Phishing , Vishing & Smishing
Concept & Safety Concern

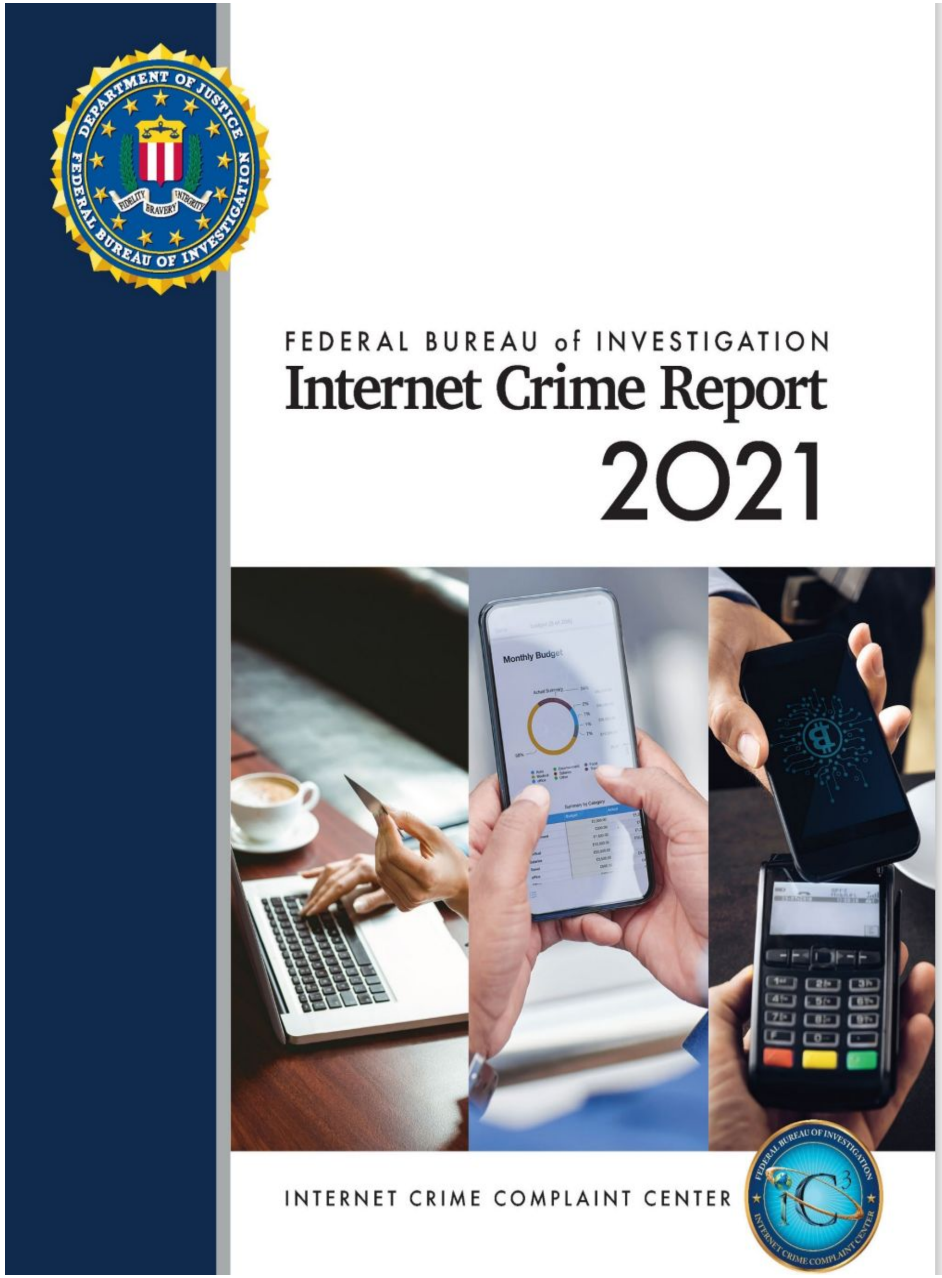
Chandni Agarwal

Social Engineering Attacks

A social engineering attack takes place in three steps. First, the attacker targets a victim. Second, they earn their trust. Third, they gain what they were after, usually breaking security practices or stealing information.

These attacks tend to work based on six principles:

- Authority and trust: where the attacker poses as an authority figure.
- Consensus and social proof: where peer pressure forces someone to commit an action.
- Scarcity: the idea that a victim will miss out if they don’t act.
- Urgency: the idea that the victim will miss out if they don’t act fast.

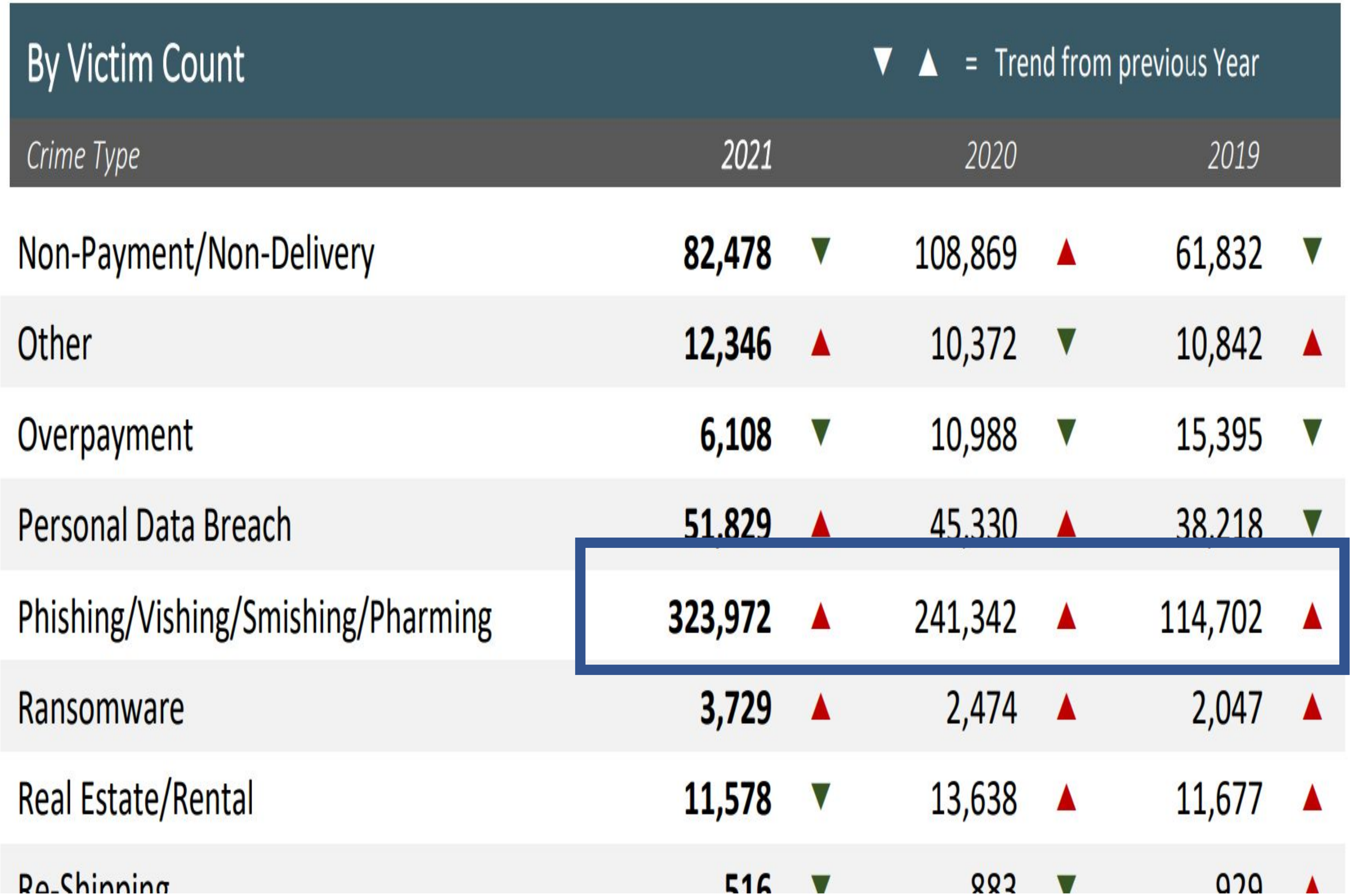


FEDERAL BUREAU of INVESTIGATION

Internet Crime Report 2021

INTERNET CRIME COMPLAINT CENTER

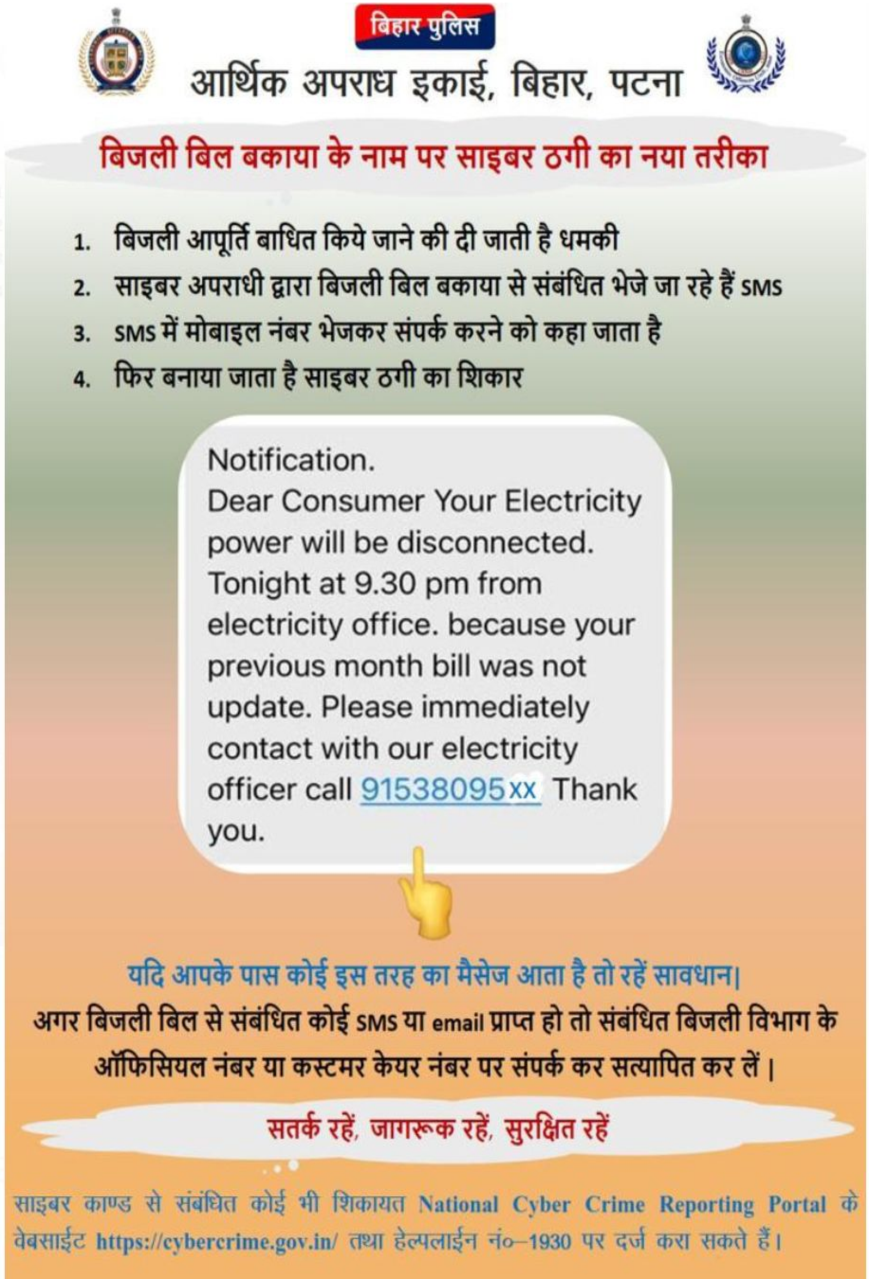
Last 3 Year Complaint Count Comparison



By Victim Count

▼ ▲ = Trend from previous Year

Crime Type	2021		2020		2019	
Non-Payment/Non-Delivery	**82,478**	▼	108,869	▲	61,832	▼
Other	**12,346**	▲	10,372	▼	10,842	▲
Overpayment	**6,108**	▼	10,988	▼	15,395	▼
Personal Data Breach	**51,829**	▲	45,330	▲	38,218	▼
Phishing/Vishing/Smishing/Pharming	**323,972**	▲	241,342	▲	114,702	▲
Ransomware	**3,729**	▲	2,474	▲	2,047	▲
Real Estate/Rental	**11,578**	▼	13,638	▲	11,677	▲
Re-Shipping	**516**	▼	883	▼	929	▲



बिहार पुलिस

आर्थिक अपराध इकाई, बिहार, पटना

बिजली बिल बकाया के नाम पर साइबर ठगी का नया तरीका

1. बिजली आपूर्ति बाधित किये जाने की दी जाती है धमकी
2. साइबर अपराधी द्वारा बिजली बिल बकाया से संबंधित भेजे जा रहे हैं SMS
3. SMS में मोबाइल नंबर भेजकर संपर्क करने को कहा जाता है
4. फिर बनाया जाता है साइबर ठगी का शिकार

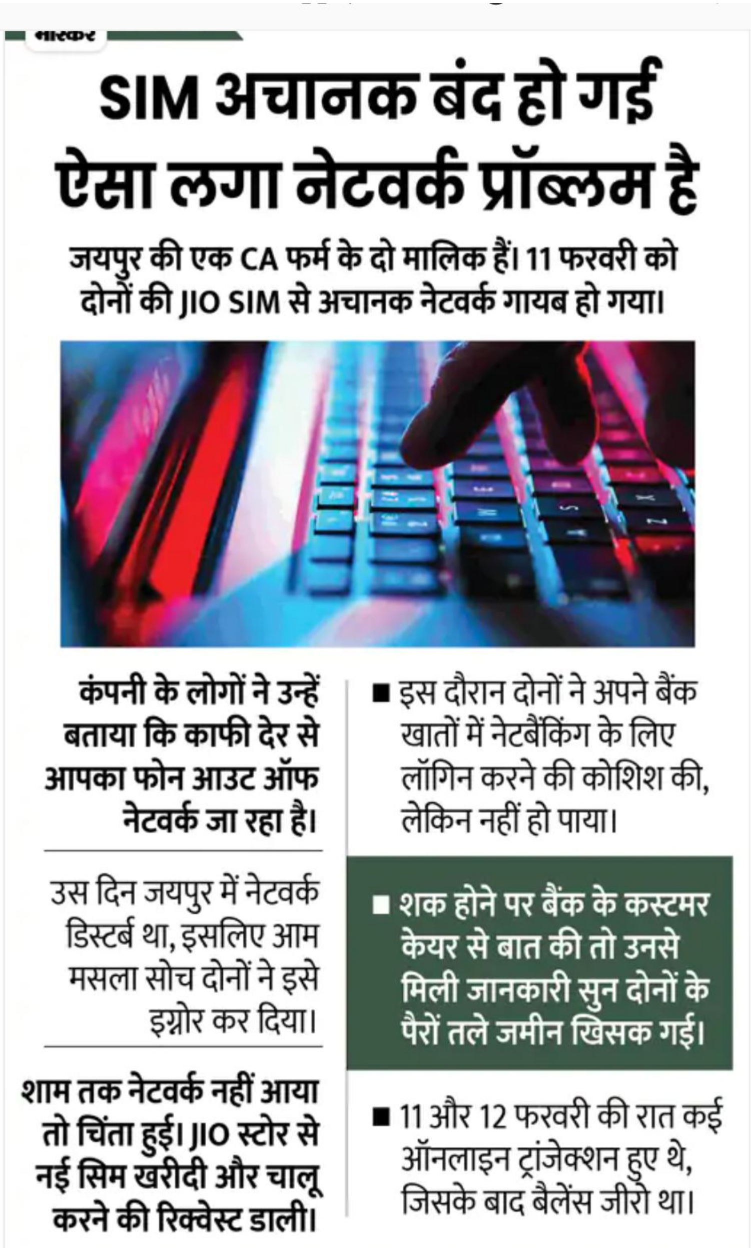
> Notification.
> Dear Consumer Your Electricity power will be disconnected. Tonight at 9.30 pm from electricity office. because your previous month bill was not update. Please immediately contact with our electricity officer call 91538095xx Thank you.

यदि आपके पास कोई इस तरह का मैसेज आता है तो रहें सावधान।

अगर बिजली बिल से संबंधित कोई SMS या email प्राप्त हो तो संबंधित बिजली विभाग के ऑफिसियल नंबर या कस्टमर केयर नंबर पर संपर्क कर सत्यापित कर लें।

सतर्क रहें, जागरूक रहें, सुरक्षित रहें

साइबर काण्ड से संबंधित कोई भी शिकायत National Cyber Crime Reporting Portal के वेबसाईट https://cybercrime.gov.in/ तथा हेल्पलाईन नं०–1930 पर दर्ज करा सकते हैं।



SIM अचानक बंद हो गई ऐसा लगा नेटवर्क प्रॉब्लम है

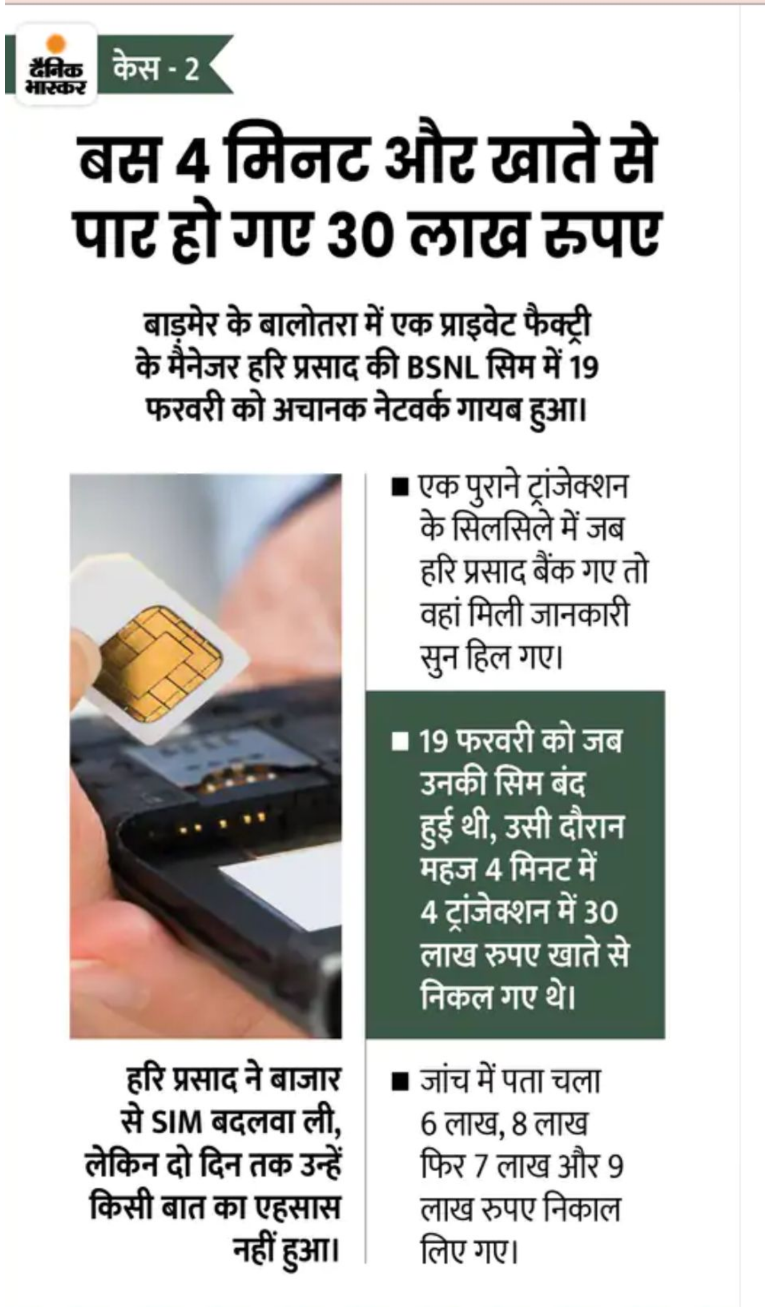
जयपुर की एक CA फर्म के दो मालिक हैं। 11 फरवरी को दोनों की JIO SIM से अचानक नेटवर्क गायब हो गया।

कंपनी के लोगों ने उन्हें बताया कि काफी देर से आपका फोन आउट ऑफ नेटवर्क जा रहा है।

उस दिन जयपुर में नेटवर्क डिस्टर्ब था, इसलिए आम मसला सोच दोनों ने इसे इग्नोर कर दिया।

शाम तक नेटवर्क नहीं आया तो चिंता हुई। JIO स्टोर से नई सिम खरीदी और चालू करने की रिक्वेस्ट डाली।

- इस दौरान दोनों ने अपने बैंक खातों में नेटबैंकिंग के लिए लॉगिन करने की कोशिश की, लेकिन नहीं हो पाया।
- **शक होने पर बैंक के कस्टमर केयर से बात की तो उनसे मिली जानकारी सुन दोनों के पैरों तले जमीन खिसक गई।**
- 11 और 12 फरवरी की रात कई ऑनलाइन ट्रांजेक्शन हुए थे, जिसके बाद बैलेंस जीरो था।



दैनिक भास्कर केस - 2

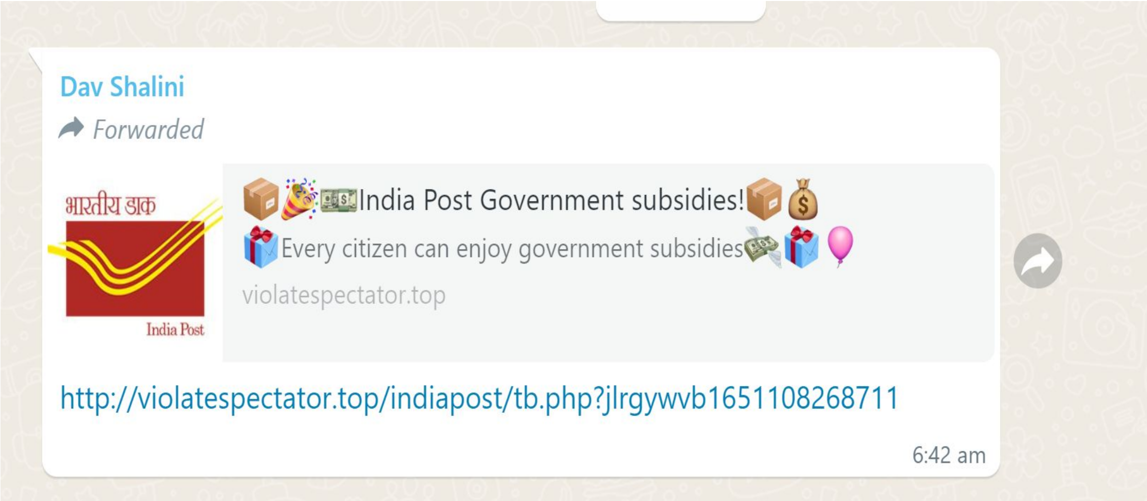
बस 4 मिनट और खाते से पार हो गए 30 लाख रुपए

बाड़मेर के बालोतरा में एक प्राइवेट फैक्ट्री के मैनेजर हरि प्रसाद की BSNL सिम में 19 फरवरी को अचानक नेटवर्क गायब हुआ।

हरि प्रसाद ने बाजार से SIM बदलवा ली, लेकिन दो दिन तक उन्हें किसी बात का एहसास नहीं हुआ।

- एक पुराने ट्रांजेक्शन के सिलसिले में जब हरि प्रसाद बैंक गए तो वहां मिली जानकारी सुन हिल गए।
- **19 फरवरी को जब उनकी सिम बंद हुई थी, उसी दौरान महज 4 मिनट में 4 ट्रांजेक्शन में 30 लाख रुपए खाते से निकल गए थे।**
- जांच में पता चला 6 लाख, 8 लाख फिर 7 लाख और 9 लाख रुपए निकाल लिए गए।

Real life cases



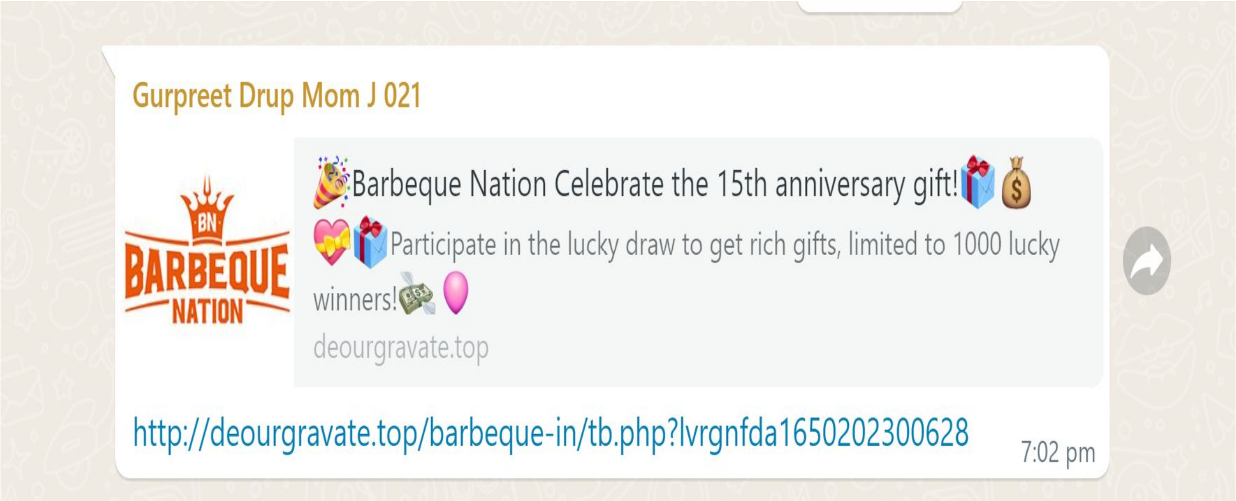
Dav Shalini

Forwarded

📦🎉💵India Post Government subsidies!📦💰
🎁Every citizen can enjoy government subsidies💸🎁🎈
violatespectator.top

http://violatespectator.top/indiapost/tb.php?jlrgywvb1651108268711

6:42 am

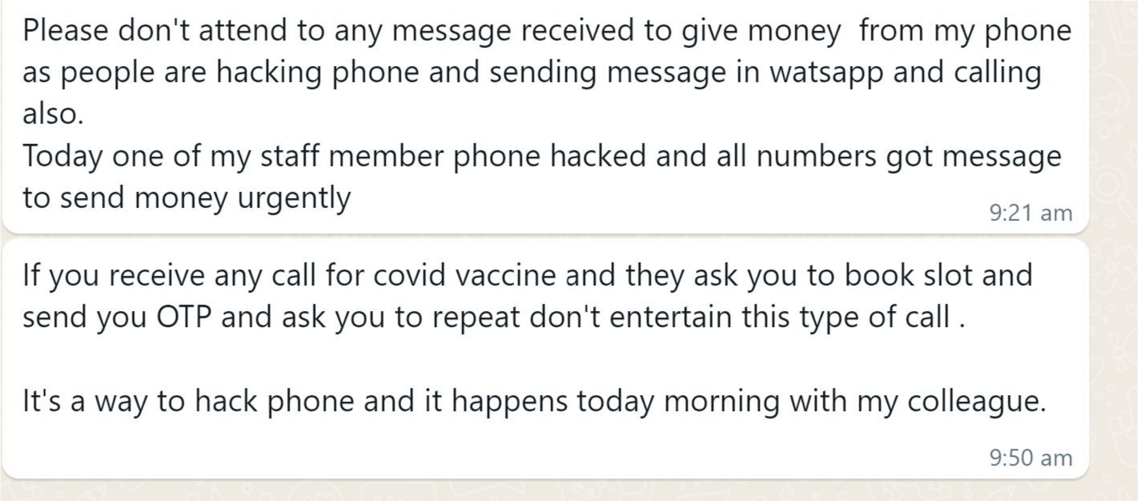


Gurpreet Drup Mom J 021

🎉Barbeque Nation Celebrate the 15th anniversary gift!🎁💰
💝🎁Participate in the lucky draw to get rich gifts, limited to 1000 lucky winners!💸🎈
deourgravate.top

http://deourgravate.top/barbeque-in/tb.php?lvrgnfda1650202300628

7:02 pm



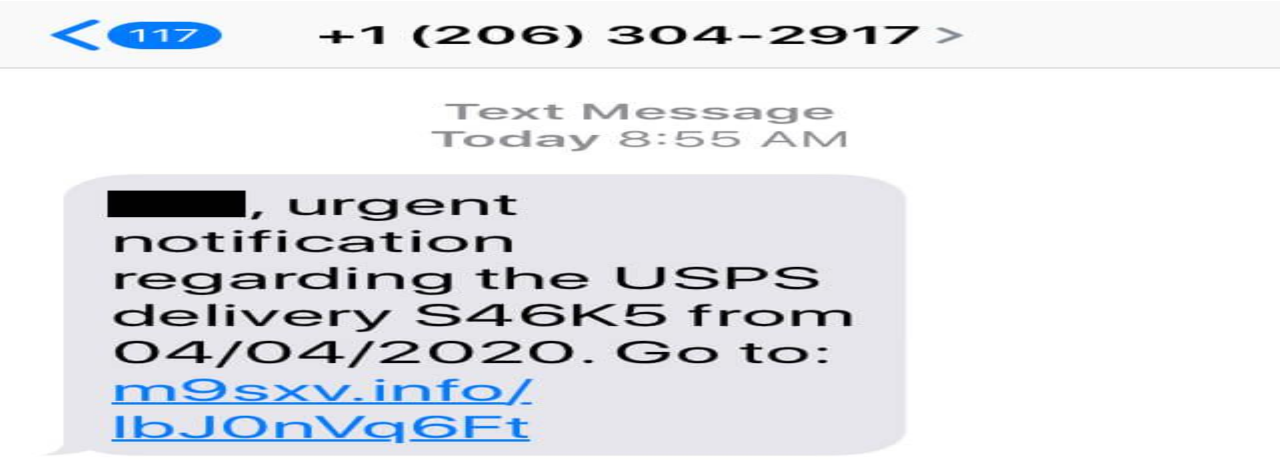
Please don't attend to any message received to give money from my phone as people are hacking phone and sending message in watsapp and calling also.
Today one of my staff member phone hacked and all numbers got message to send money urgently

9:21 am

If you receive any call for covid vaccine and they ask you to book slot and send you OTP and ask you to repeat don't entertain this type of call .

It's a way to hack phone and it happens today morning with my colleague.

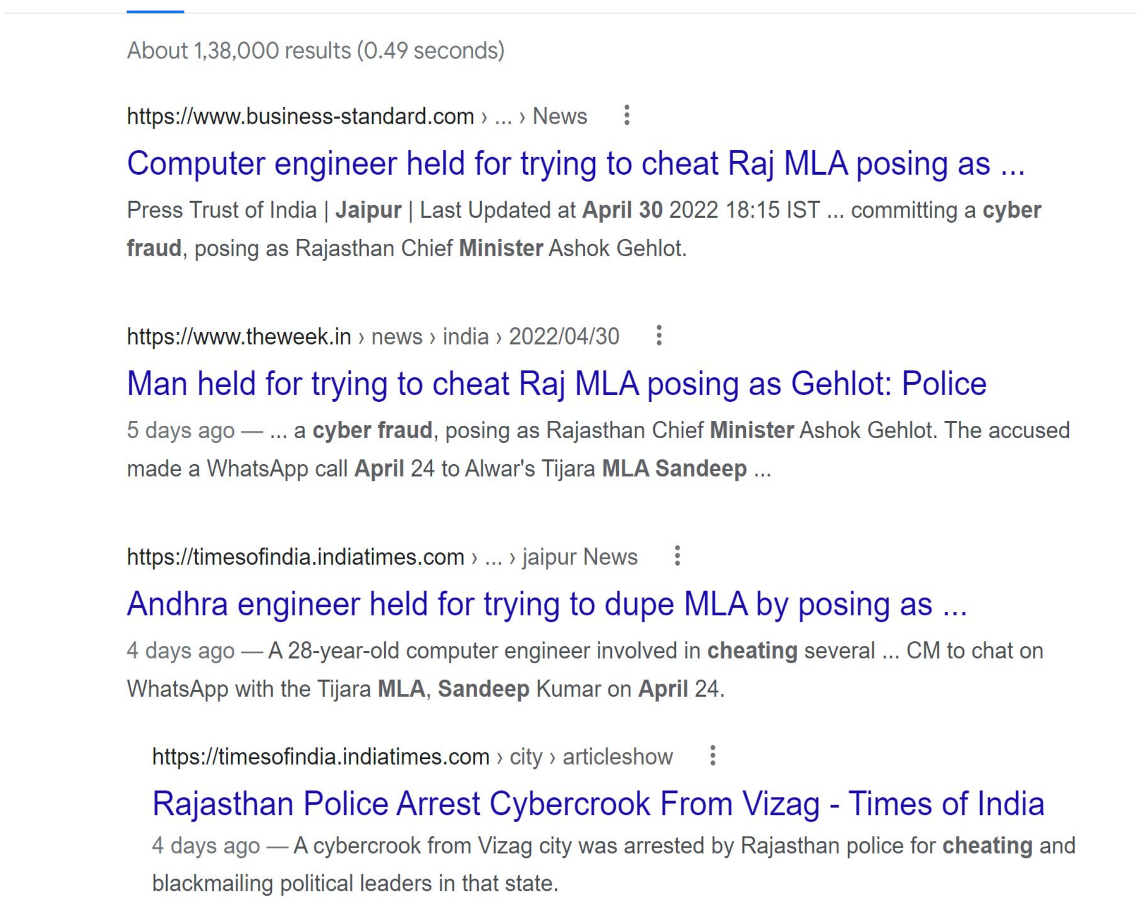
9:50 am



+1 (206) 304-2917 >

Text Message
Today 8:55 AM

[redacted], urgent notification regarding the USPS delivery S46K5 from 04/04/2020. Go to: m9sxv.info/IbJOnVq6Ft



About 1,38,000 results (0.49 seconds)

https://www.business-standard.com › ... › News

Computer engineer held for trying to cheat Raj MLA posing as ...

Press Trust of India | **Jaipur** | Last Updated at **April 30** 2022 18:15 IST ... committing a **cyber fraud**, posing as Rajasthan Chief **Minister** Ashok Gehlot.

https://www.theweek.in › news › india › 2022/04/30

Man held for trying to cheat Raj MLA posing as Gehlot: Police

5 days ago — ... a **cyber fraud**, posing as Rajasthan Chief **Minister** Ashok Gehlot. The accused made a WhatsApp call **April** 24 to Alwar's Tijara **MLA Sandeep** ...

https://timesofindia.indiatimes.com › ... › jaipur News

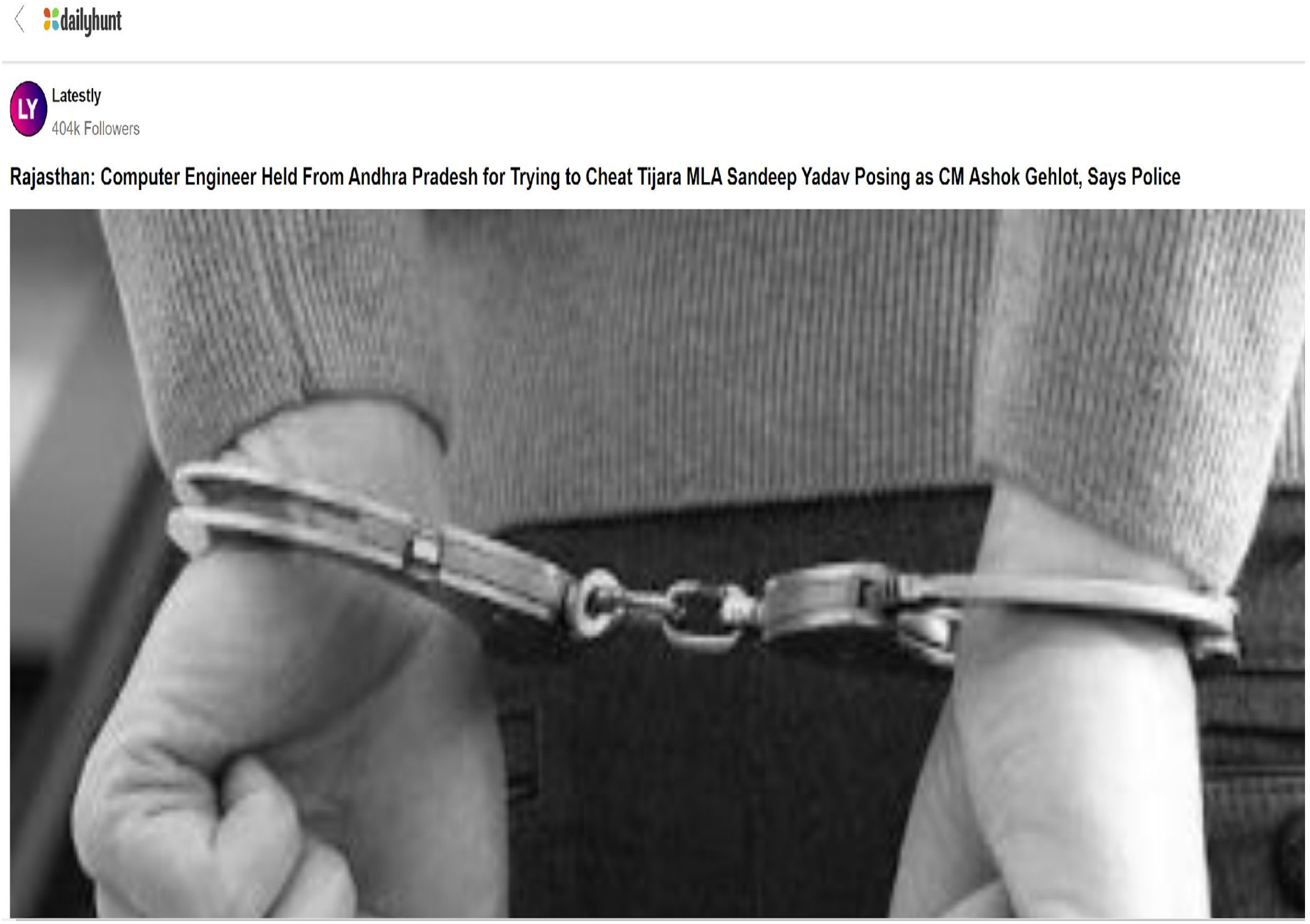
Andhra engineer held for trying to dupe MLA by posing as ...

4 days ago — A 28-year-old computer engineer involved in **cheating** several ... CM to chat on WhatsApp with the Tijara **MLA**, **Sandeep** Kumar on **April** 24.

https://timesofindia.indiatimes.com › city › articleshow

Rajasthan Police Arrest Cybercrook From Vizag - Times of India

4 days ago — A cybercrook from Vizag city was arrested by Rajasthan police for **cheating** and blackmailing political leaders in that state.

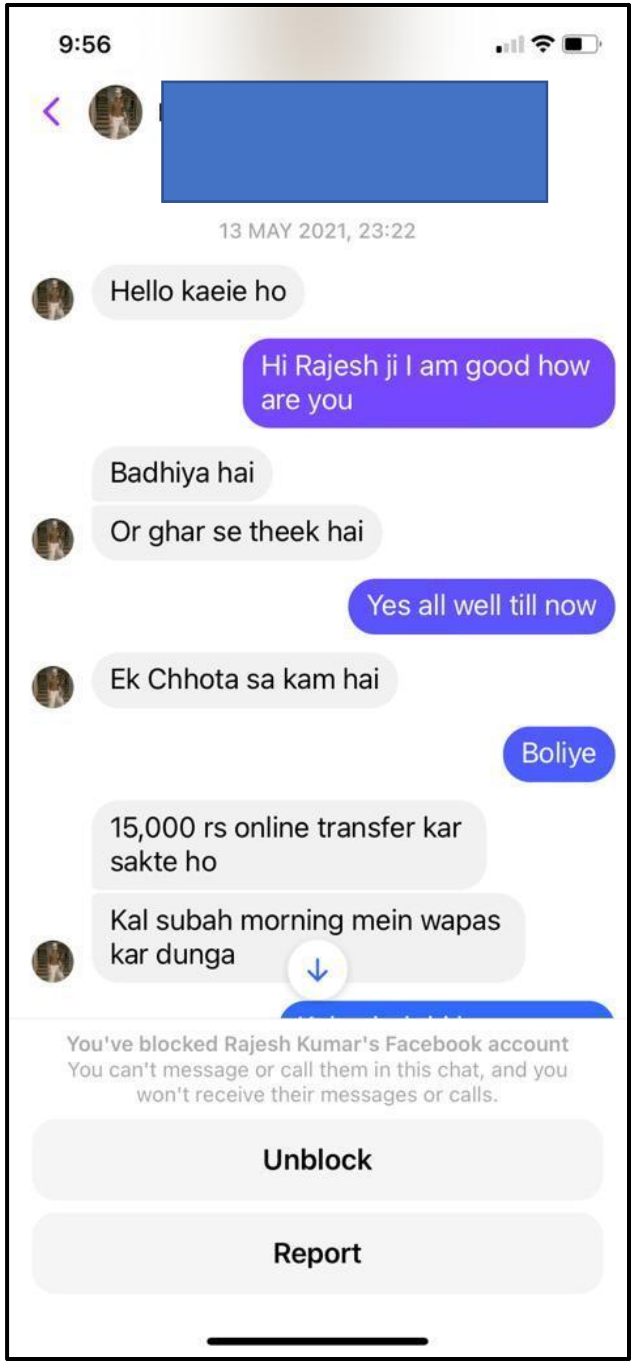


dailyhunt

Latestly
404k Followers

Rajasthan: Computer Engineer Held From Andhra Pradesh for Trying to Cheat Tijara MLA Sandeep Yadav Posing as CM Ashok Gehlot, Says Police

- On April 30 in Jaipur A 28 year old computer engineer caught for the vishing fraud. He asked for money transfer from Tijara MLA posing as Rajasthan Chief Minister Ashok Gehlot through virtual number.
- With a profile picture of Gehlot family on the whatsapp account he had a brief chat with the MLA and asked 30000 rupees to transfer thru Google Pay.
- On suspicion MLA asked Chief Minister and enquired about the number.
- Once it is clear case of cheating , bhiwadi police traced the number and arrested the accused after investigartion process from Vishakhapatnam.



[redacted]

13 MAY 2021, 23:22

Hello kaeie ho

Hi Rajesh ji I am good how are you

Badhiya hai

Or ghar se theek hai

Yes all well till now

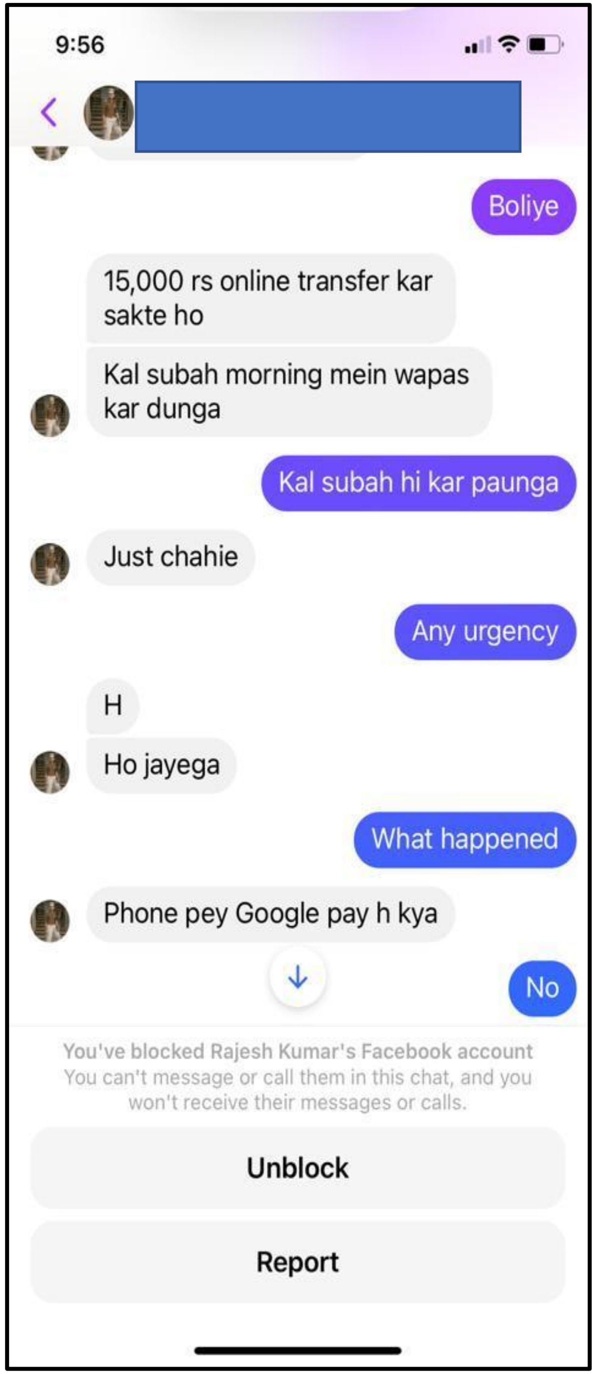
Ek Chhota sa kam hai

Boliye

15,000 rs online transfer kar sakte ho

Kal subah morning mein wapas kar dunga

You've blocked Rajesh Kumar's Facebook account
You can't message or call them in this chat, and you won't receive their messages or calls.



[redacted]

Boliye

15,000 rs online transfer kar sakte ho

Kal subah morning mein wapas kar dunga

Kal subah hi kar paunga

Just chahie

Any urgency

H

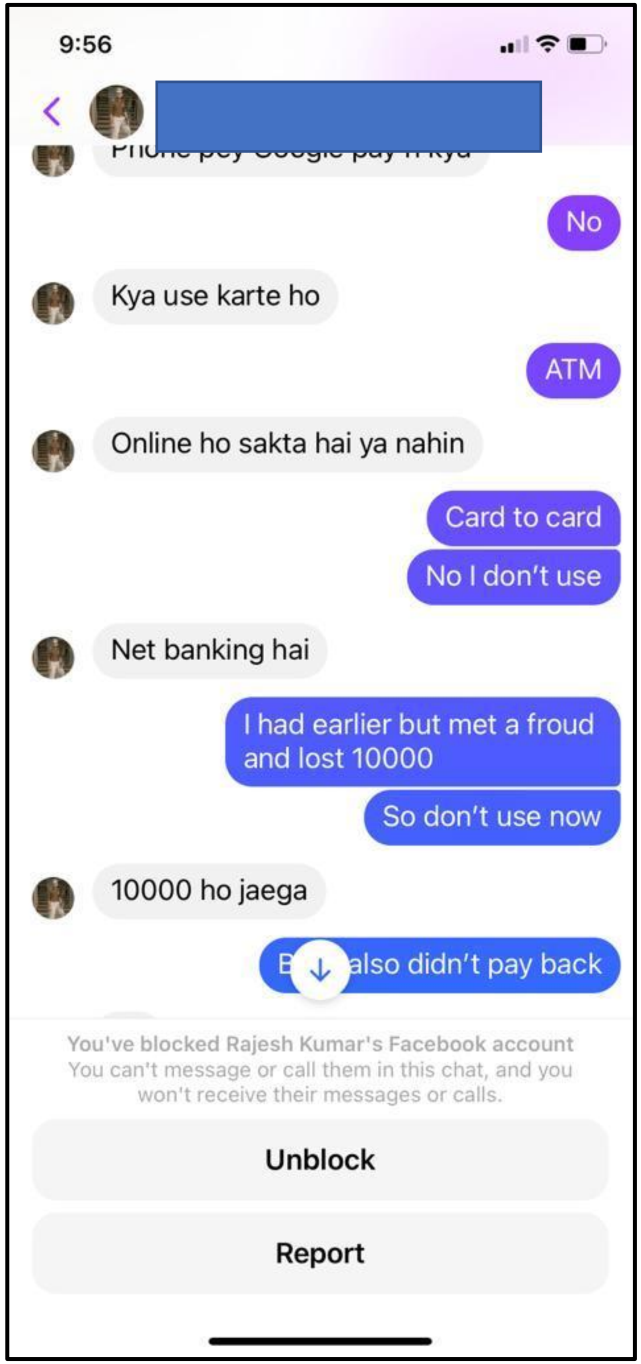
Ho jayega

What happened

Phone pey Google pay h kya

No

You've blocked Rajesh Kumar's Facebook account
You can't message or call them in this chat, and you won't receive their messages or calls.



[redacted]

Phone pey Google pay h kya

No

Kya use karte ho

ATM

Online ho sakta hai ya nahin

Card to card

No I don't use

Net banking hai

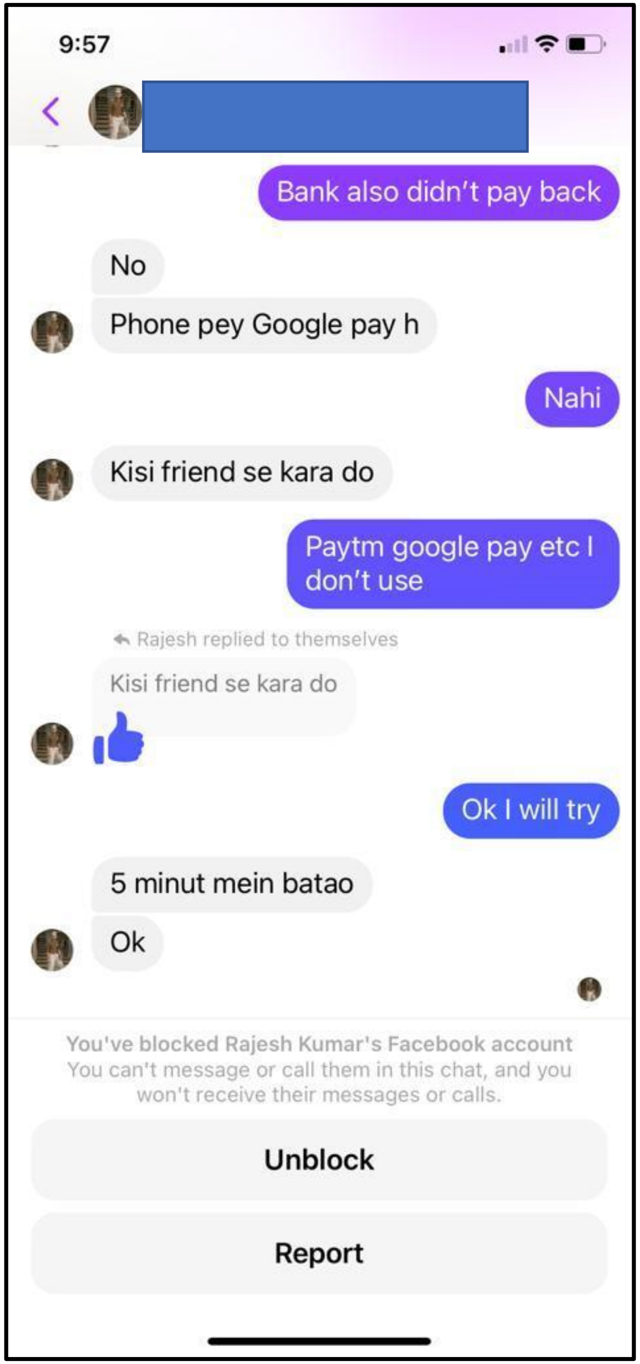
I had earlier but met a froud and lost 10000

So don't use now

10000 ho jaega

B also didn't pay back

You've blocked Rajesh Kumar's Facebook account
You can't message or call them in this chat, and you won't receive their messages or calls.



[redacted]

Bank also didn't pay back

No

Phone pey Google pay h

Nahi

Kisi friend se kara do

Paytm google pay etc I don't use

Rajesh replied to themselves

Kisi friend se kara do

👍

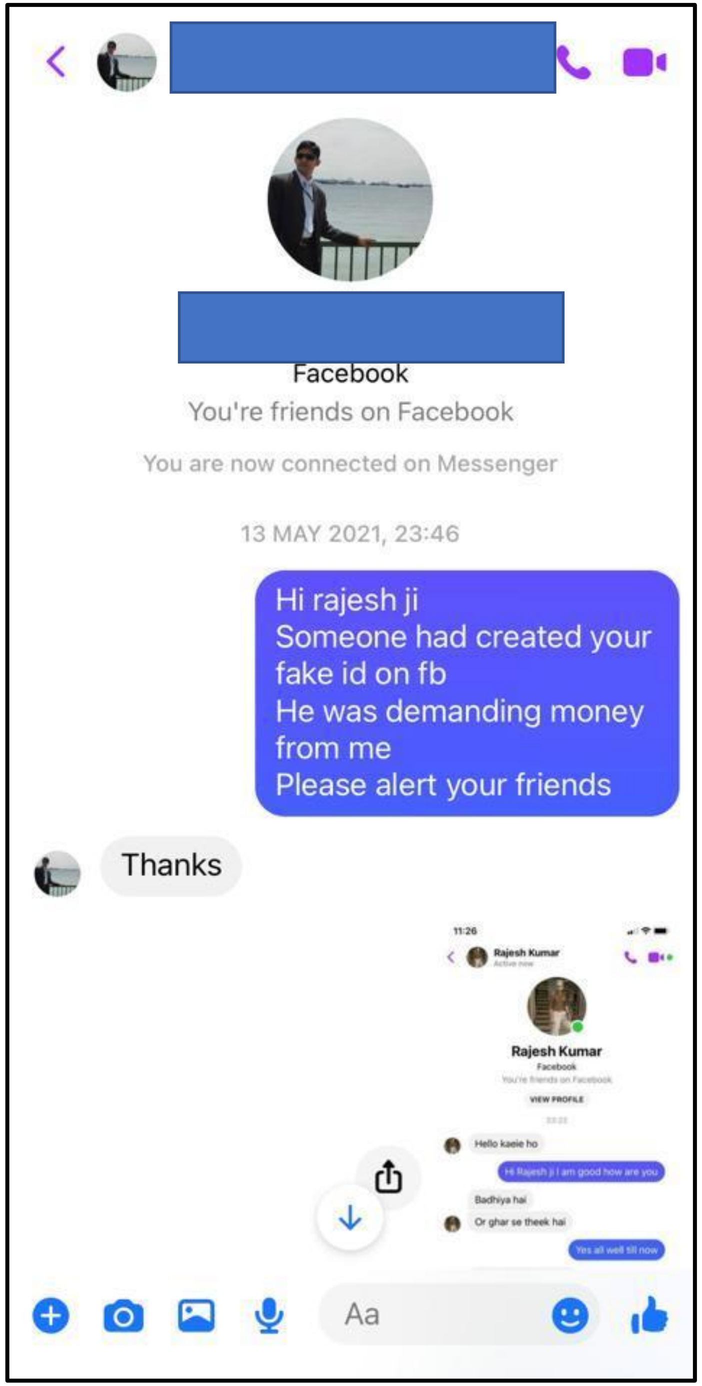
Ok I will try

5 minut mein batao

Ok

You've blocked Rajesh Kumar's Facebook account
You can't message or call them in this chat, and you won't receive their messages or calls.

Conversation with Actual person saved the victim



[redacted]

[redacted]

Facebook

You're friends on Facebook

You are now connected on Messenger

13 MAY 2021, 23:46

Hi rajesh ji
Someone had created your fake id on fb
He was demanding money from me
Please alert your friends

Thanks

11:26

Rajesh Kumar

Active now

Rajesh Kumar

Facebook

You're friends on Facebook

VIEW PROFILE

Hello kaeie ho

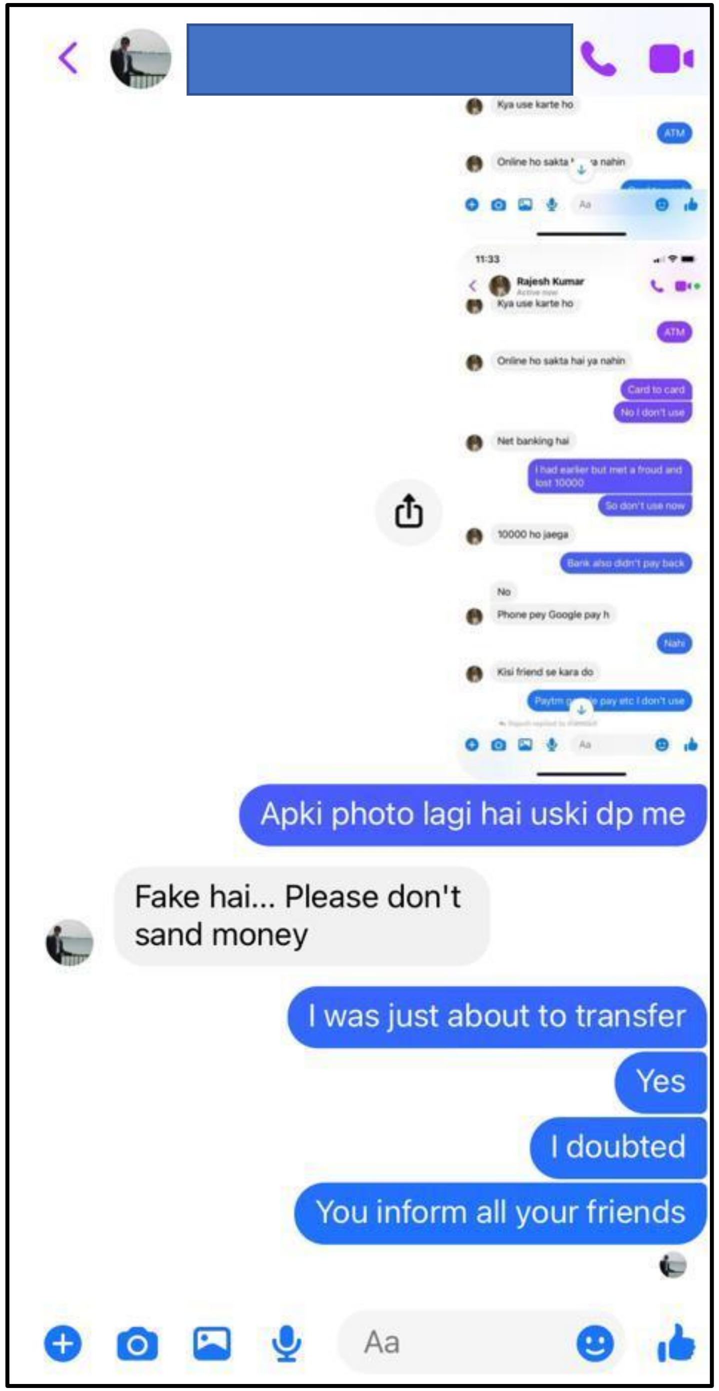
Hi Rajesh ji I am good how are you

Badhiya hai

Or ghar se theek hai

Yes all well till now

Aa



[redacted]

Kya use karte ho

ATM

Online ho sakta h[illegible]a nahin

Aa

11:33

Rajesh Kumar

Active now

Kya use karte ho

ATM

Online ho sakta hai ya nahin

Card to card

No I don't use

Net banking hai

I had earlier but met a froud and lost 10000

So don't use now

10000 ho jaega

Bank also didn't pay back

No

Phone pey Google pay h

Nahi

Kisi friend se kara do

Paytm g[illegible]e pay etc I don't use

Aa

Apki photo lagi hai uski dp me

Fake hai... Please don't sand money

I was just about to transfer

Yes

I doubted

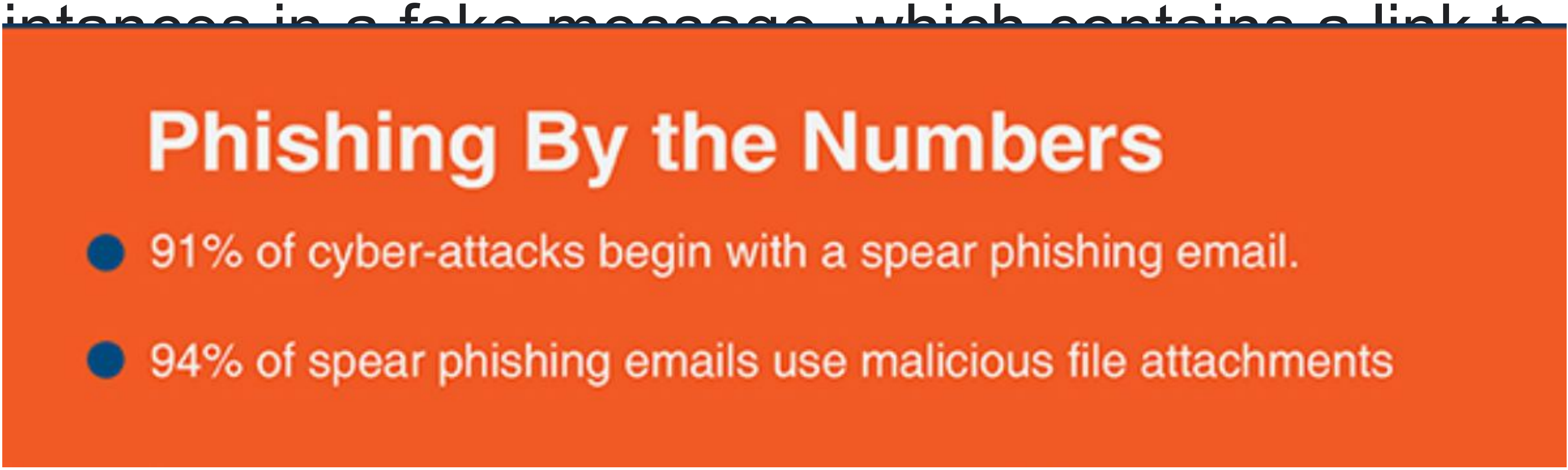
You inform all your friends

Aa

Phishing

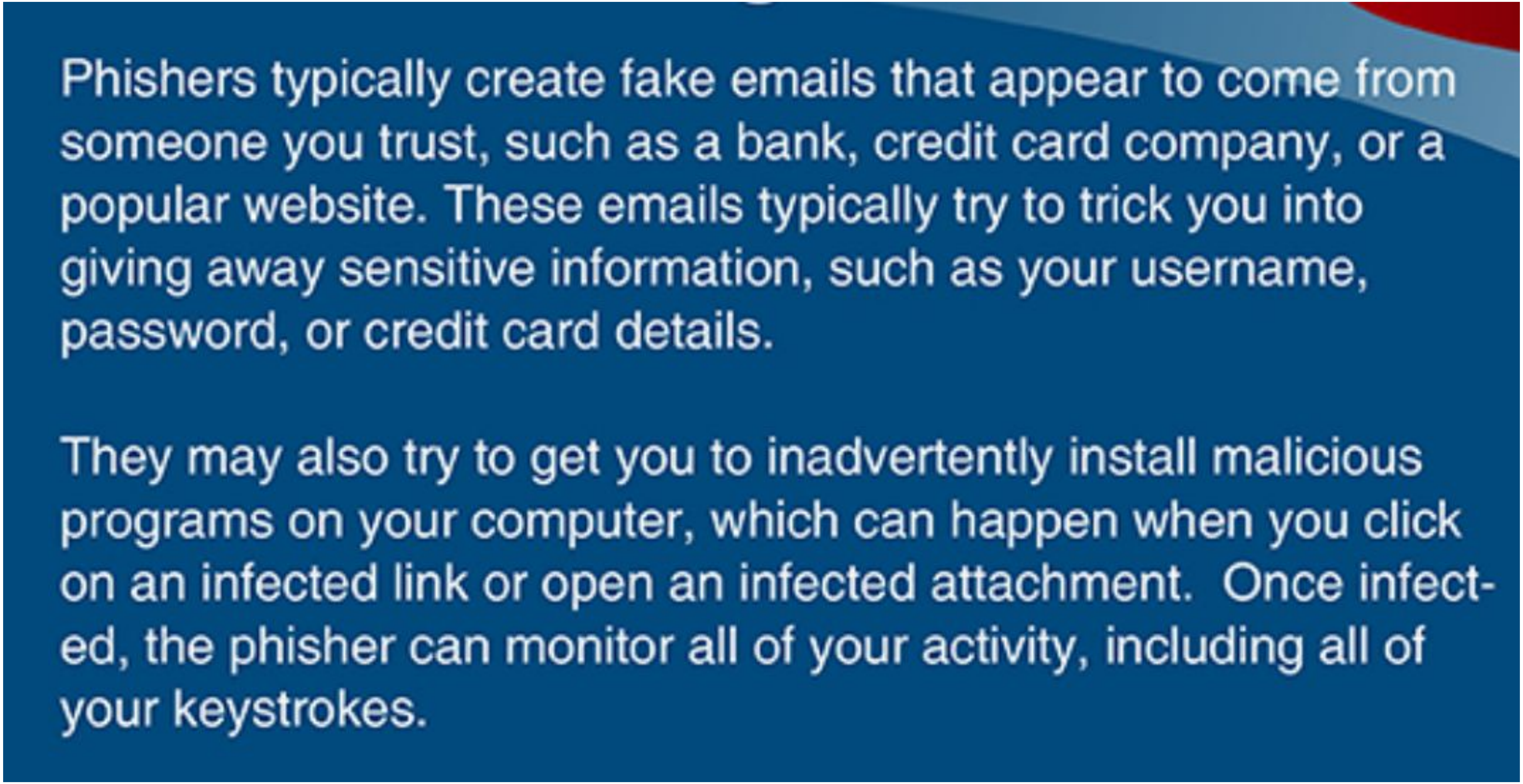
Phishing

- Phishing is an attack that attempts to steal your money, or your identity, by getting you to reveal personal information -- such as credit card numbers, bank information, or passwords -- on websites that pretend to be legitimate.
- Cybercriminals typically pretend to be reputable companies, friends, or acqua[illegible] a phishing



Phishing By the Numbers

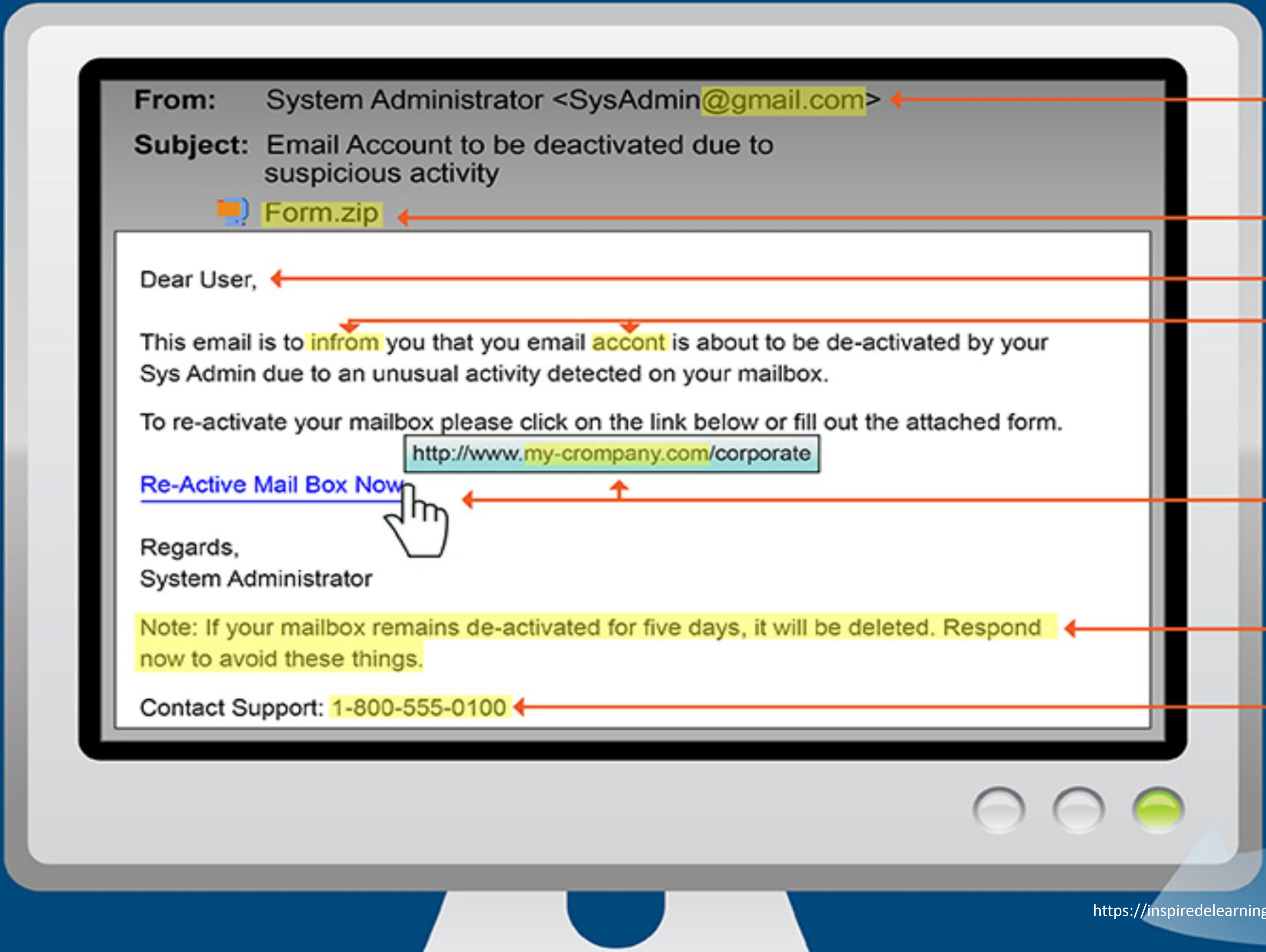
- 91% of cyber-attacks begin with a spear phishing email.
- 94% of spear phishing emails use malicious file attachments



Phishers typically create fake emails that appear to come from someone you trust, such as a bank, credit card company, or a popular website. These emails typically try to trick you into giving away sensitive information, such as your username, password, or credit card details.

They may also try to get you to inadvertently install malicious programs on your computer, which can happen when you click on an infected link or open an infected attachment. Once infected, the phisher can monitor all of your activity, including all of your keystrokes.

The Anatomy of a Phishing Email



From: System Administrator <SysAdmin@gmail.com>

Subject: Email Account to be deactivated due to suspicious activity

Form.zip

Dear User,

This email is to infrom you that you email accont is about to be de-activated by your Sys Admin due to an unusual activity detected on your mailbox.

To re-activate your mailbox please click on the link below or fill out the attached form.

http://www.my-crompany.com/corporate

Re-Active Mail Box Now

Regards,
System Administrator

Note: If your mailbox remains de-activated for five days, it will be deleted. Respond now to avoid these things.

Contact Support: 1-800-555-0100

1 Emails sent from public email addresses.

2 Unsolicited attachments.

3 Generic greetings.

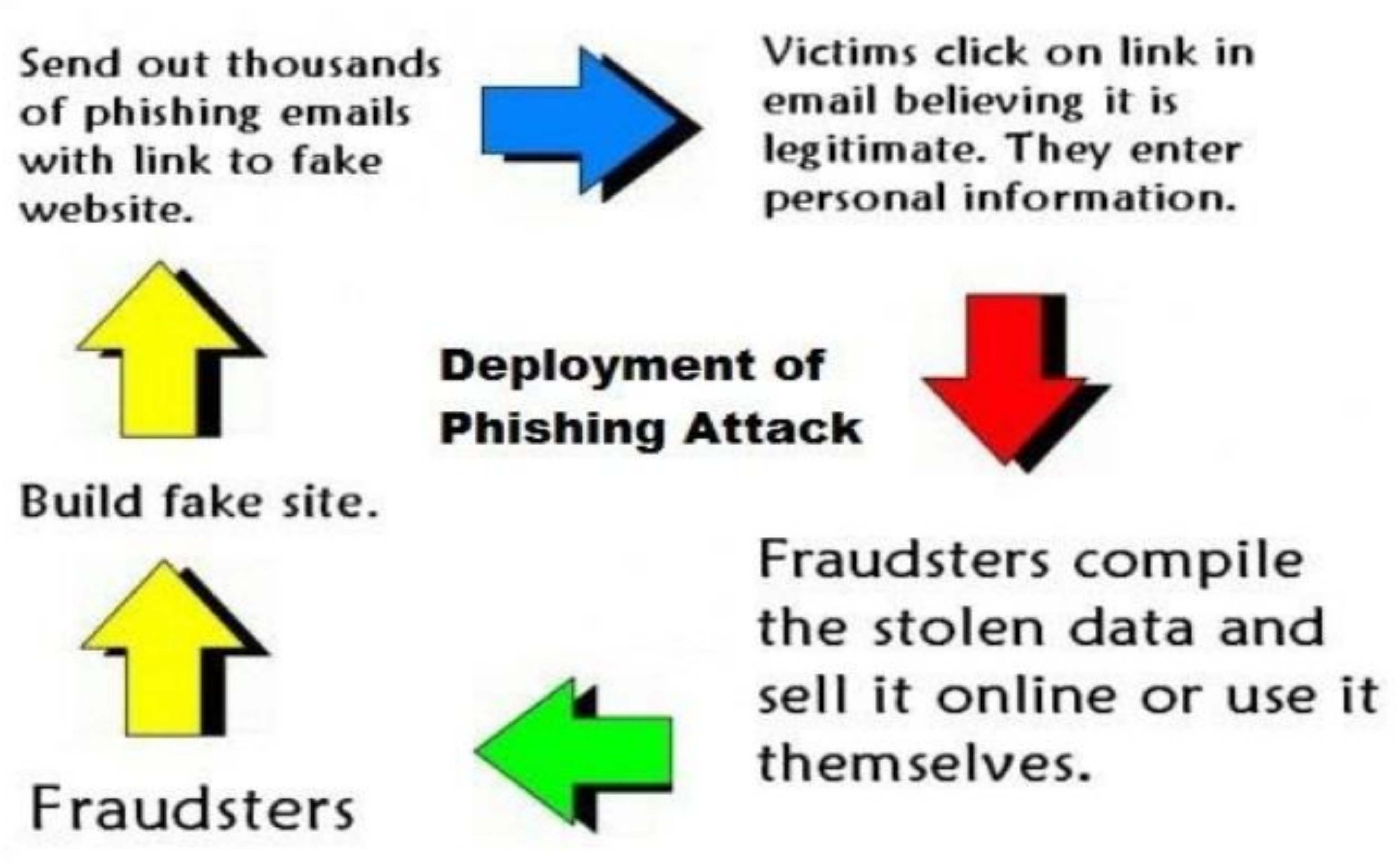
4 Spelling and grammar mistakes.

5 Links to unrecognized sites or slightly misspelled sites.

6 Threats or enticements that create a sense of urgency.

7 Toll free numbers in suspicious emails that do not match known numbers.

https://inspiredelearning.com/blog/phishing-infographic-how-to-detect-a-phishing-email/



Send out thousands of phishing emails with link to fake website.

Victims click on link in email believing it is legitimate. They enter personal information.

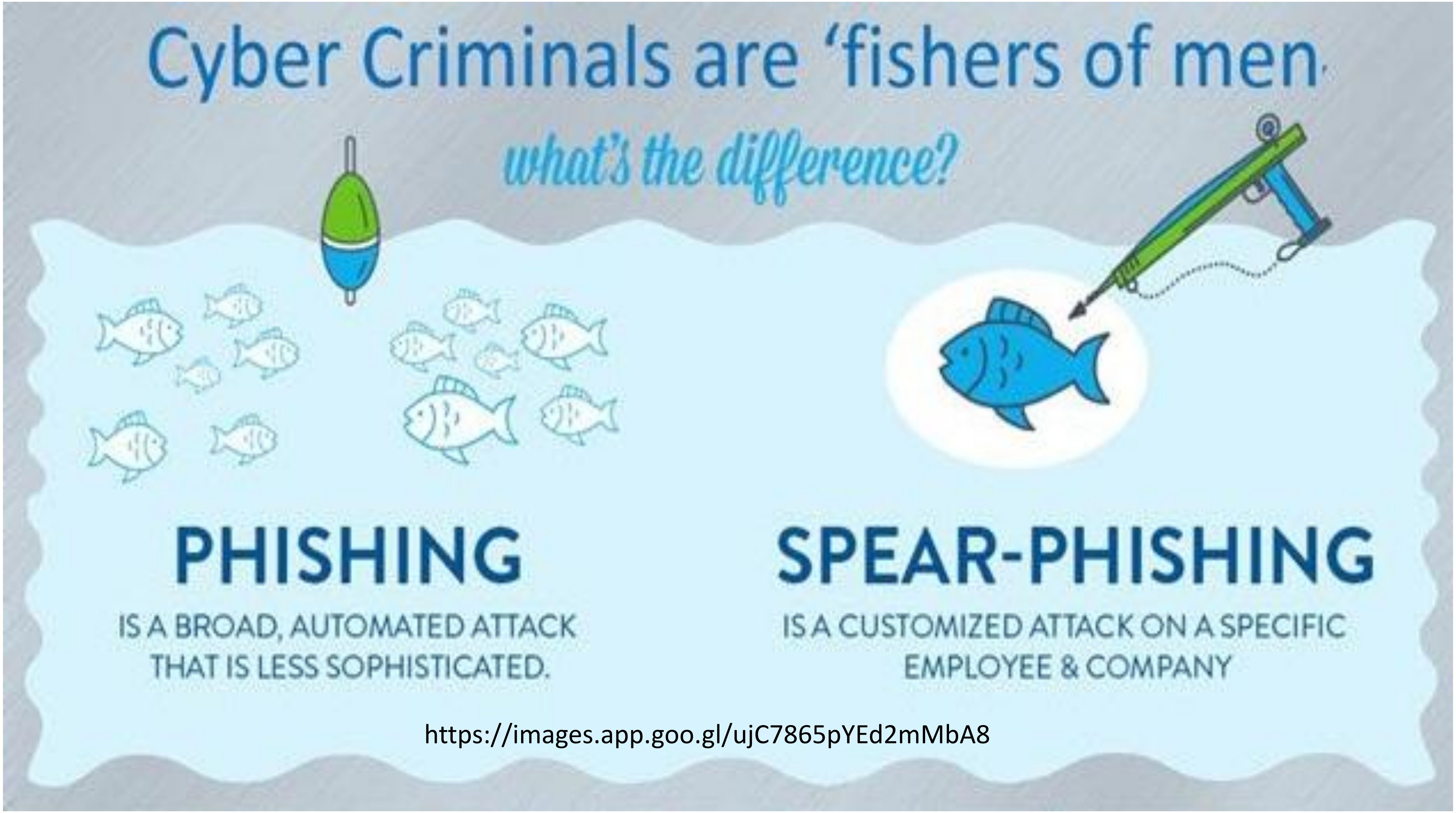
Deployment of Phishing Attack

Build fake site.

Fraudsters compile the stolen data and sell it online or use it themselves.

Fraudsters

https://www.kratikal.com/blog/understanding-the-difference-between-spear-phishing-and-phishing/



Cyber Criminals are 'fishers of men

what's the difference?

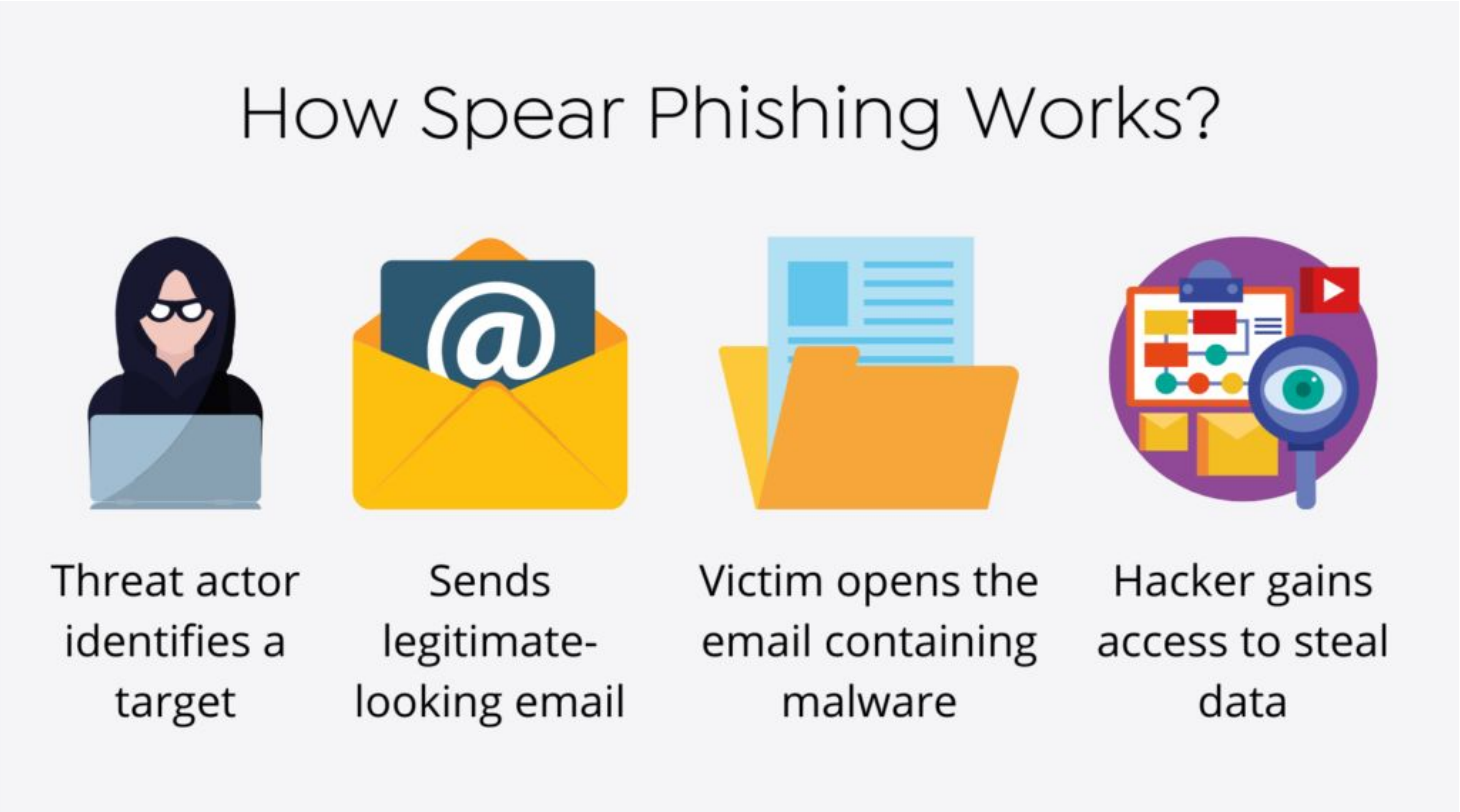
PHISHING

IS A BROAD, AUTOMATED ATTACK THAT IS LESS SOPHISTICATED.

SPEAR-PHISHING

IS A CUSTOMIZED ATTACK ON A SPECIFIC EMPLOYEE & COMPANY

https://images.app.goo.gl/ujC7865pYEd2mMbA8



How Spear Phishing Works?

Threat actor identifies a target

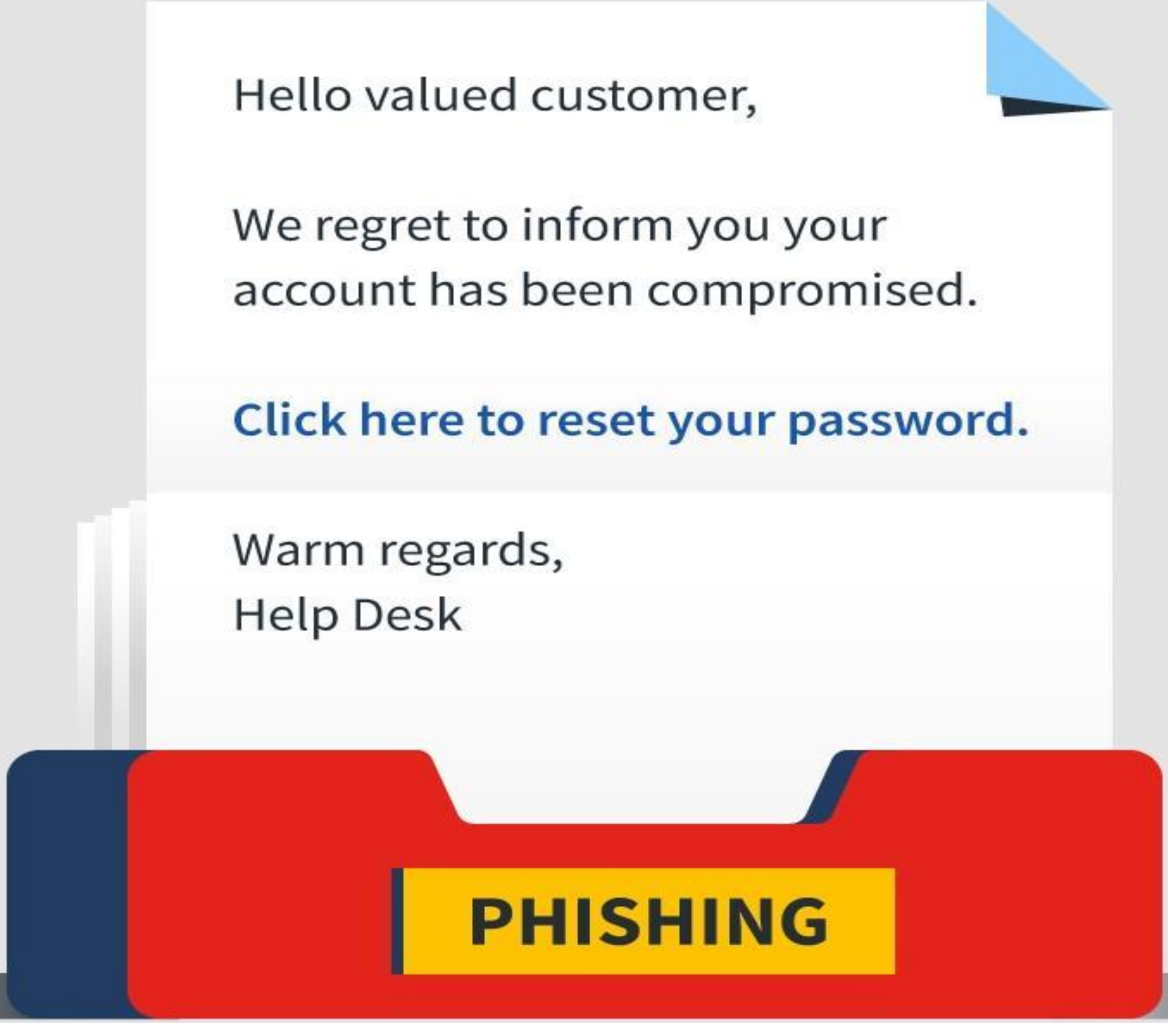
Sends legitimate-looking email

Victim opens the email containing malware

Hacker gains access to steal data

https://socradar.io/how-to-identify-spear-phishing/

Spear Phishing vs. Phishing Emails

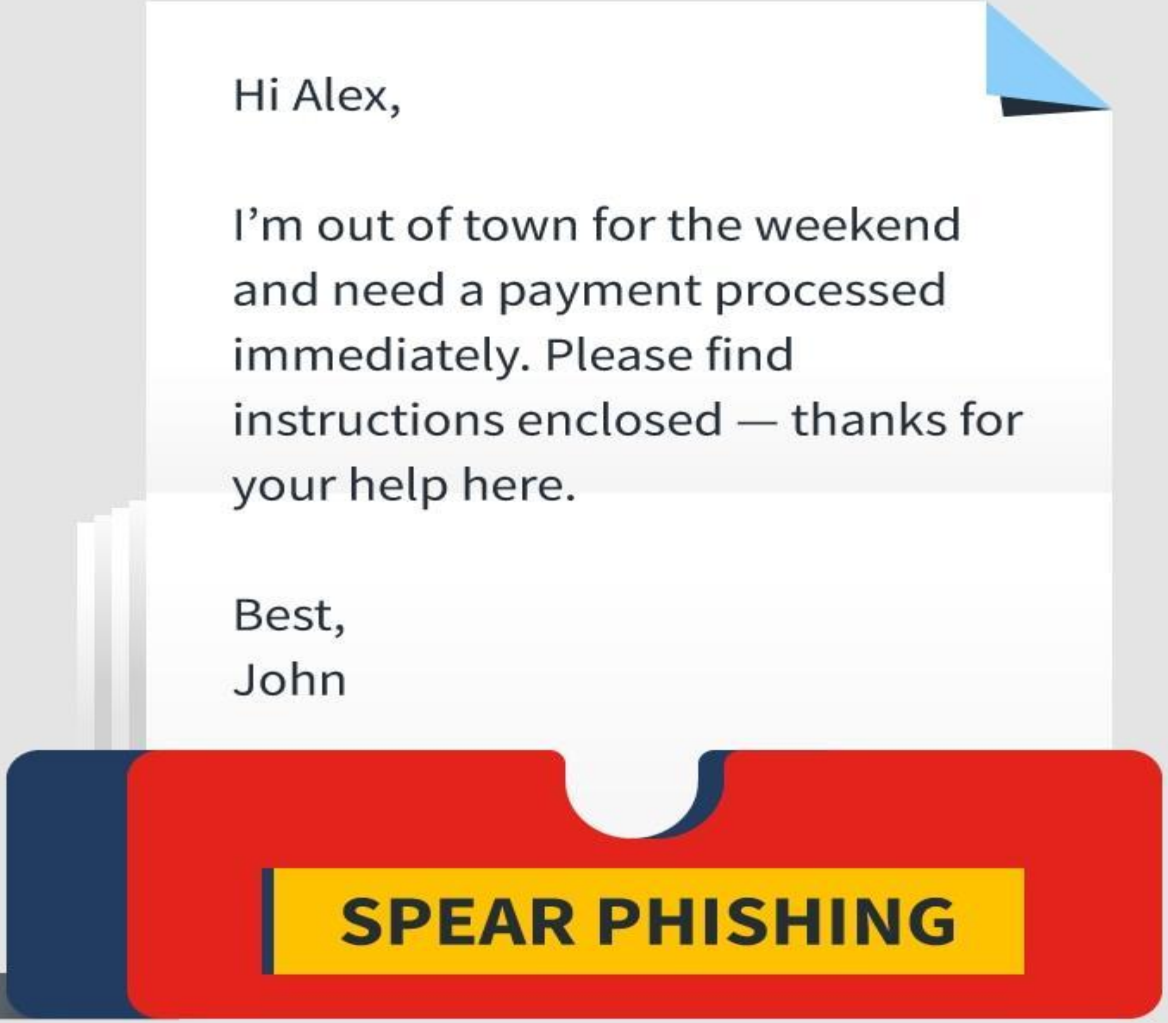


Hello valued customer,

We regret to inform you your account has been compromised.

Click here to reset your password.

Warm regards,
Help Desk



Hi Alex,

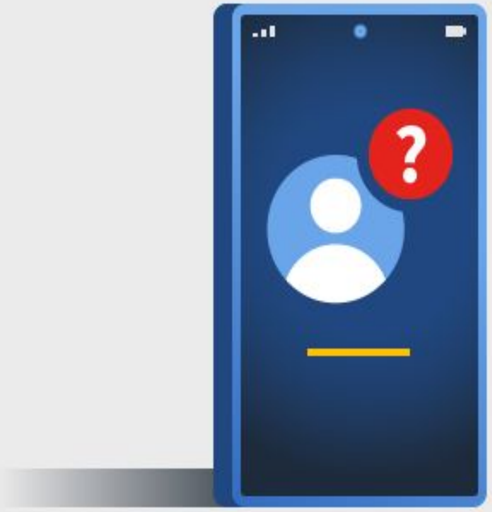
I'm out of town for the weekend and need a payment processed immediately. Please find instructions enclosed — thanks for your help here.

Best,
John

How to Identify a Spear Phishing Attack

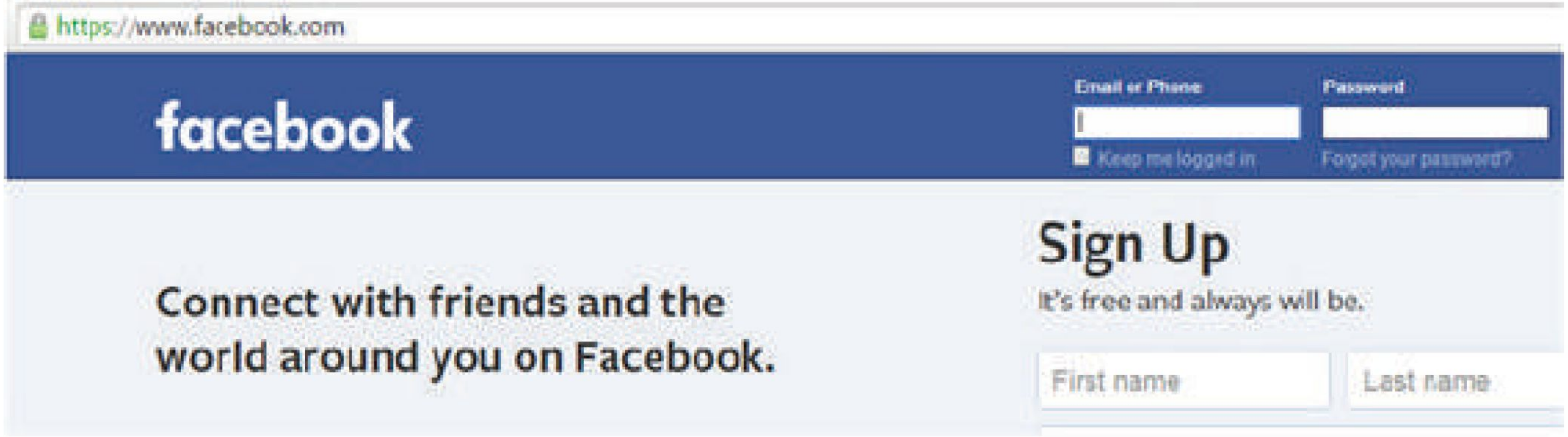
Verify the **sender's email address**

Verify the URL by hovering over it



Call or text the sender to verify

https://in.norton.com/internetsecurity-malware-what-spear-phishing.html

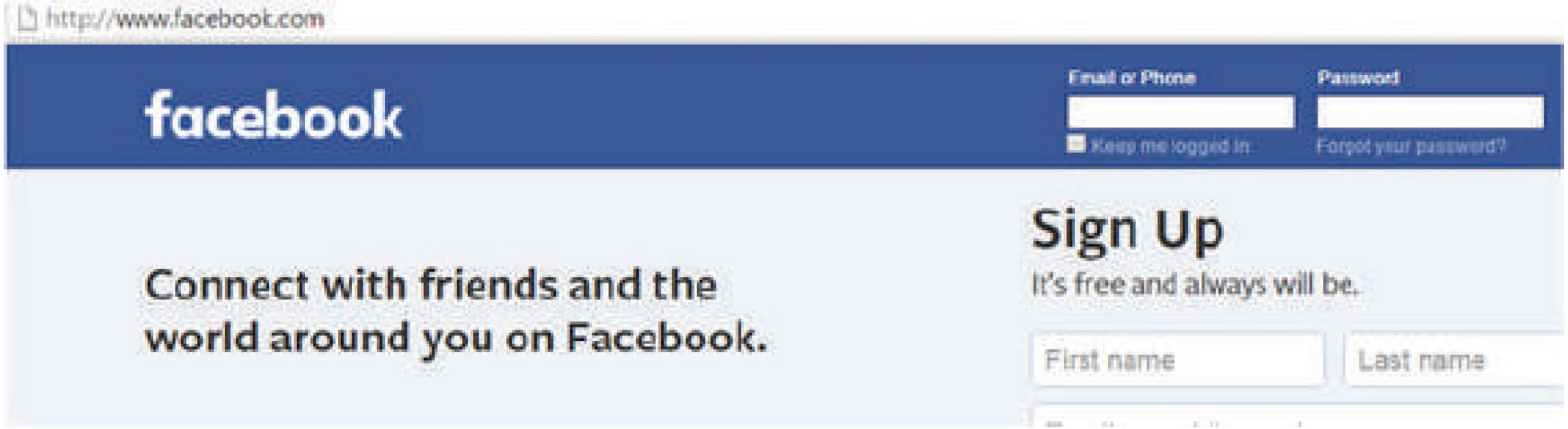


https://www.facebook.com

Connect with friends and the world around you on Facebook.

Sign Up

It's free and always will be.



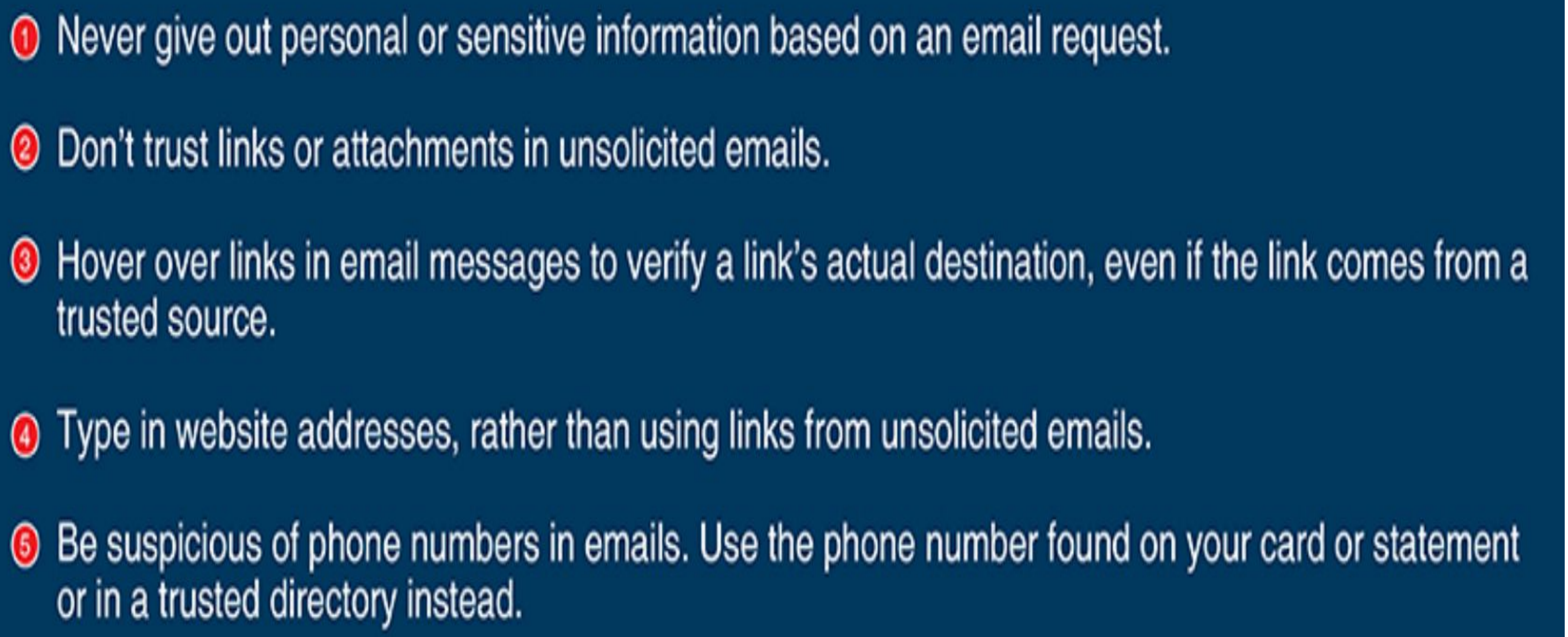
http://www.facebook.com

Connect with friends and the world around you on Facebook.

Sign Up

It's free and always will be.

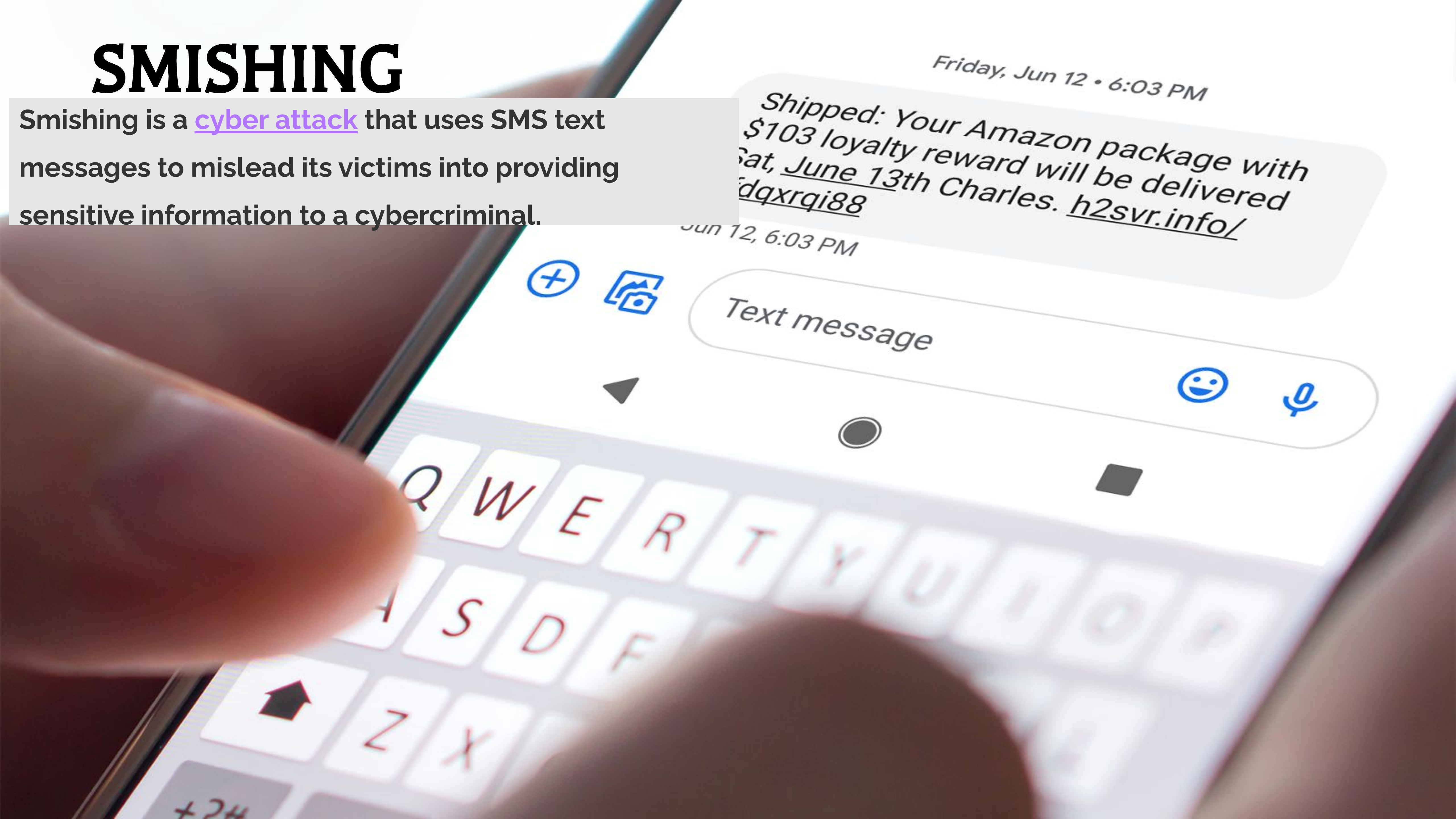
Prevention from Phishing



1. Never give out personal or sensitive information based on an email request.
2. Don’t trust links or attachments in unsolicited emails.
3. Hover over links in email messages to verify a link’s actual destination, even if the link comes from a trusted source.
4. Type in website addresses, rather than using links from unsolicited emails.
5. Be suspicious of phone numbers in emails. Use the phone number found on your card or statement or in a trusted directory instead.

SMISHING

Smishing is a cyber attack that uses SMS text messages to mislead its victims into providing sensitive information to a cybercriminal.

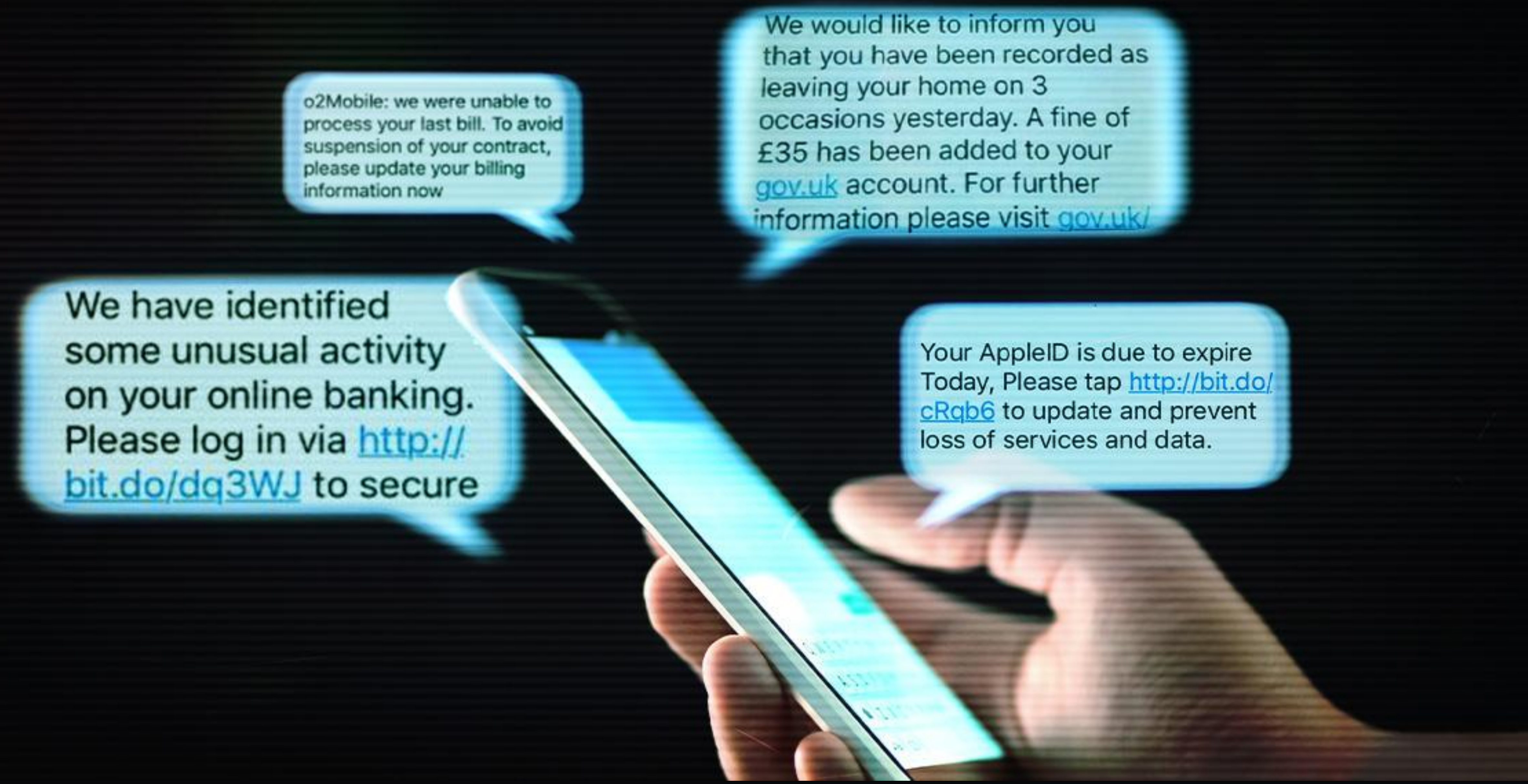


Friday, Jun 12 • 6:03 PM

Shipped: Your Amazon package with $103 loyalty reward will be delivered Sat, June 13th Charles. h2svr.info/dqxrqi88

Jun 12, 6:03 PM

Smishing Attacks



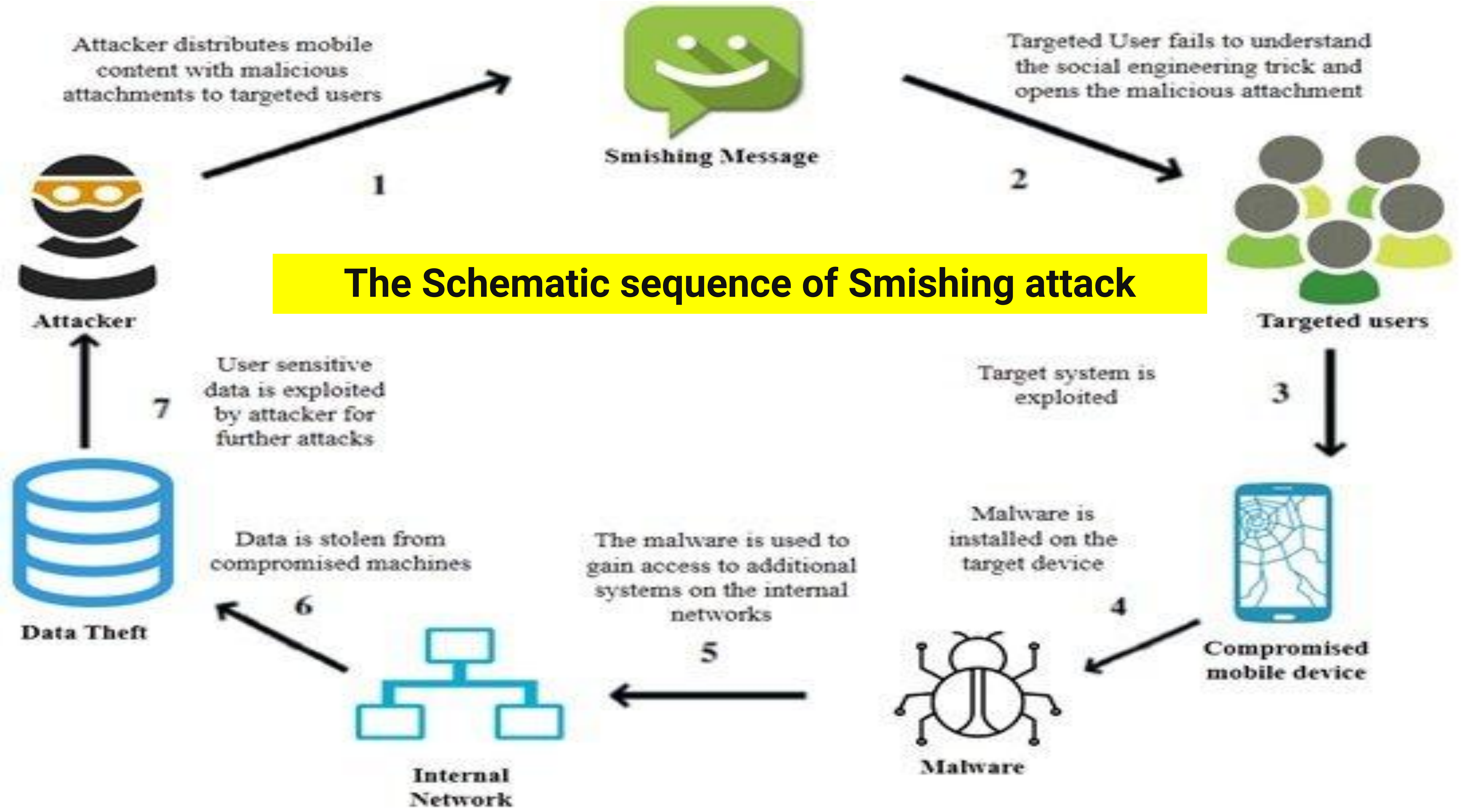
o2Mobile: we were unable to process your last bill. To avoid suspension of your contract, please update your billing information now

We would like to inform you that you have been recorded as leaving your home on 3 occasions yesterday. A fine of £35 has been added to your gov.uk account. For further information please visit gov.uk/

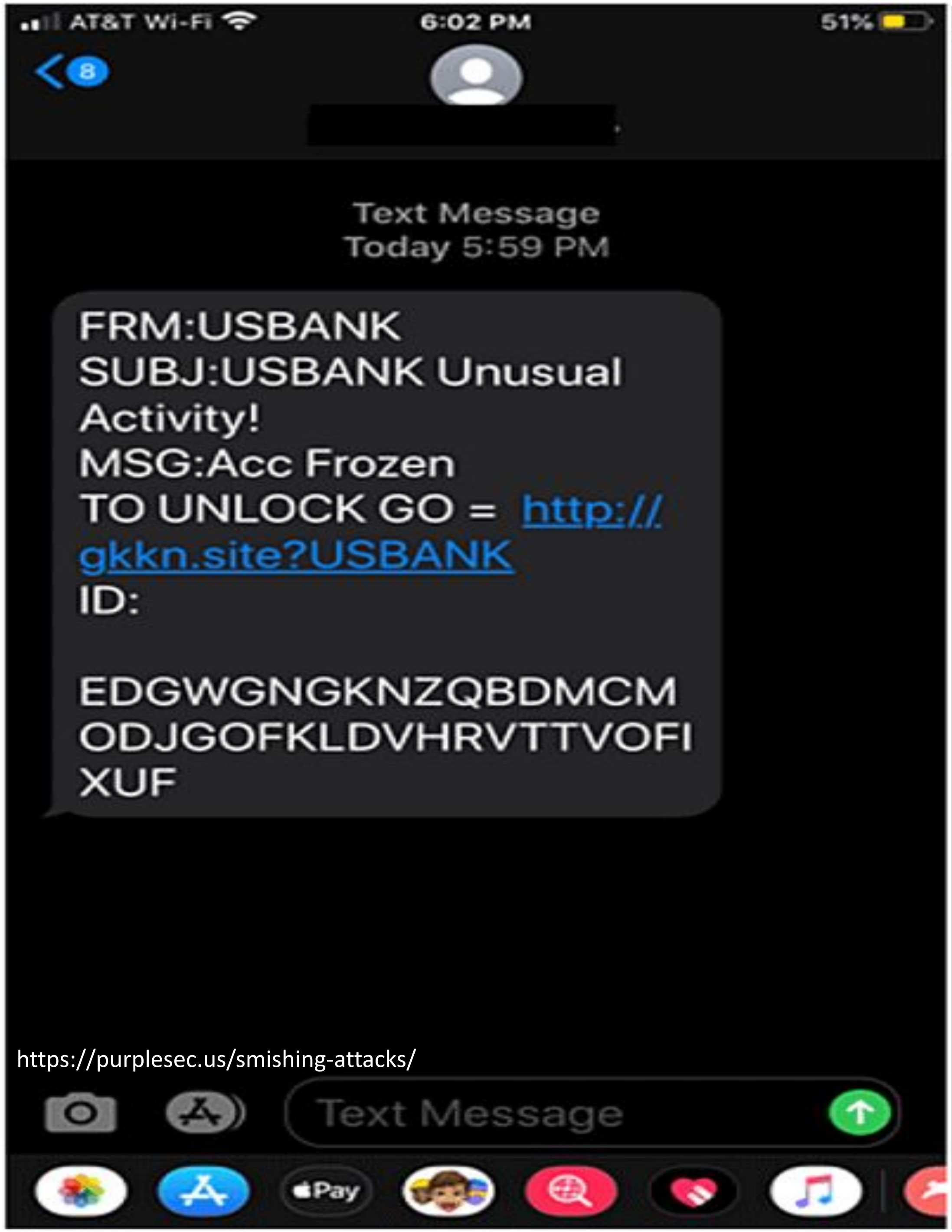
We have identified some unusual activity on your online banking. Please log in via http://bit.do/dq3WJ to secure

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

The Schematic sequence of Smishing attack


Attacker distributes mobile content with malicious attachments to targeted users
1
Smishing Message
Targeted User fails to understand the social engineering trick and opens the malicious attachment
2
Attacker
Targeted users
User sensitive data is exploited by attacker for further attacks
7
Target system is exploited
3
Malware is installed on the target device
Data is stolen from compromised machines
The malware is used to gain access to additional systems on the internal networks
6
4
Data Theft
5
Compromised mobile device
Internal Network
Malware

Priyadarshini, Ishaani. (2019). Introduction to Blockchain Technology. 10.1002/9781119488330.ch6.



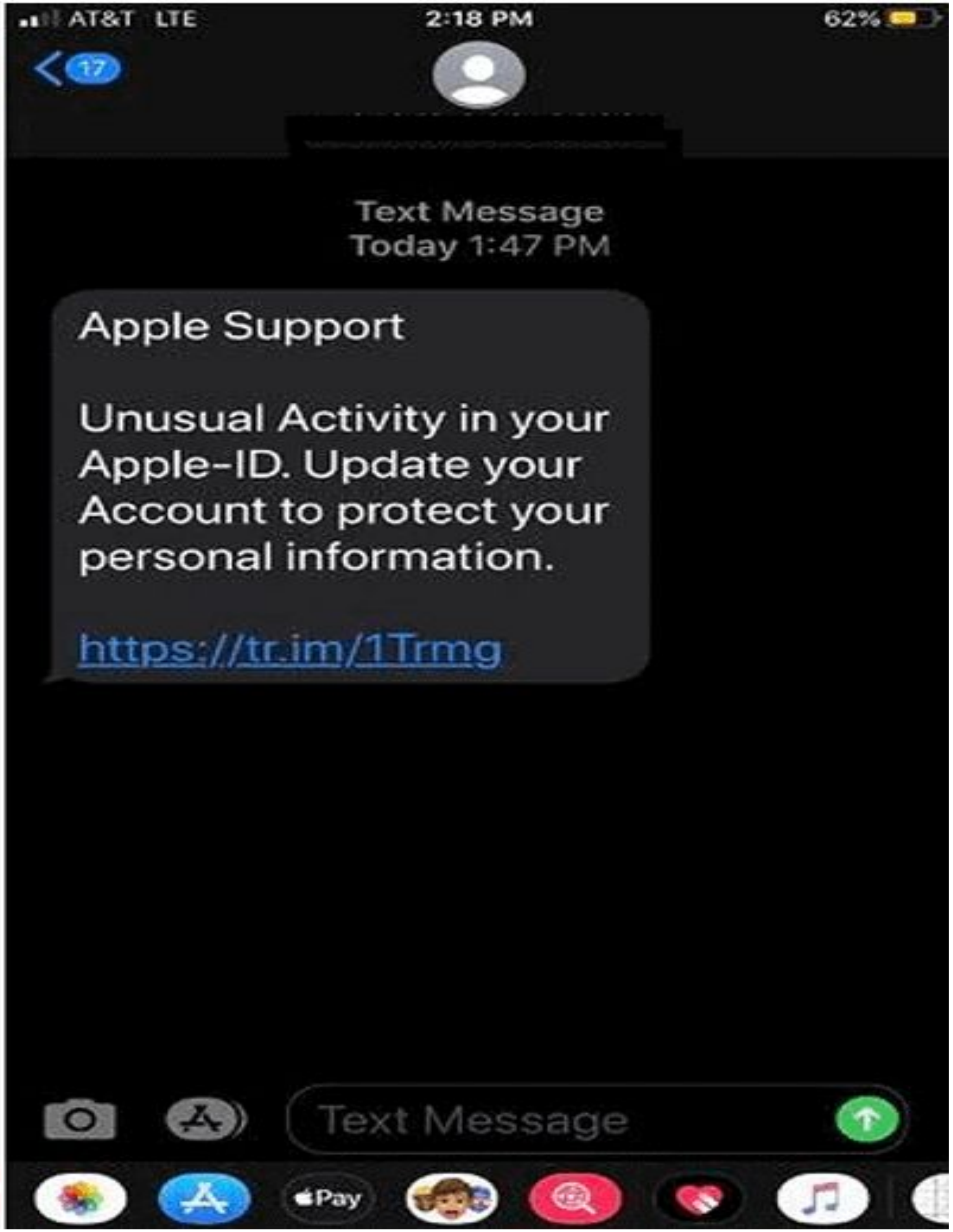
[redacted]

Text Message
Today 5:59 PM

FRM:USBANK
SUBJ:USBANK Unusual Activity!
MSG:Acc Frozen
TO UNLOCK GO = http://gkkn.site?USBANK
ID:

EDGWGNGKNZQBDMCMODJGOFKLDVHRVTTVOFIXUF

https://purplesec.us/smishing-attacks/



[redacted]

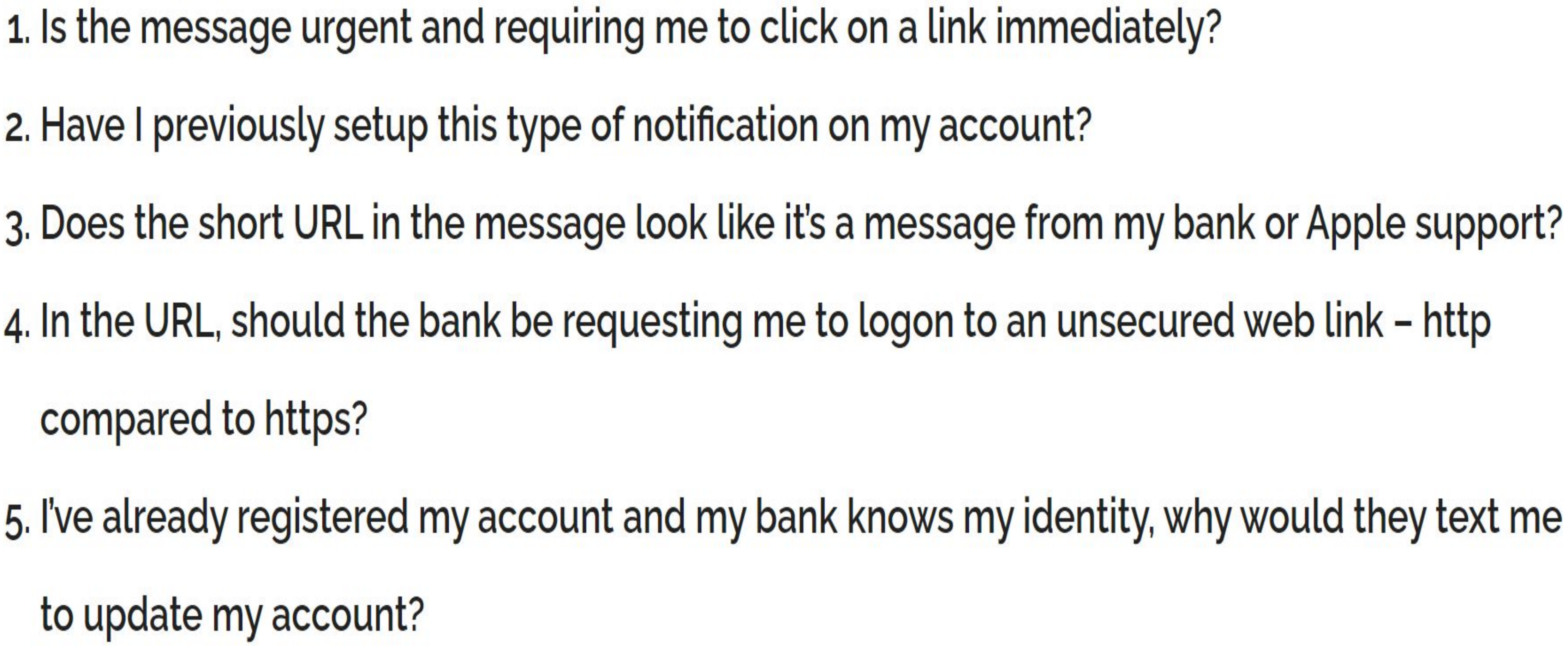
Text Message
Today 1:47 PM

Apple Support

Unusual Activity in your Apple-ID. Update your Account to protect your personal information.

https://tr.im/1Trmg

How to spot SMISHING attack?



1. Is the message urgent and requiring me to click on a link immediately?
2. Have I previously setup this type of notification on my account?
3. Does the short URL in the message look like it's a message from my bank or Apple support?
4. In the URL, should the bank be requesting me to logon to an unsecured web link – http compared to https?
5. I've already registered my account and my bank knows my identity, why would they text me to update my account?

Preventive tips - SMISHING attack

- Don’t respond to text messages that request private or financial information from you.
- If you get a message that appears to be from your bank, financial institution, or other entity that you do business with, contact that business directly to determine if they sent you a legitimate request. Review this entity’s policy on sending text messages to customers.
- Beware of messages that have a suspicious number in beginning or some other number that is not a cell number. Scammers often mask their identity by using email-to-text services to avoid revealing their actual phone number.
- If a text message is urging you to act or respond quickly, stop and think about it. Remember that criminals use this as a tactic to get you to do what they want.
- Never reply to a suspicious text message without doing your research and verifying the source. If your bank is really going to cancel your credit card, you should be able to call the number on the back of your card to discuss this matter with them.
- Never call a phone number from an unknown texter.

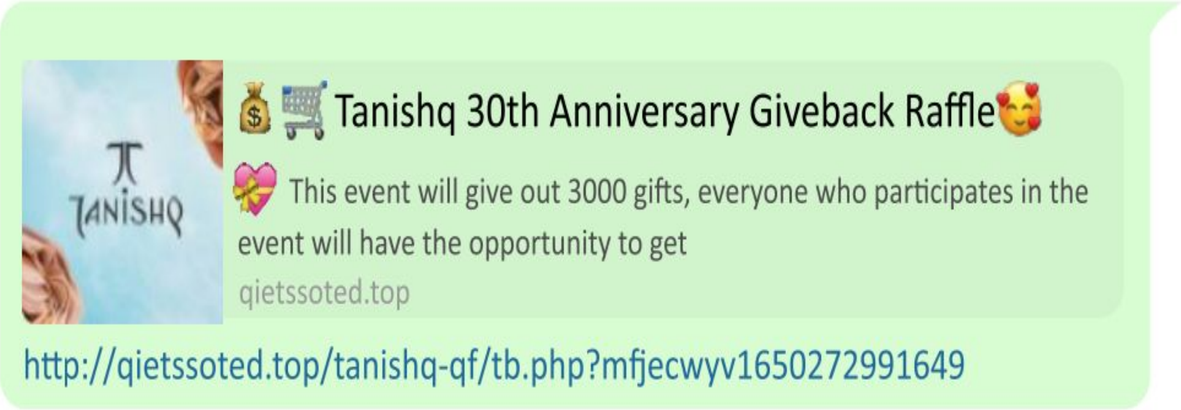
www.isea.gov.in

Fraud Alert

For more details visit : www.InfoSec awareness.in

Beware of 'Fake online offers'

Be aware of the fake links being circulated on social media platforms by fraudsters as bait to lure people. They make use of these links to gather critical user information to siphon money, hack accounts/passwords, infect devices, etc. Using the fake offer message as bait, they manage to convince people to forward it to a chain of people to victimize as many citizens as possible.



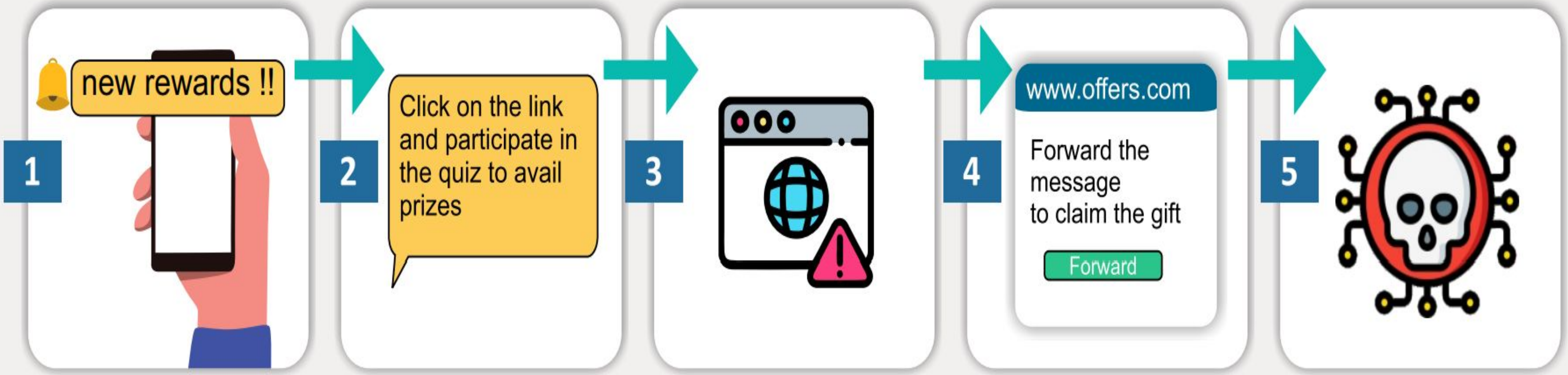
💰🛒 Tanishq 30th Anniversary Giveback Raffle🥰

💝 This event will give out 3000 gifts, everyone who participates in the event will have the opportunity to get

qietssoted.top

http://qietssoted.top/tanishq-qf/tb.php?mfjecwyv1650272991649

Modus Operandi


1
new rewards !!
2
Click on the link and participate in the quiz to avail prizes
3
4
www.offers.com
Forward the message to claim the gift
Forward
5

User receives messages / links/ posts of offers / gifts/rewards.

Prompts the user to click on the link or participate in Quiz/survey

Redirects the user to suspicious sites/links

Prompts to forward the message to a chain of people for claiming the gift

Leads to data leaks, malware/virus attacks, and cyber frauds

Warning Sings - Few pointers to spot the scam

- Tweaked website or email id of the sender
- No genuine website would ask you to share the link with your contacts
- Impersonalized / generic message/mail
- Messages with spelling & punctuation mistakes
- Requesting unrelated personal details
- Can sound too good to be true
- Fake reviews/ comments on the fake website links

Avoid searching for customer care numbers on google, as they can be misleading

Never believe the gift offers messages or emails circulated which are usually used as bait by cyber fraudsters

Immediately block the number and report against such fake offers

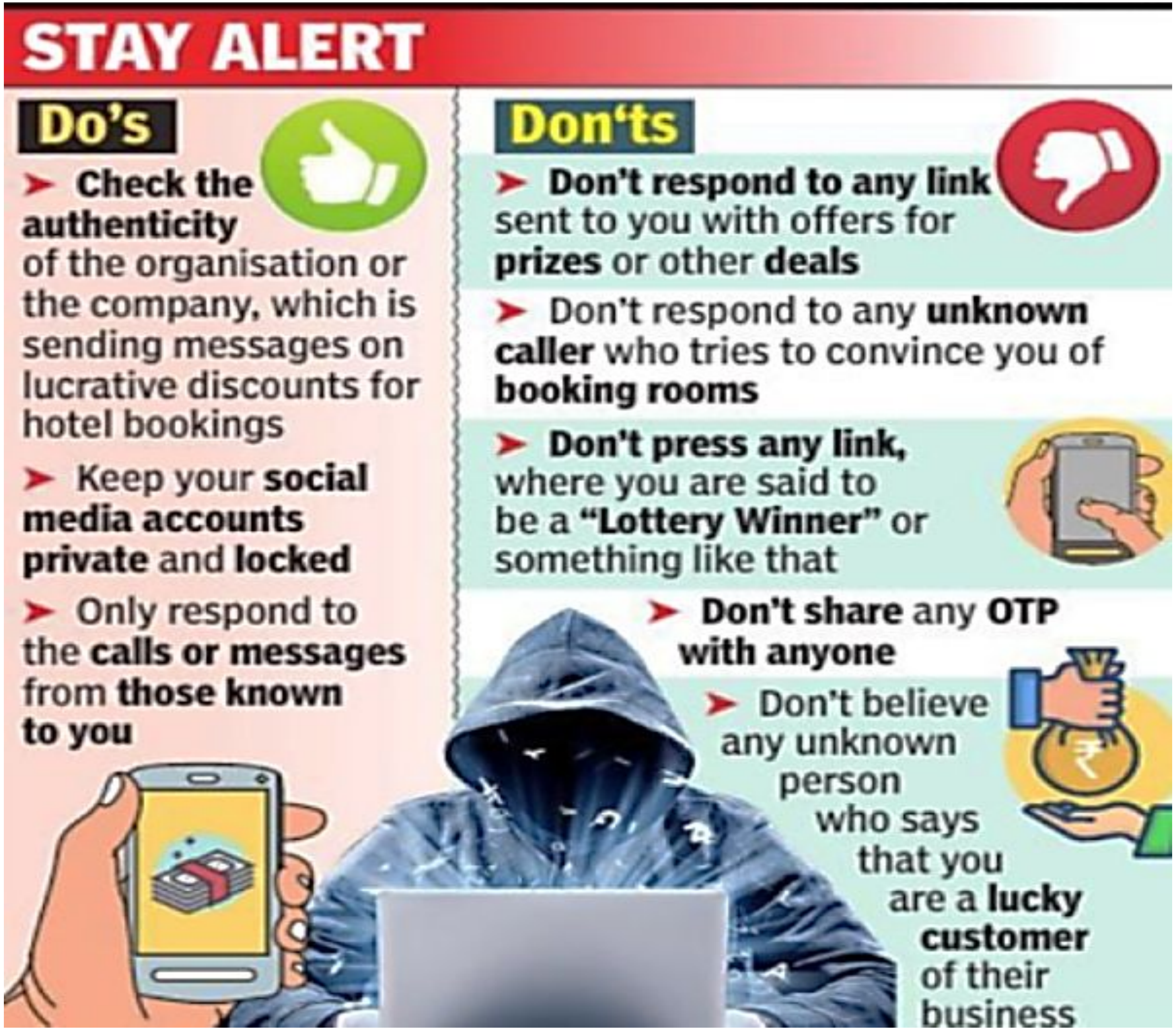
Only visit authorized/legitimate company/organization website for valid information

Never share your personal details or financial information like login credentials/passwords/credit or debit card details

Never click on unknown links or download unauthorized apps or software on your digital device s as it can install malicious software on your device.

Install anti-virus on your digital devices for security and protection.

Do not forward fake messages, links, or mails to people as prompted by senders without proper verification or authentication.



STAY ALERT

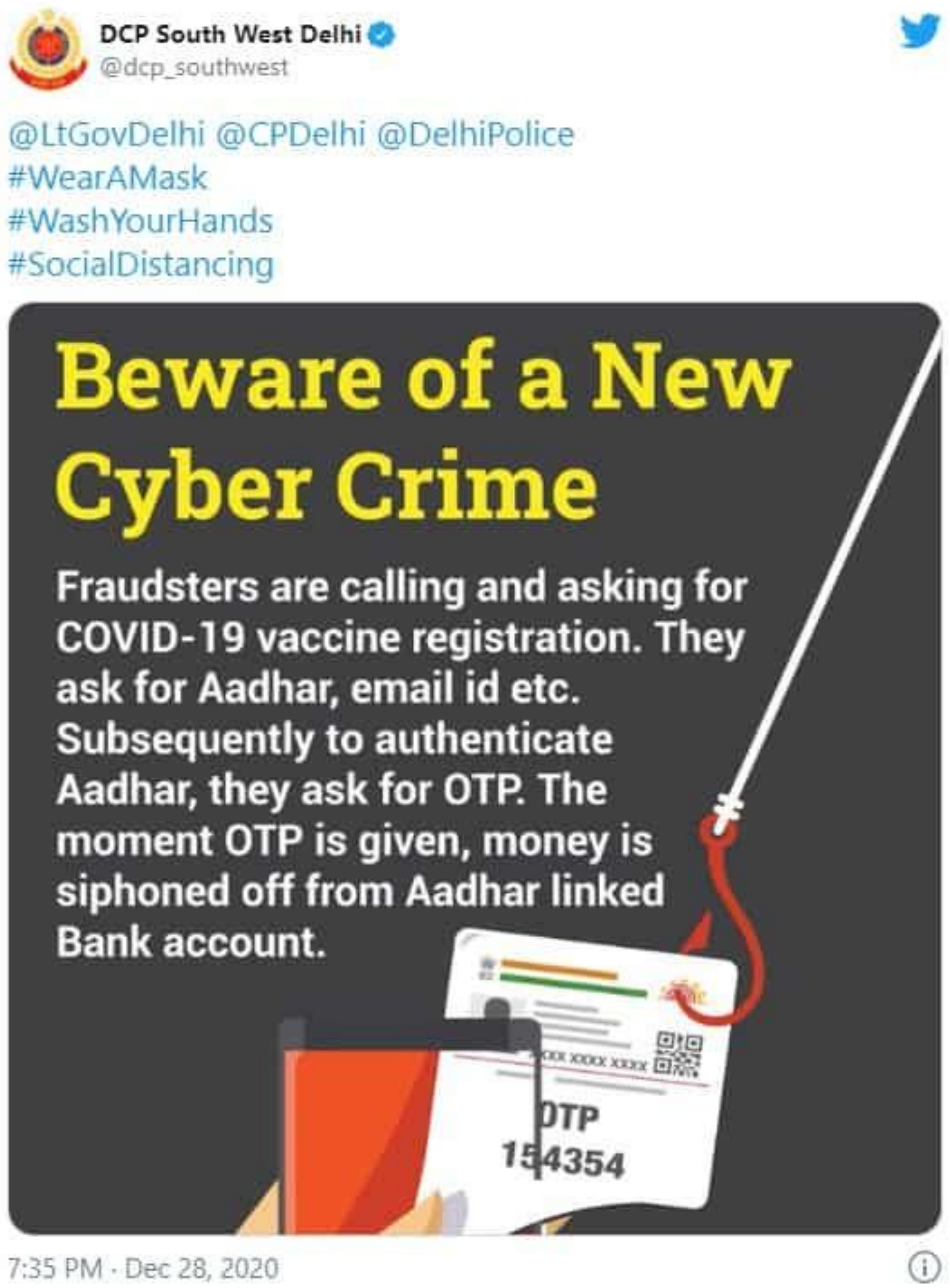
Do's

- **Check the authenticity** of the organisation or the company, which is sending messages on lucrative discounts for hotel bookings
- Keep your **social media accounts private** and **locked**
- Only respond to the **calls or messages** from **those known to you**

Don'ts

- **Don't respond to any link** sent to you with offers for **prizes** or other **deals**
- Don't respond to any **unknown caller** who tries to convince you of **booking rooms**
- **Don't press any link,** where you are said to be a **"Lottery Winner"** or something like that
- **Don't share** any **OTP with anyone**
- Don't believe any unknown person who says that you are a **lucky customer** of their business

Vishing Attacks



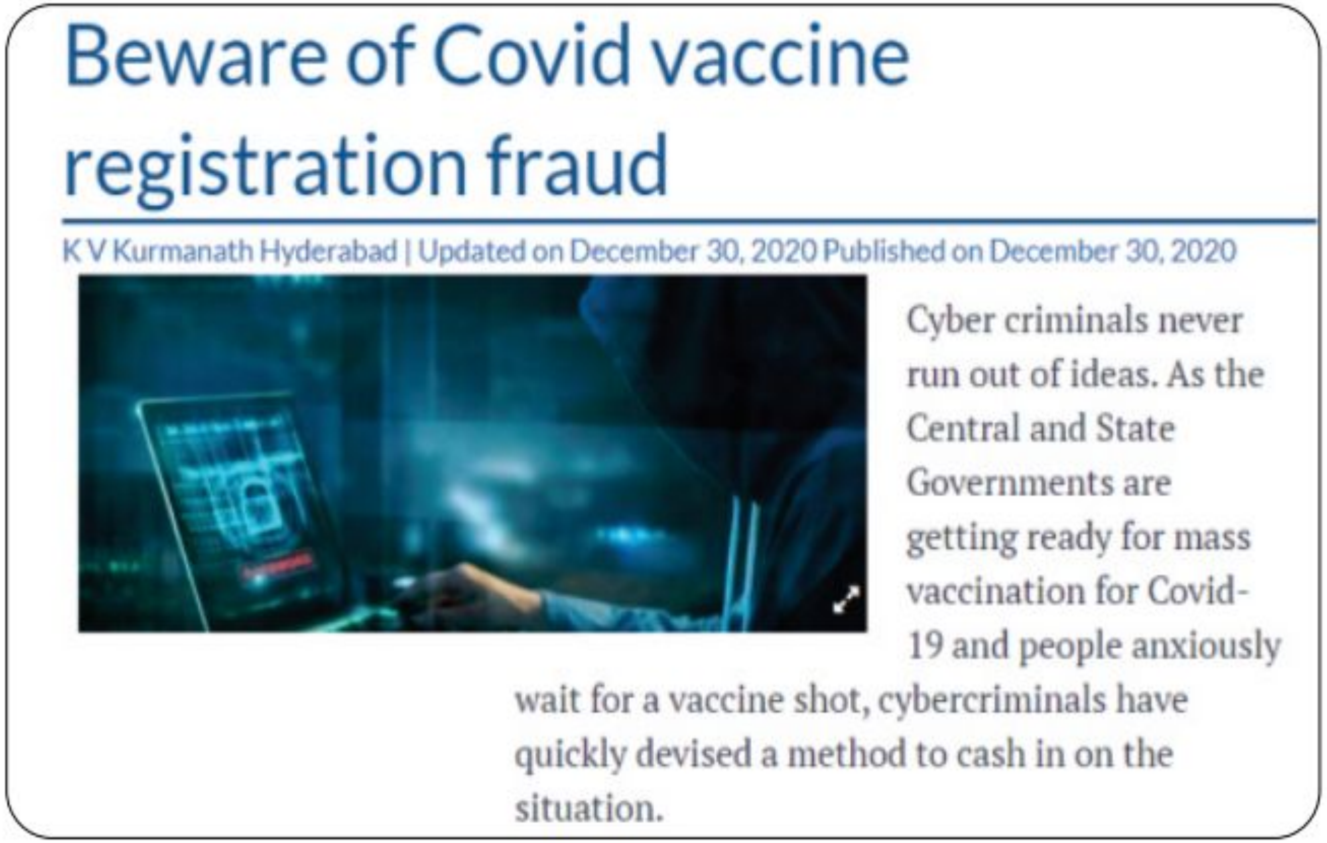
DCP South West Delhi
@dcp_southwest

@LtGovDelhi @CPDelhi @DelhiPolice
#WearAMask
#WashYourHands
#SocialDistancing

Beware of a New Cyber Crime

Fraudsters are calling and asking for COVID-19 vaccine registration. They ask for Aadhar, email id etc. Subsequently to authenticate Aadhar, they ask for OTP. The moment OTP is given, money is siphoned off from Aadhar linked Bank account.

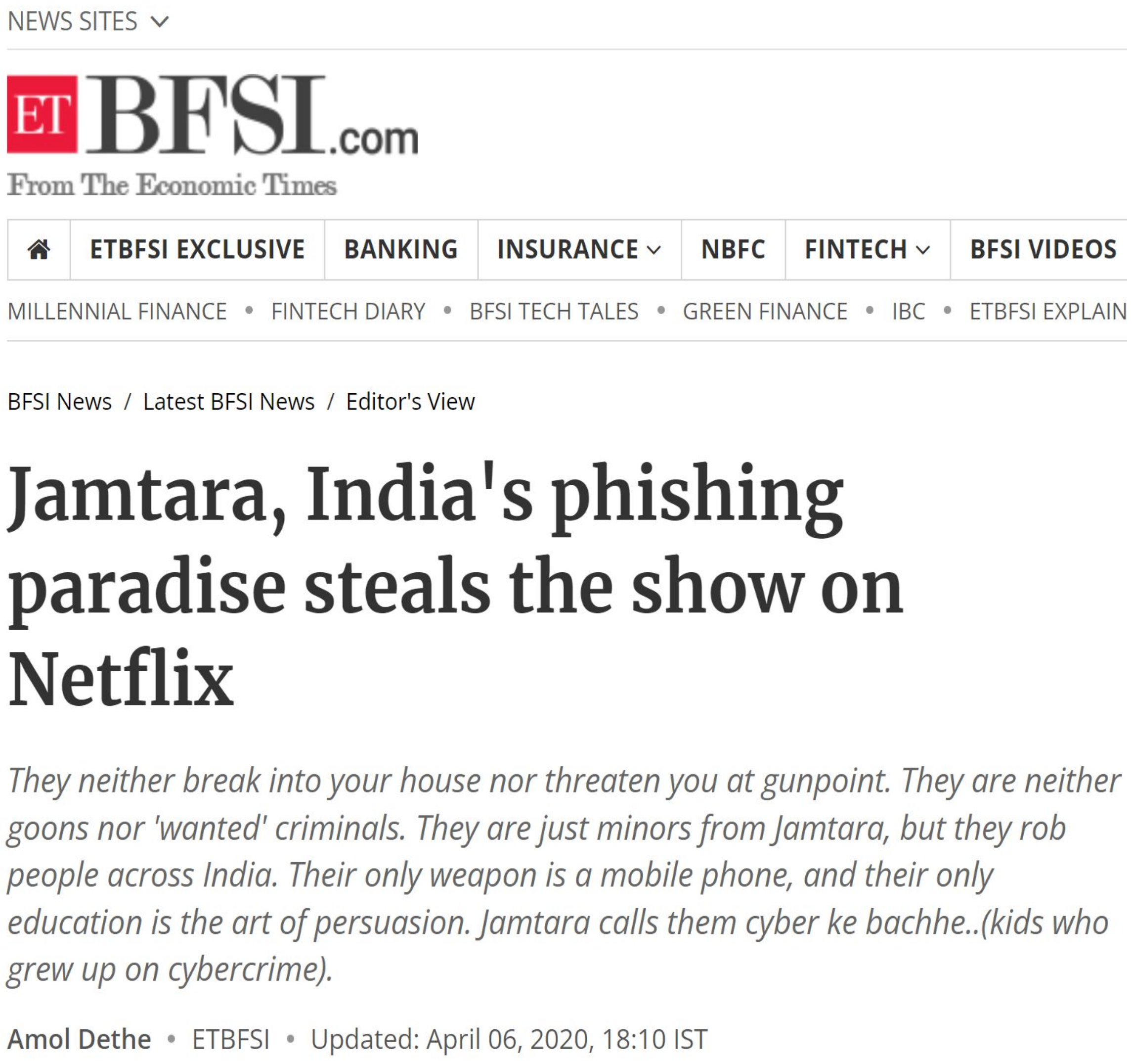
7:35 PM · Dec 28, 2020



Beware of Covid vaccine registration fraud

K V Kurmanath Hyderabad | Updated on December 30, 2020 Published on December 30, 2020

Cyber criminals never run out of ideas. As the Central and State Governments are getting ready for mass vaccination for Covid-19 and people anxiously wait for a vaccine shot, cybercriminals have quickly devised a method to cash in on the situation.



BFSI News / Latest BFSI News / Editor's View

Jamtara, India's phishing paradise steals the show on Netflix

They neither break into your house nor threaten you at gunpoint. They are neither goons nor 'wanted' criminals. They are just minors from Jamtara, but they rob people across India. Their only weapon is a mobile phone, and their only education is the art of persuasion. Jamtara calls them cyber ke bachhe..(kids who grew up on cybercrime).

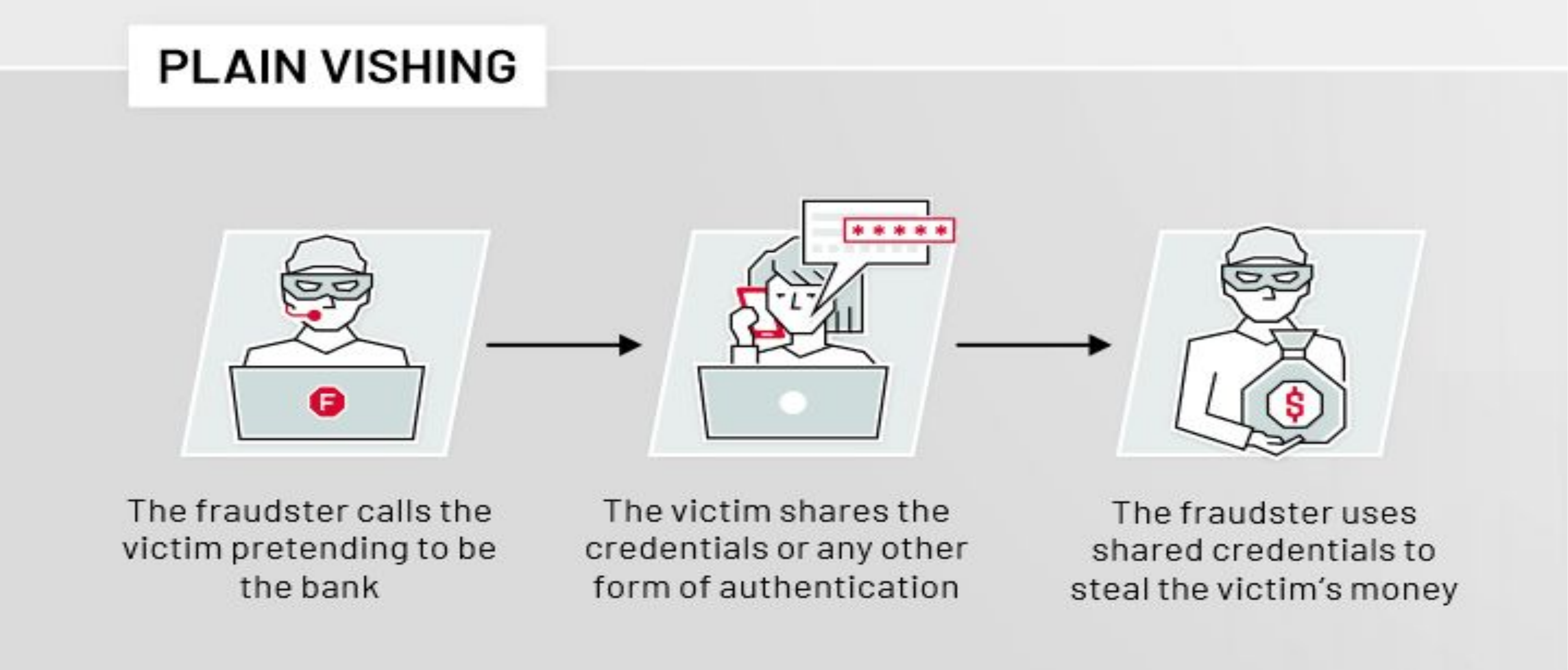
Amol Dethe • ETBFSI • Updated: April 06, 2020, 18:10 IST

INDIA'S BIGGEST HACKERS
EXPOSED
Asghar, Call Scammer, Jamtara, Jharkhand
Please give your 16-digit card number, with the date at the bottom and turn it over for the 3-digit CVVcode.

Vishing follows the familiar social engineering setup:

- An attacker creates a scenario to prey on human emotions, commonly greed or fear, and convinces the victim to disclose sensitive information, like credit card numbers or passwords.

- In that sense, vishing techniques mirror the phishing scams that have been around since the 1990s. But vishing calls exploit the fact that we're more likely to trust a human voice — and may target the elderly and technophobic who are naive and have no experience with these types of scams.



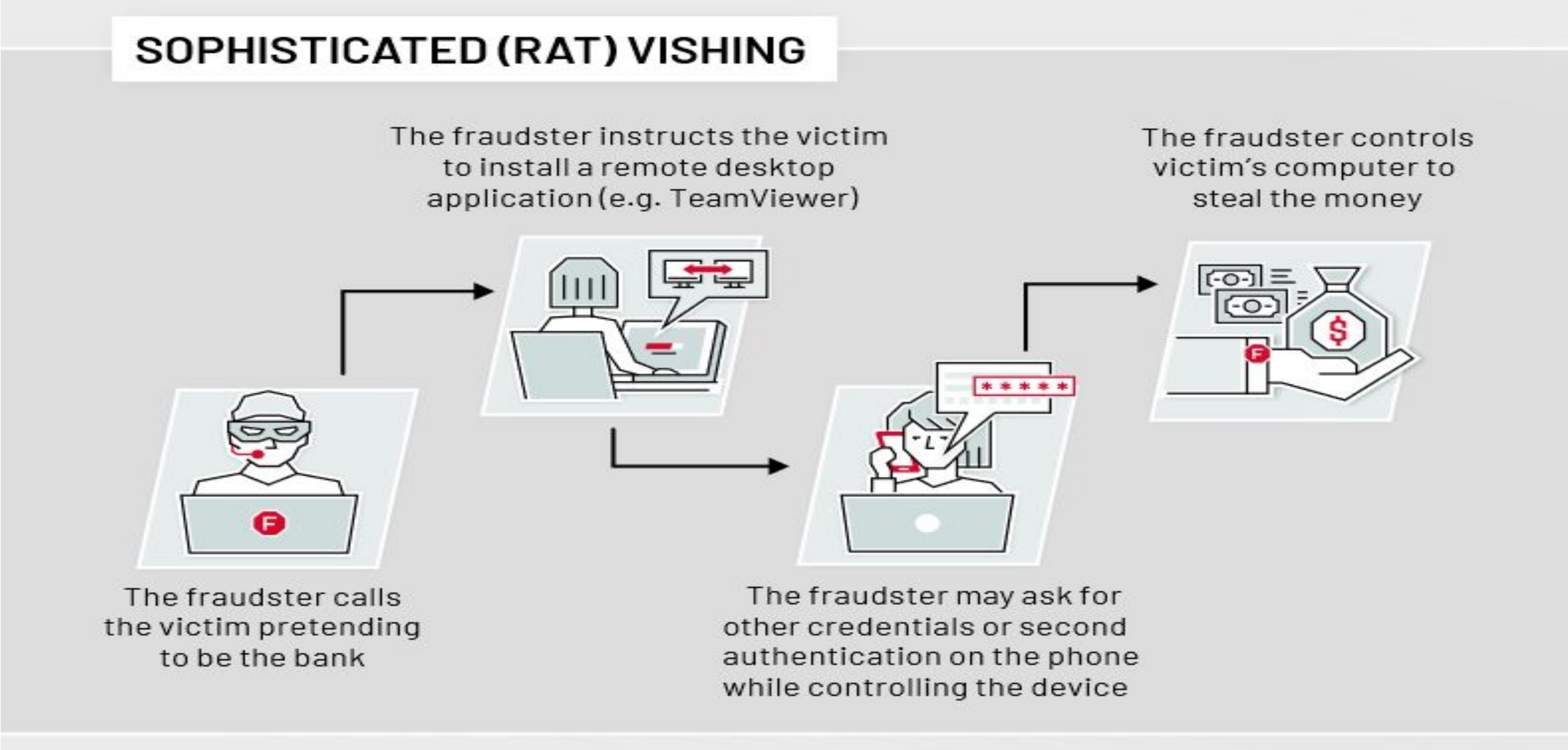
PLAIN VISHING

The fraudster calls the victim pretending to be the bank

The victim shares the credentials or any other form of authentication

The fraudster uses shared credentials to steal the victim's money

In *plain vishing* type, the fraudster calls the victim pretending to be the bank and by implying urgency and authority sways the user to share the credentials and/or any other incoming second form of authentication. In this type, the fraud is completed on the fraudster's computer.



SOPHISTICATED (RAT) VISHING

The fraudster calls the victim pretending to be the bank

The fraudster instructs the victim to install a remote desktop application (e.g. TeamViewer)

The fraudster may ask for other credentials or second authentication on the phone while controlling the device

The fraudster controls victim's computer to steal the money

In this sophisticated vishing type of an attack the fraudster persuades the user to install a remote access tool (such as TeamViewer), share the credentials, second authentication factors, and any other information if needed. Once the software is installed by the user, the fraudster assumes control of their computer and continues to use the banking systems as they wish.

Four Common Vishing Techniques

1. Wardialing

The cyber criminal uses software to call specific area codes, using a message that involves a local bank, business, police department, or other local organization. When the call is answered, the automated message begins, urging the person to provide their full name, credit card details, bank account information, mailing address, and even social security details. The recorded message may suggest that this information is needed to confirm that the victim’s account has not

2. VoIP

VoIP makes it very easy for cyber criminals to create fake numbers and hide behind them. These numbers are tough to track and be used to create phone numbers that appear local or use a 1-800 prefix. Some cyber criminals will create VoIP numbers that appear to come from a government department, local hospital, or police department.

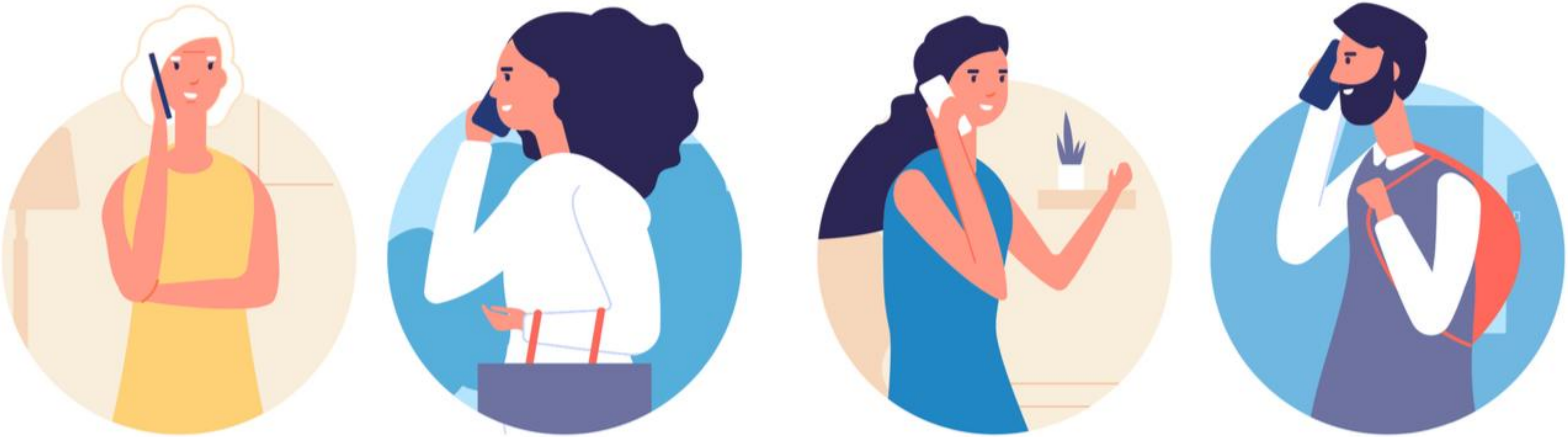
Four Common Vishing Techniques

3. Caller ID Spoofing

Like VoIP vishing, the cyber criminal hides behind a fake phone number by spoofing the caller ID. They may list their name as Unknown or pretend to represent a legitimate caller, using an ID such as Government, Tax Department, Police, etc.

4. Dumpster Diving

A simple and popular method of collecting valid phone numbers is to dig through dumpsters behind banks, office buildings, and random organizations. Often criminals will find enough information to deliver a targeted spear vishing attack against the victim.



Prevention from Vishing Attacks

HOW TO DEFEND AGAINST VISHING ATTACKS

BE VIGILANT

BE HELPFUL BUT DEFENSIVE

DON'T PANIC

CALL THEM BACK!

DON'T GIVE OUT VALUABLE INFORMATION OVER THE PHONE

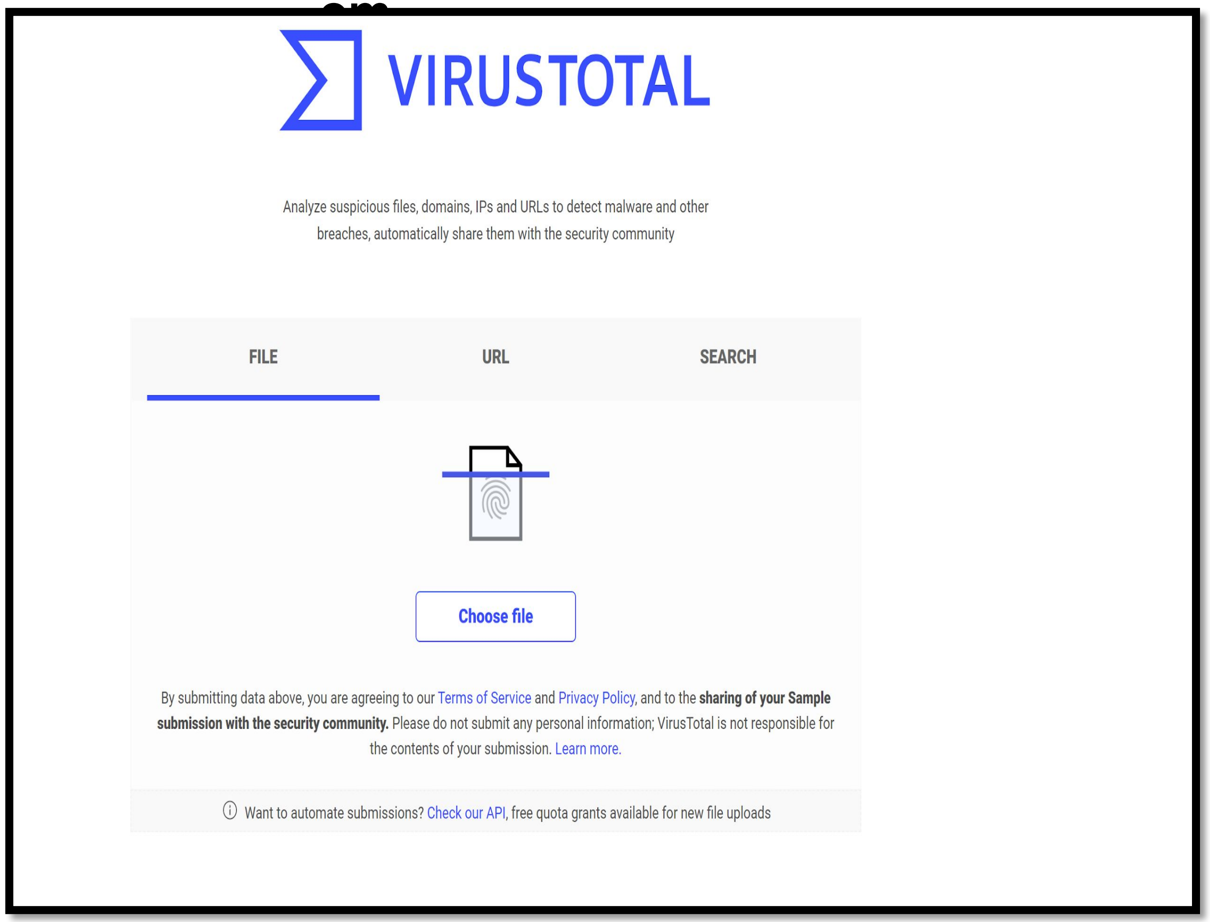
TREAT URGENCY AS A RED FLAG

DON'T BE AFRAID TO SAY NO

Vishing Prevention Techniques

- Remain Vigilant and Pay Attention During Phone calls.
- Verify the identity of those who ask for information in person or over the phone, before you release any information.
- Be Cautious When Giving Out Your Information.
- Be Suspicious of Unrecognized Phone Numbers.
- check your bank statement regularly.

www.virustotal.com

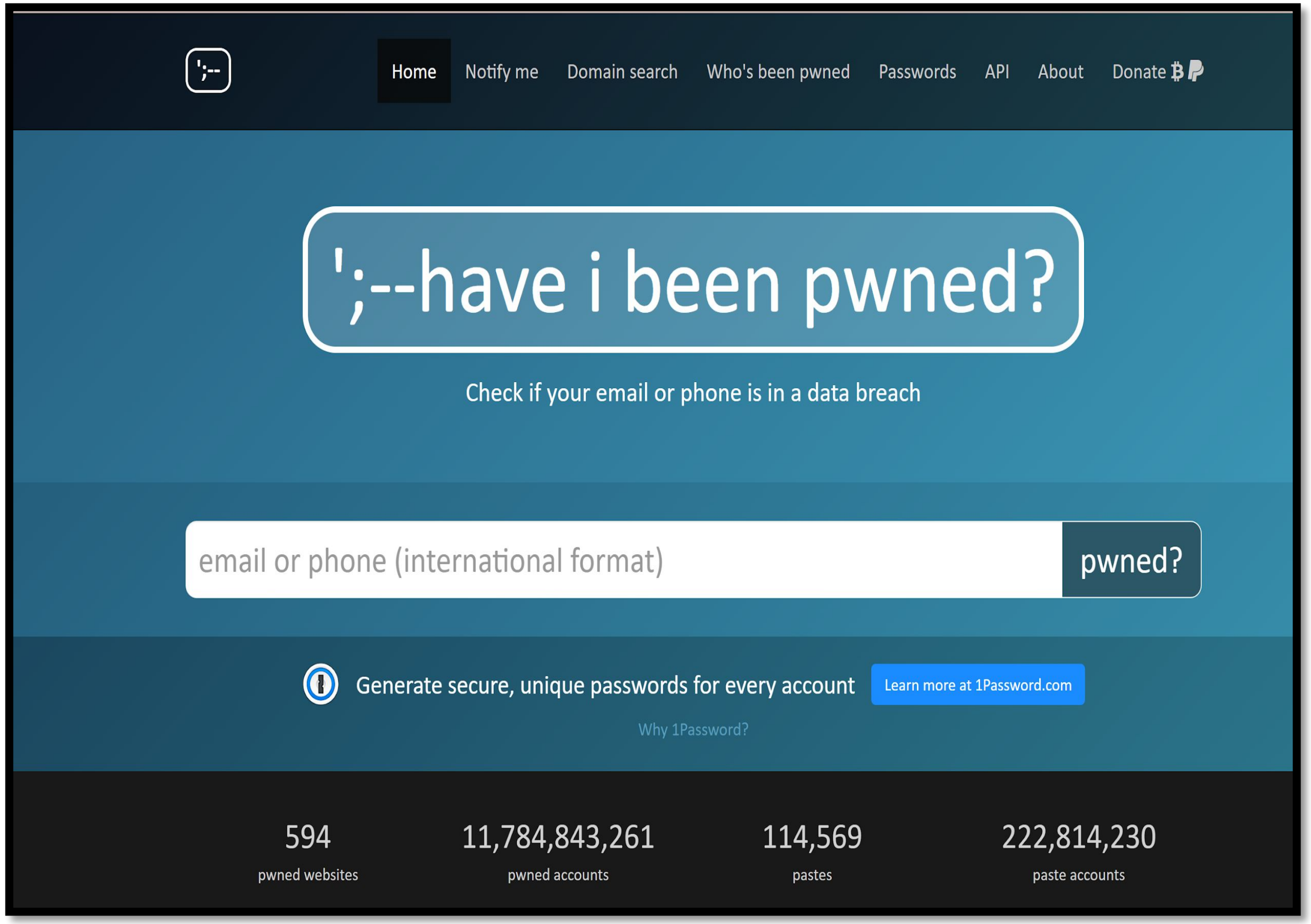


VIRUSTOTAL

Analyze suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community

By submitting data above, you are agreeing to our Terms of Service and Privacy Policy, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.

ⓘ Want to automate submissions? Check our API, free quota grants available for new file uploads



';--have i been pwned?

Check if your email or phone is in a data breach

Generate secure, unique passwords for every account

594 pwned websites

11,784,843,261 pwned accounts

114,569 pastes

222,814,230 paste accounts

https://haveibeenpwned.com/

FOR PARENTS

CYBER PREDATORS

81% INCREASE since the start of the COVID-19 pandemic.[1]

MALWARE

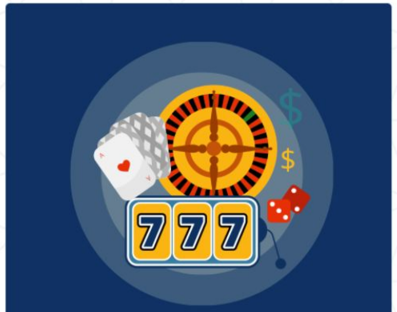
Installed on **50,000+ DEVICES** through apps & children's games in February 2020.[2]

MALICIOUS ADS

Google removed **OVER 790,000** malicious apps in 2019.[3]

IDENTITY THEFT

OVER ONE MILLION minors were identity fraud victims in 2017.[4]



ONLINE GAMING

13% OF YOUTHS 11 – 16 have played gambling-style games online.[5]

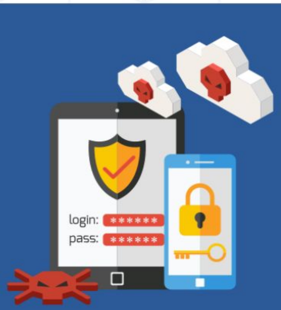
Five cybersecurity tips for parents:

1. **Teach** passwords & privacy
2. **Monitor** & communicate
3. **Protect** identity & location
4. Use **secure** Wi-Fi
5. Utilize **parental controls**

Cybersecurity Threats faced by Students

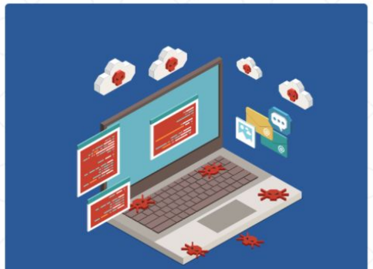
DATA THEFT

Can cost **$200** per educational record.[1]



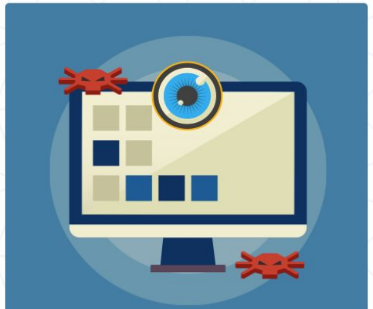
MOBILE MALWARE

Targeted attacks have **RISEN BY 50%** since 2018.[2]



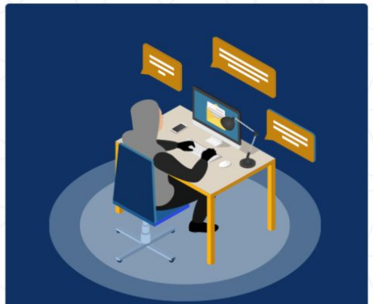
MALICIOUS SOCIAL MEDIA MESSAGING

Facebook phishing **INCREASED 155.5%** in Q1 2019.[3]



CAMFECTING

1 IN 2 Americans are clueless about webcam hacking.[4]



SOCIAL ENGINEERING

Relied on by **98%** of cyber attacks.[5]

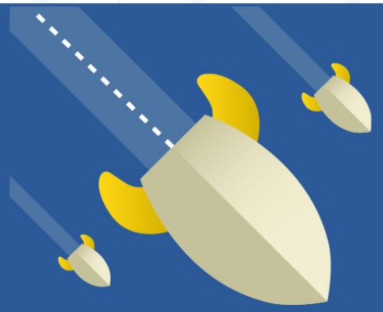
Five cybersecurity tips for learners:

1. Avoid sharing **personal information**
2. Use virus **protection**
3. Keep **software** up-to-date
4. Be on guard for **phishing**
5. Be **careful** what you click

FOR TEACHERS

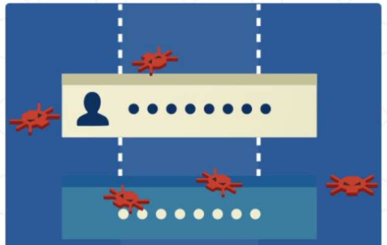
PHISHING

Marks the start of **OVER 90%** of modern cyberattacks.[1]



DISTRIBUTED DENIAL-OF-SERVICE (DDOS)

Can cost victims up to **$40,000 PER HOUR**.[2]



DATA BREACH

Attacks nearly **TRIPLED** in the last year.[3]

RANSOMWARE

Impacted **89** universities, colleges & school districts in 2019.[4]

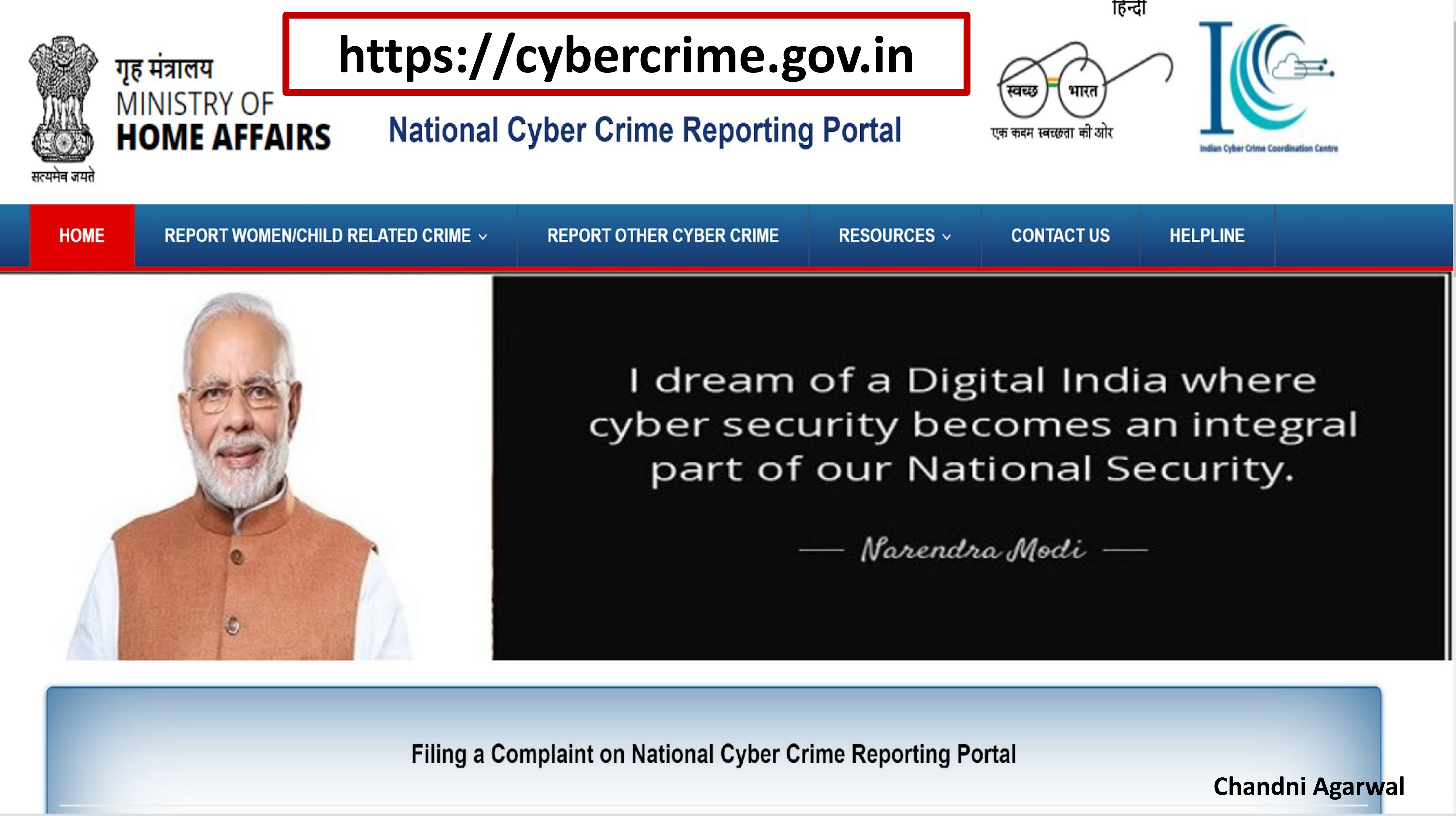
IoT VULNERABILITIES

Responsible for an average of **5,200 ATTACKS PER MONTH**.[5]

Five cybersecurity tips for teachers:

1. **Encrypt** your data
2. Comply with your institution's cyber **protocols**
3. **Safeguard** your devices from physical attacks
4. **Back up** your data
5. Practice good **password** management

https://cybercrime.gov.in



गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

सत्यमेव जयते

National Cyber Crime Reporting Portal

I dream of a Digital India where cyber security becomes an integral part of our National Security.

— Narendra Modi —

Filing a Complaint on National Cyber Crime Reporting Portal

Chandni Agarwal