Ministry of Housing and Urban Affairs

Interactive Session-cum-Training Program on Cyber Hygiene

सत्यमेव जयते

G20 भारत 2023 INDIA
वसुधैव कुटुम्बकम्
ONE EARTH • ONE FAMILY • ONE FUTURE

Indian Cyber Crime Coordination Centre

Azadi Ka Amrit Mahotsav

Indian Cyber Crime Coordination Centre (I4C)

I4C scheme was created to act as a nodal point in the fight against cyber crime

Seven Verticals of I4C

Introduction

Cyber Crime Facts & Statistics

More than 19 Lac complaints reported till date on National Cyber Crime Reporting Portal (Since, August 2019)

More than Rs 250 Crore saved using 1930 Cyber Helpline

Over 50% crimes reported are financial frauds

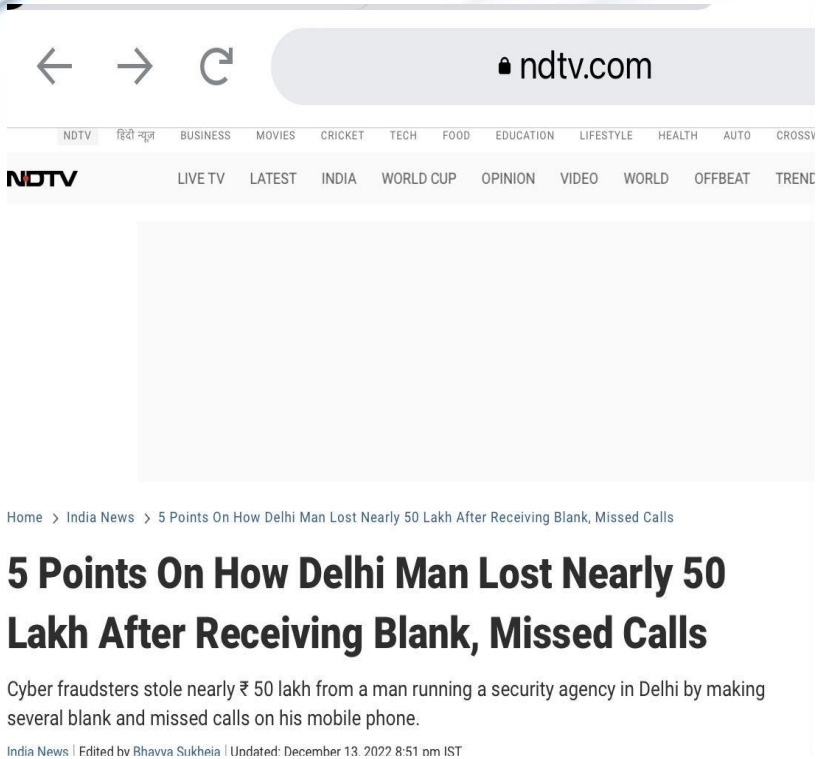
Average **4000 complaints** reported daily (July, 2022)

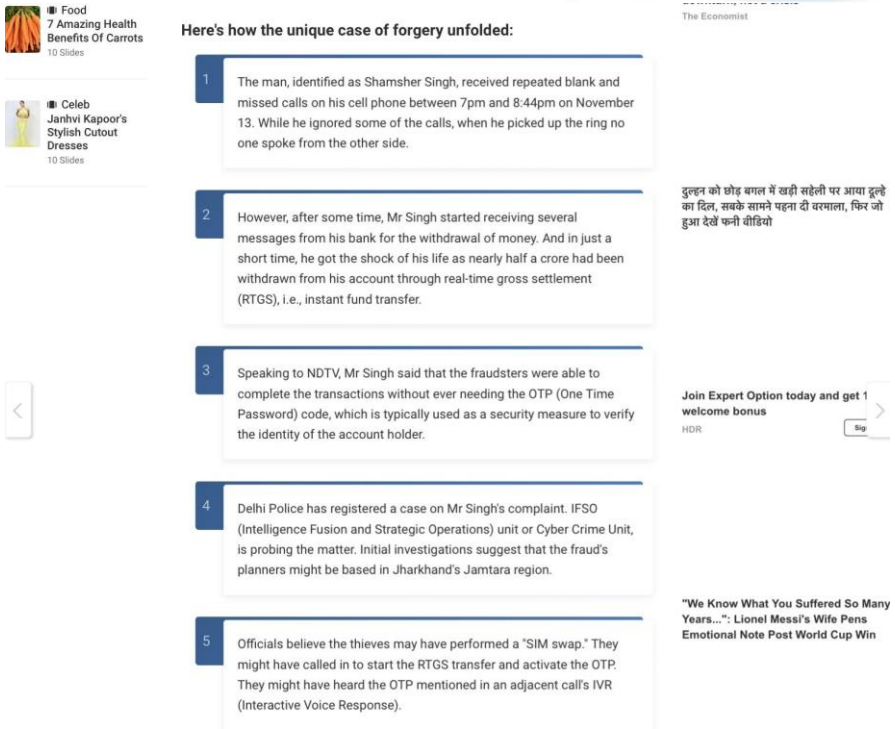
Know Your Enemy

If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle

—Sun Tzu, The Art of War

Delhi man duped of Rs 50 lakhs





More Cases

Many B'lureans lose cash to sim card swap fraud

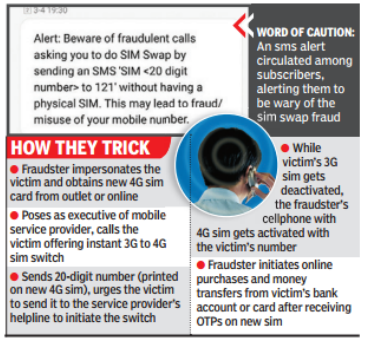
Bank Insiders Part Of Ploy: Investigators

Petlee.Peter@timesgroup.com

Bengaluru: If you are using a cellphone number with a 3G sim card and your online banking account is linked to it, you could be the next victim of a thriving 'sim card swap fraud'. At least 30 Bengalureans have reportedly fallen prey to scamsters, losing huge sums of money since mid-2016.

BEWARE THE TRAP

For insurance executive Aroop Ghosh (39) from Domlur, the ordeal began when he attended a phone call at his lunch table in mid-February. "The male caller claimed he was calling from a mobile service provider and confirmed with me if I was still using a 3G sim. He told me that there is an offer for easy swapping to 4G for better internet speed and sent me a 20-digit number by SMS after disconnecting the call," he said.



An ignorant Ghosh took the bait by texting the 20-digit number to the mobile service provider's helpline and selected option 1 to confirm the 4G swap as advised by the conman. "Within a few seconds my sim card got deactivated and it remained so," rued Ghosh. The following day, electronics good worth over Rs 2 lakh were purchased online using his HDFC bank account.

According to an investigating officer with the CID's cybercrime unit, the modus operandi is thus: The culprits obtain a new 4G sim for the victim's cellphone number by either impersonating him at an outlet of the service provider or online, using the 4G sim swap page on the service provider's website. The new sim is then delivered to the given address within a day.

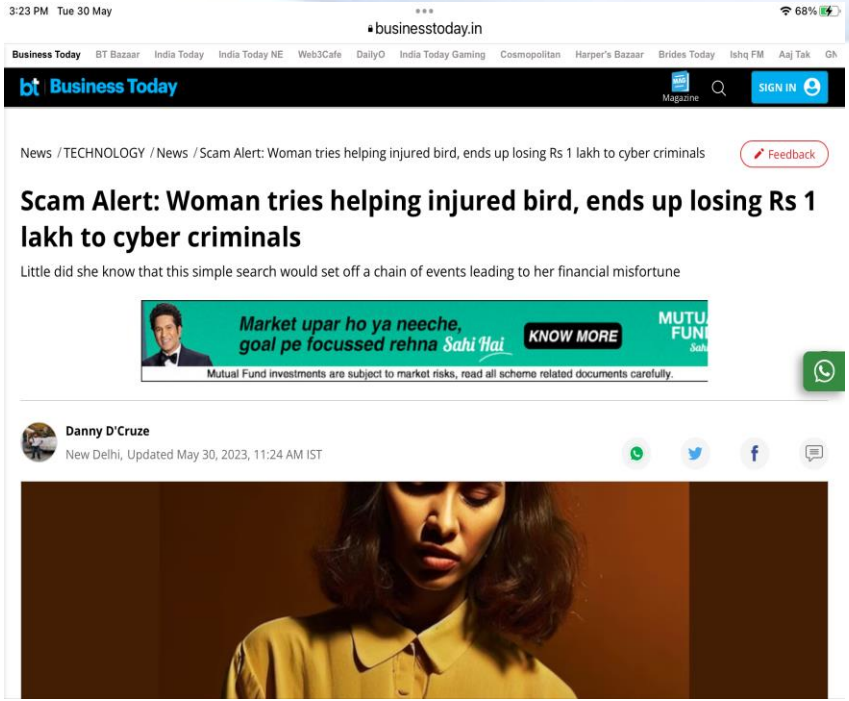
"The culprits then call the victim claiming to be executives from the service provider and send the 20-digit number printed on the new 4G sim card via SMS and convince him or her to activate it. Once the 3G sim on the victim's cellphone becomes inactive, the 4G one on the fraudsters' cellphone becomes active. The fraudsters then use it to receive OTPs," the officer added.

Investigators suspect the scamsters must be obtaining victims' confidential bank account or card details, including cellphone details, from bank insiders. "They try every number pertaining to the accounts and some 3G sim card users fall for it," the officer added.

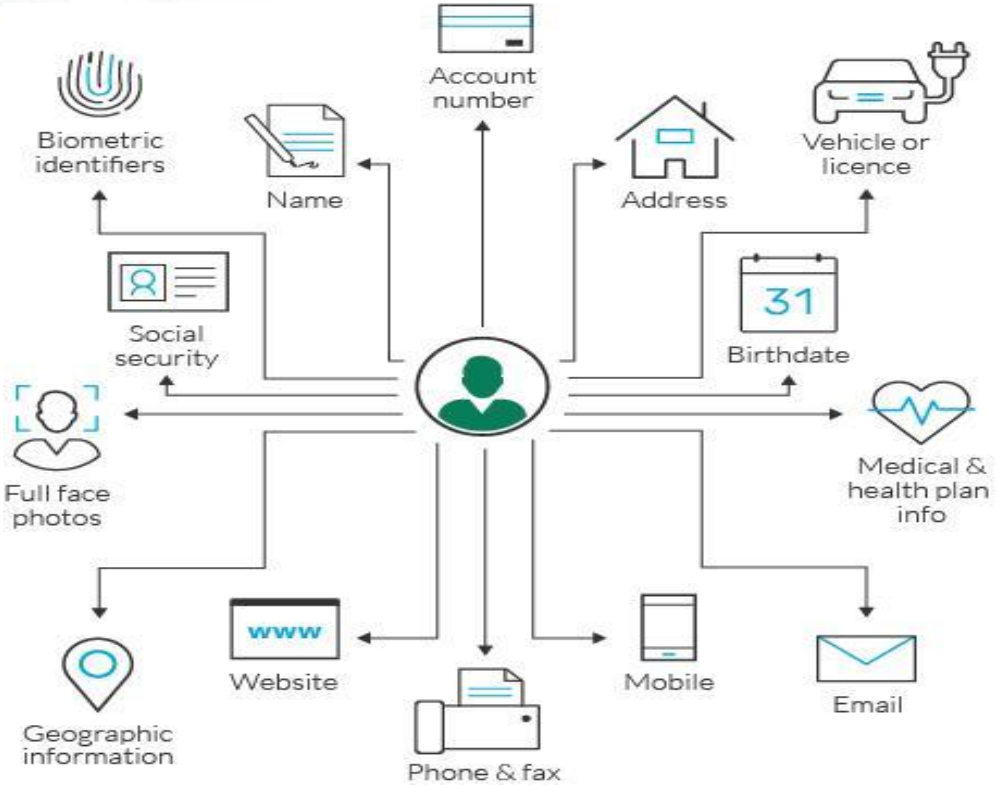
Over 30 victims of the sim swap fraud have approached cybercrime police stations of state CID and Bengaluru city police (BCP) since mid-2016.

Some like Manish Raj, a city-based BPO employee, who are tech aware have also fallen prey to the fraud. "I didn't receive a call but only an internet-generated SMS with the 20-digit number from the fraudster, which I carelessly activated and lost Rs 30,000 from my ICICI account," recalled Raj.

(Names of victims have been changed on request).



Personal Identification Information



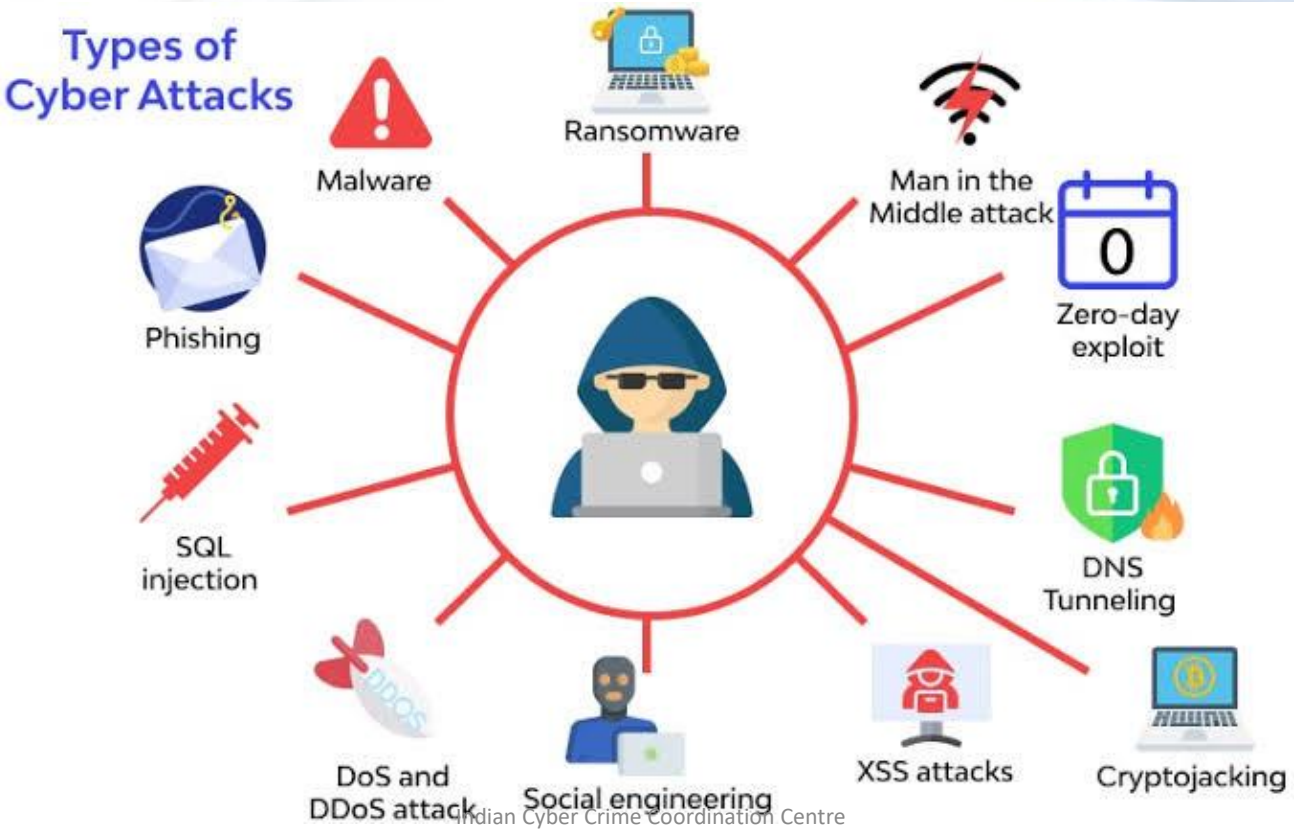
Cyber Security

- Cyber Attack
- Device Security
- Social Engineering Attacks

Motives of Cyber Crime

- Disrupting business continuity
- Information theft and manipulating data
- Creating fear and chaos by disrupting critical infrastructure
- Financial loss to target
- Achieving strategic military objective
- Demanding Ransom
- Damaging reputation of the target
- Propagating religious and political beliefs

Cyber Attack



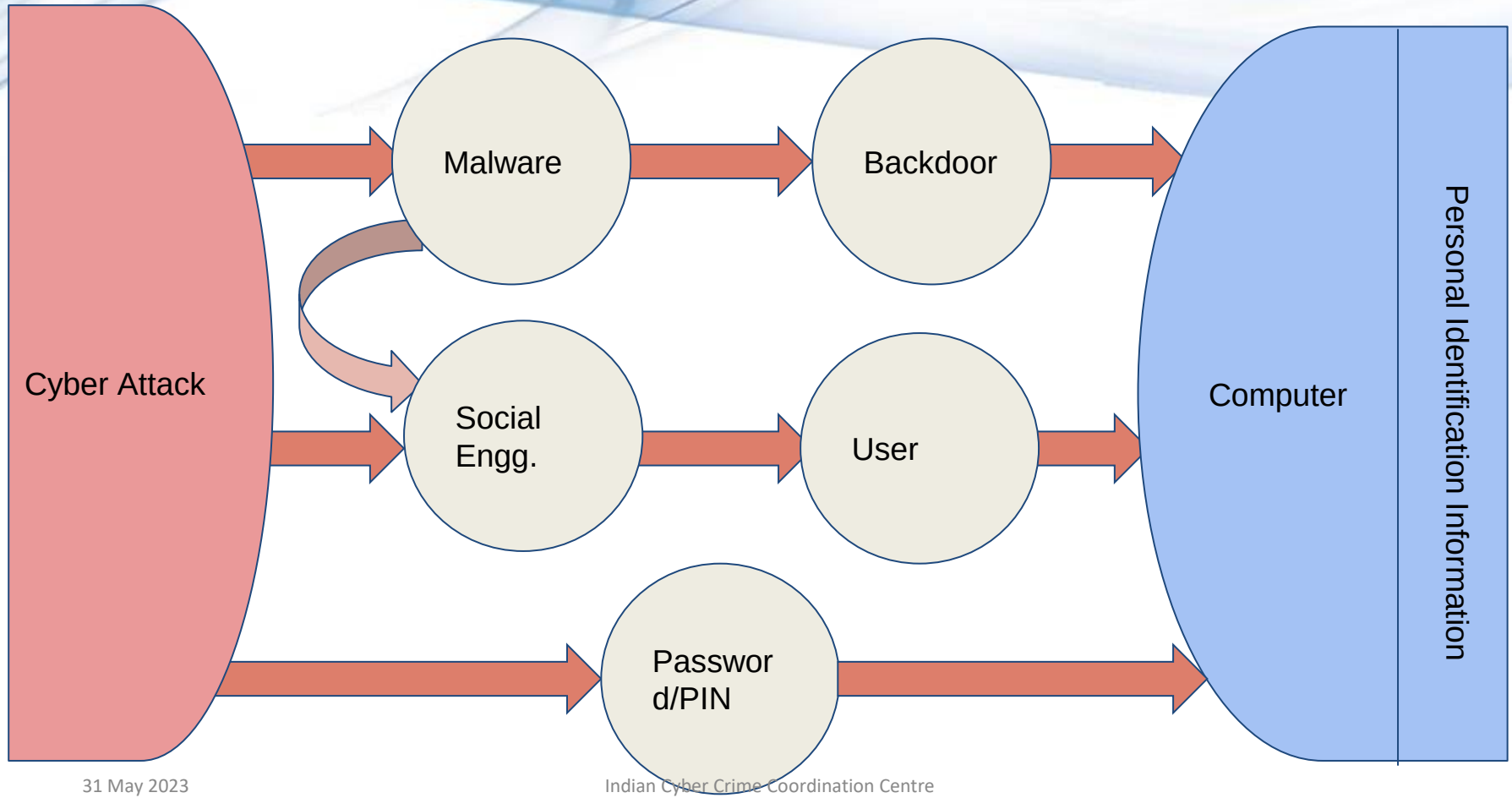
Cyber Attack

Password Attack

Malware Attack

Social Engineering

Cyber Attack Vectors



Malware

- Virus
- Worms
- Trojan Horse
- Key logger
- Spyware
- Adware
- Ransom ware

Password Attack

- Dictionary
- Brute Force
- Keylogger
- Shoulder Surfing
- Rainbow Table

Password Hygiene Shortcomings

The Ponemon Institute's latest research report on password practices reveals several areas where real-world practices fall short of password best practices.

SOURCE: 2020 STATE OF PASSWORD AND AUTHENTICATION SECURITY BEHAVIORS REPORT SURVEY OF 2,507 IT RESPONDENTS; CONDUCTED BY PONEMON INSTITUTE AND SPONSORED BY YUBICO; ILLUSTRATIONS: INUENG/GETTY IMAGES

Keeping Passwords Safe and Secure

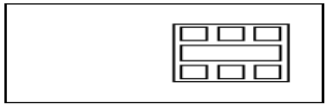
- Avoid using the same password for different accounts
- Change passwords on a regular basis
- Keep passwords at least 12 characters long (and ideally longer)
- Passwords must involve a mix of upper- and lower-case letters plus symbols and numbers
- Avoid the obvious - such as using sequential numbers(“1234”) or personal information that someone who knows me might guess, such as my date of birth or pet’s name.
- Change the default passwords on my IoT devices, WiFi router etc.
- Avoid writing my passwords down or sharing them with others
- Use a password manager to help generate, store, and manage all my passwords in one secure online account

Keeping Passwords Safe and Secure

Top 200 Most Common Passwords

Rank	Password	Time to Crack	Count	Rank3	Password2	Time to Crack2	Count4	Rank2	Password3	Time to Cra	Count3	Rank4	Password4	Time to Cra	Count2
1	password	< 1 Second	3,490,216	51	asdf1234	< 1 Second	2,225	101	qwerty12	< 1 Second	1,134	151	Rohit@123	3 Hours	778
2	123456	< 1 Second	166,757	52	Password@1	2 Seconds	2,213	102	vicky123	2 Seconds	1,096	152	gaurav@123	3 Hours	770
3	12345678	< 1 Second	114,073	53	haribol1	2 Minutes	2,163	103	reset123	< 1 Second	1,082	153	kumar123	2 Seconds	762
4	bigbasket	5 Minutes	75,081	54	password1	< 1 Second	2,153	104	12341234	< 1 Second	1,080	154	indya123D	17 Seconds	757
5	123456789	< 1 Second	30,424	55	priyanka	< 1 Second	2,115	105	amit1234	5 Seconds	1,071	155	ashish@123	3 Hours	752
6	pass@123	2 Seconds	20,792	56	welcome1	< 1 Second	2,108	106	1234abcd	< 1 Second	1,054	156	Login@123	3 Hours	751
7	1234567890	< 1 Second	14,715	57	Admin@123	13 Seconds	1,951	107	bangalore	< 1 Second	1,044	157	abhi1234	9 Seconds	749
8	anmol123	17 Minutes	10,143	58	Sara2000	6 Seconds	1,902	108	abc@1234	41 Seconds	1,026	158	a1b2c3d4	< 1 Second	748
9	abcd1234	< 1 Second	8,941	59	qwerty1234	< 1 Second	1,900	109	qwerty123456	< 1 Second	1,017	159	harekrishna	1 Second	748
10	googledummy	23 Minutes	8,435	60	qwerty12345	< 1 Second	1,899	110	abhi@123	17 Minutes	1,006	160	heer2504	3 Hours	748
11	Indya123	2 Seconds	7,512	61	abhishek	< 1 Second	1,891	111	priya@123	29 Minutes	1,006	161	godisgreat	< 1 Second	746
12	qwerty123	< 1 Second	7,289	62	1234	< 1 Second	1,842	112	sairam123	3 Seconds	1,002	162	neha@123	17 Minutes	728
13	sahilji1	3 Hours	7,115	63	11111111	< 1 Second	1,840	113	123123	< 1 Second	995	163	manish@123	2 Minutes	726
14	987654321	< 1 Second	7,074	64	bankking	1 Hour	1,747	114	ravi@123	17 Minutes	981	164	asdf@1234	17 Minutes	723
15	kapil*12345	3 Hours	7,041	65	basket@123	53 Minutes	1,728	115	computer	< 1 Second	976	165	vijay@123	3 Minutes	723
16	123456789a	< 1 Second	6,133	66	rahul@123	3 Hours	1,668	116	deepak@123	2 Hours	946	166	1q2w3e4r	< 1 Second	713
17	p@ssw0rd	< 1 Second	5,643	67	pantaloons	12 Days	1,666	117	66778899	2 Seconds	939	167	aaaa1111	< 1 Second	710
18	India@123	11 Seconds	5,321	68	sairam	< 1 Second	1,649	118	Apple@123	10 Minutes	926	168	ankit123	9 Seconds	696
19	india123	< 1 Second	5,207	69	santosh1234	1 Minute	1,608	119	nirankar	10 Seconds	924	169	q1w2e3r4	< 1 Second	693
20	12345	< 1 Second	4,903	70	krishna	< 1 Second	1,583	120	ankit@123	4 Minutes	923	170	deepak123	5 Seconds	691
21	qwertyuiop	< 1 Second	4,723	71	qwer1234	< 1 Second	1,560	121	Krishna@123	49 Minutes	907	171	madish123	3 Hours	688
22	welcome123	< 1 Second	4,668	72	qwertyui	< 1 Second	1,529	122	786786786	< 1 Second	904	172	sandeep	< 1 Second	688
23	shopping	< 1 Second	4,445	73	Test@123	17 Minutes	1,524	123	zepo@123	17 Minutes	904	173	India@1234	4 Minutes	687
24	Welcome@123	16 Seconds	4,235	74	pass@1234	49 Seconds	1,515	124	shopping@123	37 Minutes	897	174	deepak	< 1 Second	684
25	Password@123	8 Seconds	3,974	75	Welcome@1	7 Seconds	1,497	125	shopping123	12 Seconds	894	175	9876543	< 1 Second	683
26	abcd@1234	6 Seconds	3,914	76	a1234567	< 1 Second	1,454	126	11112222	< 1 Second	892	176	aditya	< 1 Second	682
27	Hisss0143	9 Hours	3,753	77	abc123	< 1 Second	1,438	127	indian	< 1 Second	887	177	skingre123	1 Day	682
28	iphone5s	3 Minutes	3,647	78	abcdefgh	< 1 Second	1,409	128	wipro@123	7 Seconds	885	178	99999999	< 1 Second	681

3 Factors of Authentication

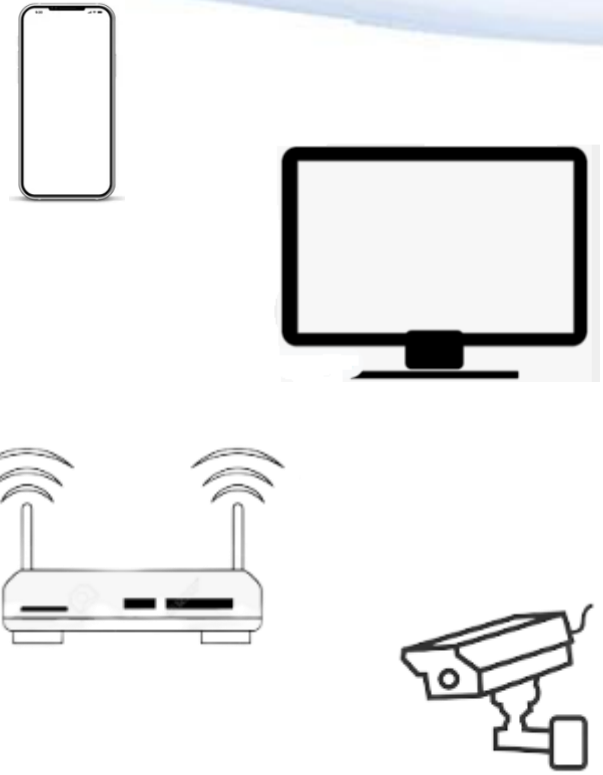
Knowledge Factor (something you know)	Possession Factor (something you have)	Inherence Factor (something you are)
**** Password	 Smartphone	 Fingerprint
 Security Question	 Smart Card	 Retina Pattern
1 2 3 4 PIN	 Hardware Token	 Face Recognition

Using Multi-Factor Authentication

- Protect all essential accounts – such as email, social media, or banking apps – with multi-factor authentication (MFA)

Device Security

- Mobile
- Computer/Desktop
- Wi-Fi Router
- CCTV and IoT



Mobile Security

- Buy Smartphone having licensed OS
- Keep your Phone operating system up to date
- Back up your phone's data regularly
- Set up a pass code longer than the 4-number
- Enable two-factor authentication
- Take advantage of built-in security features
- Make sure your WiFi network is secure
- Use different Passwords for Phone, UPI, Bank Accounts etc.
- Activate the "Find my Phone" feature

Mobile Security

- Set the phone to “self destruct” i.e., wipe itself after 10 failed password attempts
- Regularly change iCloud, Google Drive and iTunes passwords
- Use only trusted charging stations
- Disable voice assistant on the lock screen
- Revoke app permissions to use the camera, microphone, etc.
- Encrypt your data and wipe your phone before selling
- Buy apps only from Google Play Store or App Store
- Disable the Unknown Sources to avoid installation of 3rd party applications.
- Don't Jailbreak or Root your phone

Wifi Router Security

- **Wifi Attacks**
  - Evil Twin Attack
  - Jamming Signals
  - Misconfiguration Attack
  - Honey Spot Attack
  - Unauthorised/Adhoc Connection Attack
- **Precautions**
  - Avoid public WiFi networks
  - Use VPN connection if you have to use public WiFi network.
  - Always change the default credentials of your router.

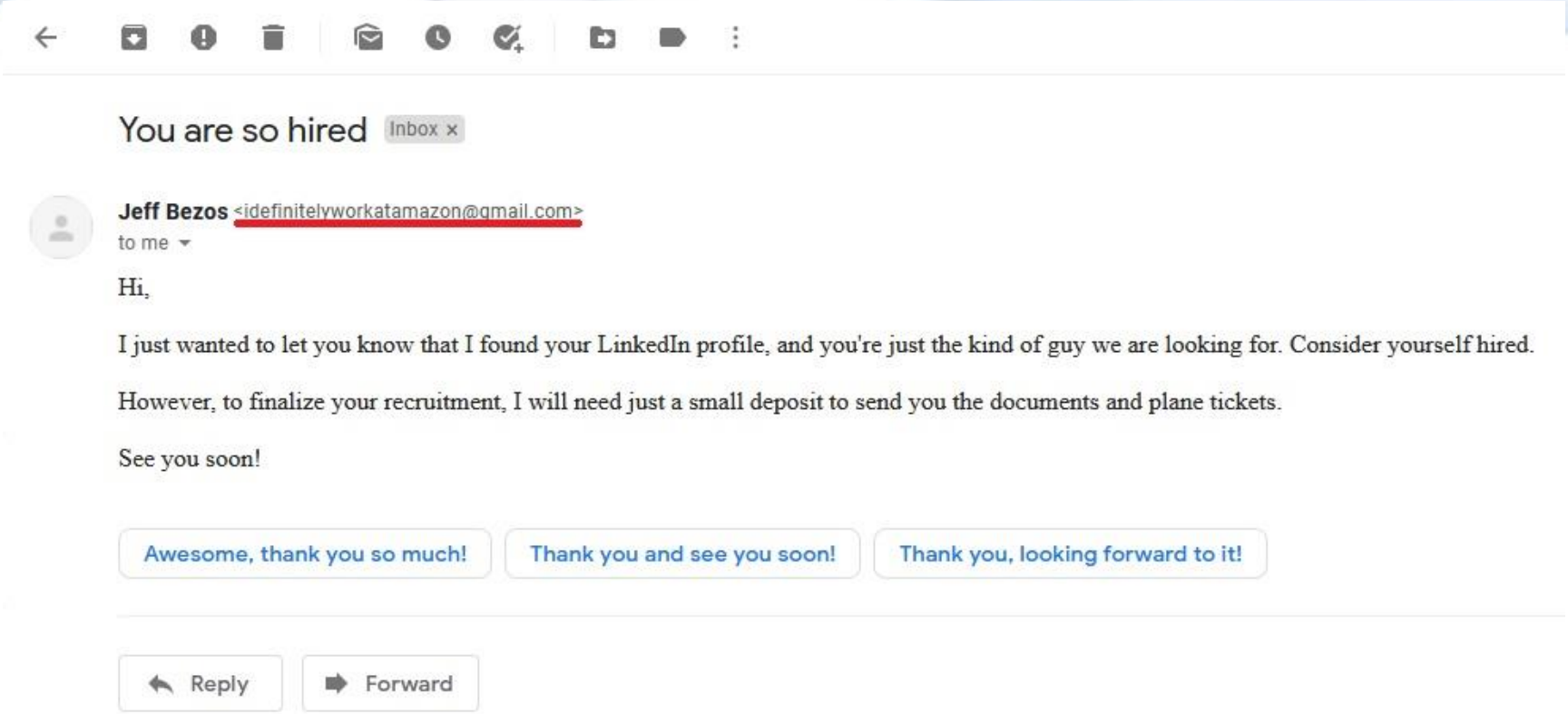
Bluetooth Security

- Always keep Bluetooth in off state when not in use.
- Hackers can exploit open bluetooth for-
  - Bluesnarfing
  - Eavesdropping
  - Denial of Service
  - Viruses and Worms
  - Bluetooth headset vulnerabilities
- Avoid pairing Bluetooth devices in crowded spaces.

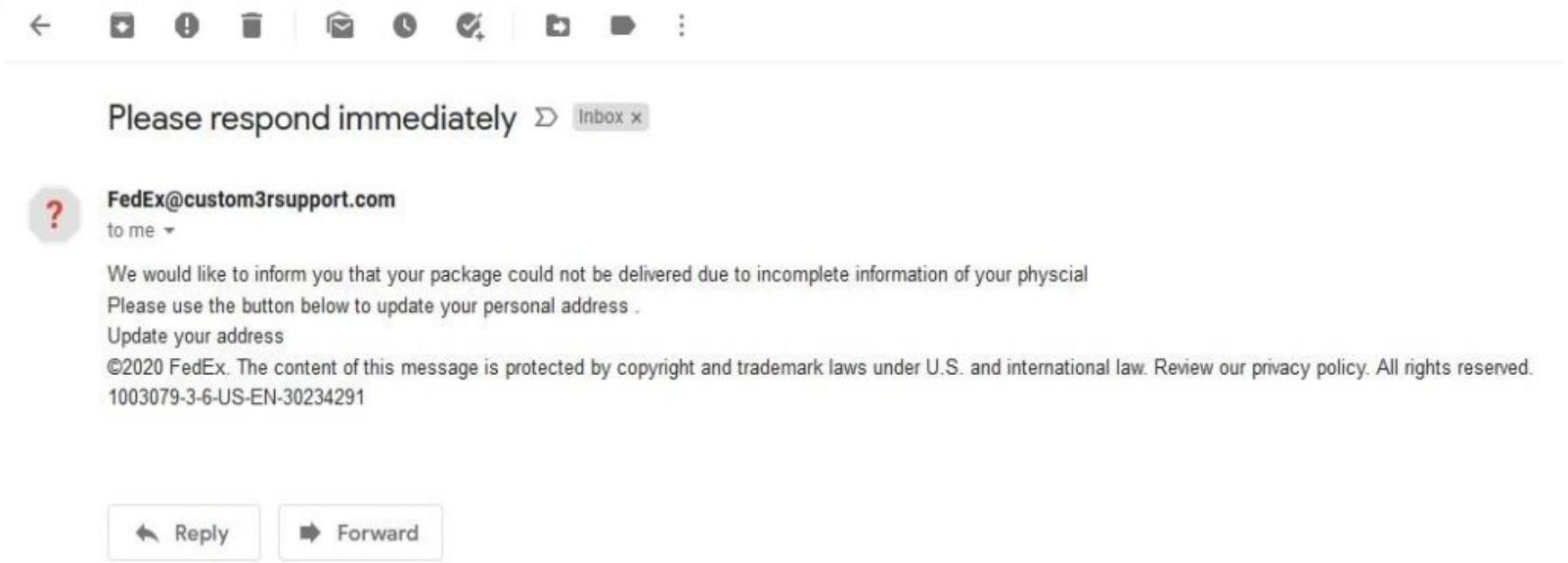
Email Spoofing

- Fraud
- Phishing
- Malware
- Account Takeover
- Email Interception

Email Spoofing -via Display Name



Email Spoofing -via Lookalike Domains



Please respond immediately Inbox ×

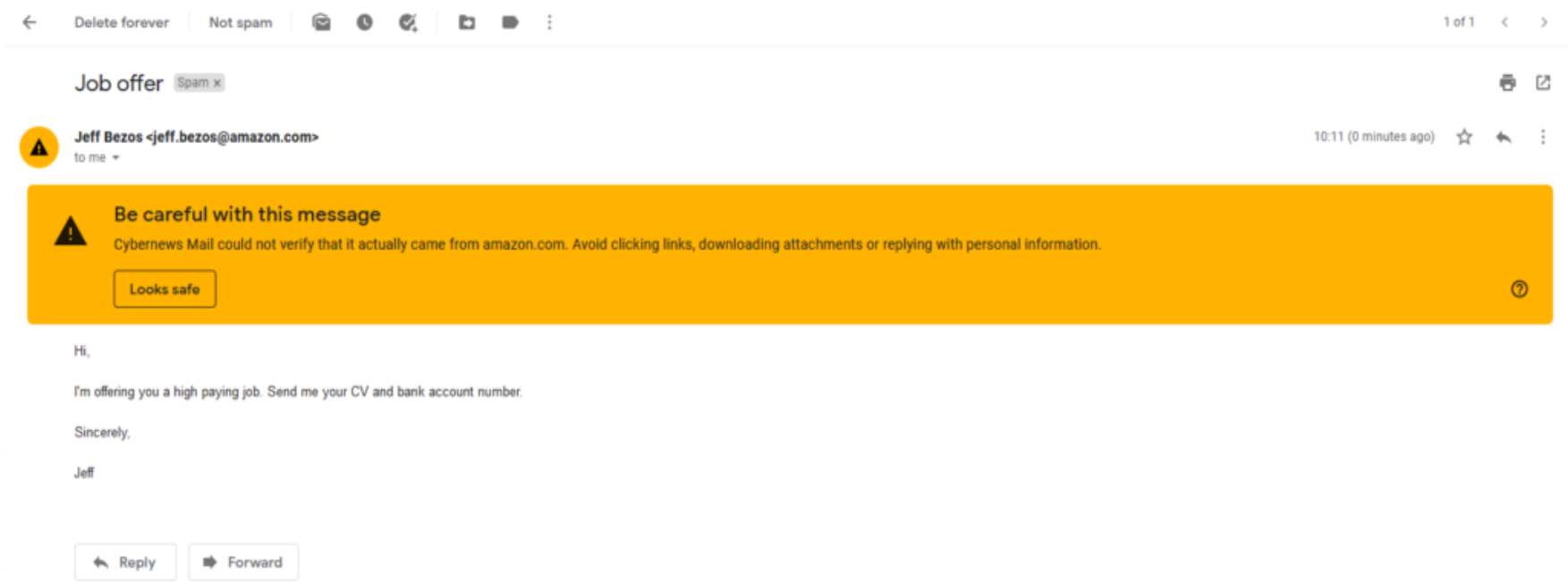
FedEx@custom3rsupport.com
to me

We would like to inform you that your package could not be delivered due to incomplete information of your physcial
Please use the button below to update your personal address .
Update your address

1003079-3-6-US-EN-30234291

Reply Forward

Email Spoofing -via Legitimate Domains



Email Takeover

- Purchasing lists of previously stolen credentials
- Brute force attacks
- Phishing attacks
- Web browser infections
- Spyware

eMail Spoofing - Example

Spoofed Govt Emails

Dear All,

There is a notification from NIC regarding NIC Account Suspension that users will not be allowed to use NIC email services from July 15th onwards due to implementation of KAVACH.
Kindly verify if your KAVACH application is working properly. If a user does not install KAVACH properly his/her account will not be accessible w.e.f. July 16th, And account will be disabled after one week of inactivity.

Verify/Install KAVACH : https://email.gov.in//kavach/verification

From [redacted]88@gov.in>
To: "[redacted]" <[redacted]ar.kandle@gov.in>
Sent: Monday, June 28, 2021 6:15:50 PM
Subject: IAF Attack Jammu : Key Points to note

IAF Attack Jammu 27-June-2021.pdf (53.2 KB) | Download | Briefcase

Dear Sir!

Plz find att docu FYI
Password to unrar: Jammu@27june

Regards,

Informational

URL https://beechtree.co.in/Admin/kavach/index.php is external to the mailing system. Hence, you are requested to go through the URL and ensure its authenticity and then click "Yes" to proceed. Else, click "No" to cancel.

Yes No

HA OJHA Show more...
NSHU PANDE Deepak Virmani

ing NIC Account Suspension that use
rvices from July 15th onwards due to

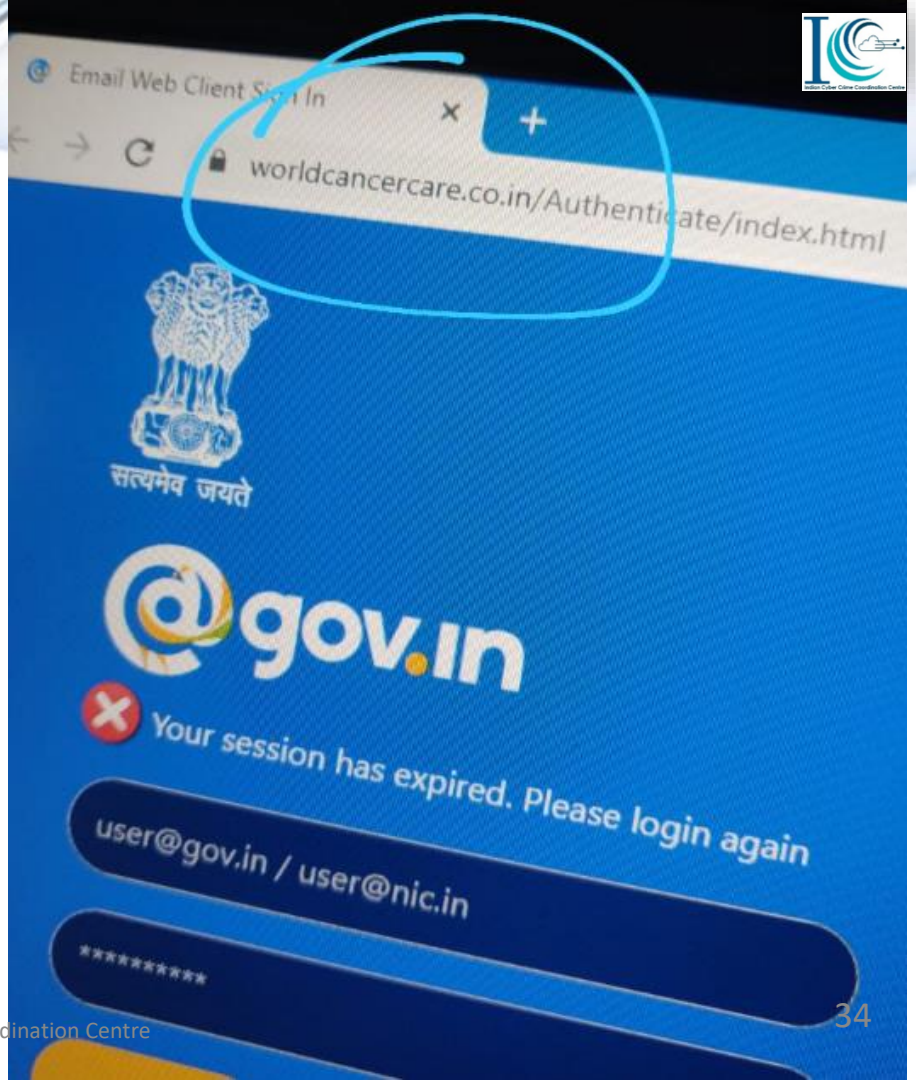
n is working properly. If a user does n
install KAVACH properly his/her account will not be accessible w.e.f. July 16
And account will be disabled after one week of inactivity.

Verify/Install KAVACH : https://em[redacted]gov.in//kavach/verification

Jul 20 6:15 PM
For Comments
Jul 14 4:35 PM

How they hack your eMail?

1. Send a lookalike Email (js@gov.in - js-gov.in)
2. Hack a Government Email Send you an email.
3. Virus Attack – Malware Links, Virus Attachment etc.
4. Virus Attachment type – Document, Installation file, PDF file etc.



Email Security

- Never divert your official mails to other mail servers like gmail, hotmail etc.

Disposable Aliases
kumardavinder@gmail.com
kumar.davinder@gmail.com
kumardavinder+india@gmail.com
k.umardavinder@gmail.com
kumardavinder+2022@gmail.com

Temporary email services
https://temp-mail.org
https://10minutemail.com
https://emailnator.com
https://www.guerrillamail.com/
https://www.emailondeck.com/

Be Careful About Domain Names in Links

onlinesbi.co onlinesbi.co.in onlinesbi.net onlinesbi.sbi onlinesbi.com onlinesbi.info online.sbi.co.in netbank.sbi.com	ssbi.co.in sbi.co.in sb1.co.in sbit.co.in sbi.com sbi.net sbj.co.in wwwsbi.co.in
google.com	google.com

Typoglycemia

1. www.faecbook.com
2. www.tiwtter.com
3. www.timseofindia.com
4. www.hindutsantimes.com
5. www.punjabkseri.com
6. www.unoinbank.com
7. www.flipkrat.com

Email Security

By default, do not trust any link/emails. Verify: URL, Email Address, Sender Details.

Attachments may be dangerous: Refrain from downloading any external / untrusted attachments.

Use Antivirus/End Point Protection installed in computer and do not save password in browser.

Use multi factor authentication with strong password.

Use email encryption and securing services like ProtonMail, StartMail and PGP etc.

What if your eMail gets hacked?

01

Report incident to CERT-NIC - incident@nic-cert.nic.in

02

Immediately change password from clean computer/PC

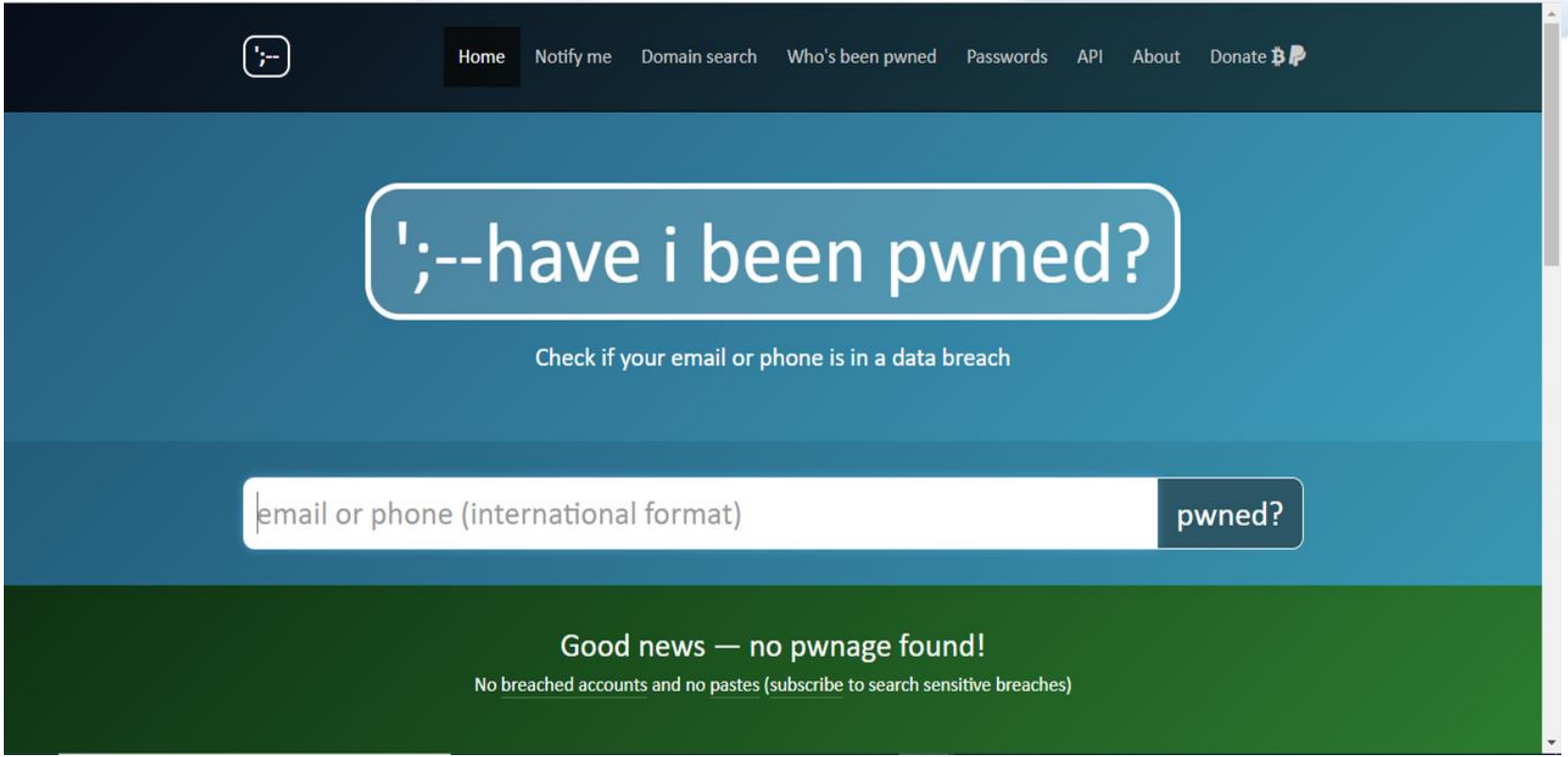
03

Change passwords of other accounts connected with email.

04

Scan computer with Antivirus for possible infection

https://haveibeenpwned.com



Critical Findings of the Cyber Security Audit in Government Departments

No Passwords, Guessable Passwords (India@123, Division_Name@123), No Auto Lock during inactivity

Unregulated USB(AutoPlay enabled), Scanning of USB not enforced

No Data Backup Policy

No Antiviruses, Outdated Antivirus

Unsupported Windows 7on several systems

E-office, NIC Mail Passwords saved in Browsers

Cracked MS Office and similar software

Remote Access Application – AnyDesk, TeamViewer, Quick Support found

No Policy for Formatting or Archiving data before transferring to any new Employee

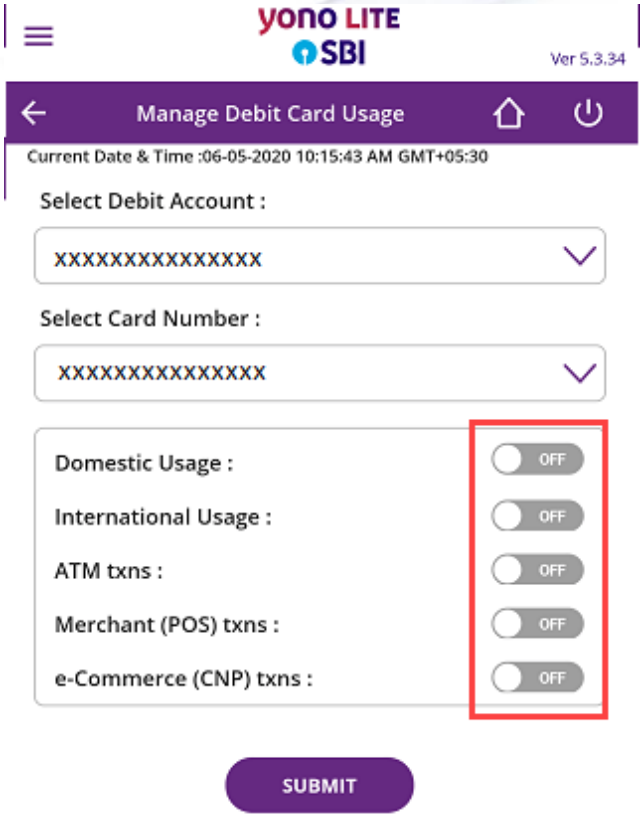
Data sharing over Google Drive, One Drive, WhatsApp

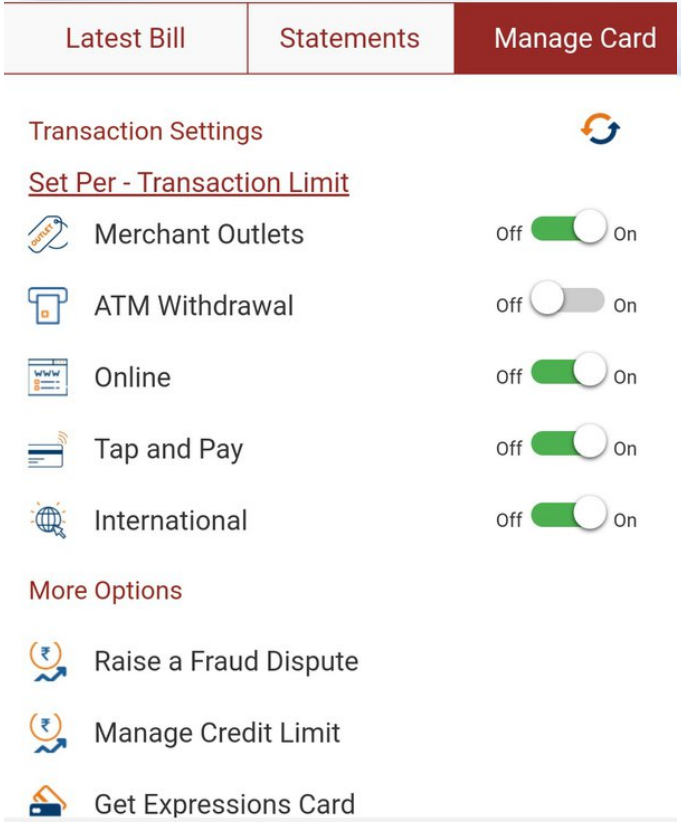
System found infected with Malware

Credit/Debit Card Usage

- Always keep your Credit/Debit Card in safe custody
- Always erase the CVV number printed on card. Write it somewhere and memorise it.
- Never share your card details with someone else including your minor children if any.
- Use EMV(Chip) enabled cards only and ensure that it doesn't has magnetic strip.
- CVV is important as it is used in online transactions. It can also be used for resetting bank account passwords along with other information on debit card.
- Never write down PIN number on card itself.

Set Limits or Switch On/Off Transactions/ATMs





Net Banking Safety Tips

1. Access your bank website only by typing the URL in the address bar of your browser	10. Scan your computer regularly with Antivirus to ensure that the system is Virus/Trojan free.
2. Do not click on any links in any e-mail message to access the site.	11. Change your Internet Banking password at periodical intervals.
3. Do not be lured if you receive an e-mail/SMS/phone call promising reward for providing your personal information or for updating your account details in the bank site.	12. Always check the last log-in date and time in the post login page.
4. Be aware of downloading any malicious application from mobile application stores that are offering Online Banking.	13. Avoid accessing Internet banking accounts from cyber cafes or shared PCs, or via public WiFi
5. Having the following will improve your internet security: • Newer version of Operating System with latest security patches. • Latest version of Browsers • Firewall is enabled. • Antivirus signatures applied	14. After you have logged in, you will not be asked to provide your username and login password again
6. Keep checking your savings account regularly	15. Do not use public computers to login
7. Always use licensed anti-virus software	16. Do not share your details with anyone
8. Ensure to sign up for banking alerts	17. Set the transaction limits in the bank account
9. Enable 2FA/MFA	18. Keep tabs on beneficiary accounts

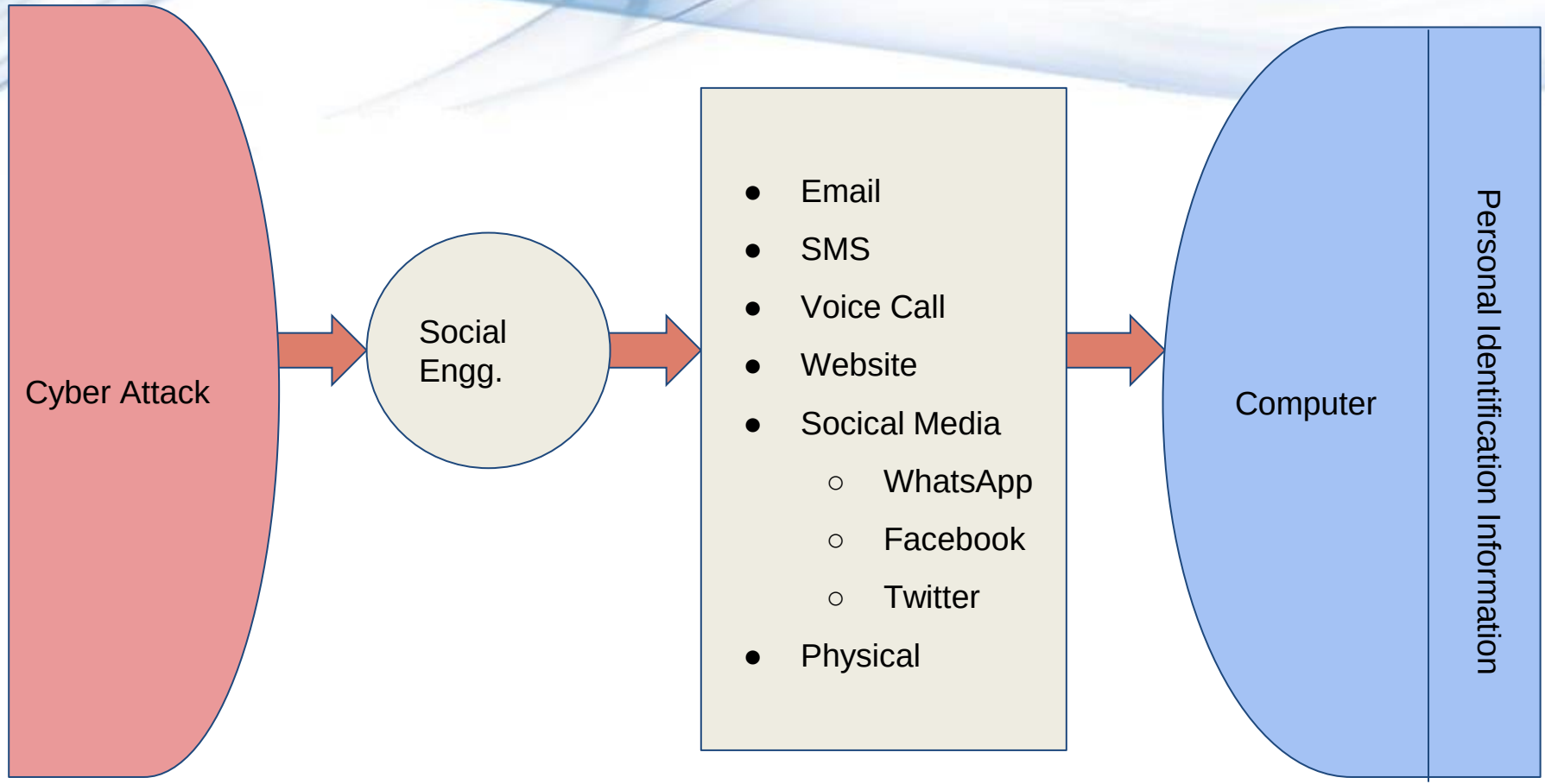
Keeping Passwords Safe and Secure

- Avoid using the same password for different accounts
- Change passwords on a regular basis
- Keep passwords at least 12 characters long (and ideally longer)
- Passwords must involve a mix of upper- and lower-case letters plus symbols and numbers
- Avoid the obvious - such as using sequential numbers(“1234”) or personal information that someone who knows me might guess, such as my date of birth or pet’s name.
- Change the default passwords on my IoT devices, WiFi router etc.
- Avoid writing my passwords down or sharing them with others
- Use a password manager to help generate, store, and manage all my passwords in one secure online account

Social Engineering

Secure Device

Cyber Attack Vectors



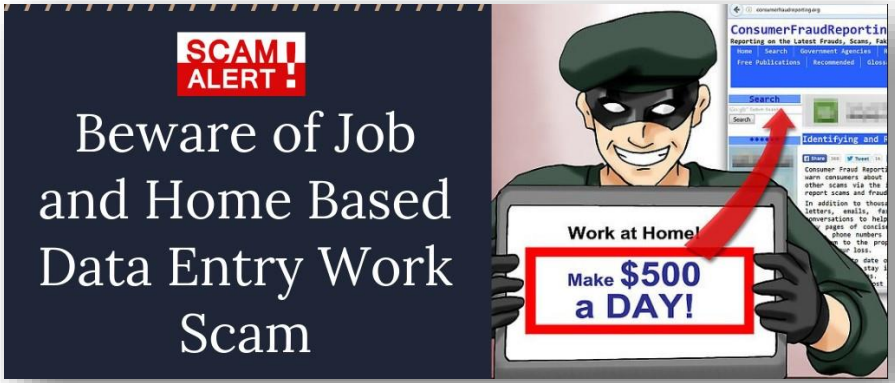
Baiting

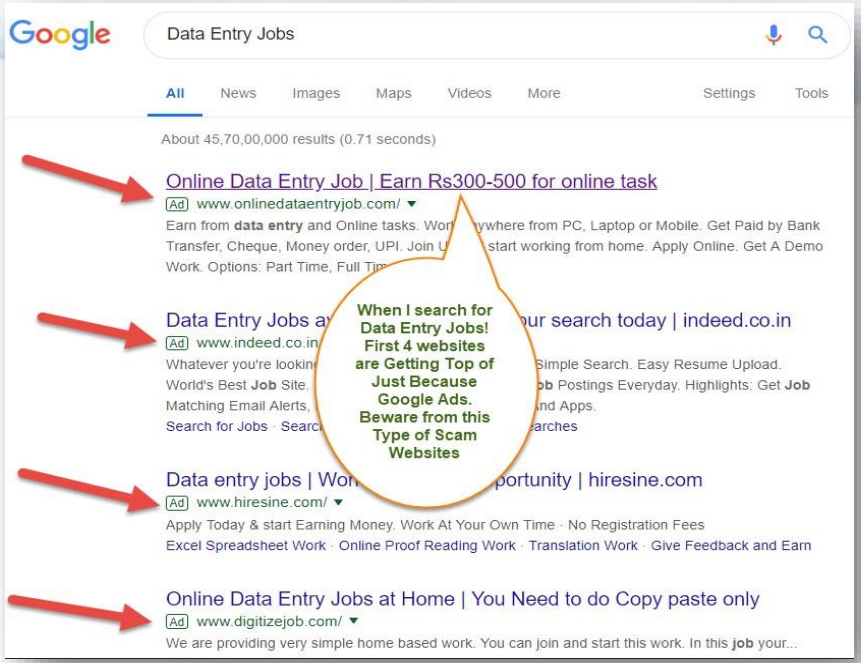

Dear user, congratulations!
We want to thank you for being a loyal Google India user! Your IP address [redacted] has been randomly selected to receive a FREE Apple iPhone X.
From time to time we select a handful of Google users to give them the opportunity to receive valuable gifts from our partners and sponsors. This is our way of thanking you for choosing Google as your preferred search engine.
Today is your lucky day! You are one of the 10 randomly selected users who will receive this gift.
To receive your gift, you simply have to complete our short and anonymous survey. But hurry! There are only a few gifts available today!
How satisfied are you with Google?
Very Satisfied
Satisfied
Unsatisfied

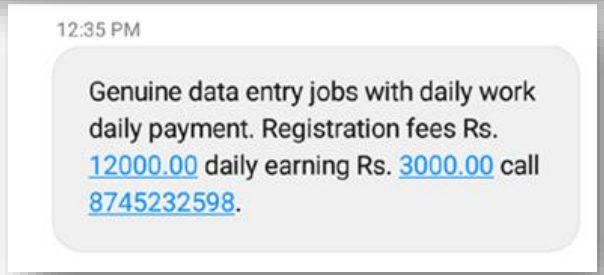
Data Entry Scams

Onlinedataentryjobsinus.Com is a fraud,scam,cheat,bogus

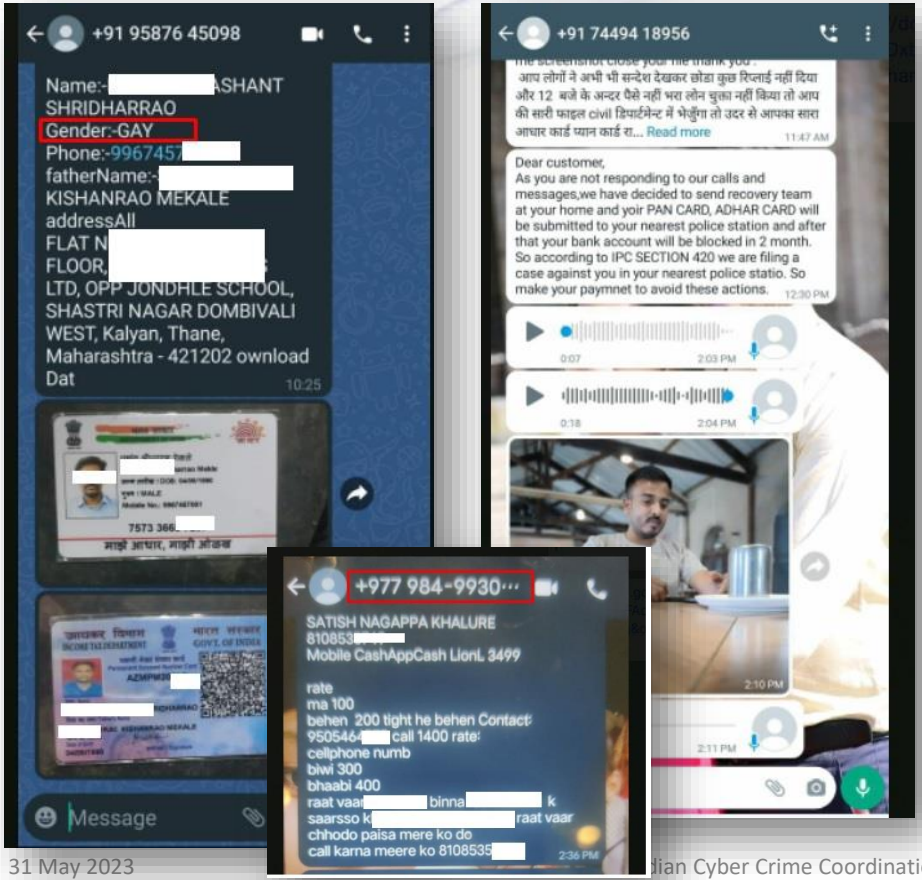
I am vineetha from andhra pradesh,I joined this fraud company on july 27 2012,by apring 3500 rs.In time I completed my work that is 3000 forms , I called them to pay my amount or refund my registration fee , since then they completely started to take the calls. The culprits involved in this fraud are manan (becoz of this idiot mesperizing words I joined the company - he is the real culprit) kunal sharma samir soni - tel. [redacted]4567 ,global.Rahool@gmail.Com anjali vadhva khaledbashwan the mail ids they use are [redacted]@onlinedataentryjobsinus.Com [redacted]@gmail.Com please check in this http:/Www.Scamadviser.Com/ They are several other fraud companies they are running www.Visionjobcare.Com www.Rupdayspa.Info www.Onlinedataentryjobsinus.Com, www.Keyurparmar.Com www.Postaresume.Co.In, kirtangraphics.Com, megabeautyzone.Com, bhavitravels.Com, www.Cyberlobe.Com, strawberrygroup.Com, please take action on them and see that I get my money back hoping to do the needful

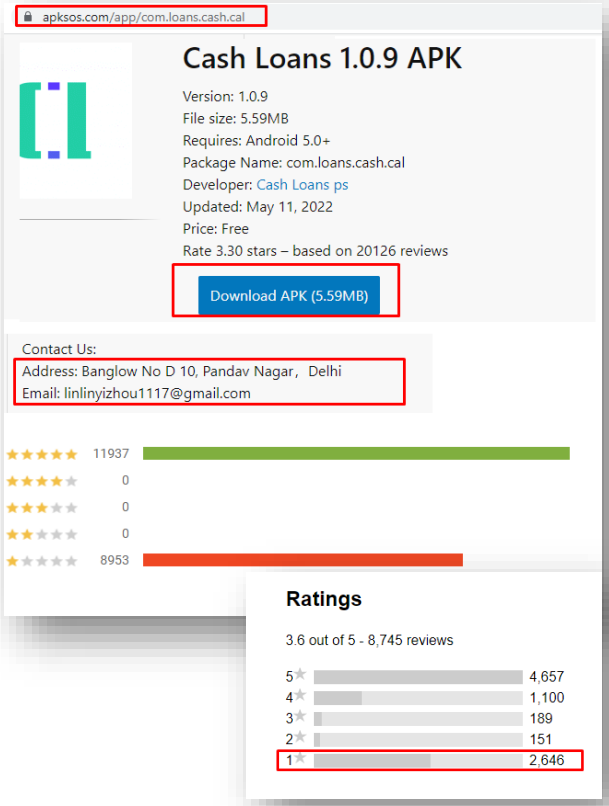




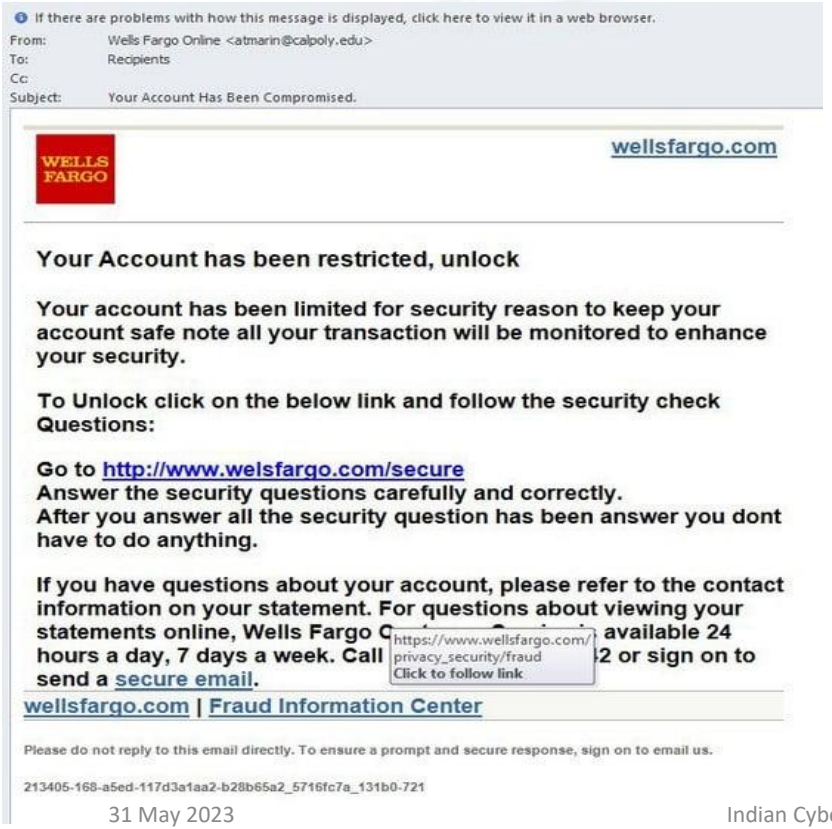


Loan App Frauds





Scareware



If there are problems with how this message is displayed, click here to view it in a web browser.

From: Wells Fargo Online <atmarin@calpoly.edu>
To: Recipients
Cc:
Subject: Your Account Has Been Compromised.

WELLS FARGO

wellsfargo.com

Your Account has been restricted, unlock

Your account has been limited for security reason to keep your account safe note all your transaction will be monitored to enhance your security.

To Unlock click on the below link and follow the security check Questions:

Go to http://www.welsfargo.com/secure
Answer the security questions carefully and correctly.
After you answer all the security question has been answer you dont have to do anything.

If you have questions about your account, please refer to the contact information on your statement. For questions about viewing your statements online, Wells Fargo C... available 24 hours a day, 7 days a week. Call ...2 or sign on to send a secure email.

https://www.wellsfargo.com/privacy_security/fraud
Click to follow link

wellsfargo.com | Fraud Information Center

Please do not reply to this email directly. To ensure a prompt and secure response, sign on to email us.

213405-168-a5ed-117d3a1aa2-b28b65a2_5716fc7a_131b0-721

TrustedB...

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Risk of Pop-ups – Malware/Spyware Installation

Pretexting

Pretexting Scenario: The Internet Service Provider

An "internet service provider" shows up on your doorstep for a routine check. Once inside, they have free reins to snoop through your devices and valuable information.

TIP

If a service provider arrives without an appointment, don't just let them inside. Verify their legitimacy by asking questions about your plan.

Pretexting Scenario: Gift Card Eligibility

You receive an email alerting you that you're eligible for a gift card, but you just need to share some personal information to redeem it.

Congratulations, Steve!

You're eligible for a $5,000 gift card.
To redeem, please share your banking information for wire transfer and also your home address.

Sincerely,
Notareal Co.

TIP

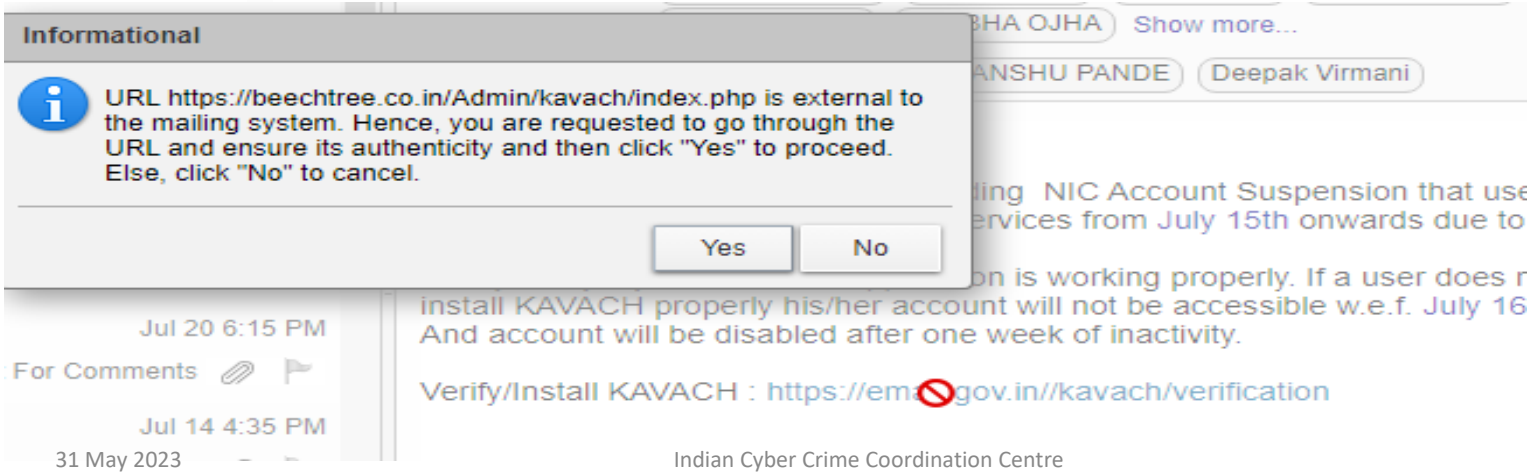
Never share sensitive information via email, phone, or text.

Phishing

Dear All,

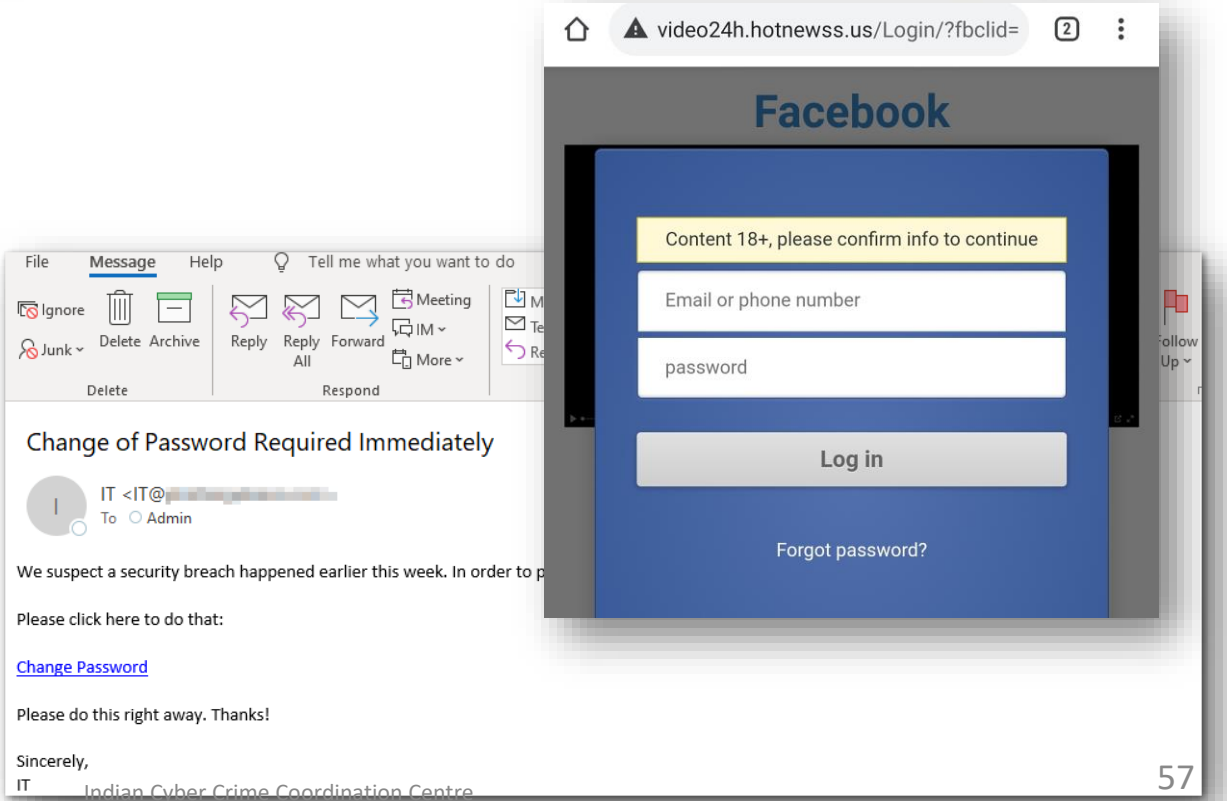
There is a notification from NIC regarding NIC Account Suspension that users will not be allowed to use NIC email services from July 15th onwards due to implementation of KAVACH.
Kindly verify if your KAVACH application is working properly. If a user does not install KAVACH properly his/her account will not be accessible w.e.f. July 16th, And account will be disabled after one week of inactivity.

Verify/Install KAVACH : https://email.gov.in//kavach/verification



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



Quid Pro Quo

From: AdminNotice <ordersender-prod@ansmtp.ariba.com>
Sent: Friday, April 8, 2022 7:39 PM
To. @unitrends.com>
Subject: {Confidential Password} Notification for @unitrends.com

[EXTERNAL]

Office365

@unitrends.com Service Desk

Your credential is due to expire TODAY (Friday, April 8, 2022)

Please take note that you are about to lose access to your mailbox if no action is taken.

Keep Using Current Password

Remote Assistance

BEWARE OF FRAUDULENT
SMS & CALLS ABOUT KYC UPDATION,
BANK ACCOUNT SUSPENSION OR
SIM EXPIRATION

Watering Hole

Diversion Theft

Diversion Theft

- **A Con**
  - Persuade deliver person that **delivery is requested elsewhere** - "*Round the Corner*"
  - When deliver is redirected, attacker pursuades delivery driver to **unload delivery near address**
  - **Ex**: Attacker parks **security van outside a bank**. **Victims going to deposit money** into a night safe are told that the **night safe is out of order**. **Victims then give money to attacker** to put in the fake security van
  - Most companies do not prepare employees for this type of attack

Honey Trap

- A friend request is sent from some unknown person probably a female having mutual friends on Facebook, which is often accepted by the user.
- The request sender starts chatting and during conversation in many cases, people share whatsapp number with the unknown fraudster,
- subsequently, a video chat request is received and the fraudster plays a trick and gets undressed and also instigate the users as well and mostly people are trapped.
- the fraudster records the chat video with live image and starts blackmailing for money to avoid publishing obscene video on social media and to the friends of users.
- Once the money is paid, the demand goes on increasing.


Soniya Patel
Origin Lahore
Playing field South India
Ishanika Ahir
Origin Lahore
Playing field North India
Jasmeet Kaur
Origin Rawalpindi
Playing field Punjab, Haryana
Niha Sharma
Origin Rawalpindi
Playing field North India
RAWALPINDI
LAHORE
PAKISTAN
HYDERABAD
Ankita Kaur
Origin Lahore
Playing field East India
Payal Sharma
Origin Lahore
Playing field North India
The names mentioned are pseudonyms; pictures are from DPs on social media

SANJAY SINGH YADAV, HAWALDAR

DANUNJAY YADAV

RAJESH KUMAR, HAWALDAR

SWAROOP SING, SUBEDAR (RETD)

RAKESH KUMAR, HAWALDAR

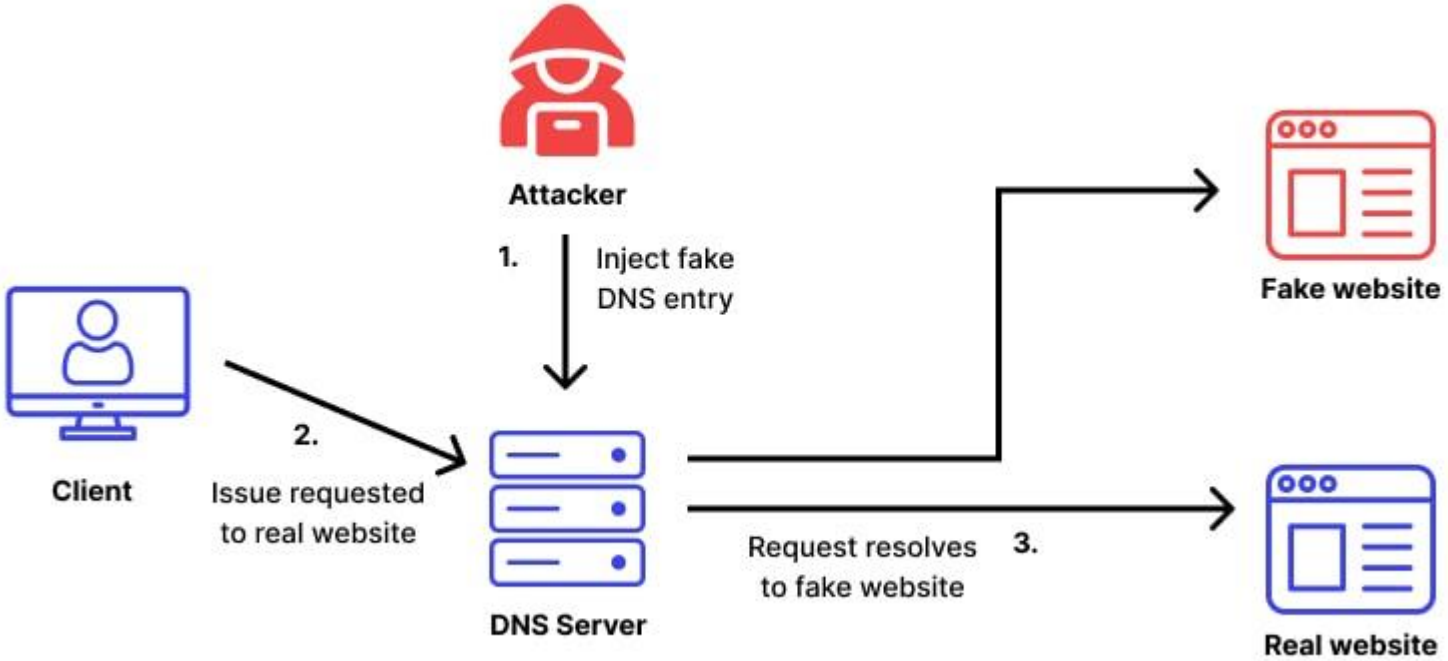
GORDHAN SINGH

Dumpster Diving

Sensitive Contracts of Pentagon Found In Dumping Grounds of Ghana

In the recycling process, the recklessly dumped drives or data assets go through multiple vendors. They can seamlessly access and exploit customer information. Ghana is one of the most toxic electronic-waste dumpsites in the world. Agbogbloshie, a commercial district of Nigeria's capital Accra, is known for conducting recycling processes like reuse, repair, or recycling effective components. Nearly a substantial amount of e-waste is dumped here every single day. Scavengers use the sight to extract valuable metals from the trash alongside technology components like power banks, batteries, CPUs, storage mediums, casings, circuit boards, and so on. Sensitive U.S. security data were reportedly found amidst the e-waste i Ghana, as journalism students on study tour purchased hard drives in open-air market. Further examination of hard drives revealed that it contained multimillion-dollar defense contracts between the Pentagon, Department of Homeland Security and Northrop Grumman, one of the largest military contractors in the U.S. Such paramount lapses and breach of security normally goes unnoticed unless recorded, but it does bring to fore the hassles of dumpster diving and the need to prevent the same.

Pharming


Attacker
1.
Inject fake
DNS entry
Fake website
Client
2.
Issue requested
to real website
DNS Server
Request resolves
to fake website
3.
Real website

Curiosity

FedEx®

Express

Parcel Tracking

Dear Customer,

There is a package bearing your name at our local dispatch facility.

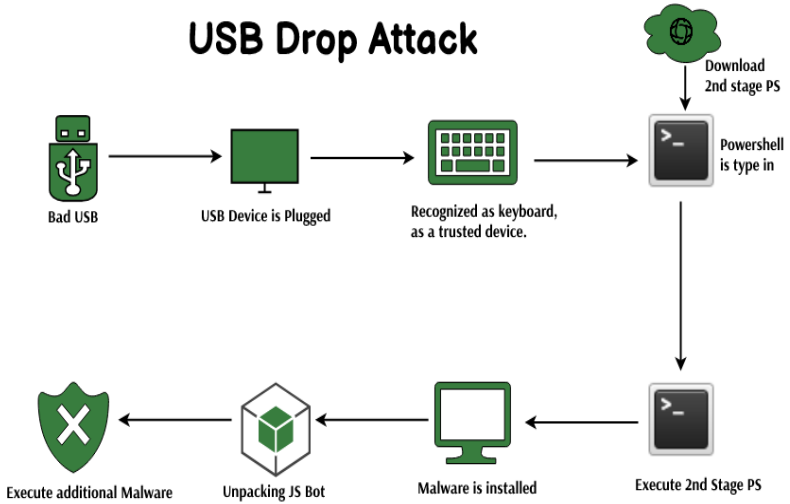
Our courier was unable to deliver the parcel due to incorrect delivery d

Please see below to confirm your delivery address with us to ensure sm

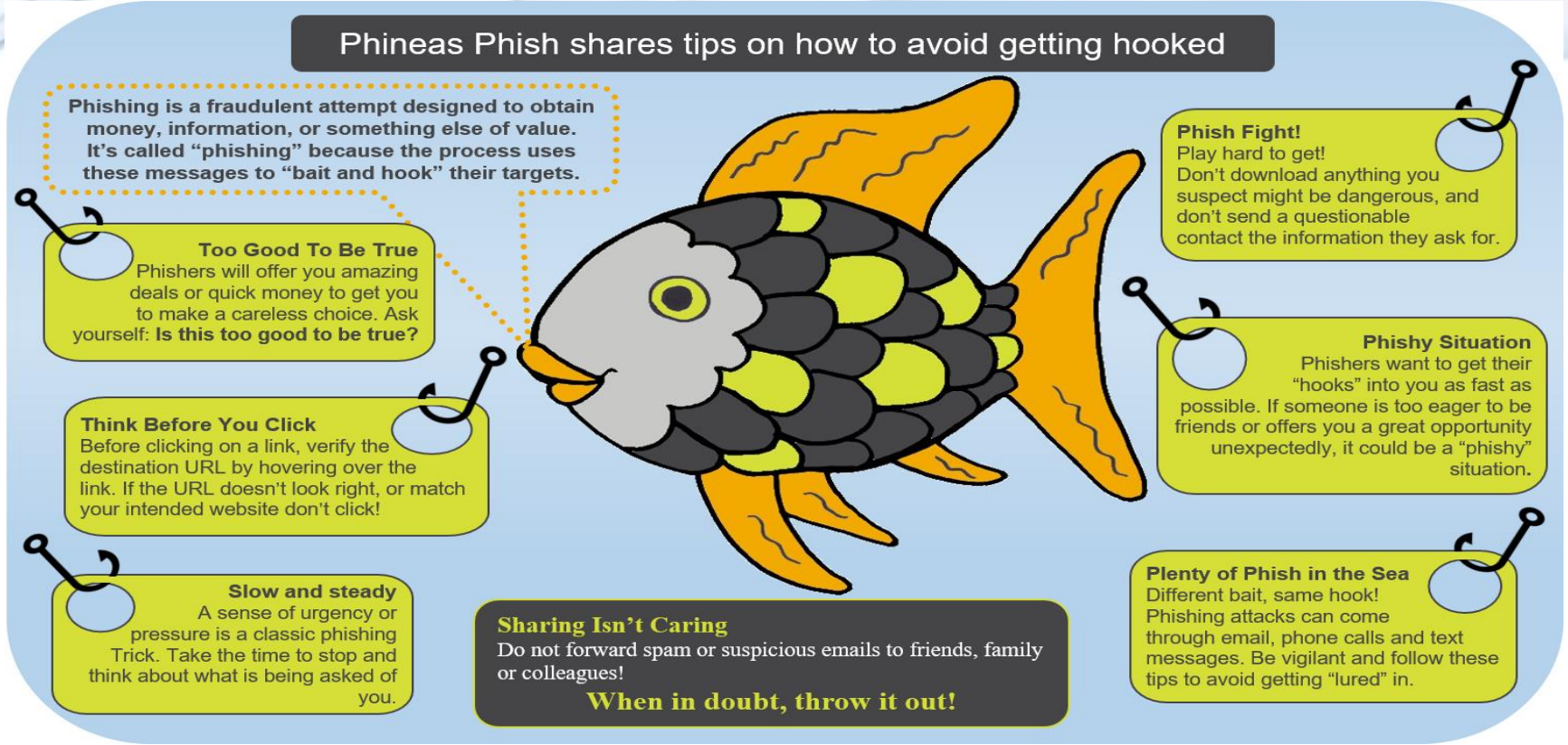
FedEx Parcel Tracking Info

Best Regards

FedEx Redstar Express



How to Prevent Phishing



How To Prevent Phishing

1. Learn to Identify Phishing • Urgency • Money Baits • Grammer Mistakes • Impersonal Messages	**2. Don't Fall Into the False Sense of Security** • Be Aware of Spear Phishing • Learn to Recognise Targeted Phishing Tactics
3. Don't Click on That Link • Triple-Check the Authenticity of Every Mail • Do Not Click on Links Inside Email Messages	**4. Don't Trust Unsecure Sites** • Ensure the URL of the Website Starts with https:// • Ensure there is closed padlock icon next to the URL
5. Don't Disclose Personal Information • Never Enter Personal Information on Suspect Sites • Do Not Share Sensitive Information on Your Social Media	**6. Update Regularly** • Keep Your Software Up to Date • Turn On Automatics Updates • Always Update Your Browser
7. Block Pop-Ups to Prevent Phishing • Use Popup-Blocking and Anti-Phishing Addons • Always Close Pop-Ups Using the X Sign in One of the Corners	**8. Enable 2FA With WenAuthn/U2F Security Keys** • Deploy Two-Factor Authentication or Multi-Factor Authentication For All Your Users • Use WebAuthn/U2F Security Keys to Prevent Phishing
9. Enable Firewalls • Enable Filtering on Your Email Server • Use Network Firewall • Use Desktop Firewall	**9. Raise Phishing Awareness** • Conduct a Security Training For Your Employees • Be Aware of Other Kinds of Cyberattacks

Mitigation

Table 1	
Maximum Liability of a Customer under paragraph 7 (ii)	
Type of Account	Maximum liability (₹)
• BSBD Accounts	5,000
• All other SB accounts • Pre-paid Payment Instruments and Gift Cards • Current/ Cash Credit/ Overdraft Accounts of MSMEs • Current Accounts/ Cash Credit/ Overdraft Accounts of Individuals with annual average balance (during 365 days preceding the incidence of fraud)/ limit up to Rs.25 lakh • Credit cards with limit up to Rs.5 lakh	10,000
• All other Current/ Cash Credit/ Overdraft Accounts • Credit cards with limit above Rs.5 lakh	25,000

Table 2	
Summary of Customer's Liability	
Time taken to report the fraudulent transaction from the date of receiving the communication	Customer's liability (₹)
Within 3 working days	Zero liability
Within 4 to 7 working days	The transaction value or the amount mentioned in Table 1, whichever is lower
Beyond 7 working days	As per bank's Board approved policy

Mitigation

- Immediately call at 1930 (within one hour of fraud)
- Register your complaint at https://cybercrime.gov.in
- Keep screen shots and bank details handy for uploading on the site
- Register your complaint with the Bank or FinTech company, whatever is applicable

Resources

S.No	Resource URL	Description
1	https://www.meity.gov.in/cyber-security-division	Laws, Policies & Guidelines
2	https://www.cert-in.org.in/	Security Advisories, Guidelines & Alerts
3	https://nic-cert.nic.in/	Security Advisories, Guidelines & Alerts
4	https://www.csk.gov.in/	Security Tools & Best Practices
5	https://infosecawareness.in/	Security Awareness Materials
6	http://cybercrime.gov.in/	Report Cyber Crime, Cyber Safety Tips
7	https://infosecawareness.in/article/govt-emp-guidelines	Cyber Security Guidelines for Govt. Employees
8	https://rbidocs.rbi.org.in/rdocs/content/pdfs/BEAWARE07032022.pdf	BE(A)WARE: A Booklet on Modus Operandi of Financial Fraudster

Quiz