his profile and by him his a civil engineer 6 Y profession and he works for UNDPEN Allepo Syria on ahumantarian project. He said since his working in Syria, he do not hare access to his bank account. So he asked me to arrange his international tickets. I helped him with Rs one lac first on 16th Oct and 1.5 lac on 19th Oct. I transferred the amount in 4 different account. After sending the amount he insisted me to give more money i.e GBP 7000 which is amount 2.5 lac in Indian currency.

https://t.co/dmNZXoNTjD

There are many more ways a person can defraud using internet/phone. Most important aspect is to be vigil all the time, don't trust easily, don't share personal pics/videos easily and last but not the least - keep greed/lust under control.

15/16

Disclaimer:
1. All the FIR images uses in this thread are real and have been obtained from publicly available police portals.
2. Intent of this thread is not to malign or discredit anyone but to spread awareness.
3. Names & phone numbers of complainants have been removed.

16/16