गृह मंत्रालय
MINISTRY OF
**HOME AFFAIRS**

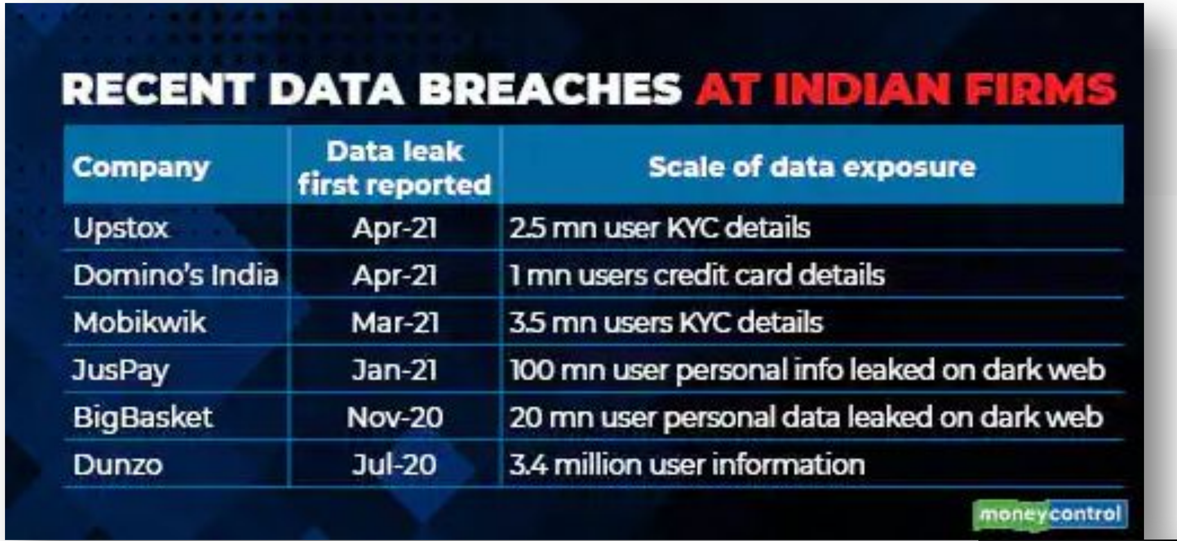
सत्यमेव जयते

## Cyber Jagrookta Diwas

# MALWARE PREVENTION

Indian Cyber Crime
Coordination Centre

07.10.2022

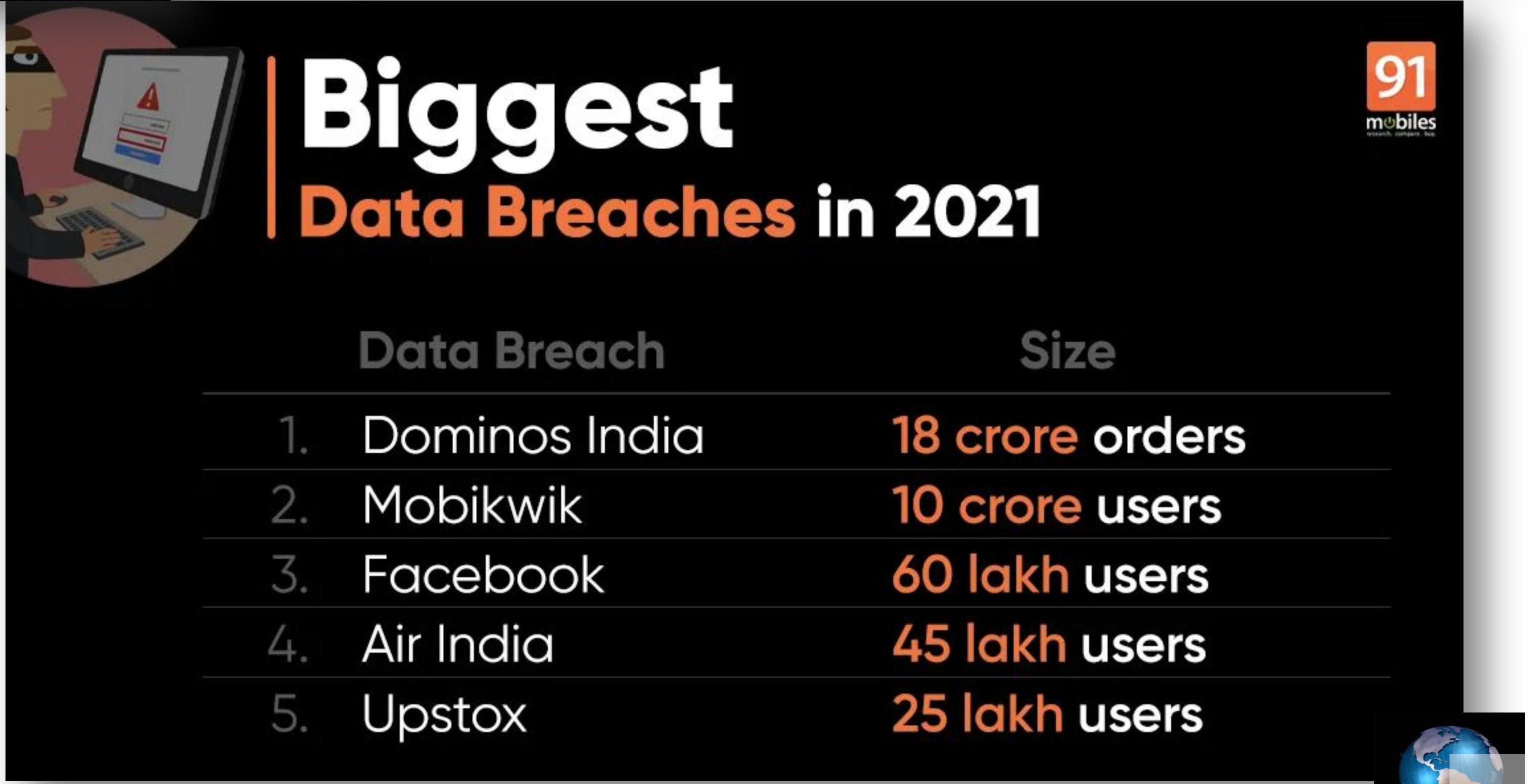


## RECENT DATA BREACHES AT INDIAN FIRMS

| Company | Data leak first reported | Scale of data exposure |
|---|---|---|
| Upstox | Apr-21 | 2.5 mn user KYC details |
| Domino's India | Apr-21 | 1 mn users credit card details |
| Mobikwik | Mar-21 | 3.5 mn users KYC details |
| JusPay | Jan-21 | 100 mn user personal info leaked on dark web |
| BigBasket | Nov-20 | 20 mn user personal data leaked on dark web |
| Dunzo | Jul-20 | 3.4 million user information |

moneycontrol

**APT harbingers** are using **Honey Traps** to attack Indian Defence.

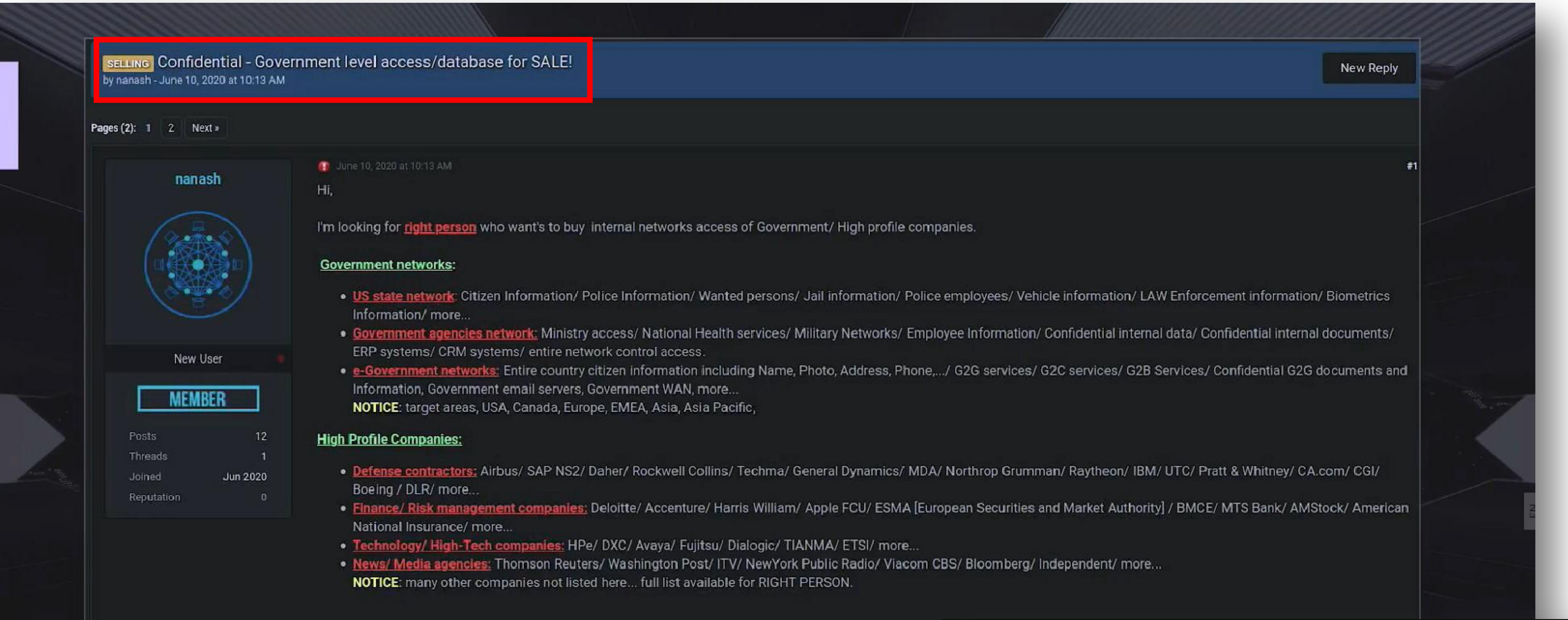


## Biggest Data Breaches in 2021

91 mobiles

| | Data Breach | Size |
|---|---|---|
| 1. | Dominos India | 18 crore orders |
| 2. | Mobikwik | 10 crore users |
| 3. | Facebook | 60 lakh users |
| 4. | Air India | 45 lakh users |
| 5. | Upstox | 25 lakh users |

# DATA BREACH ON DARKWEB



SELLING Confidential - Government level access/database for SALE!
by nanash - June 10, 2020 at 10:13 AM

nanash

New User

MEMBER

| | |
|---|---|
| Posts | 12 |
| Threads | 1 |
| Joined | Jun 2020 |
| Reputation | 0 |

June 10, 2020 at 10:13 AM #1

Hi,

I'm looking for right person who want's to buy internal networks access of Government/ High profile companies.

Government networks:

- US state network: Citizen Information/ Police Information/ Wanted persons/ Jail information/ Police employees/ Vehicle information/ LAW Enforcement information/ Biometrics Information/ more...
- Government agencies network: Ministry access/ National Health services/ Military Networks/ Employee Information/ Confidential internal data/ Confidential internal documents/ ERP systems/ CRM systems/ entire network control access.
- e-Government networks: Entire country citizen information including Name, Photo, Address, Phone,.../ G2G services/ G2C services/ G2B Services/ Confidential G2G documents and Information, Government email servers, Government WAN, more...
  **NOTICE**: target areas, USA, Canada, Europe, EMEA, Asia, Asia Pacific,

High Profile Companies:

- Defense contractors: Airbus/ SAP NS2/ Daher/ Rockwell Collins/ Techma/ General Dynamics/ MDA/ Northrop Grumman/ Raytheon/ IBM/ UTC/ Pratt & Whitney/ CA.com/ CGI/ Boeing / DLR/ more...
- Finance/ Risk management companies: Deloitte/ Accenture/ Harris William/ Apple FCU/ ESMA [European Securities and Market Authority] / BMCE/ MTS Bank/ AMStock/ American National Insurance/ more...
- Technology/ High-Tech companies: HPe/ DXC/ Avaya/ Fujitsu/ Dialogic/ TIANMA/ ETSI/ more...
- News/ Media agencies: Thomson Reuters/ Washington Post/ ITV/ NewYork Public Radio/ Viacom CBS/ Bloomberg/ Independent/ more...
  **NOTICE**: many other companies not listed here... full list available for RIGHT PERSON.

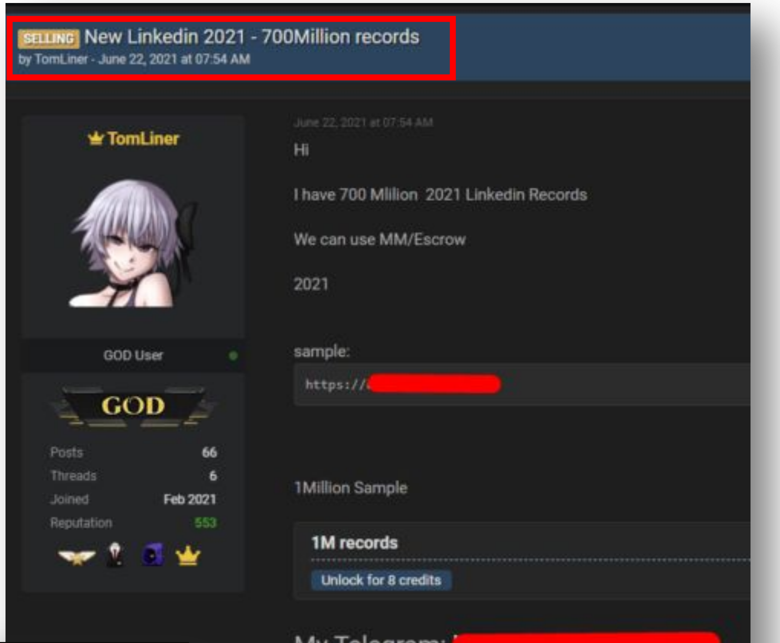
- All access sold only 1 time to 1 person. Full dedicated access, not shared. remove from list after sold eacl

- Many scenarios can be implemented on these networks such as State Sponsored APT, Ransomware, Data

- All access sold with Network design, Domain Admin privilege, All network device password, kdbx/keepass for lateral movements...

Contact:
**keybase:** l3ak
**xmpp:** l3ak@xmpp.jp

Government Database Sale



SELLING New Linkedin 2021 - 700Million records
by TomLiner - June 22, 2021 at 07:54 AM

TomLiner

GOD User

GOD

| | |
|---|---|
| Posts | 66 |
| Threads | 6 |
| Joined | Feb 2021 |
| Reputation | 553 |

June 22, 2021 at 07:54 AM

Hi

I have 700 Mllion 2021 Linkedin Records

We can use MM/Escrow

2021

sample:

```
https://[redacted]
```

1Million Sample

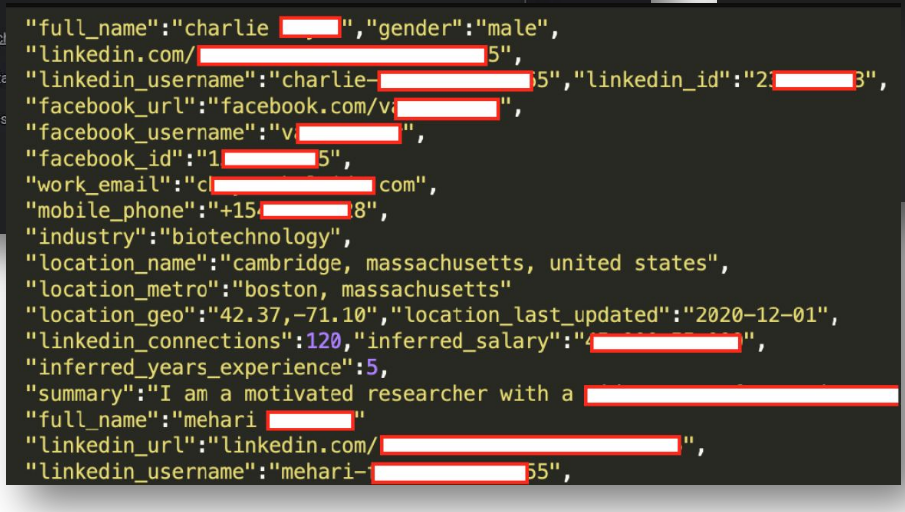
**1M records**

Unlock for 8 credits

My Telegram: [redacted]

My Telegram: @TomLiner

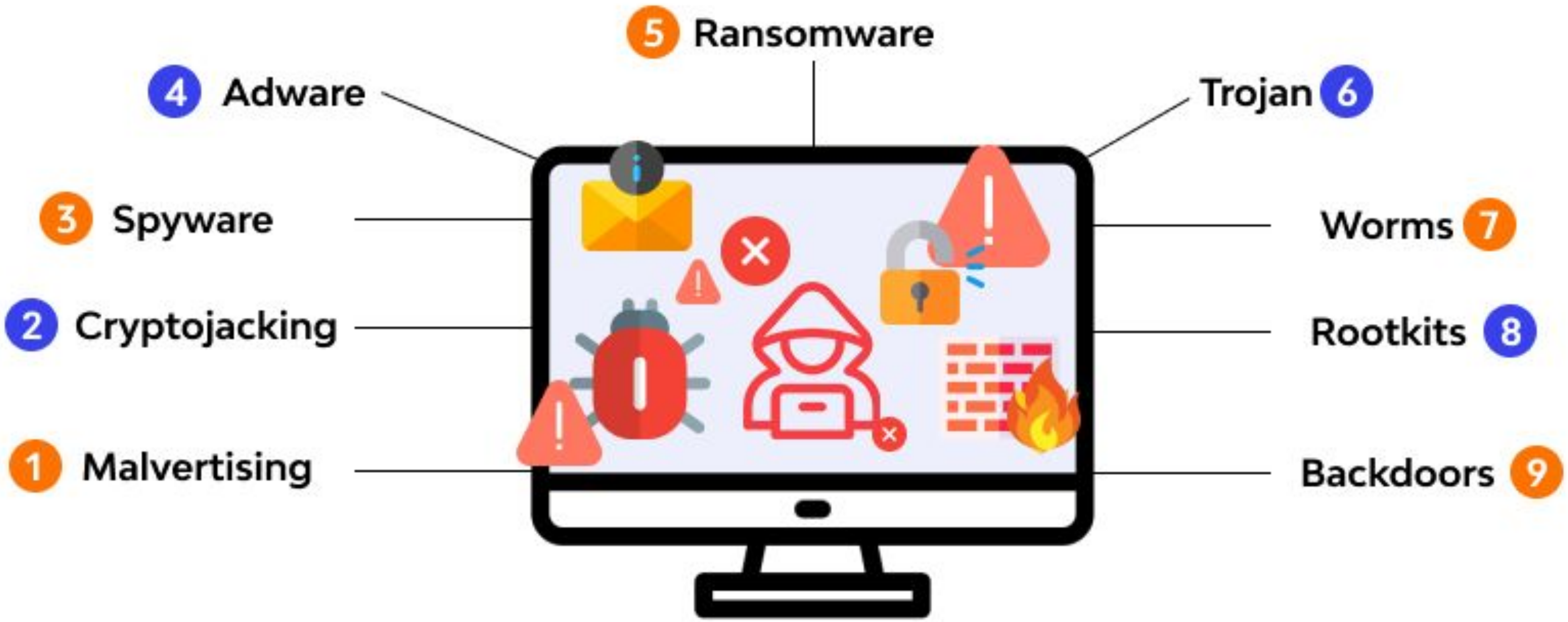
https://t[redacted]



```
"full_name":"charlie [redacted]","gender":"male",
"linkedin.com/[redacted]5",
"linkedin_username":"charlie-[redacted]5","linkedin_id":"2[redacted]3",
"facebook_url":"facebook.com/v[redacted]",
"facebook_username":"v[redacted]",
"facebook_id":"1[redacted]5",
"work_email":"c[redacted]com",
"mobile_phone":"+15[redacted]8",
"industry":"biotechnology",
"location_name":"cambridge, massachusetts, united states",
"location_metro":"boston, massachusetts",
"location_geo":"42.37,-71.10","location_last_updated":"2020-12-01",
"linkedin_connections":120,"inferred_salary":"[redacted]",
"inferred_years_experience":5,
"summary":"I am a motivated researcher with a [redacted]
"full_name":"mehari [redacted]"
"linkedin_url":"linkedin.com/[redacted]",
"linkedin_username":"mehari-[redacted]55",
```

LinkedIN DataLeak

# MALWARE



1 Malvertising

2 Cryptojacking

3 Spyware

4 Adware

5 Ransomware

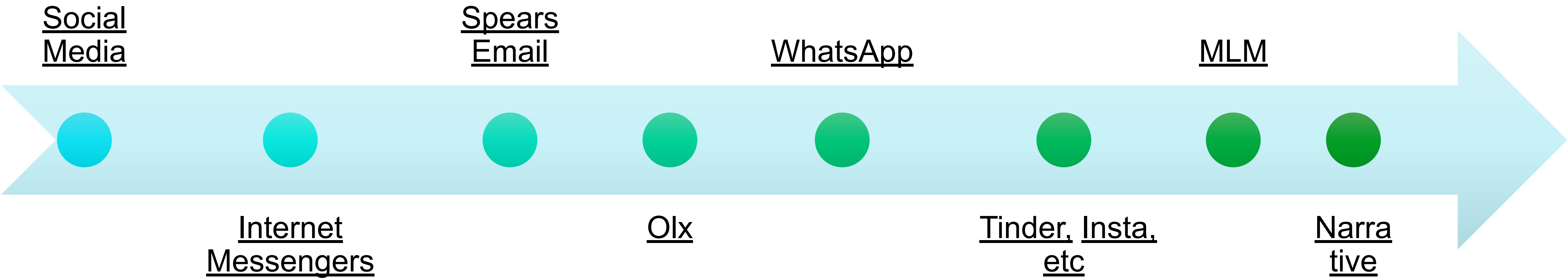
6 Trojan

7 Worms

8 Rootkits

9 Backdoors

# Attack Vectors and TTPs



Social Media

Internet Messengers

Spears Email

Olx

WhatsApp

Tinder, Insta, etc

MLM

Narra tive

# CYBER ATTACK: GOAL PROFILE & TARGETS

□ **Goals of Cyber Attack**

- Money
- Power
- Control
- Publicity
- Revenge
- Crackers
- Learning
- Strategic operation
- Embed Sleepers
- Espionage/Sabotage

□ **Attackers Profile**

- State/Nation Sponsored
- Hobbyist & Learners
- Activist & Enthusiasts
- Insiders
- Organized Gangs
- Ideological Criminals

□ **Targets & Motives**

- Corporate
  - ✓ Defacement, Takeover Control
  - ✓ Financial , Extortion, Revenge
  - ✓ Information, Data Theft
  - ✓ Reputation Damage
- Individual Personal
  - ✓ Yours and Family
  - ✓ Ransomware
  - ✓ Stalking, Blackmail, Scams
- Critical National Infrastructure
- Government & Political

# MALWARE ATTACKING METHODS IN SYSTEM

flaw in a system that can leave it open to attack.

attachments and payloads

advertisements

source or DarkWeb and using compromised account credentials as weapon

SMS, Internet messengers, Groups etc.

attacks etc.

HARDWARE

SOFTWARE

NETWORK DEVICES

WEB-SERVICES

PHYSICAL SITE

EMAIL

# Ones the malware can then cause any number of detrimental effects

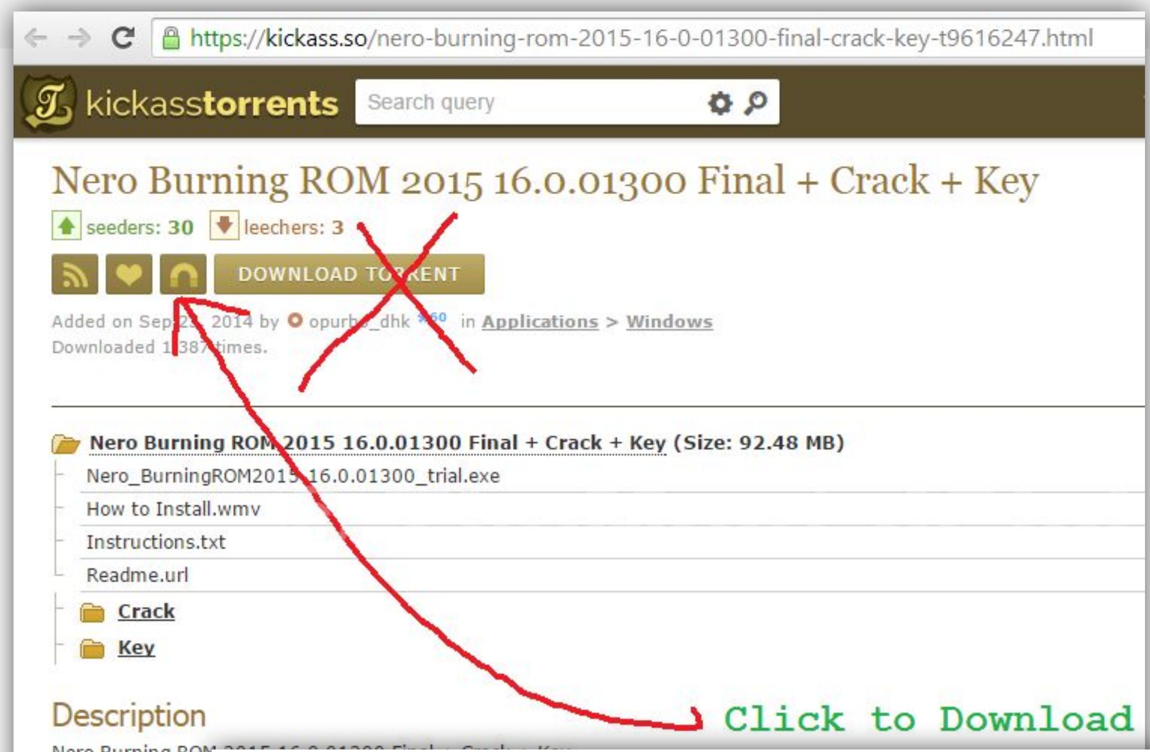
private accounts, services, etc.

services for unauthorized purposes

user's mobile device, accounts, etc.

on a mobile device, services, etc.

ways on a user's devices, services, etc.



https://kickass.so/nero-burning-rom-2015-16-0-01300-final-crack-key-t9616247.html

Nero Burning ROM 2015 16.0.01300 Final + Crack + Key

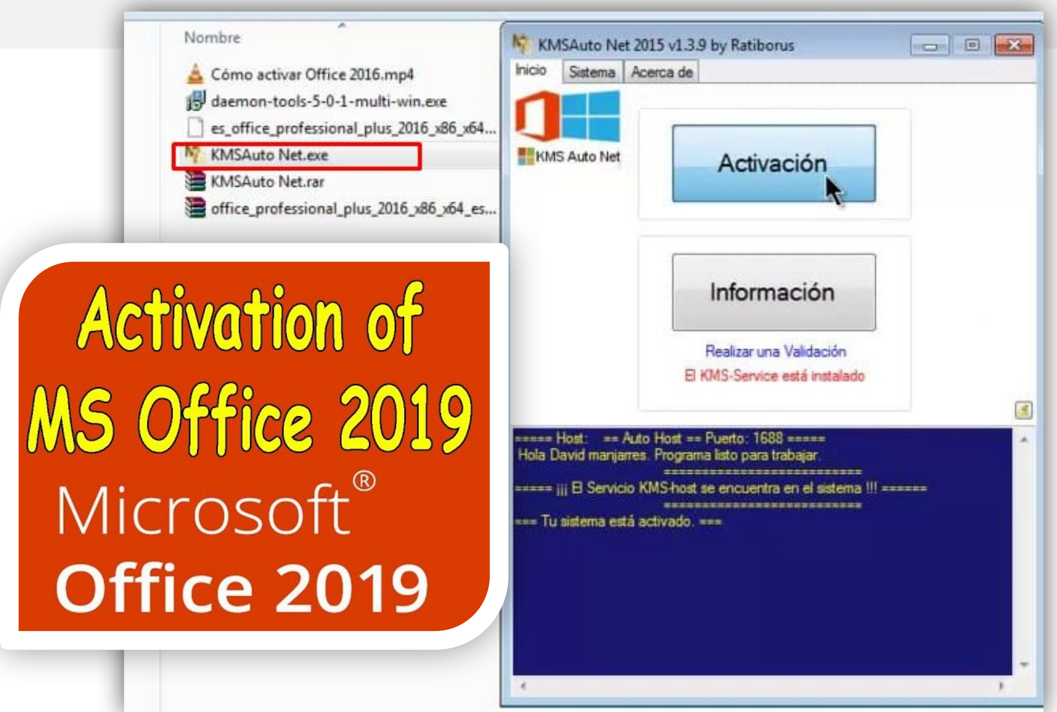
seeders: 30 leechers: 3

Added on Sep 25, 2014 by opurbo_dhk 60 in Applications > Windows
Downloaded 1 387 times.

Nero Burning ROM 2015 16.0.01300 Final + Crack + Key (Size: 92.48 MB)
- Nero_BurningROM2015 16.0.01300_trial.exe
- How to Install.wmv
- Instructions.txt
- Readme.url
- Crack
- Key

Description

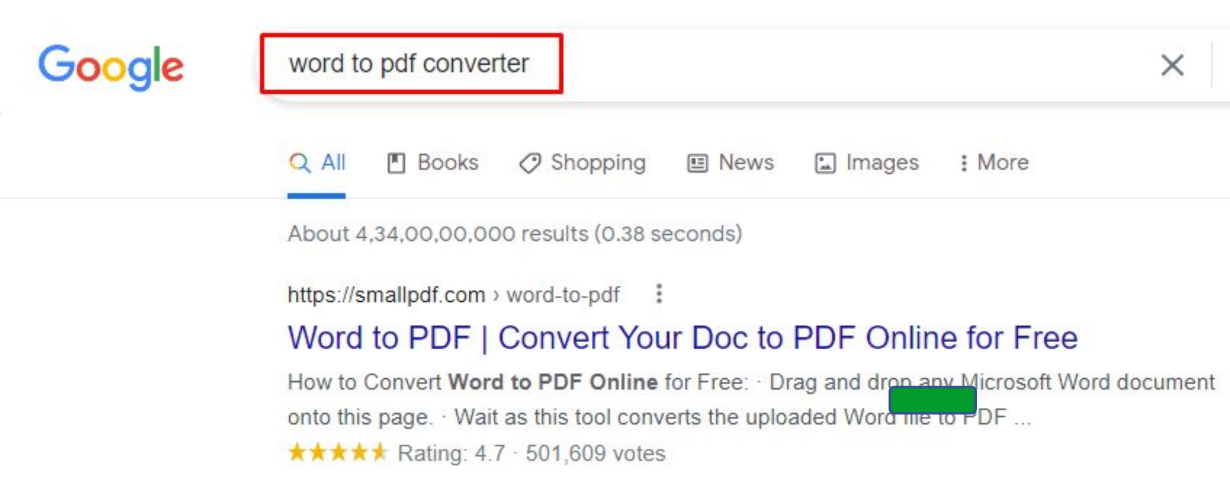
Nero Burning ROM 2015 16.0.01300 Final + Crack + Key



Nombre
- Cómo activar Office 2016.mp4
- daemon-tools-5-0-1-multi-win.exe
- es_office_professional_plus_2016_x86_x64...
- KMSAuto Net.exe
- KMSAuto Net.rar
- office_professional_plus_2016_x86_x64_es...

KMSAuto Net 2015 v1.3.9 by Ratiborus

```
===== Host:   == Auto Host == Puerto: 1688 =====
Hola David manjarres. Programa listo para trabajar.
             ===========================
===== ¡¡¡ El Servicio KMS-host se encuentra en el sistema !!! ======
             ===========================
=== Tu sistema está activado. ===
```



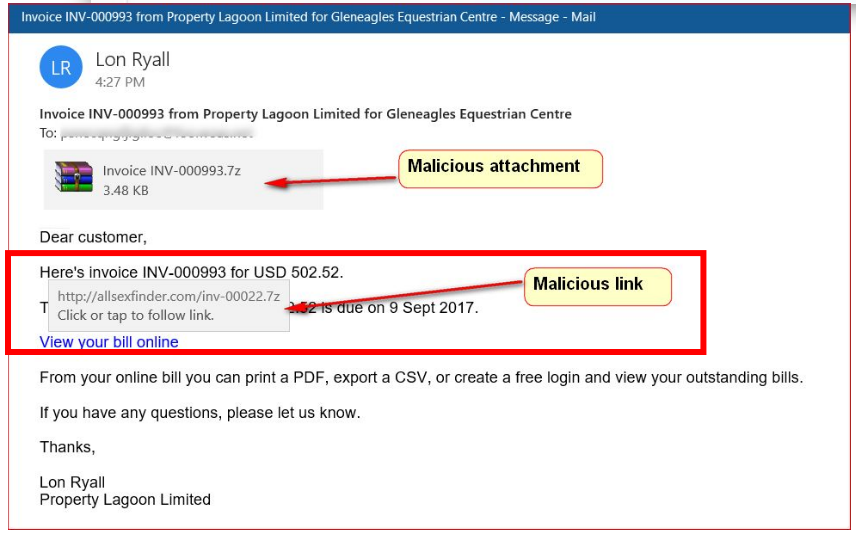
About 4,34,00,00,000 results (0.38 seconds)

https://smallpdf.com › word-to-pdf

Word to PDF | Convert Your Doc to PDF Online for Free

How to Convert **Word to PDF Online** for Free: · Drag and drop any Microsoft Word document onto this page. · Wait as this tool converts the uploaded Word file to PDF ...

★★★★★ Rating: 4.7 · 501,609 votes



Invoice INV-000993 from Property Lagoon Limited for Gleneagles Equestrian Centre - Message - Mail

Lon Ryall
4:27 PM

**Invoice INV-000993 from Property Lagoon Limited for Gleneagles Equestrian Centre**
To: [redacted]

Invoice INV-000993.7z
3.48 KB

Dear customer,

Here's invoice INV-000993 for USD 502.52.

T http://allsexfinder.com/inv-00022.7z
Click or tap to follow link. 52 is due on 9 Sept 2017.

View your bill online

From your online bill you can print a PDF, export a CSV, or create a free login and view your outstanding bills.

If you have any questions, please let us know.

Thanks,

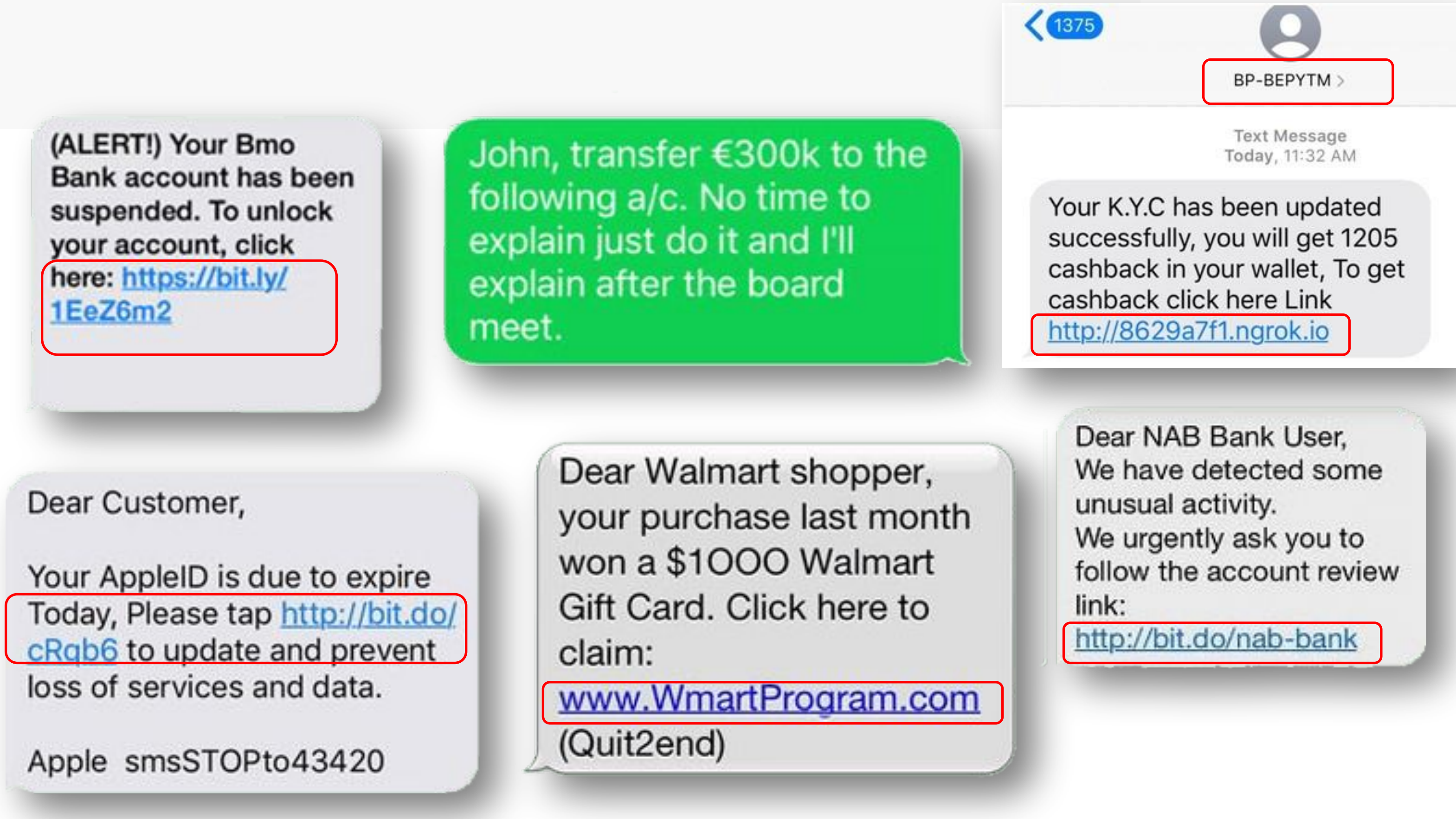
Lon Ryall
Property Lagoon Limited

# SMISHING

Term combines "SMS" (short message services, better known as texting) and "phishing."

A form of phishing that uses mobile phones medium as the attack platform.

Type of social engineering attack that relies on exploiting human trust rather than technical exploits.



(ALERT!) Your Bmo Bank account has been suspended. To unlock your account, click here: https://bit.ly/1EeZ6m2

John, transfer €300k to the following a/c. No time to explain just do it and I'll explain after the board meet.

Your K.Y.C has been updated successfully, you will get 1205 cashback in your wallet, To get cashback click here Link http://8629a7f1.ngrok.io

Dear Customer,

Your AppleID is due to expire Today, Please tap http://bit.do/cRqb6 to update and prevent loss of services and data.

Apple smsSTOPto43420

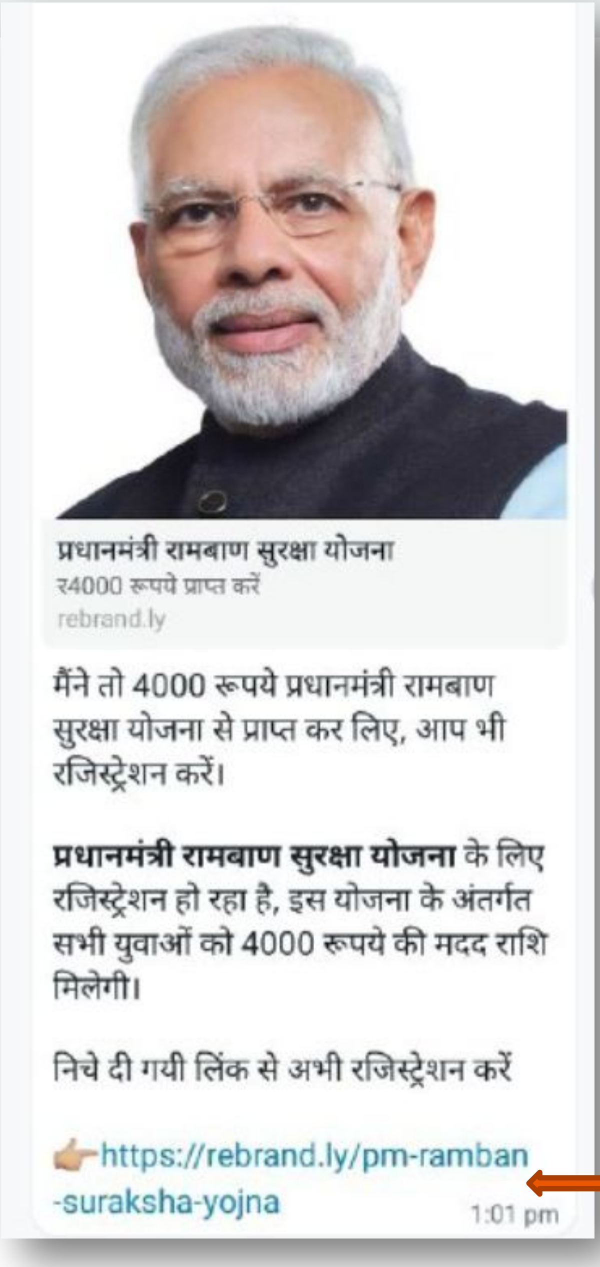
Dear Walmart shopper, your purchase last month won a $1OOO Walmart Gift Card. Click here to claim: www.WmartProgram.com (Quit2end)

Dear NAB Bank User,
We have detected some unusual activity.
We urgently ask you to follow the account review link: http://bit.do/nab-bank

*Some sample SMS contains suspicious URLS*

Smishing scams increasing by **more than 300%** within the past two years.

# SOME EXAMPLES SUSPICIOUS SMS and Messages



प्रधानमंत्री रामबाण सुरक्षा योजना
₹4000 रूपये प्राप्त करें
rebrand.ly

मैंने तो 4000 रूपये प्रधानमंत्री रामबाण सुरक्षा योजना से प्राप्त कर लिए, आप भी रजिस्ट्रेशन करें।

**प्रधानमंत्री रामबाण सुरक्षा योजना** के लिए रजिस्ट्रेशन हो रहा है, इस योजना के अंतर्गत सभी युवाओं को 4000 रूपये की मदद राशि मिलेगी।

निचे दी गयी लिंक से अभी रजिस्ट्रेशन करें

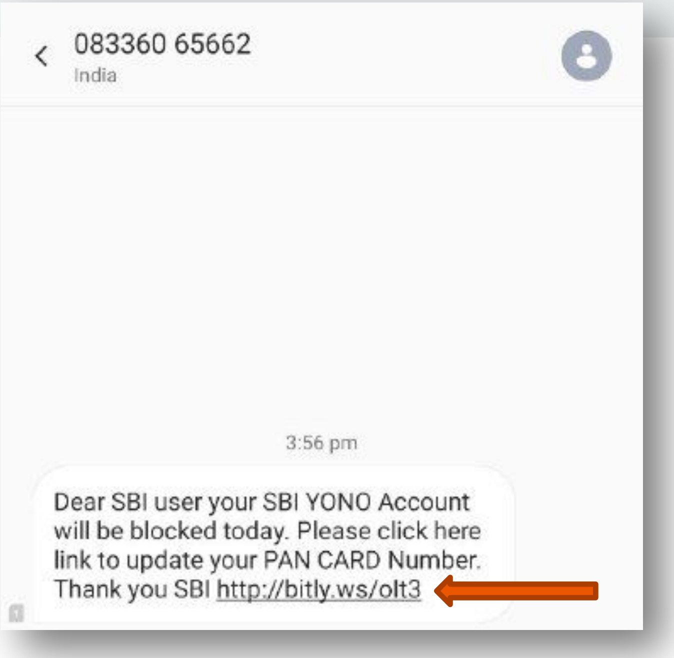
👉https://rebrand.ly/pm-ramban-suraksha-yojna

1:01 pm

→ Here the cyber criminal is using an image of our hon'ble PM so that user may think it's a legitimate link.

In this SMS the cyber criminal is creating a sense of urgency that the user's bank account will be blocked ←

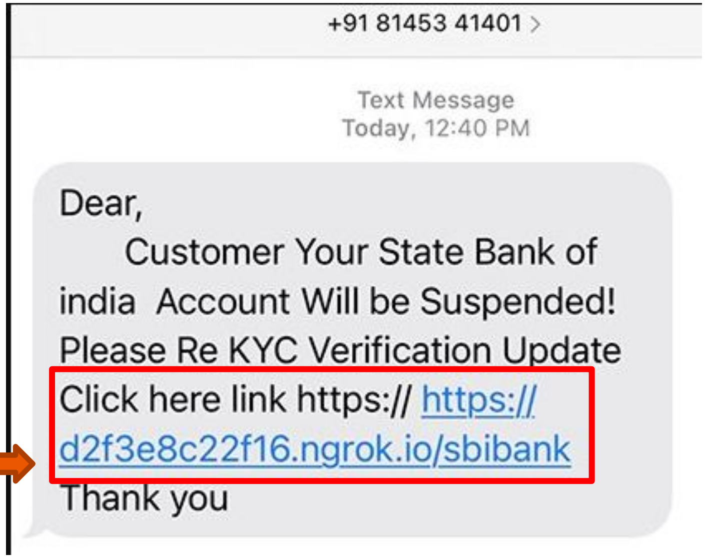
These links (bitly.ws, ngrok.io, rebrand.ly) as well many such URLS may contain some malicious websites, applications which becomes a medium for them to deploy a malware on your mobile devices



083360 65662
India

3:56 pm

Dear SBI user your SBI YONO Account will be blocked today. Please click here link to update your PAN CARD Number. Thank you SBI http://bitly.ws/olt3

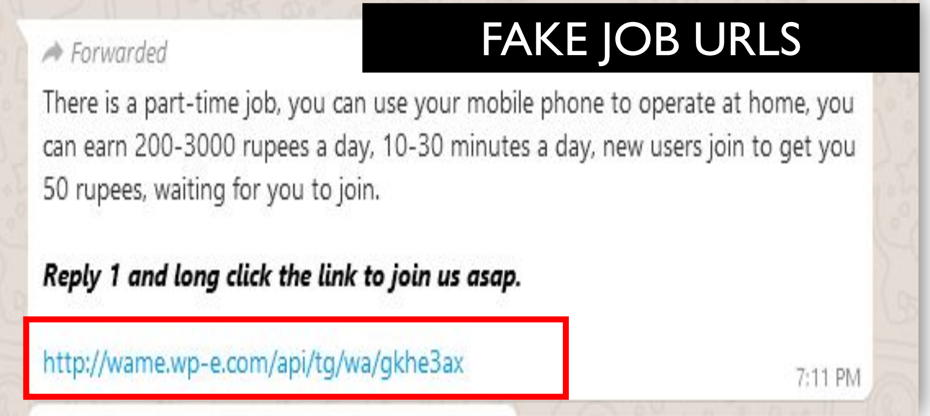


+91 81453 41401 >

Text Message
Today, 12:40 PM

Dear,
Customer Your State Bank of india Account Will be Suspended! Please Re KYC Verification Update Click here link https:// https://d2f3e8c22f16.ngrok.io/sbibank
Thank you

# SOME EXAMPLES



FAKE JOB URLS

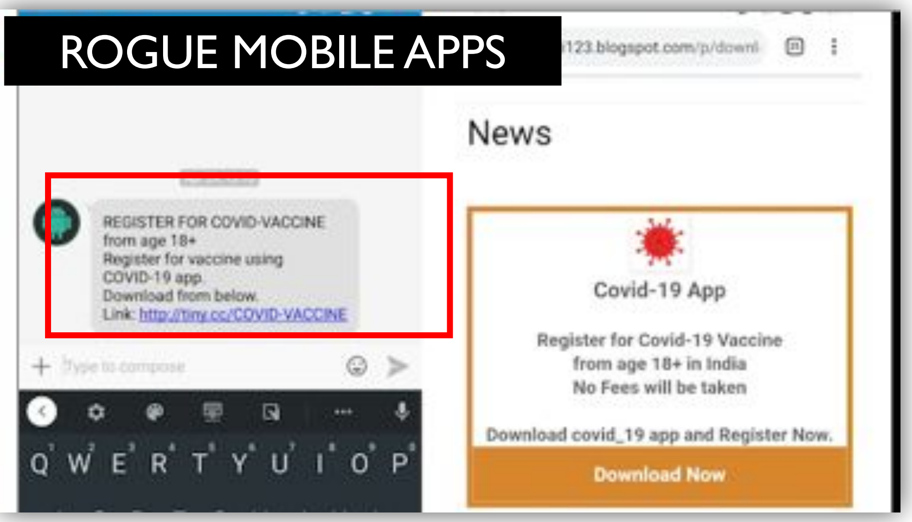
Forwarded

There is a part-time job, you can use your mobile phone to operate at home, you can earn 200-3000 rupees a day, 10-30 minutes a day, new users join to get you 50 rupees, waiting for you to join.

***Reply 1 and long click the link to join us asap.***

http://wame.wp-e.com/api/tg/wa/gkhe3ax

7:11 PM



ROGUE MOBILE APPS

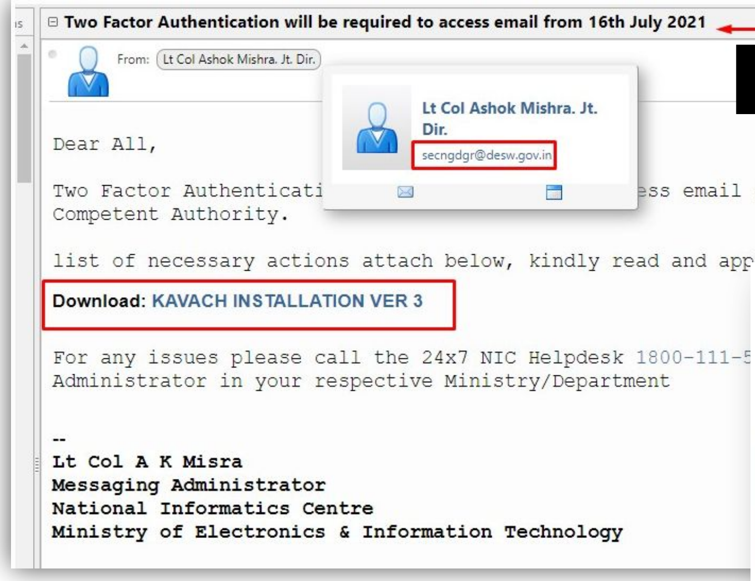
REGISTER FOR COVID-VACCINE
from age 18+
Register for vaccine using
COVID-19 app.
Download from below.
Link: http://tiny.cc/COVID-VACCINE

News

Covid-19 App

Register for Covid-19 Vaccine
from age 18+ in India
No Fees will be taken

Download covid_19 app and Register Now.



MALICIOUS MAIL

**Two Factor Authentication will be required to access email from 16th July 2021**

From: Lt Col Ashok Mishra. Jt. Dir.

Lt Col Ashok Mishra. Jt. Dir.
secngdgr@desw.gov.in

Dear All,

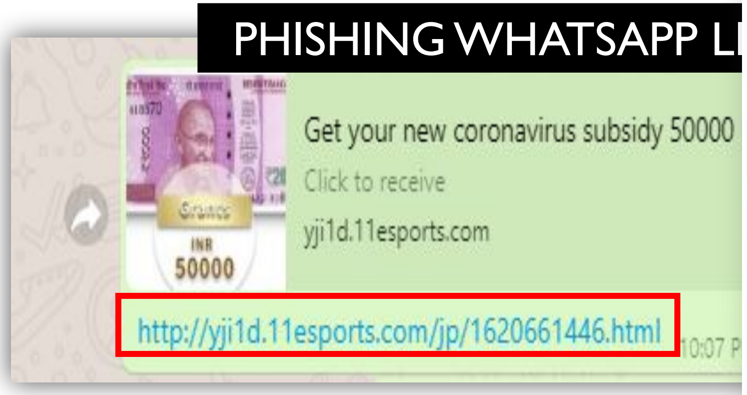
Two Factor Authenticati ess email from 16th July 2021 as per directive from
Competent Authority.

list of necessary actions attach below, kindly read and apply for continued use of eMail

**Download: KAVACH INSTALLATION VER 3**

For any issues please call the 24x7 NIC Helpdesk 1800-111-5
Administrator in your respective Ministry/Department

--
**Lt Col A K Misra**
**Messaging Administrator**
**National Informatics Centre**
**Ministry of Electronics & Information Technology**



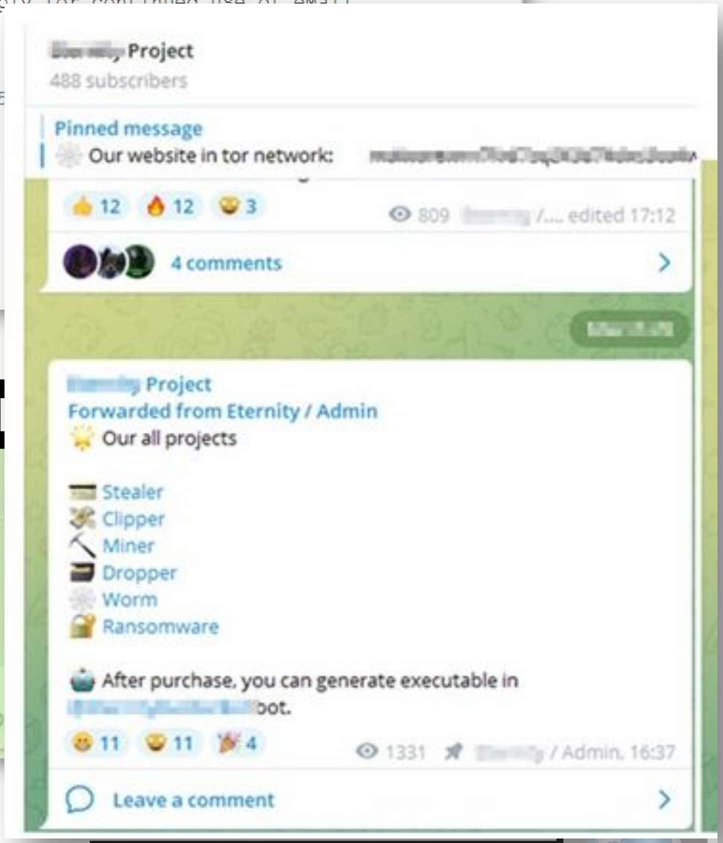
PHISHING WHATSAPP LI

Get your new coronavirus subsidy 50000

Click to receive

yji1d.11esports.com

http://yji1d.11esports.com/jp/1620661446.html



[redacted] Project
488 subscribers

Pinned message
Our website in tor network: [redacted]

👍 12 🔥 12 😁 3
809 [redacted] /... edited 17:12
4 comments

[redacted]

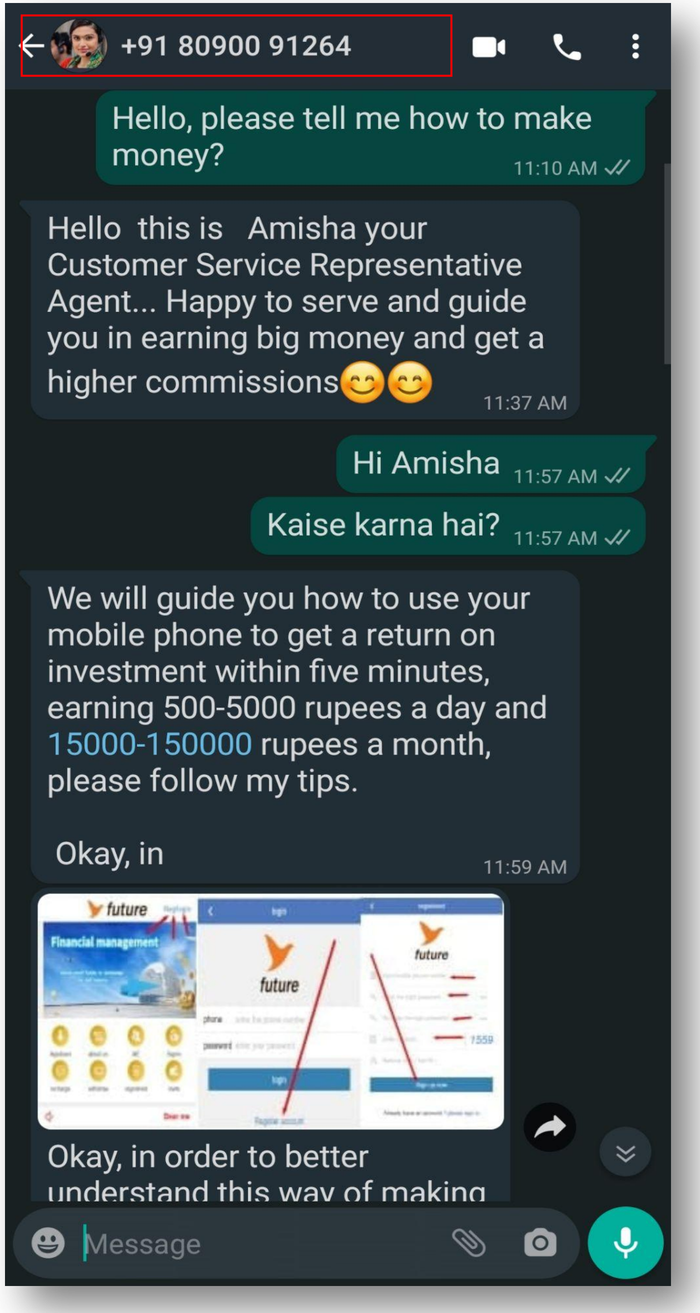
[redacted] Project
Forwarded from Eternity / Admin
🌟 Our all projects

Stealer
Clipper
Miner
Dropper
Worm
Ransomware

After purchase, you can generate executable in [redacted]bot.

😁 11 😁 11 🎉 4
1331 [redacted] / Admin, 16:37
Leave a comment

IM OFFERS



+91 80900 91264

Hello, please tell me how to make money? 11:10 AM

Hello this is Amisha your Customer Service Representative Agent... Happy to serve and guide you in earning big money and get a higher commissions😊😊 11:37 AM

Hi Amisha 11:57 AM

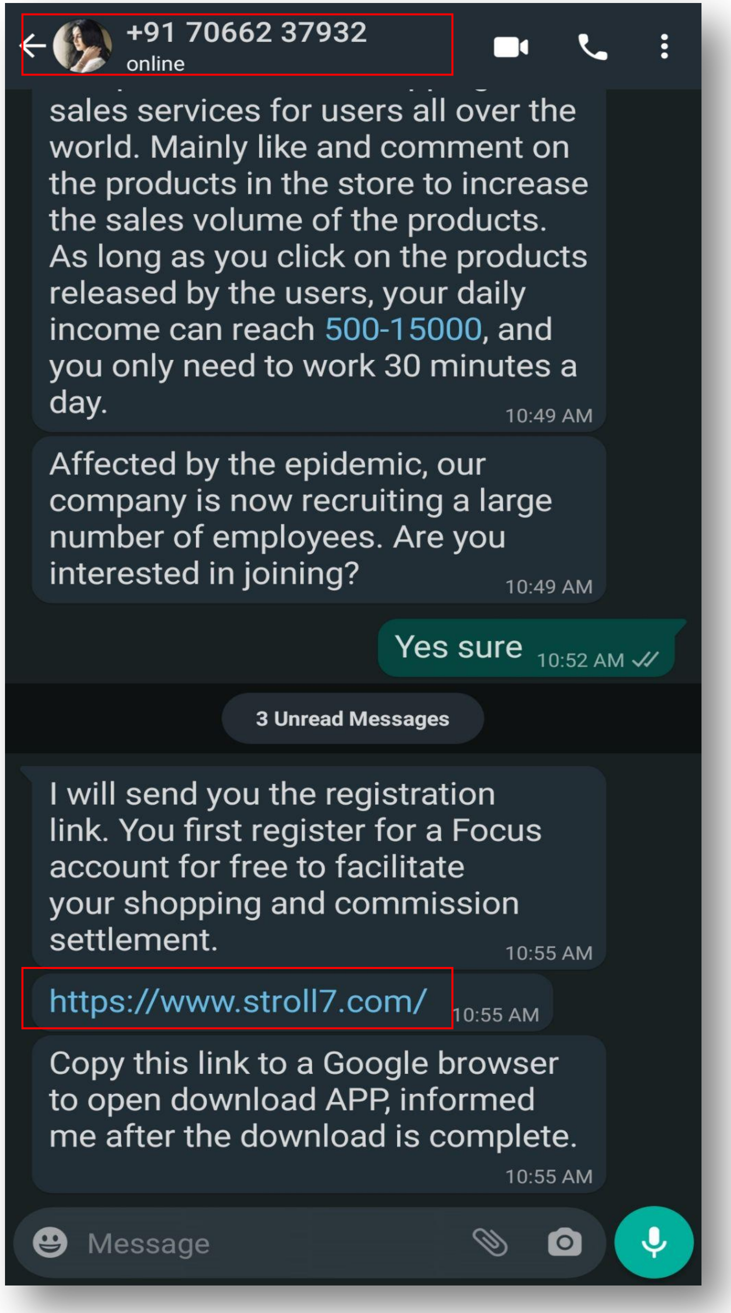
Kaise karna hai? 11:57 AM

We will guide you how to use your mobile phone to get a return on investment within five minutes, earning 500-5000 rupees a day and 15000-150000 rupees a month, please follow my tips.

Okay, in 11:59 AM

Okay, in order to better understand this way of making

Message



+91 70662 37932
online

sales services for users all over the world. Mainly like and comment on the products in the store to increase the sales volume of the products. As long as you click on the products released by the users, your daily income can reach 500-15000, and you only need to work 30 minutes a day. 10:49 AM

Affected by the epidemic, our company is now recruiting a large number of employees. Are you interested in joining? 10:49 AM

Yes sure 10:52 AM

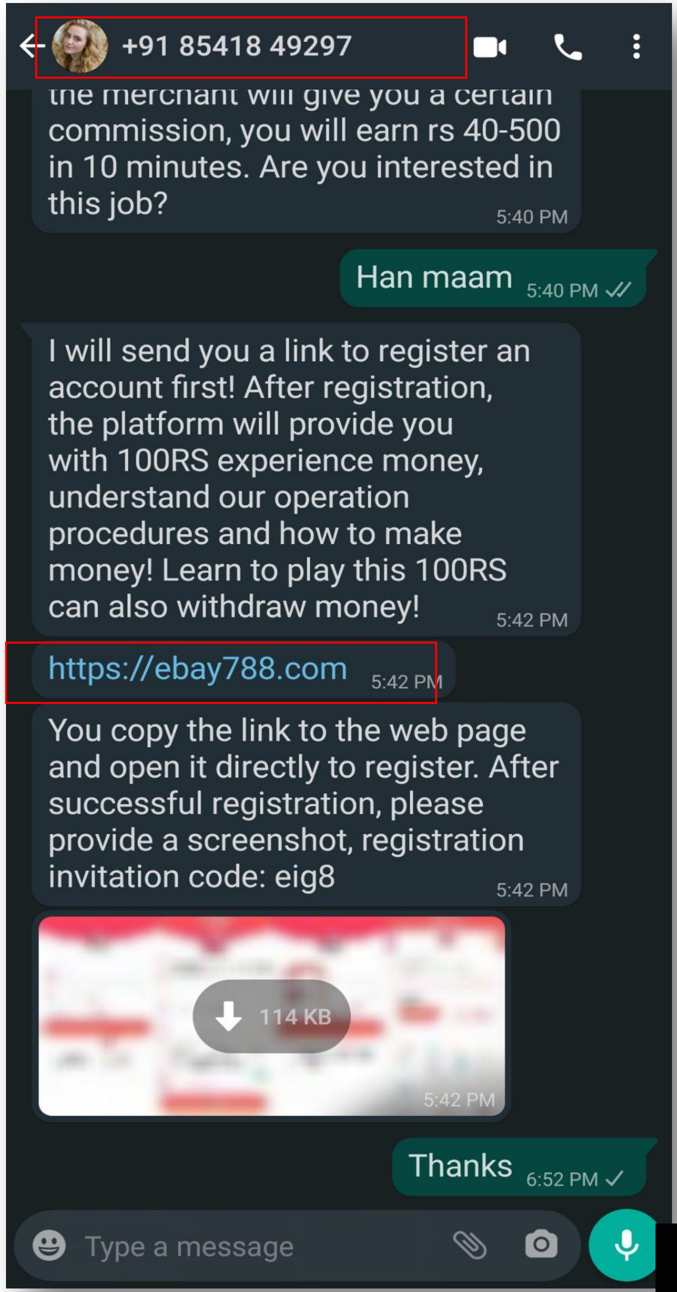
3 Unread Messages

I will send you the registration link. You first register for a Focus account for free to facilitate your shopping and commission settlement. 10:55 AM

https://www.stroll7.com/ 10:55 AM

Copy this link to a Google browser to open download APP, informed me after the download is complete. 10:55 AM

Message



+91 85418 49297

the merchant will give you a certain commission, you will earn rs 40-500 in 10 minutes. Are you interested in this job? 5:40 PM

Han maam 5:40 PM

I will send you a link to register an account first! After registration, the platform will provide you with 100RS experience money, understand our operation procedures and how to make money! Learn to play this 100RS can also withdraw money! 5:42 PM

https://ebay788.com 5:42 PM

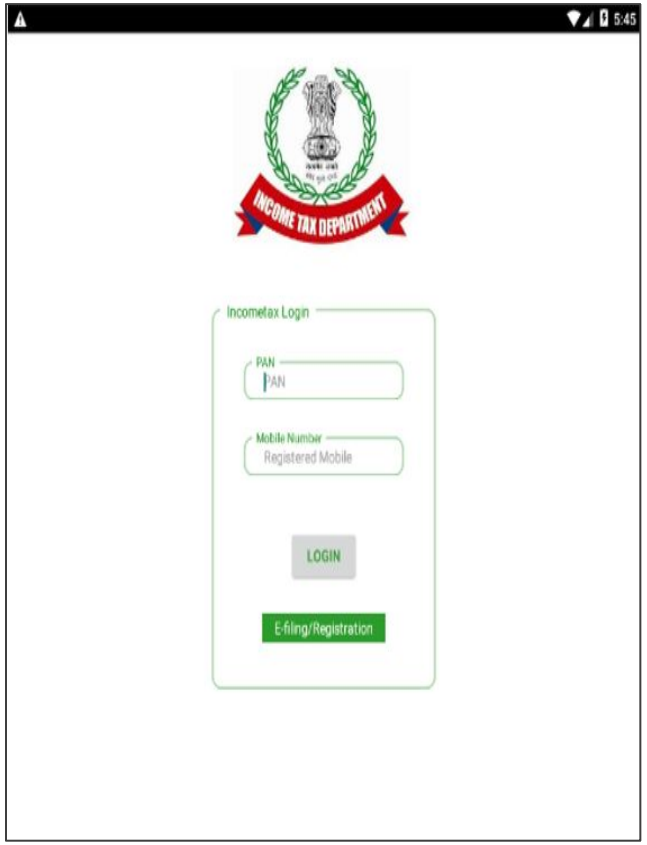
You copy the link to the web page and open it directly to register. After successful registration, please provide a screenshot, registration invitation code: eig8 5:42 PM

114 KB 5:42 PM

Thanks 6:52 PM

Type a message

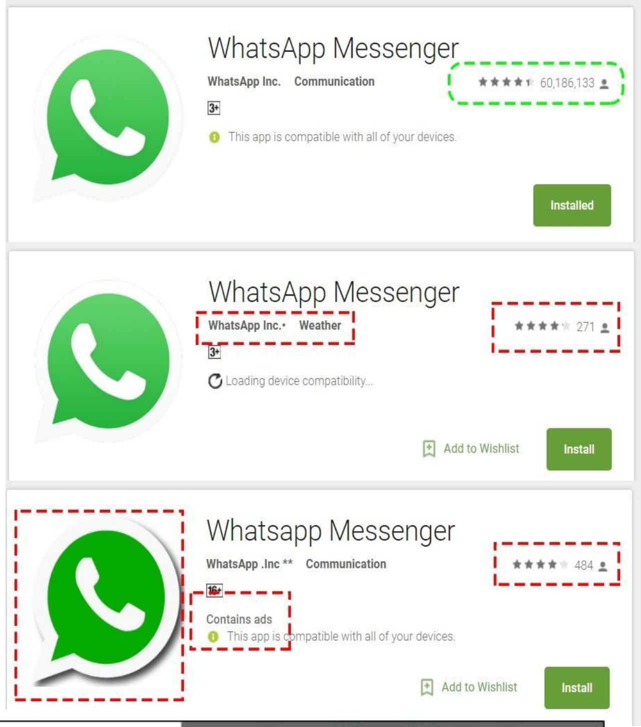
# FAKE APPS



Incometax Login

PAN: PAN

Mobile Number: Registered Mobile


WhatsApp Messenger

WhatsApp Inc. Communication ★★★★½ 60,186,133

3+

This app is compatible with all of your devices.

WhatsApp Messenger

WhatsApp Inc.• Weather ★★★★ 271

3+

Loading device compatibility...

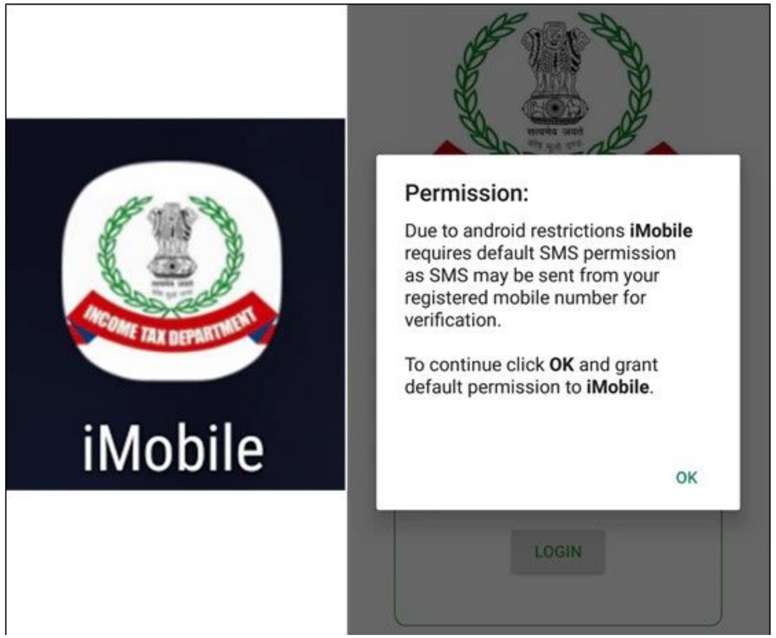
Whatsapp Messenger

WhatsApp .Inc ** Communication ★★★★ 484

16+

Contains ads

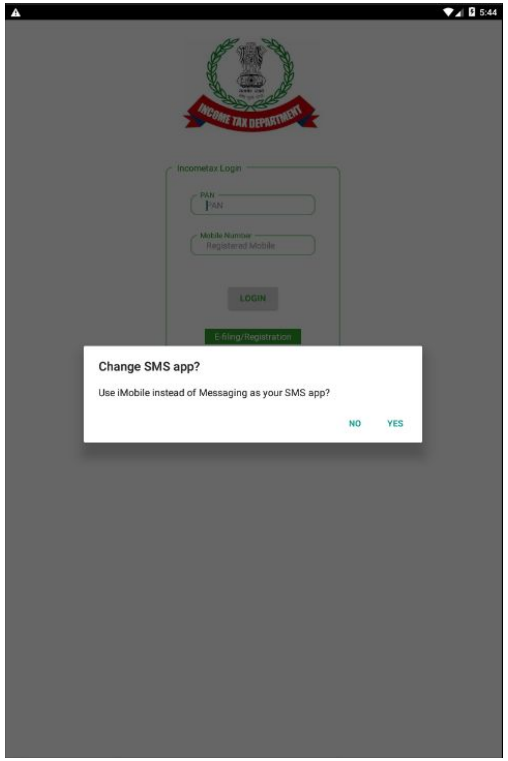
This app is compatible with all of your devices.



**Permission:**

Due to android restrictions **iMobile** requires default SMS permission as SMS may be sent from your registered mobile number for verification.

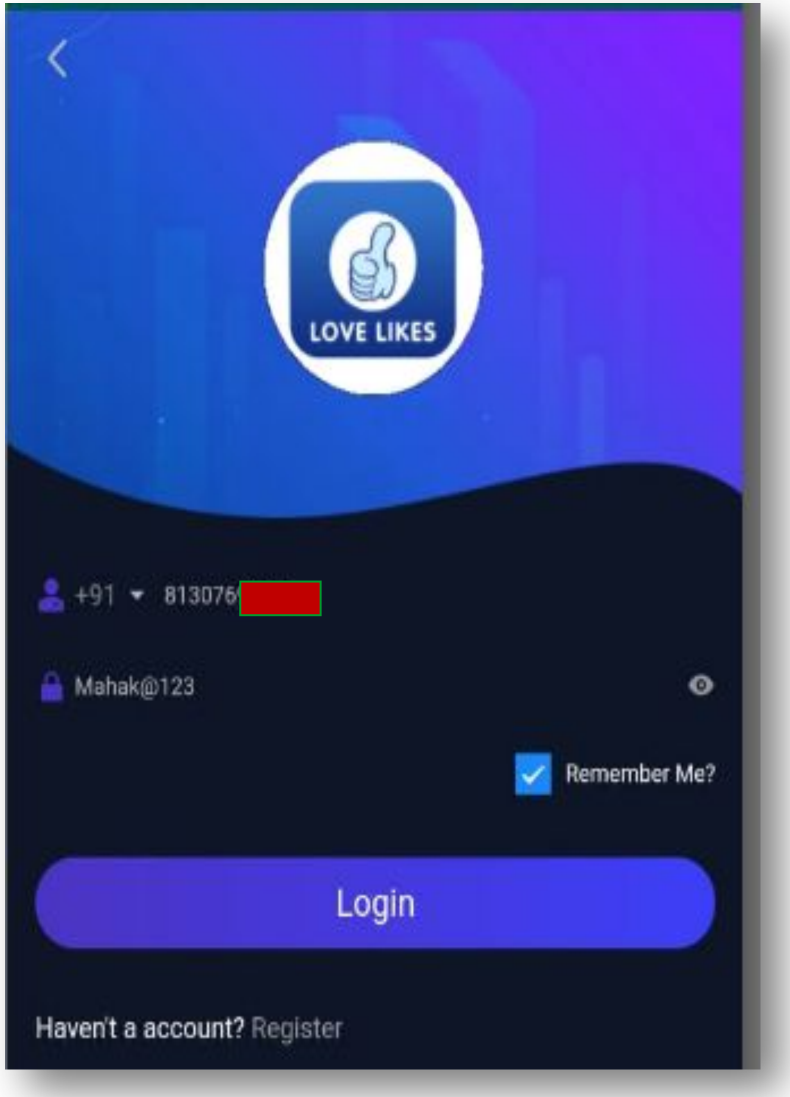
To continue click **OK** and grant default permission to **iMobile**.



**Change SMS app?**

Use iMobile instead of Messaging as your SMS app?

# SOME EXAMPLES



LOVE LIKES

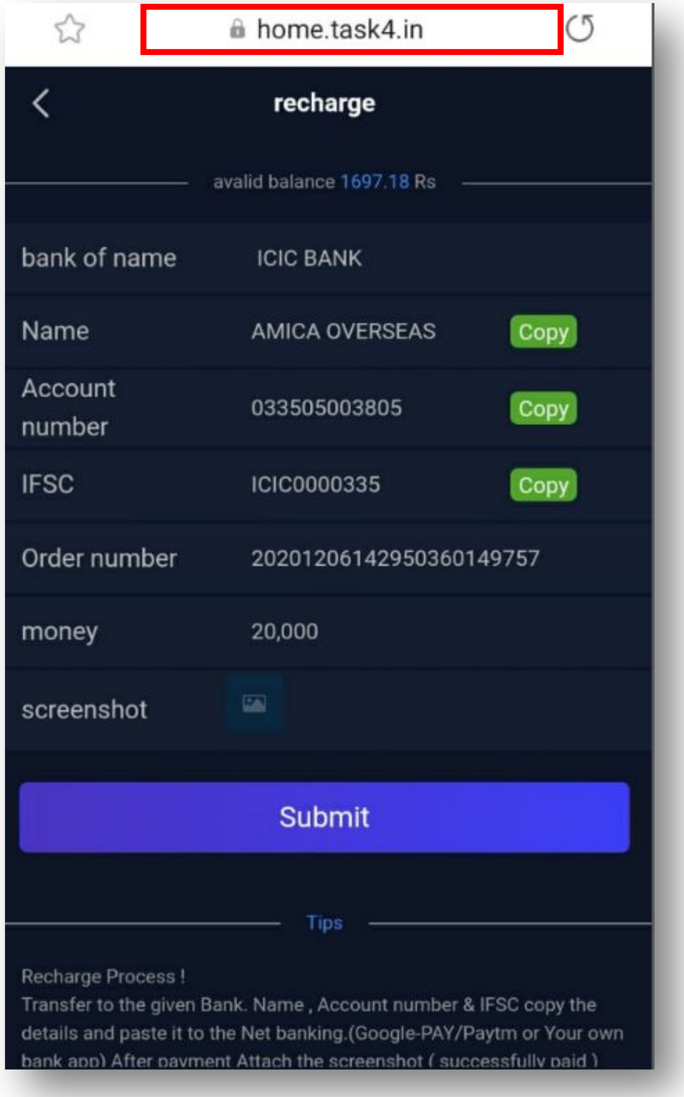
+91 ▾ 813076[redacted]

Mahak@123

☑ Remember Me?

Login

Haven't a account? Register



home.task4.in

recharge

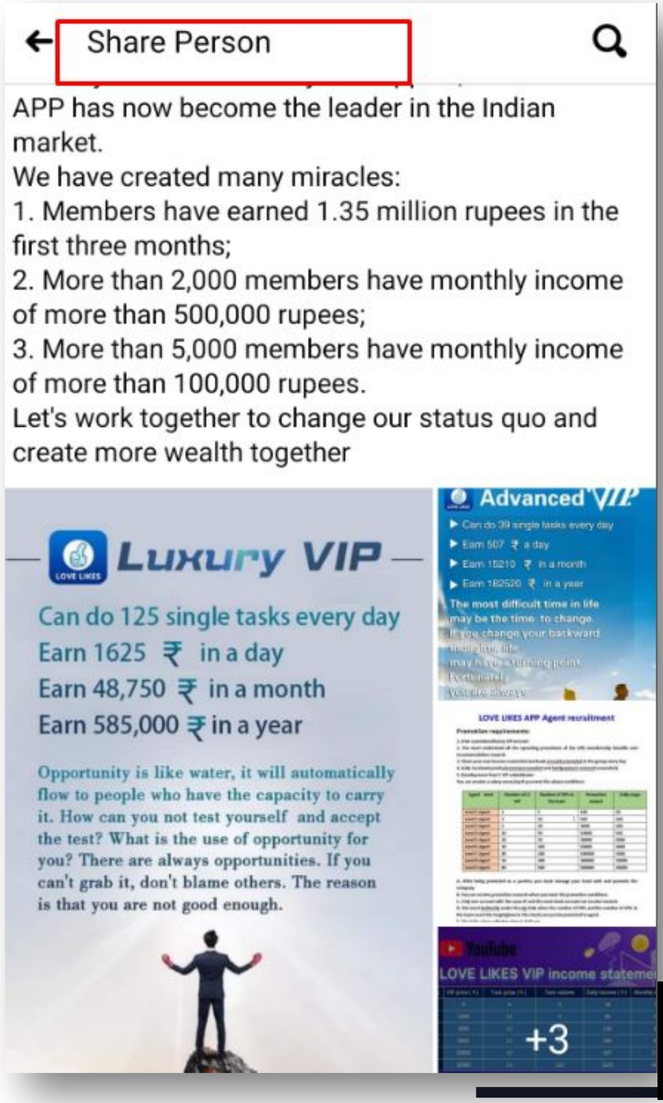
avalid balance 1697.18 Rs

| | | |
|---|---|---|
| bank of name | ICIC BANK | |
| Name | AMICA OVERSEAS | Copy |
| Account number | 033505003805 | Copy |
| IFSC | ICIC0000335 | Copy |
| Order number | 20201206142950360149757 | |
| money | 20,000 | |
| screenshot | | |

Submit

Tips

Recharge Process !
Transfer to the given Bank. Name , Account number & IFSC copy the details and paste it to the Net banking.(Google-PAY/Paytm or Your own bank app) After payment Attach the screenshot ( successfully paid )



Share Person

APP has now become the leader in the Indian market.
We have created many miracles:
1. Members have earned 1.35 million rupees in the first three months;
2. More than 2,000 members have monthly income of more than 500,000 rupees;
3. More than 5,000 members have monthly income of more than 100,000 rupees.
Let's work together to change our status quo and create more wealth together

Luxury VIP

Can do 125 single tasks every day
Earn 1625 ₹ in a day
Earn 48,750 ₹ in a month
Earn 585,000 ₹ in a year

Opportunity is like water, it will automatically flow to people who have the capacity to carry it. How can you not test yourself and accept the test? What is the use of opportunity for you? There are always opportunities. If you can't grab it, don't blame others. The reason is that you are not good enough.

Advanced VIP

- Can do 39 single tasks every day
- Earn 507 ₹ a day
- Earn 15210 ₹ in a month
- Earn 182520 ₹ in a year

The most difficult time in life may be the time to change. If you change your backward thinking, life may have a turning point. Fortunately, you are always

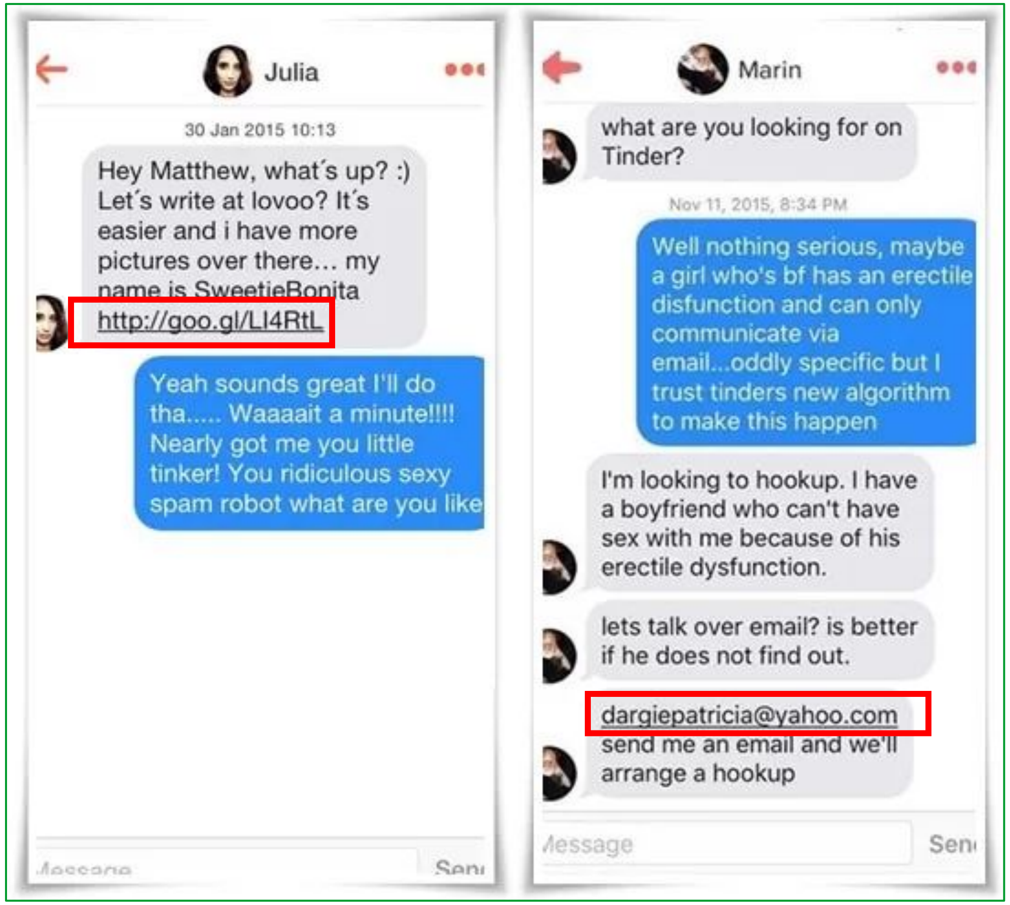
LOVE LIKES APP Agent recruitment

YouTube

LOVE LIKES VIP income stateme

+3

# CLASSIC BOT ATTACKS



Julia

30 Jan 2015 10:13

Hey Matthew, what´s up? :) Let´s write at lovoo? It´s easier and i have more pictures over there… my name is SweetieBonita http://goo.gl/LI4RtL

Yeah sounds great I'll do tha….. Waaaait a minute!!!! Nearly got me you little tinker! You ridiculous sexy spam robot what are you like

Message Send

Marin

what are you looking for on Tinder?

Nov 11, 2015, 8:34 PM

Well nothing serious, maybe a girl who's bf has an erectile disfunction and can only communicate via email...oddly specific but I trust tinders new algorithm to make this happen

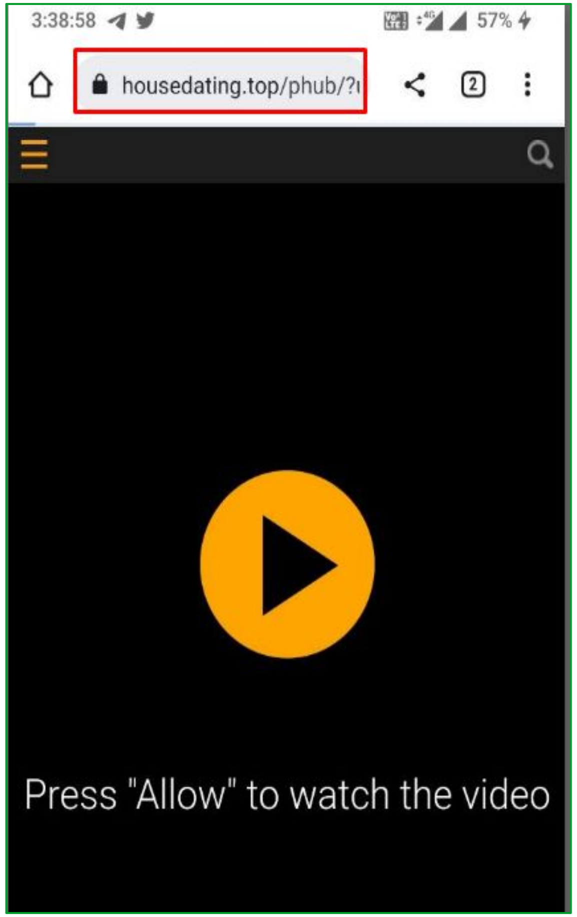
I'm looking to hookup. I have a boyfriend who can't have sex with me because of his erectile dysfunction.

lets talk over email? is better if he does not find out.

dargiepatricia@yahoo.com send me an email and we'll arrange a hookup

Message Send

Shortening URL

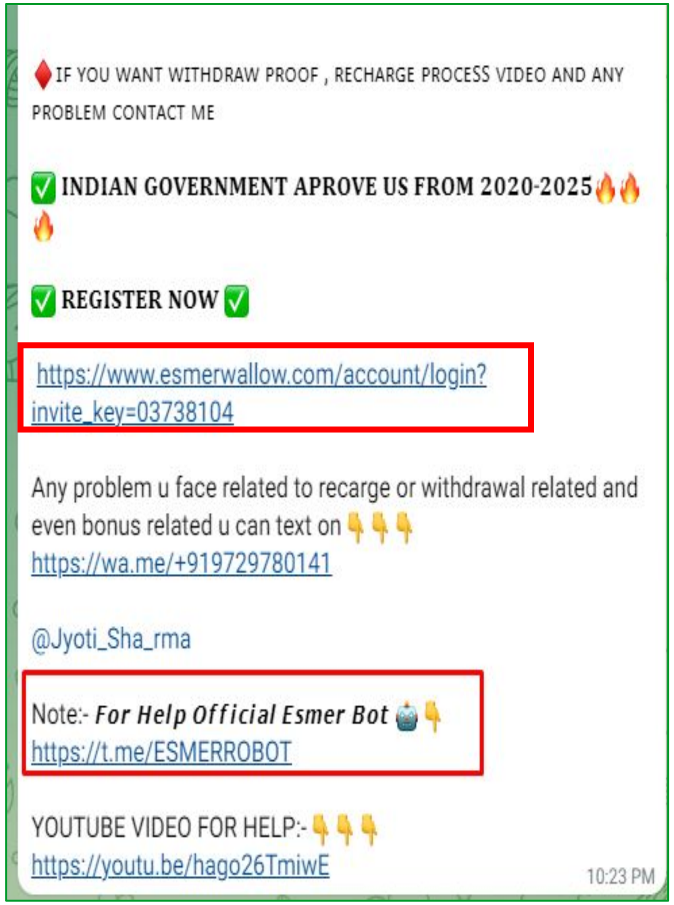


3:38:58 57%

housedating.top/phub/?

Press "Allow" to watch the video

Malicious Drive by Downloads



♦IF YOU WANT WITHDRAW PROOF , RECHARGE PROCESS VIDEO AND ANY PROBLEM CONTACT ME

✅ INDIAN GOVERNMENT APROVE US FROM 2020-2025🔥🔥🔥

✅ REGISTER NOW ✅

https://www.esmerwallow.com/account/login?invite_key=03738104

Any problem u face related to recarge or withdrawal related and even bonus related u can text on 👇👇👇
https://wa.me/+919729780141

@Jyoti_Sha_rma

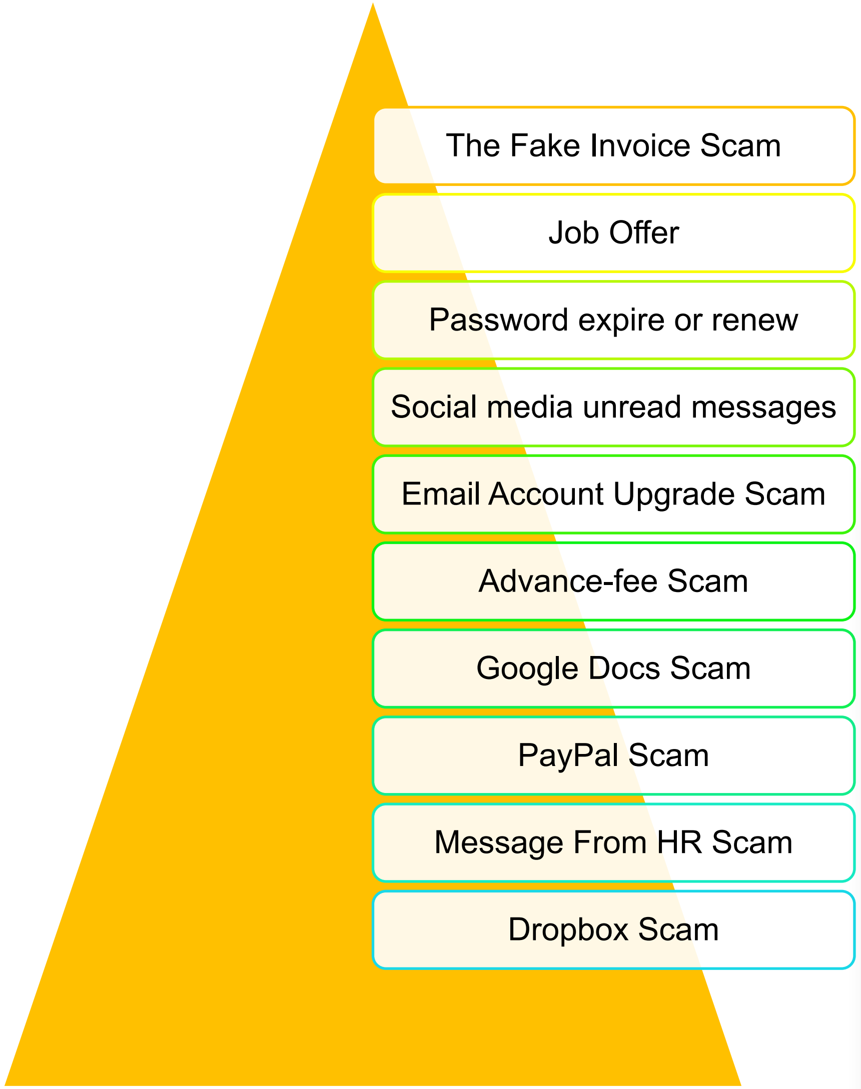
Note:- *For Help Official Esmer Bot* 🤖👇
https://t.me/ESMERROBOT

YOUTUBE VIDEO FOR HELP:- 👇👇👇
https://youtu.be/hago26TmiwE

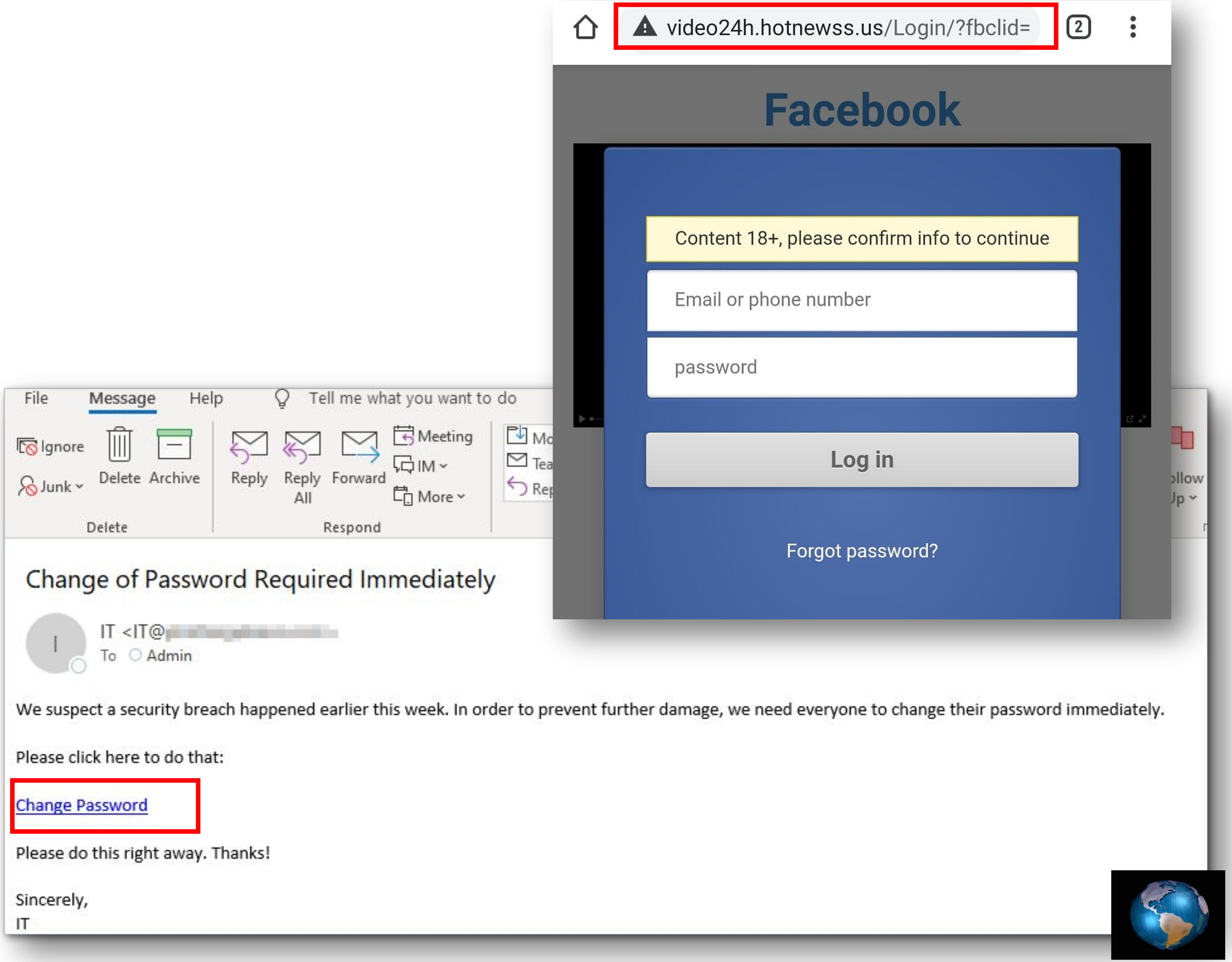
10:23 PM

BoT Support

# PHISHING



- The Fake Invoice Scam
- Job Offer
- Password expire or renew
- Social media unread messages
- Email Account Upgrade Scam
- Advance-fee Scam
- Google Docs Scam
- PayPal Scam
- Message From HR Scam
- Dropbox Scam



Content 18+, please confirm info to continue

Email or phone number

password

## Change of Password Required Immediately

IT <IT@[redacted]

To ○ Admin

We suspect a security breach happened earlier this week. In order to prevent further damage, we need everyone to change their password immediately.

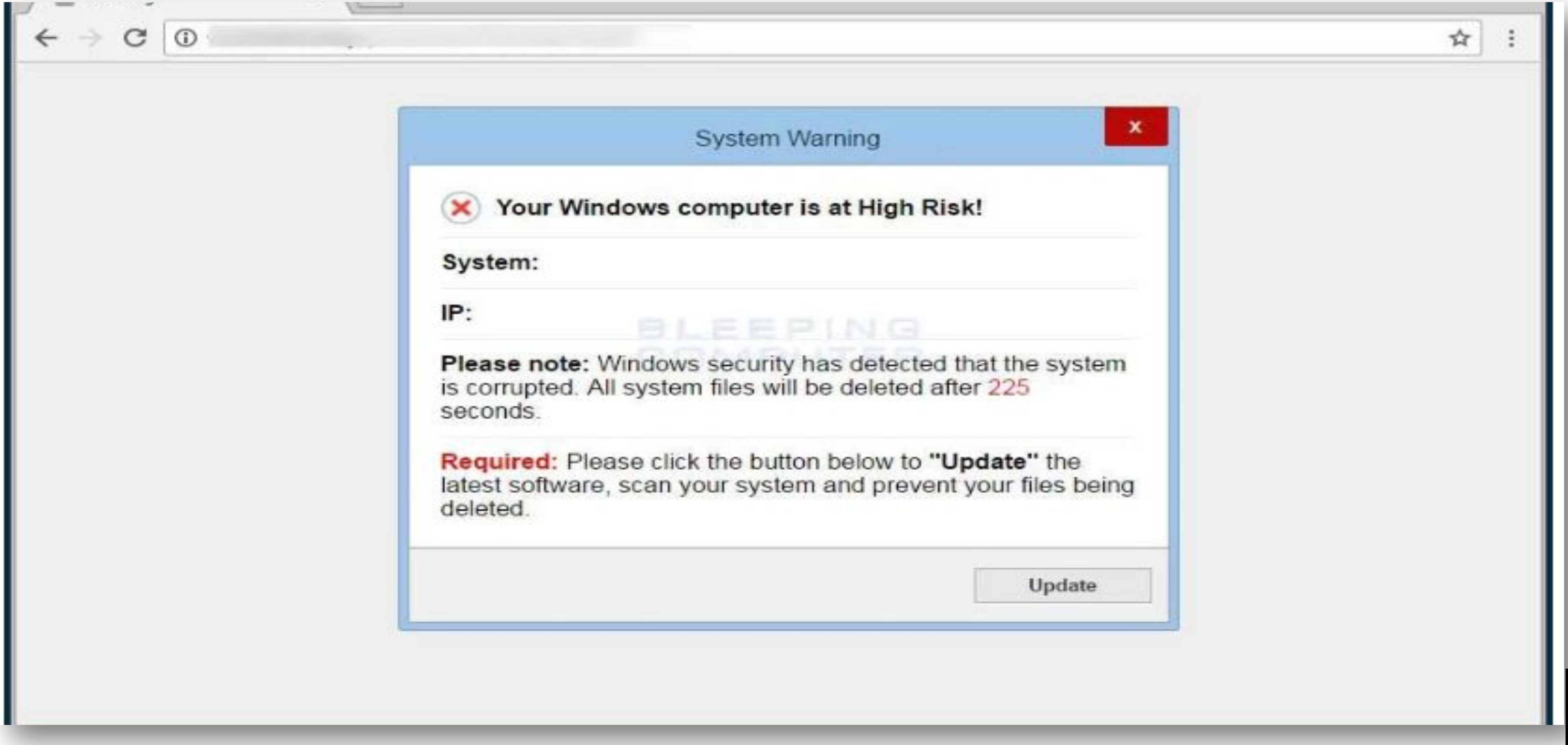
Please click here to do that:

Change Password

Please do this right away. Thanks!

Sincerely,
IT

# RISK OF POP-UPS – MALWARE/SPYWARE INSTALLATION



System Warning

Your Windows computer is at High Risk!

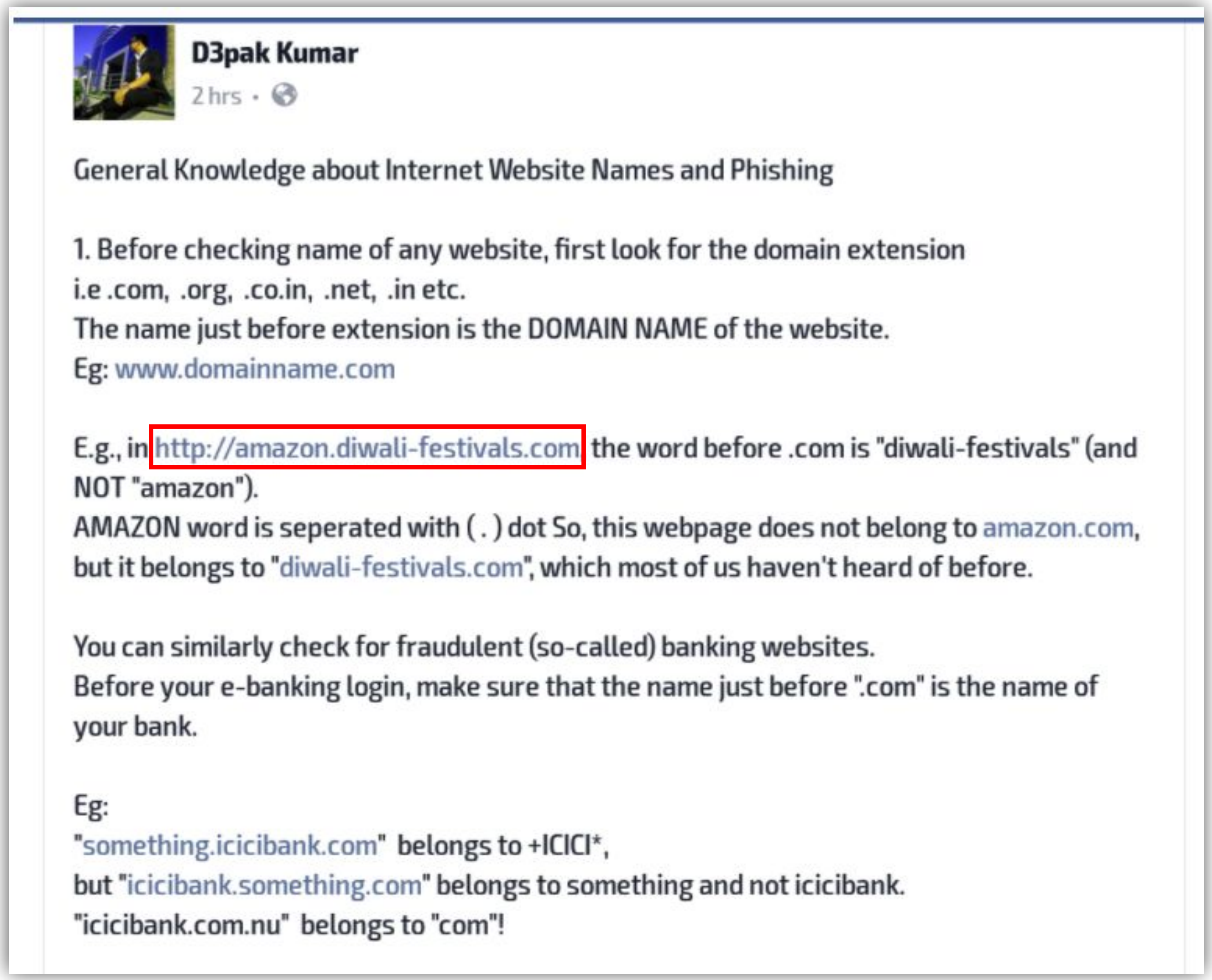
System:

IP:

**Please note:** Windows security has detected that the system is corrupted. All system files will be deleted after 225 seconds.

**Required:** Please click the button below to **"Update"** the latest software, scan your system and prevent your files being deleted.

# PHISHING TACTICS



**D3pak Kumar**

2 hrs ·

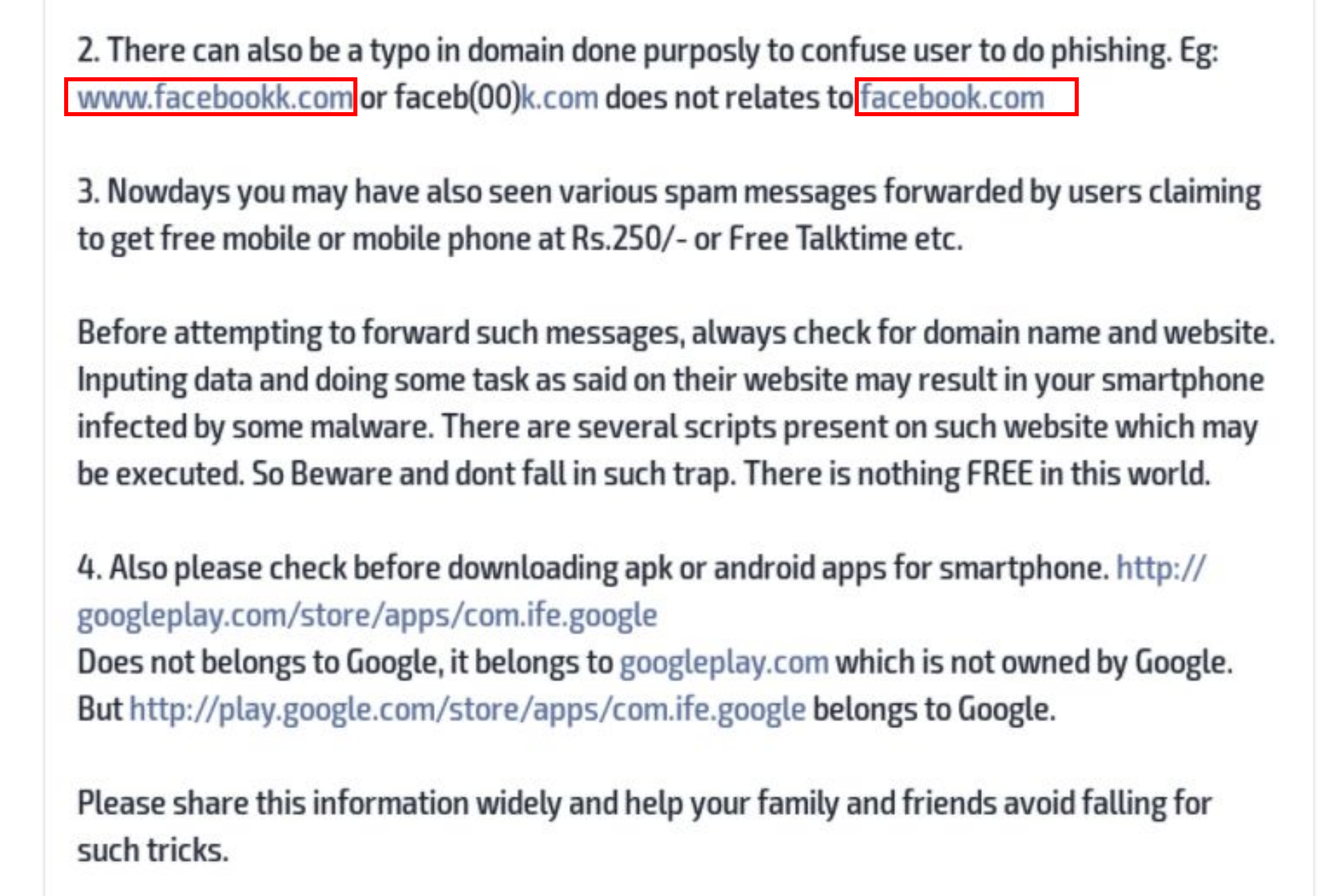
General Knowledge about Internet Website Names and Phishing

1. Before checking name of any website, first look for the domain extension
i.e .com, .org, .co.in, .net, .in etc.
The name just before extension is the DOMAIN NAME of the website.
Eg: www.domainname.com

E.g., in http://amazon.diwali-festivals.com the word before .com is "diwali-festivals" (and NOT "amazon").
AMAZON word is seperated with ( . ) dot So, this webpage does not belong to amazon.com, but it belongs to "diwali-festivals.com", which most of us haven't heard of before.

You can similarly check for fraudulent (so-called) banking websites.
Before your e-banking login, make sure that the name just before ".com" is the name of your bank.

Eg:
"something.icicibank.com" belongs to +ICICI*,
but "icicibank.something.com" belongs to something and not icicibank.
"icicibank.com.nu" belongs to "com"!



2. There can also be a typo in domain done purposly to confuse user to do phishing. Eg: www.facebookk.com or faceb(00)k.com does not relates to facebook.com

3. Nowdays you may have also seen various spam messages forwarded by users claiming to get free mobile or mobile phone at Rs.250/- or Free Talktime etc.

Before attempting to forward such messages, always check for domain name and website. Inputing data and doing some task as said on their website may result in your smartphone infected by some malware. There are several scripts present on such website which may be executed. So Beware and dont fall in such trap. There is nothing FREE in this world.

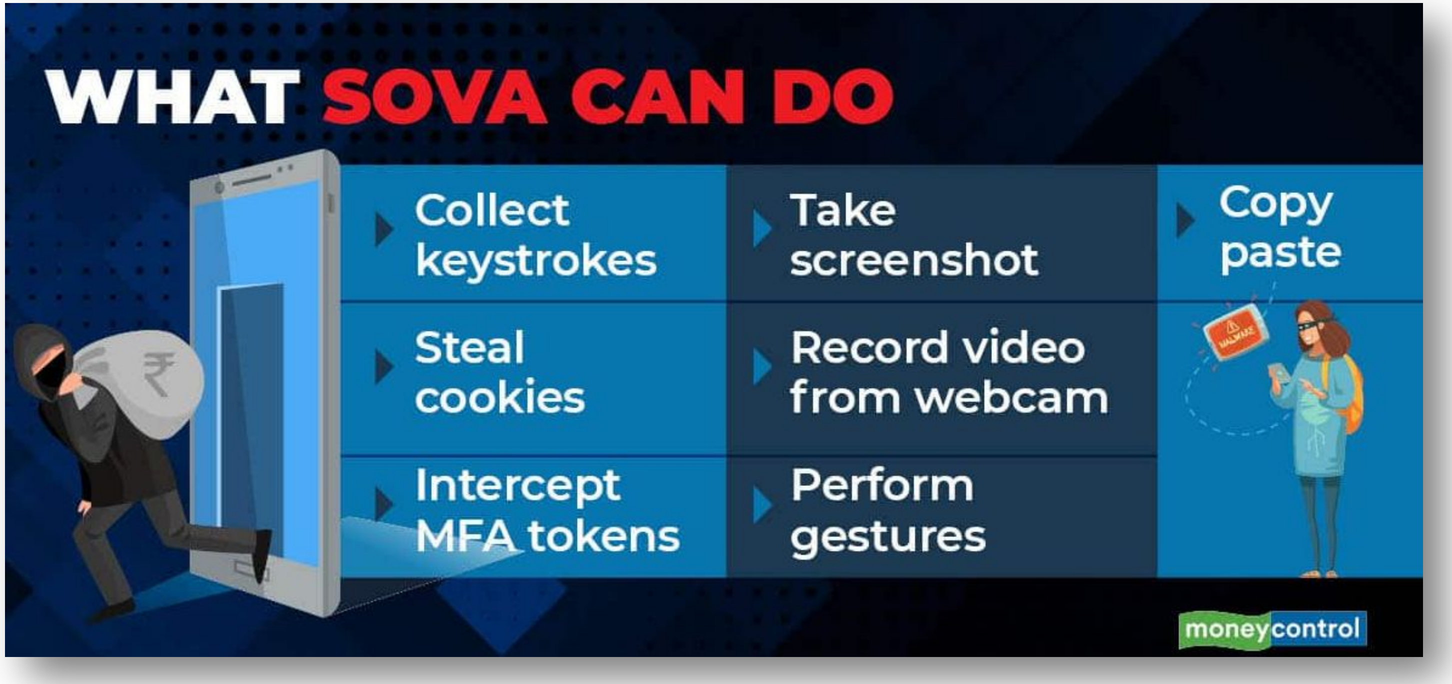
4. Also please check before downloading apk or android apps for smartphone. http://googleplay.com/store/apps/com.ife.google
Does not belongs to Google, it belongs to googleplay.com which is not owned by Google.
But http://play.google.com/store/apps/com.ife.google belongs to Google.

Please share this information widely and help your family and friends avoid falling for such tricks.

# Some examples of SMS attacks

**Emotet — SMS Phishing and Malware/Trojan :** In early 2020, a banking trojan called EMOTET was used by cybercriminals to trick customers into credential theft and malware infection through text messages (SMS)

**Filecoder — Android SMS ransomware :**In July 2019, reports of new ransomware targeting Google Android devices had begun to surface. Known as Android/Filecoder.C, this threat spreads via text message and can lock down your phone files via data encryption.



# SOME CYBER MALWARE THREATS

# 1 SPIKE IN RANSOMWARE ATTACKS

In ransomware attacks, cybercriminals steal or encrypt an organization's information and demand a ransom. If the organization refuses to pay, attackers threaten to publicly release or permanently delete the data, which forces the organization to choose between settling a large ransom or bearing the large scale reputational and financial loss.

**Global research predicts that businesses will fall victim to ransomware attacks every 11 seconds in 2021 compared to every 14 seconds in 2019.**

**THE ESTIMATED COST OF RANSOMWARE TO BUSINESSES WILL TOP $20 BILLION IN THE UPCOMING YEAR WITH AN AVERAGE ATTACK COSTING OVER $4 MILLION.**

One of the leading causes of this surge is that businesses have less tolerance for downtime with remote work. The lack of cybersecurity governance over remote work motivates threat actors further. It is increasingly common for breached organizations to pay ransom instead of the far more expensive post-attack remediation cost to avoid prolonged downtime, regulatory oversight, and minimize reputational damage in the public. The success of ransomware attacks encourages cybercriminals to continue this practice.

*Ref: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/*

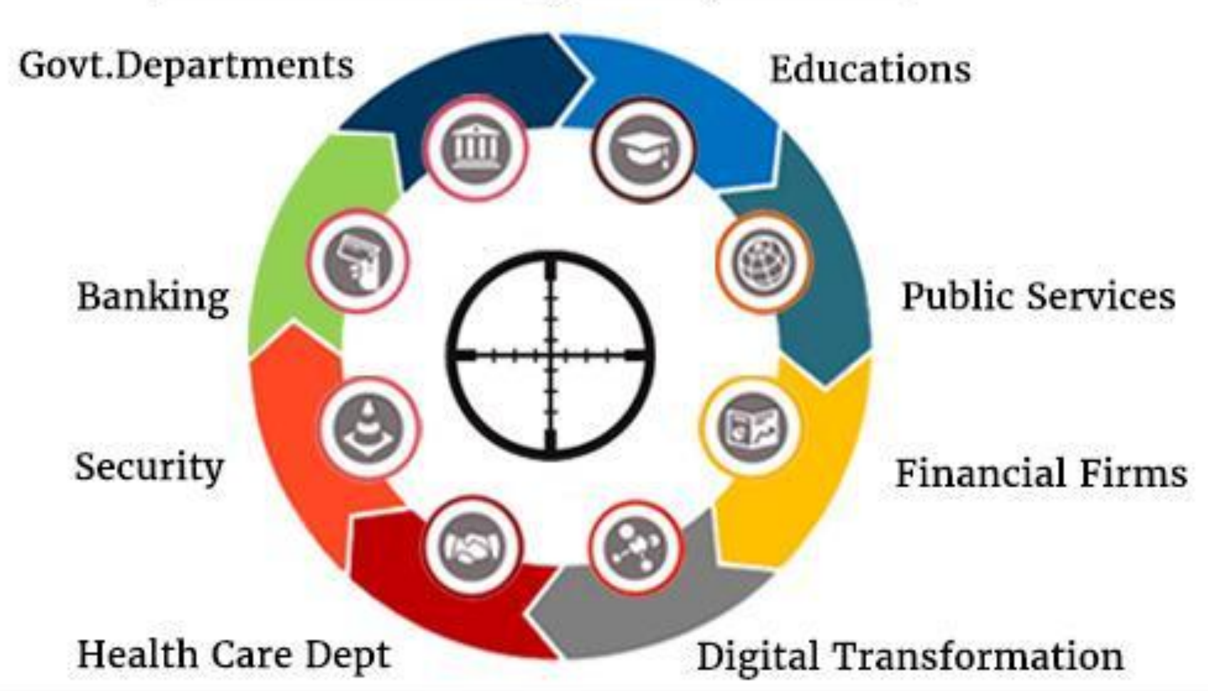
> *"The average downtime due to a Ransomware attack was 19 days in Q3 of 2020 compared to 12.1 days in Q3 2019."*
>
> *- Coveware*

> *"In 2019-2020, the average global cost to remediate a Ransomware attack was $761,106."*
>
> *- Sophos*

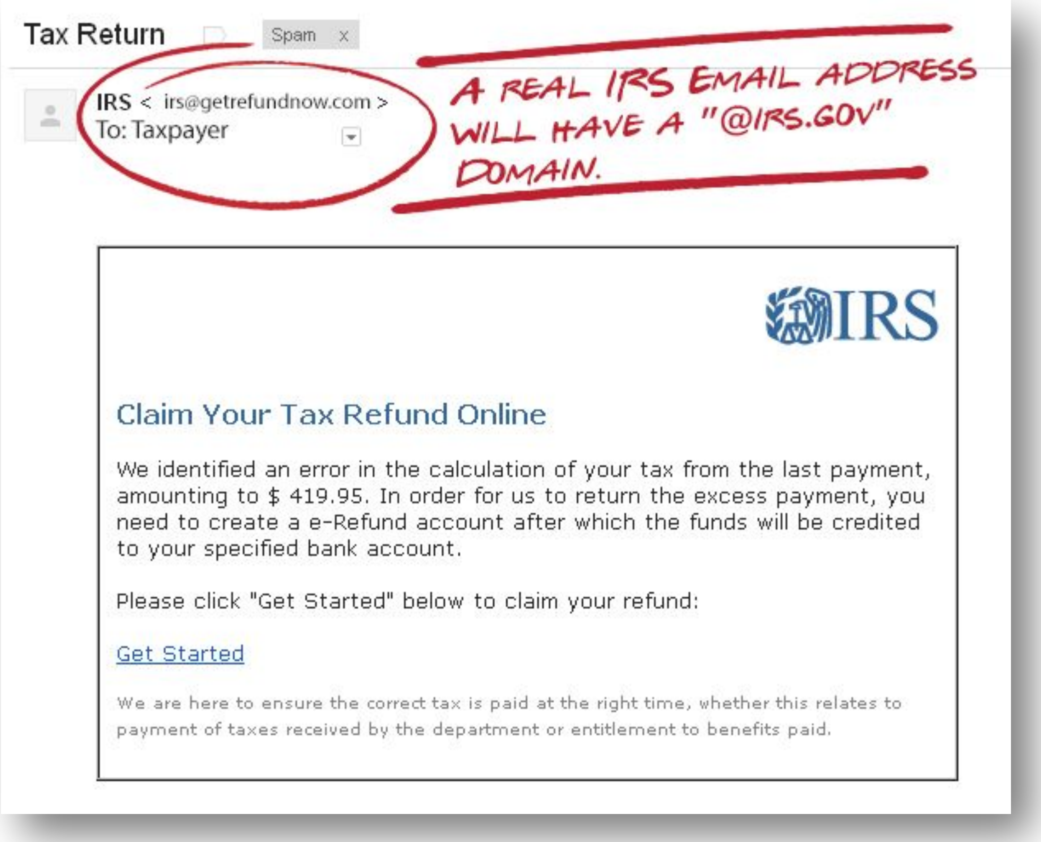
> *"The average cost of downtime is 24 times higher than the average ransom amount."*
>
> *- Datto*

# RANSOMWARE TARGETS TOP SECTORS

Today any enterprise, organisation or individuals users, big or small, is vulnerable to ransomware attack. The possibility of a it depends upon how attractive and important data your organization possess.



# Sample malicious ransomware mail/attachment



Tax Return

IRS < irs@getrefundnow.com >
To: Taxpayer

A REAL IRS EMAIL ADDRESS WILL HAVE A "@IRS.GOV" DOMAIN.

Claim Your Tax Refund Online

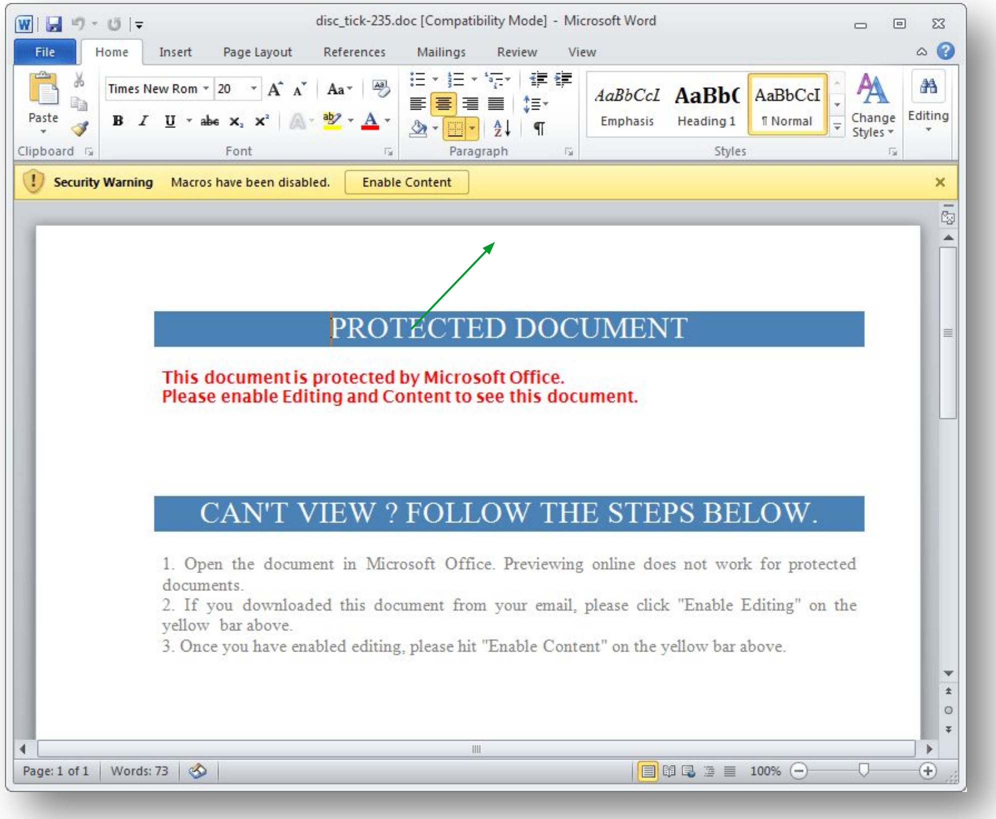
We identified an error in the calculation of your tax from the last payment, amounting to $ 419.95. In order for us to return the excess payment, you need to create a e-Refund account after which the funds will be credited to your specified bank account.

Please click "Get Started" below to claim your refund:

Get Started

We are here to ensure the correct tax is paid at the right time, whether this relates to payment of taxes received by the department or entitlement to benefits paid.

*Sample of phishing email*



disc_tick-235.doc [Compatibility Mode] - Microsoft Word

Security Warning Macros have been disabled. Enable Content

PROTECTED DOCUMENT

This document is protected by Microsoft Office.
Please enable Editing and Content to see this document.

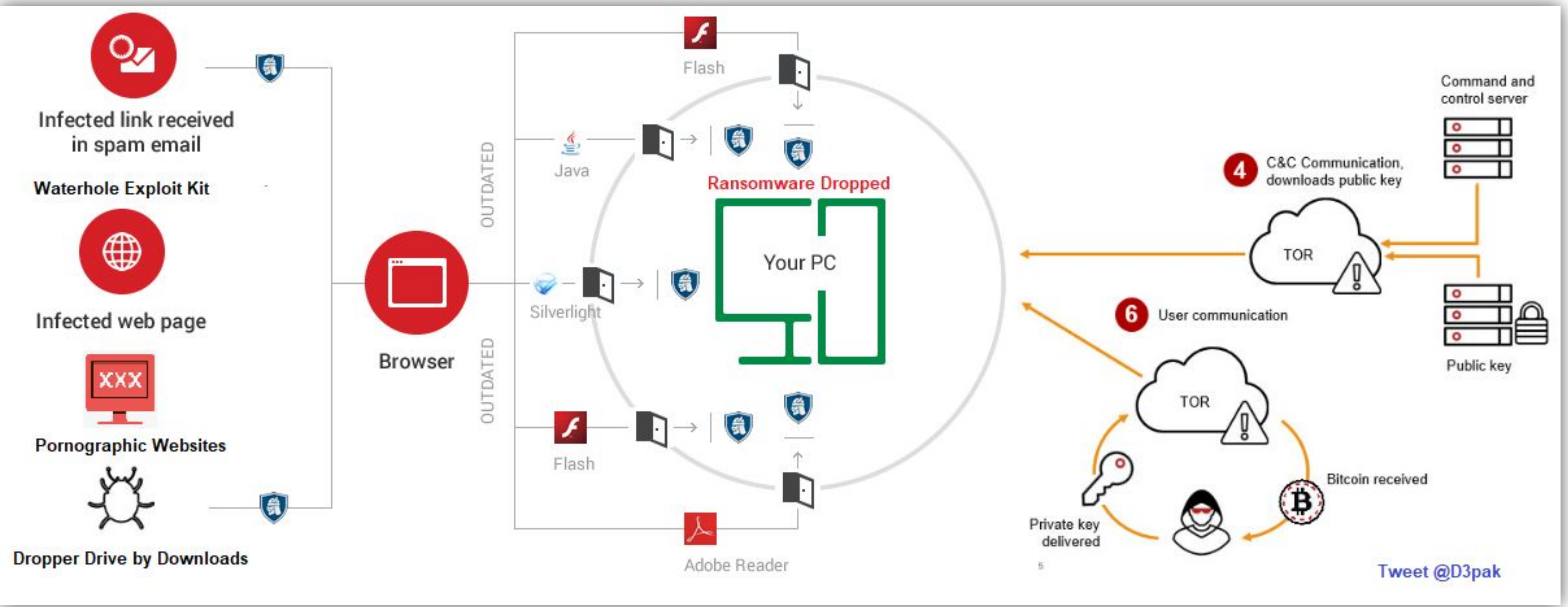
CAN'T VIEW ? FOLLOW THE STEPS BELOW.

1. Open the document in Microsoft Office. Previewing online does not work for protected documents.
2. If you downloaded this document from your email, please click "Enable Editing" on the yellow bar above.
3. Once you have enabled editing, please hit "Enable Content" on the yellow bar above.

*Sample malicious document, ask user to "Enable content"*

# Example: RANSOMWARE Now Crypto

*Hackers Mindset : Too much risk……but the target is too sweet*



## 2 BUSINESS EMAIL COMPROMISE

Business Email Compromise (BEC) is one of the most financially damaging online crimes. It exploits the fact that most organizations rely on email to conduct business. In a BEC scam, cyber-criminals send an email that appears to come from a legitimate source. After active reconnaissance on the victim's mailbox, these emails are sent to make financial requests that are timed perfectly and appear legitimate. BEC can be carried out using numerous tactics and techniques. One of the popular approaches is executive impersonation, also known as CXO Fraud.

In this scenario, the scammer assumes the personality of a high ranking executive. This tactic gives the victim a sense of urgency and persuades them to make the requested funds transfer/data disclosure with less probability of questioning the matter. One of the increasing trends to counter BEC is the correct implementation of DMARC, especially in financially sensitive sectors. Increased staff awareness and training is a high-value investment to avoid BEC.

> *"$44,000 – the average cost for a Business Email Compromise hack."*
>
> *- Verizon*

There has been a spike in BEC Fraud cases, increasing by 15% from Q2 to Q3 of 2020 - Abnormal Security

*Ref: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes*

## 3 BRAND ABUSE

The modern organization is evolving rapidly with increased cloud adoption and a greater digital presence. Accelerated by the pandemic, a majority of infrastructure and services have shifted online. Organizations are more focused on their online presence and are relying on it to conduct business. Brand abuse and brand impersonation will see a huge spike in the coming year as people rely more and more on online services.

**These attacks include impersonation on social media, job scams, next of kin scams, investment scams, fake news, and even to launch malware. With such a high variety of attack types, a new industry category dubbed Digital Risk Protection is rapidly evolving.**

**Beyond banking, finance, insurance and healthcare sectors, it is noted that online delivery services were highly targeted in 2020. Amazon and DHL were two of the most impersonated brands in 2020. It is expected that similar courier and delivery scams will increase in 2021. Brand oriented attack types also serve as launchpads for spear phishing and social engineering attacks.**

> *"83% of Spear Phishing Attacks Involve Brand Impersonation."*
>
> *- Barracu*

# 4 SUPPLY CHAIN ATTACK

Supply chain attacks are cyber attacks that compromise a target organization by penetrating a third party vendor of software package instead of the organization itself. This style of attack proves especially lucrative to attackers for several reasons; a breach on one vendor creates a ripple effect which can have a much higher impact on all organizations downstream. During 2020, there has been an increased reliance on third parties to counter limited business and engineering resources. In addition, threats are often overlooked as organizations tend to trust the vendors they use in day to day business.

**The biggest supply chain attack of 2020 was the SolarWinds hack where attackers pushed malicious code as part of an update package of the Orion software. This affected 18000+ customers of SolarWinds which including Microsoft, Cisco, Intel, and multiple US government agencies. In 2020, experts have warned of a 430% increase in supply chain attacks targeting open-source tools used across industries. These figures are expected to increase further in 2021 as organizations are deploying more third-party services and tools to facilitate their operations.**

> *"63% of all cyber-attacks could be traced either directly or indirectly to third parties."*
>
> *- PwC*

Usually IT vendors or small businesses are the perfect entry point for hackers since they lack security controls. Organizations should evaluate the cybersecurity posture of all their third-party vendors to eliminate the risk of supply chain attacks.

*Ref: https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12*

# 5 ATTACKS ON RDP/VPN

With increasing remote activity, many organizations have been implementing Remote Desktop Protocol (RDP) & Virtual Private Networking (VPN) to allow access to corporate data and servers off-site. Although RDP is already one of the most commonly attacked services online, the next year is expected to see a further spike in exploitation of RDP, VPN, and other remote services.

Despite the additional security layer that VPN provides, cybercriminals view VPN as an open gateway into an organization's entire network if access is achievable. **As data breaches increase, cybercriminals have an abundance of leaked credentials paired with exploits and brute force opportunities; thus almost doubling the attacks against RDP, VPN, and remote connection servers in 2021.**

> *"RDP Brute-force Attacks grew 400% in March and April alone."*
>
> *- Kasp*

*Ref.https://www.csoonline.com/article/3542895/attacks-against-internet-exposed-rdp-servers-surging-during-covid-19-pandemic.html*

# 6 DATA BREACHES ON CLOUD-BASED INFRASTRUCTURE AND SERVICES

Cloud adoption has its own challenges. Organizations are expected to implement their own cybersecurity infrastructure and configure them adequately to secure themselves. Infrastructure as a Service (IaaS) vendors typically have a shared security services model. Subsequently, misconfigurations may lead to data breaches and exposure of sensitive corporate information; this is a high risk.

This risk gives rise to 3 major challenges.

- **Employees do not have adequate skills and knowledge in cloud security and hence it leaves an open door for hackers.**
- **The current security frameworks lack adequate mapping to implement security measures on cloud services and this exponentially increases the risk.**
- **Exposure of mission critical or corporate data left exposed on the internet for attackers to access.**

The most common misconfiguration is over-privileged user accounts. When attackers gain access to an associated identity with broad privileged permissions, they can abuse those permissions maliciously.

*"Number of records exposed reaches a staggering 36 billion in 2020."*

*- Risk Based Security*

*"Errors caused 22% of Data Breaches."*

*- Verizon*

*"82% of cloud users have experienced security events caused by confusion over who is responsible to secure the implementations."*

*- Oracle and KPMG*

# 7 DATA EXPOSURE ON CODE REPOSITORIES

Developers routinely use code repositories such as GitHub to back up, share, and manage changes to code. It is a popular environment for collaborative development by the developer community; however, code repositories are also public by default, which means that anyone can find and access code that has been uploaded to such websites.

**And all too often, developers forget to remove sensitive data from their code or make the repositories private before uploading them on GitHub. Malicious hackers actively scan and scrape GitHub for leaked passwords, client IDs, secret keys, and API tokens, to name a few, because they know programmers are prone to such oversight.**

With the current rise in remote work, development teams are often scattered, working remotely and sharing code via online repositories. Data exposure risks will subsequently increase with limited security governance and lack of practical controls.

*Ref: https://unit42.paloaltonetworks.com/github-data-exposed/*

> *"Unit 42 researchers analyzed more than 24,000 public GitHub data uploads via GitHub's Event API and found thousands of files containing potentially sensitive information, which included: 4109 Configuration files, 2464 API keys, 2328 Hardcoded username and passwords, 2144 Private key files, 1089 OAuth tokens."*
>
> *- Palo Alto*

# 8 TARGETED THREATS LEVERAGING REMOTE WORK

New security challenges are brought on by the rapid deployment of tools, technologies, and processes that enable people to work remotely. The shift in working practices, associated devices, and locations makes it far easier for these types of threats to go unnoticed. The rapid increase of mobile devices widens the organization's potential attack surface. This threat is further amplified by the associated rise in cloud adoption and the short-term 'Use Your Own Device' (UYOD) policies that many organizations adopted to overcome remote work challenges.

**Employees working from home use devices that aren't patched, managed, or secured by the corporate IT department. This gives hackers an entry point into the network that bypasses the perimeter security. Sensitive company data is being stored on these devices, further increasing the risk of data breaches.**

Additionally, the majority of people do not manage the default settings of their home router which leaves an entry point for hackers to access the network and confidential data. Moreover they may have many IoT devices within their home network with inadequate security controls which can also prove to be a threat.

> *"In corporate contexts, decision-makers are aware of the issue: 83% of them said that their organization was at risk from Mobile Threats and 86% agreed that Mobile Threats are growing faster than others."*
>
> *- Veriz*

# 9 PHISHING, VISHING, AND SMISHING ATTACKS

Since its outbreak in March 2020, COVID-19 has been the main headline of news and media outlets. Threat actors recognized this pandemic as the most apparent bait to make their schemes more effective. The use of the COVID-19 pandemic as a theme for phishing campaigns is expected to progress into 2021. Attacks will often coincide with significant events or news, such as a spike in new cases or a new vaccine drug's announcement.

Smishing and Vishing attacks are also growing as cybercriminals turn to mediums that are trusted more than email. Smishing is a type of social engineering attack that utilizes SMS text messaging as its medium. Vishing, on the other hand, is conducted via phone calls. There is no current filter or technology where numbers are confirmed as trusted sources, making mobile phone users more vulnerable to these attacks.

**There are different variations of these campaigns.**

**For example, impersonating official healthcare entities like the WHO, hospitals, and insurance companies is a prevalent pattern. Another variation that scammers opt for is masking as relief funds and donation campaigns.**

**Other than attacks directly connected to COVID-19, a rise in activity related to the after effects of the pandemic is anticipated. These may include fictitious employment opportunities, investment propositions, threats to online collaboration activities, and various online shopping scams.**

> *"According to Verizon's 2020 Mobile Security Index, Smishing Attacks have increased from 2 percent to 13 percent in just the past year."*
>
> *- Verizon*

> *"More than 60% of Phishing Attacks involve keyloggers."*
>
> *- Cofense*

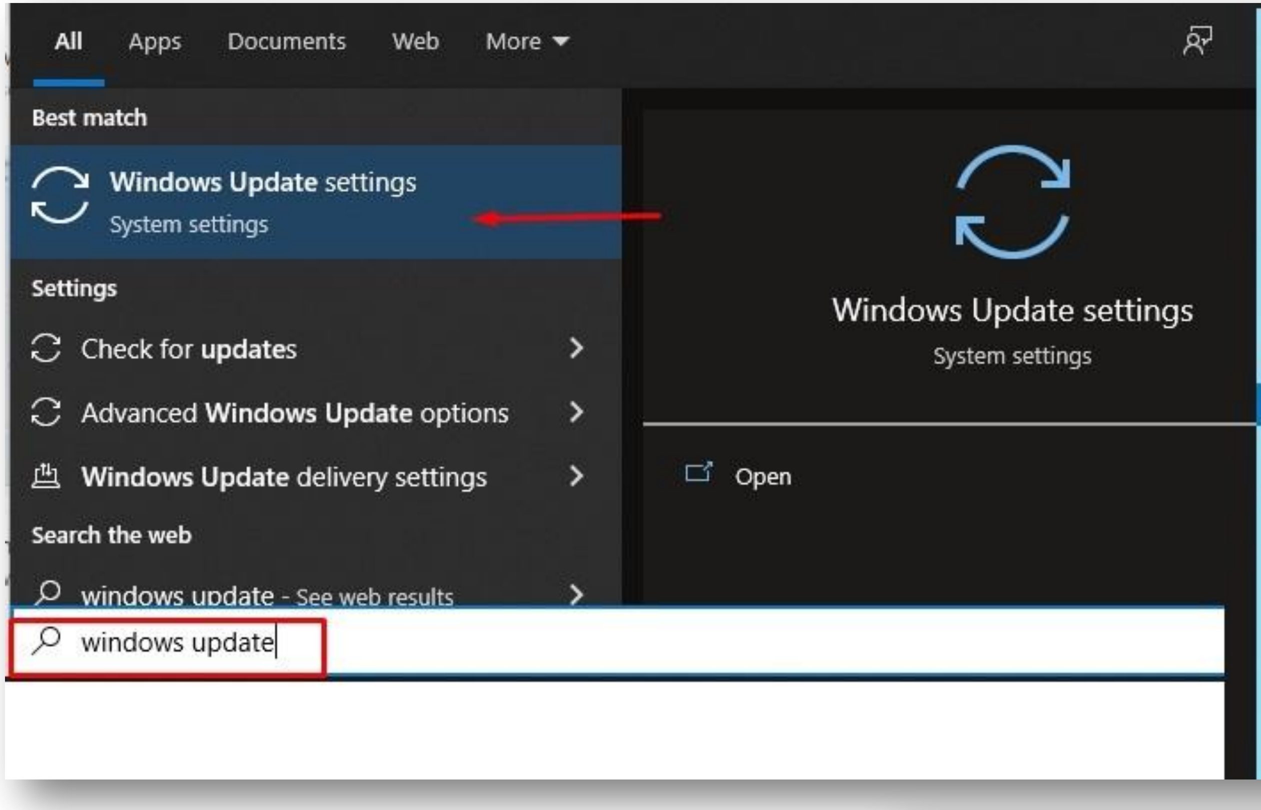
> *"A single Spear-Phishing Attack results in an average loss of $1.6 million."*
>
> *-Security Boulevard*

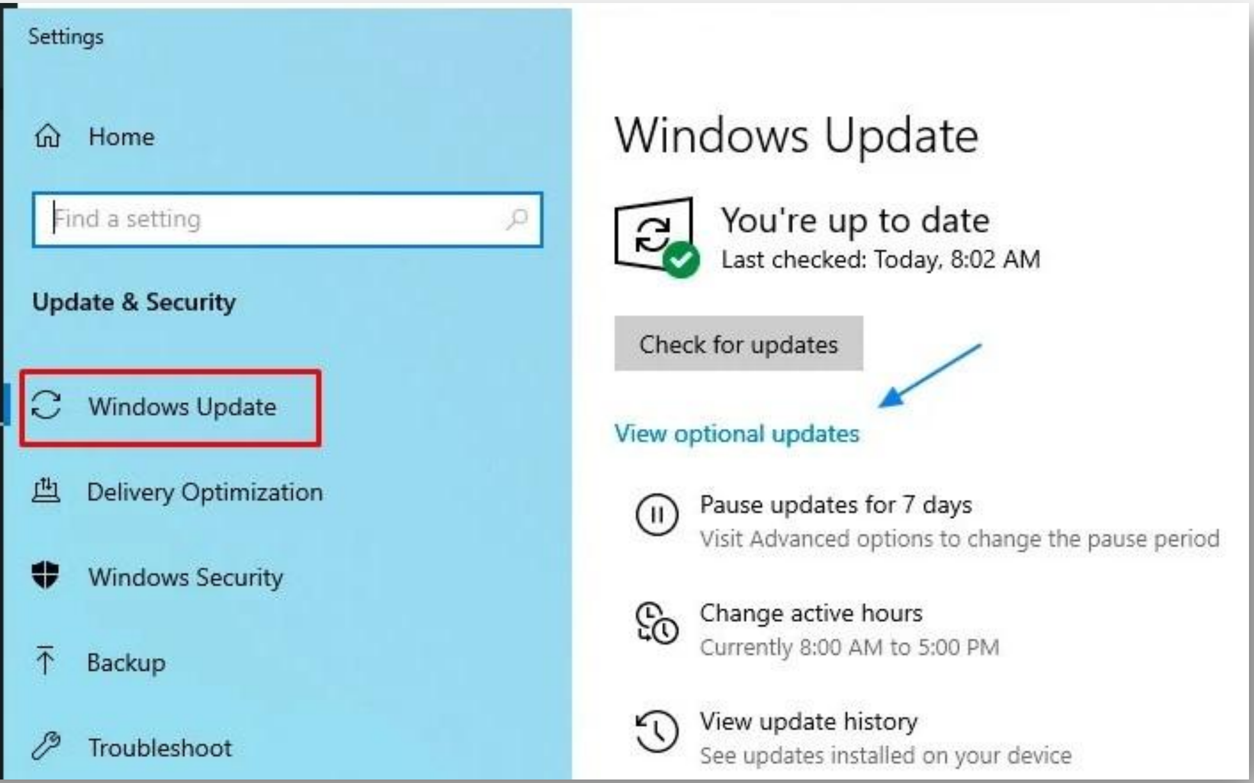
> *"In Q3 of 2020, APWG detected almost 572,000 unique Phishing websites and observed more than 367,000 unique Phishing email subjects."*
>
> *- APWG*

# COUNTERMEASURES

# SOME CYBER AWARENESS TIPS

- Use strong & complex Passwords
- Secure your computer
- Keep update anti-virus /malware & firewall solutions
- Be Social-Media Savvy
- Secure your Mobile Devices
- Update the latest operating system & application
- Secure your wireless network
- Protect your e-identity
- Report such Incidents
- Protect your Data & Take Back-up
- Be Careful while clicking on link





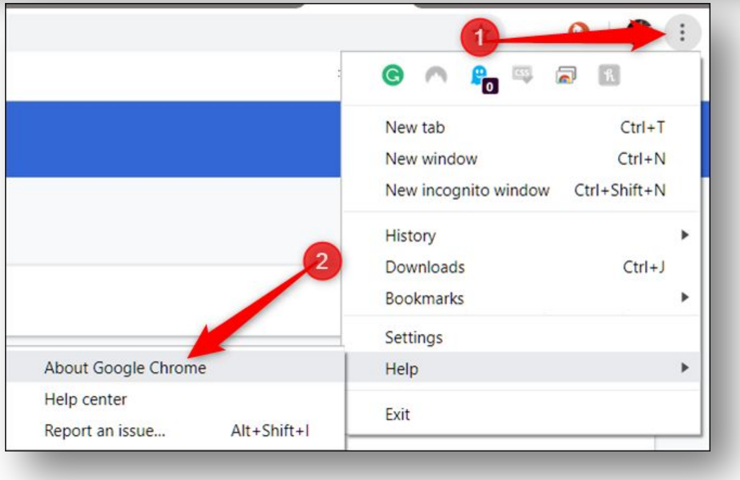
You're up to date

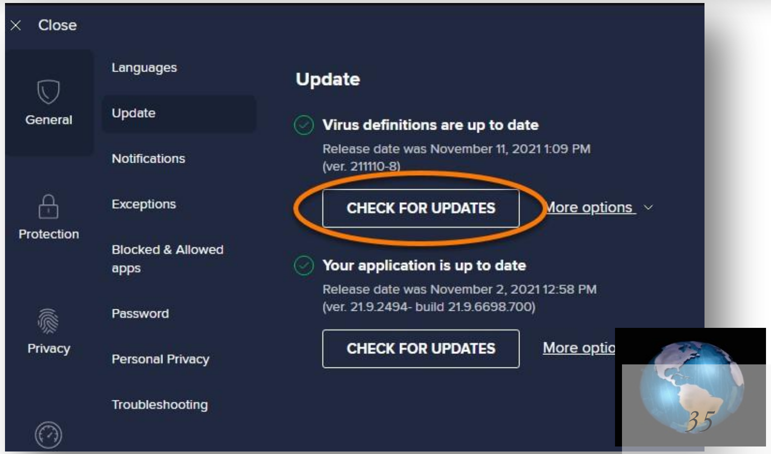
Last checked: Today, 8:02 AM

Visit Advanced options to change the pause period

Currently 8:00 AM to 5:00 PM

See updates installed on your device



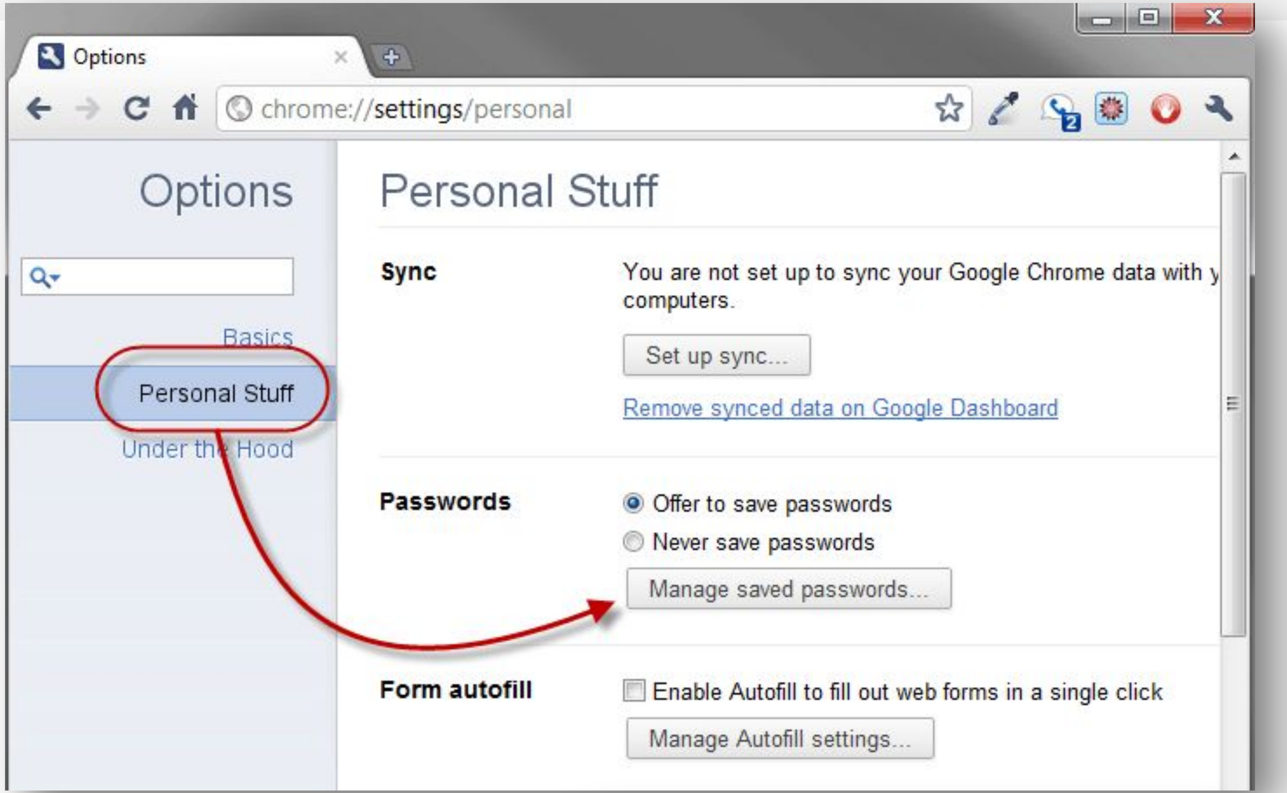


Virus definitions are up to date

Release date was November 11, 2021 1:09 PM (ver. 211110-8)

Your application is up to date

Release date was November 2, 2021 12:58 PM (ver. 21.9.2494- build 21.9.6698.700)



Options

chrome://settings/personal

Options

Basics

Personal Stuff

Under the Hood

## Personal Stuff

**Sync** — You are not set up to sync your Google Chrome data with y computers.

Set up sync...

Remove synced data on Google Dashboard

**Passwords**

● Offer to save passwords

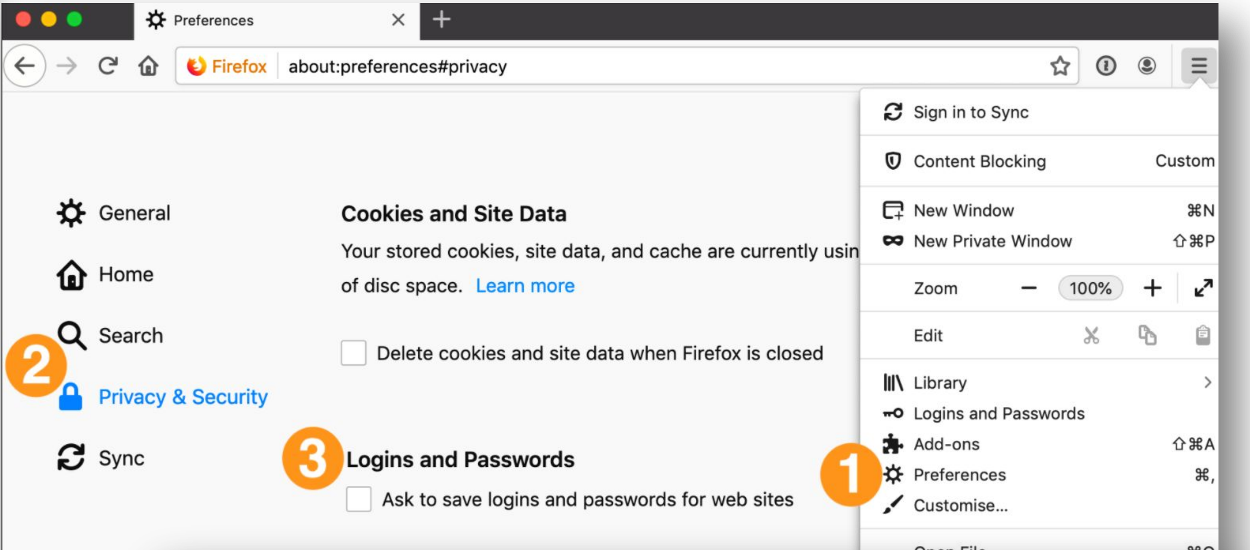
○ Never save passwords

Manage saved passwords...

**Form autofill**

□ Enable Autofill to fill out web forms in a single click

Manage Autofill settings...



Preferences

Firefox about:preferences#privacy

General

Home

Search

2 Privacy & Security

Sync

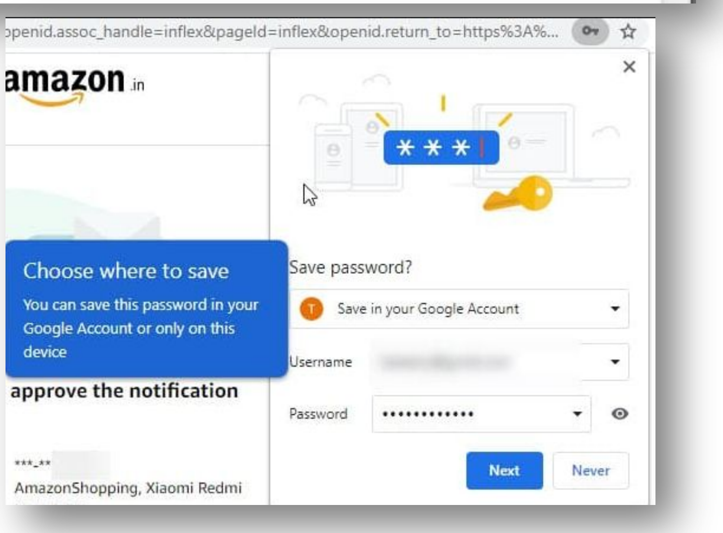
**Cookies and Site Data**

Your stored cookies, site data, and cache are currently usin of disc space. Learn more

□ Delete cookies and site data when Firefox is closed

3 **Logins and Passwords**

□ Ask to save logins and passwords for web sites



openid.assoc_handle=inflex&pageId=inflex&openid.return_to=https%3A%...

amazon.in

**Choose where to save**

You can save this password in your Google Account or only on this device

approve the notification

***_**

AmazonShopping, Xiaomi Redmi

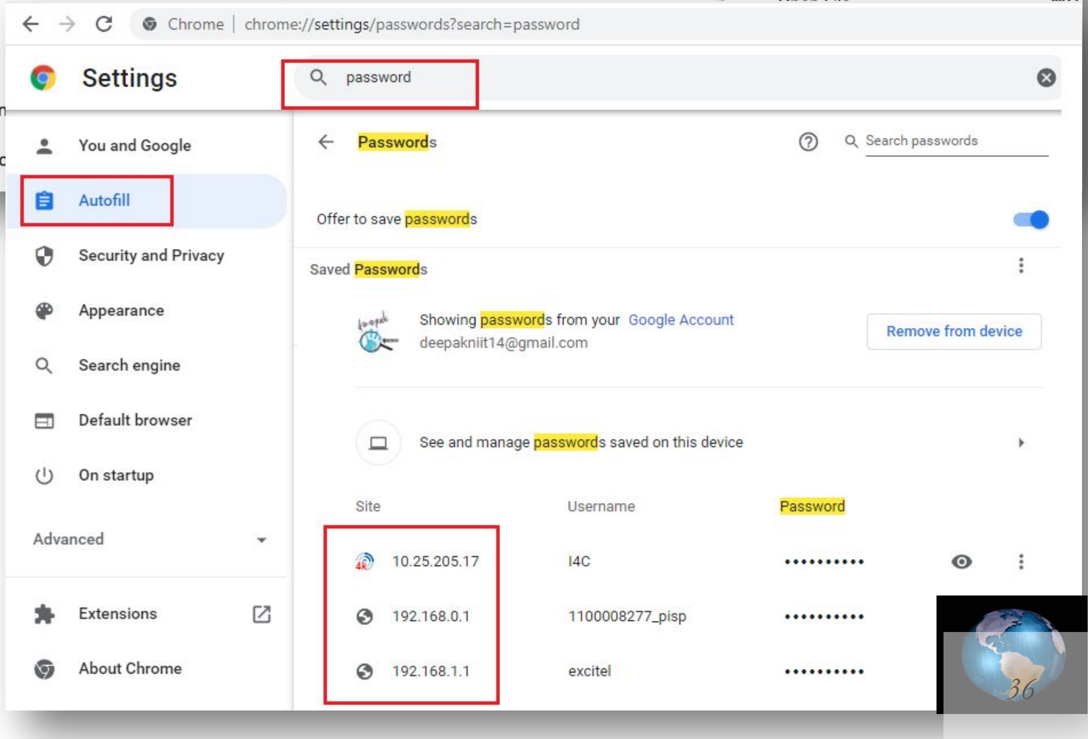
Save password?

Save in your Google Account

Username [redacted]

Password ••••••••••••

Next | Never



Chrome | chrome://settings/passwords?search=password

Settings — password

Passwords — Search passwords

Offer to save passwords

Saved Passwords

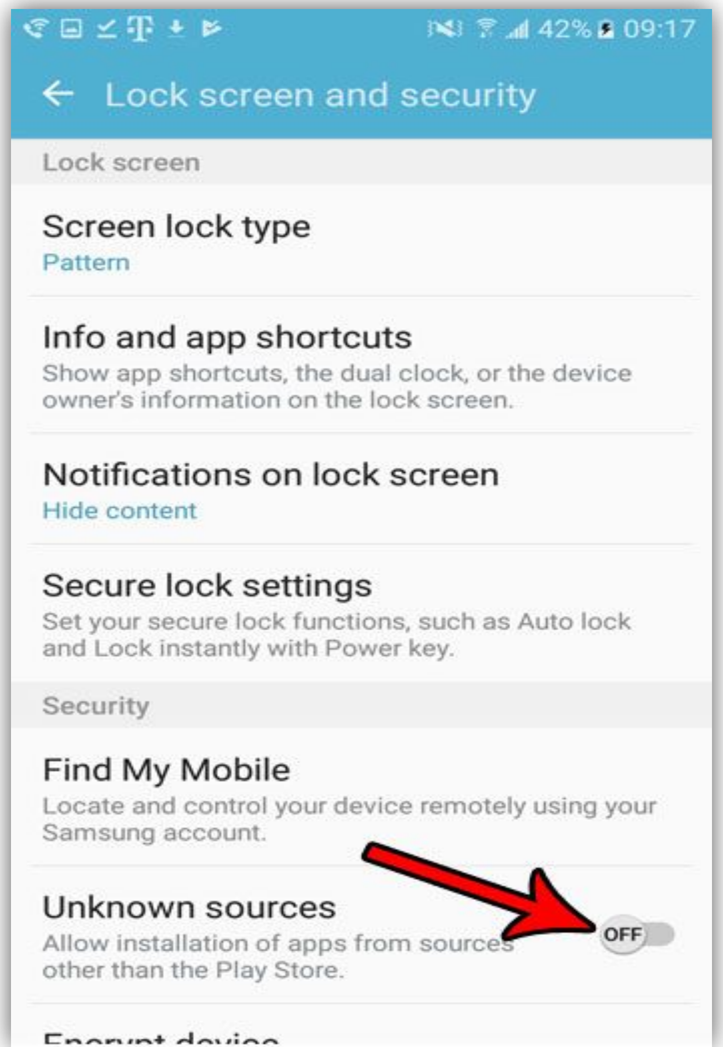
Showing passwords from your Google Account
deepakniit14@gmail.com

Remove from device

See and manage passwords saved on this device

| Site | Username | Password |
|---|---|---|
| 10.25.205.17 | I4C | •••••••••• |
| 192.168.0.1 | 1100008277_pisp | •••••••••• |
| 192.168.1.1 | excitel | •••••••••• |

# Check 3rd Party Application Installation is allowed or not



42% 09:17

Lock screen and security

Lock screen

Screen lock type
Pattern

Info and app shortcuts
Show app shortcuts, the dual clock, or the device owner's information on the lock screen.

Notifications on lock screen
Hide content

Secure lock settings
Set your secure lock functions, such as Auto lock and Lock instantly with Power key.

Security

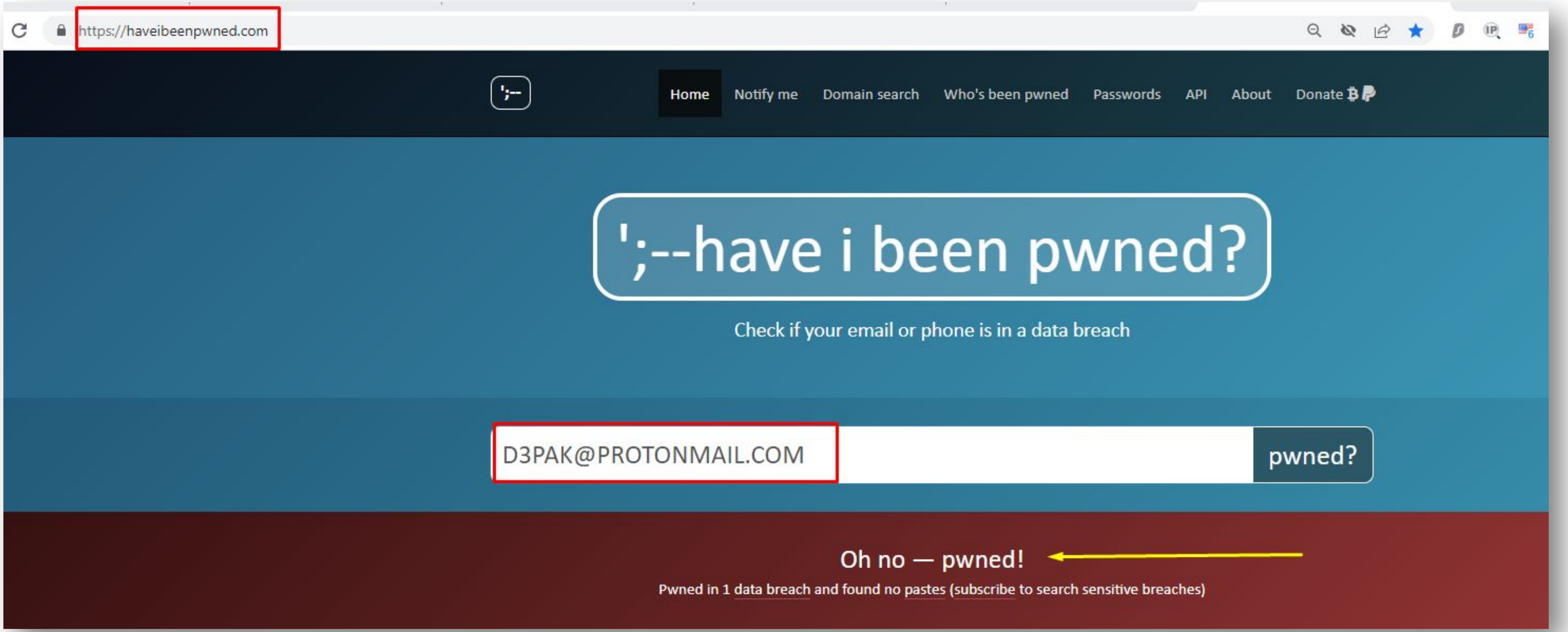
Find My Mobile
Locate and control your device remotely using your Samsung account.

Unknown sources
Allow installation of apps from sources other than the Play Store.
OFF

Encrypt device

Disable the Unknown Sources in your mobile setting to avoid installation of 3rd party applications.

# https://haveibeenpwned.com/



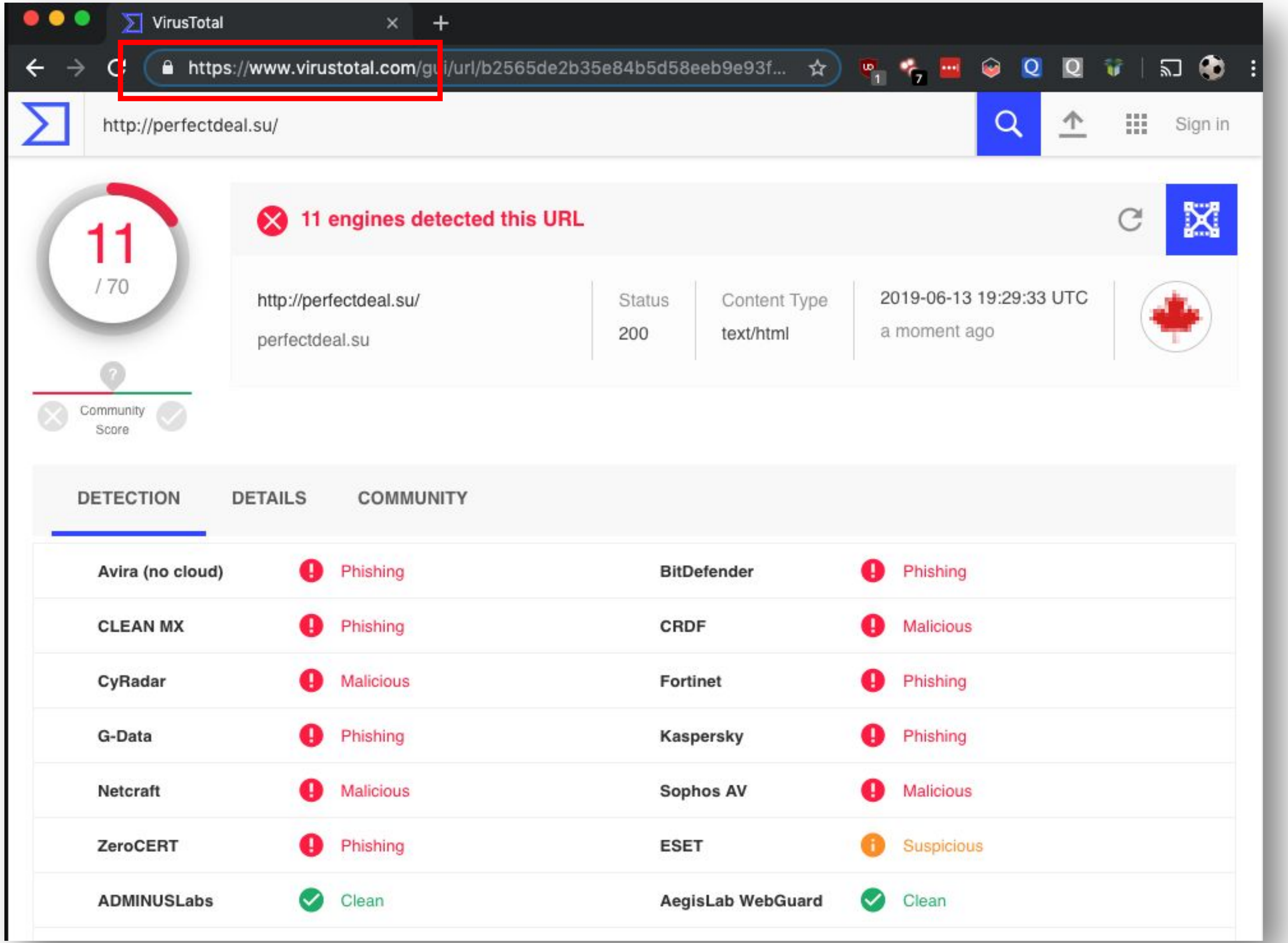
Check if your email or phone is in a data breach

D3PAK@PROTONMAIL.COM

Oh no — pwned!

Pwned in 1 data breach and found no pastes (subscribe to search sensitive breaches)

# https://www.virustotal.com/



11 engines detected this URL

| | | | | | |
|---|---|---|---|---|---|
| http://perfectdeal.su/<br>perfectdeal.su | Status<br>200 | Content Type<br>text/html | 2019-06-13 19:29:33 UTC<br>a moment ago | | |

| | | | |
|---|---|---|---|
| Avira (no cloud) | Phishing | BitDefender | Phishing |
| CLEAN MX | Phishing | CRDF | Malicious |
| CyRadar | Malicious | Fortinet | Phishing |
| G-Data | Phishing | Kaspersky | Phishing |
| Netcraft | Malicious | Sophos AV | Malicious |
| ZeroCERT | Phishing | ESET | Suspicious |
| ADMINUSLabs | Clean | AegisLab WebGuard | Clean |

# CYBER INCIDENTS – Handy links / contacts

- Report on incident@cert-in.org.in , incident@nic-cert.nic.in
- Report on www.cybercrime.gov.in (National Cyber Crime Reporting Portal)
- Visit www.csk.gov.in

# THANK YOU