CYBER JAGROOKTA 2022-2023

NAUGHTY NATU

"SEE YOURSELF IN CYBER"

WIT & BIT

Booklet on Cyber Incidents & Preventive Measures

यूको बैंक
(भारत सरकार का उपक्रम)

UCO BANK
(A Govt. of India Undertaking)

सम्मान आपके विश्वास का

Honours Your Trust

By CISO Office

यूको बैंक

UCO BANK

विज़न

सूचना की सुरक्षा हेतु बैंक के लिए
एक सुरक्षित साइबर स्पेस बनाना

Vision

To build a secure and resilient cyber space for the Bank to protect information

मिशन

बैंक की बुनियादी संरचना, व्यक्ति, प्रक्रिया और प्रौद्योगिकी के सम्मिलन से साइबर स्पेस में सूचना तथा बुनियादी संरचना की सुरक्षा करना, साइबर के खतरों को रोकना एवं अनुक्रिया करना

Mission

To protect information and information infrastructure in cyber space, build capability to prevent and respond to cyber threat, reduce vulnerabilities and minimize damage from cyber incidents through a combination of the Bank infrastructure, people, process and technology

TABLE OF CONTENTS

From the Desk of MD & CEO

Dear UCOites,

At this juncture of business evolvement through major technological advancements, the on-going exponential growth of cyber threats is a vital concern. Though tools and technologies are in place to defend cyber-attacks, inculcating a habit of cyber awareness basics among the users is a must to defy cyber-crimes exploiting human vulnerability. Lack of user awareness and ignorance is a matter of concern. Government of India is also emphasizing through various initiatives and mass campaigns to enhance cyber awareness among citizens and thereby prevent cyber crimes.

In cognizance of Government Directive, Bank is observing Cyber Jagrookta Diwas to extend cyber awareness best practices to staff members as well as customers. The month of October is also celebrated as Cyber Security Awareness Month with the theme "See Yourself in Cyber", focussing on the "People" aspect of cyber security. With the extensive awareness campaigns and initiatives designed by CISO team, each and every employee should inculcate cyber hygiene at the workplace and sensitize customers.

Security Awareness is an ongoing commitment where we all have to do our part to make cyberspace safer by embracing stronger security practices, vigilant measures and raising community awareness.

I appreciate the initiative taken by CISO team in creating mass awareness through this informative handbook covering recent cyber frauds and their best practices.

I am confident that this handbook will be beneficial in increasing cyber hygiene among a larger user-base.

With warm regards,

(**Soma Sankara Prasad**)
MD & CEO

From the Desk of Executive Director

Dear UCOites,

Over the past few years, our Bank has technologically evolved manifold with deployment of advanced tools and technologies, integration with FinTechs and other technical developments. This rapid evolvement has inevitably brought in its own unique challenges, besides aggravating the existing threat scenario. Technological proliferation with rapid adoption of cloud, robotics, artificial intelligence, machine learning, augmented reality etc. across various spheres is interlinked with expansion in cyber threat landscape. Bank has deployed robust security solutions to safeguard Bank's IT infrastructure from cyber threats, but the risks arising out of human vulnerability is a vital concern.

Government of India is also focusing on increasing cyber hygiene in both employees of the organization and public at large by focusing on inculcating habit of taking basic care of the Information, Communication & technology (ICT) devices. We can say cyber hygiene and cyber crime are inversely proportional. Therefore, more we invest on increasing cyber hygiene, more we will contribute towards decreasing cyber crimes.

I appreciate CISO team in undertaking extensive campaigns to augment cyber quotient of employees and build a cyber-secure culture at the workplace. Zonal Offices and Branches are also observing Cyber Jagrookta Diwas on the first Wednesday of every month, to sensitize our employees and customers for enhancing the overall cyber resilience of a larger user base.

This handbook written in a lucid way will assist in generating awareness on modus operandi being used by fraudsters in committing cyber crimes and also how to get themselves saved. This will also serve as an awareness initiative of the Bank for employees as well as customers.

With warm regards,

(**Ishraq Ali Khan**)
Executive Director

From the Desk of Chief Vigilance Officer

Dear Friends and Colleagues!

Technology is a double-edged sword, both empowering us, as well as making us vulnerable to threats ever evolving, even as we speak! To complicate matters further, our country is characterized by fairly low digital literacy and a low sense of cyber security awareness. Put together, the situation is ripe for an explosive situation!

Increased use of the internet, remote working and automation are contributing to this growing trend of cyber-crime. Our reliance on technology has increased exponentially and in a parallel manner so has cyber-crime intensified, especially post pandemic. Make a quick checklist of things you order online, from food, to medicines, grocery items, clothes and electronics. And this list is hardly exhaustive! Think of all your banking transactions you have moved online. We have our digital footprints all over the web and there are cyber criminals waiting to step into our shoes!!

Some of the common cyber-threats include phishing, social engineering, spam, malware and ransomware, identity and impersonation fraud that one is already familiar with, sometimes a bit too familiar as incidents like this have happened to our own known persons, maybe even to us. The only positive part ironically is that 90% of the incidents are due to human negligence so much of the preventive measures are literally in our own hands.

This booklet will hopefully throw some much needed light on cyber-security and cyber related awareness. Simple steps go a long way, like (a) pause before you click (b) do not leave your devices unattended (c) install anti-virus (d) practice good password management (e) back up your data.

Let not negligence cost us our hard earned money or reputation.

Best Wishes,

(**Ranjana Bose**)
Chief Vigilance Officer

From the Desk of Chief Information Security Officer

Dear Colleagues,

Cyber-security is the convergence of **People**, **Processes** and **Technology** that come together to protect organization, individuals or networks from digital attacks. In the backdrop of expanding cyber threat landscape, cybercriminals are leveraging advanced techniques in exploiting vulnerabilities across system software, hardware, network, as well as human resources.

Now-a-days, organizations have become well equipped with technical tools and solutions protecting the perimeter from targeted threats. As a result, hacker have inclined towards targeting users as it takes comparatively less time and efforts than finding the vulnerabilities in the system, dodging the associated security and performing the successful attack. Increased digitization has also put a thrust for the need of a safe and secure Cyber Environment.

As a part of our constant endeavor in sensitizing the mass user base on cyber security awareness, we are glad to bring out this compendium of illustrative portraying few recent trends of cyber frauds and best practices.

In this cyber predominant era, I am confident that this compendium will act as a useful resource to reskill and upskill our cyber knowledge quotient, remain vigilant, follow cyber hygiene and build a cyber safe culture in the cyber domain.

Be Cyber Jagrook and See Yourself in Cyber !!!

With warm regards,

(**Mohammad Sabir**)
Chief Information Security Officer

WHO IS NATTU?

Nattu is a mischievous character who always finds a unique way to dupe innocent people. He is an expert at pulling cyber scams with common people like us. As internet has become an inevitable part of our lives, we have become more vulnerable to SCAMMERS like Nattu.

Fake emails showing urgency to respond

Fake SMS luring with spurious links

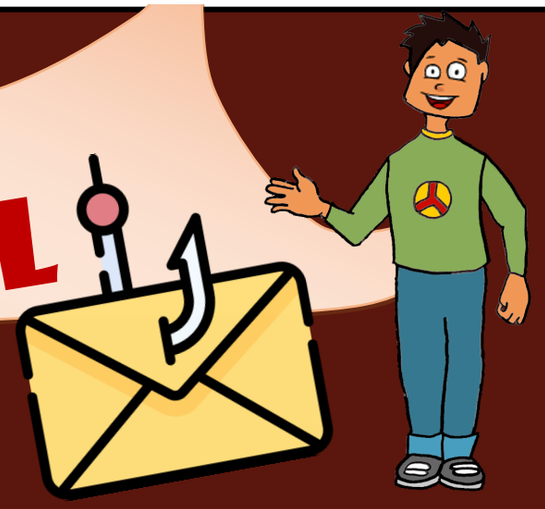
Fake Pop-ups asking for immediate action

Fake website capturing sensitive information

Fake calls asking confidential information

Beware of Nattu's Tricks!!

SCAM THROUGH FAKE EMAIL



Nattu somehow gathered the email IDs of various school authorities and sent random mails for accepting the donation of Rs.2.5 lacs for development of the school & children welfare.

From: **ABC Charitable Trust <abc420@hotmail.com>**
To: **Tanya Talwar <principal@xyz.edu>**
Subject: Avail Donation of Rs. 2.5 lacs !

Respected Principal,

We are a Non Profitable Trust that works under **State Government Educational Wellfare Committee**. We provide funds for devlopment of educational institutions and also for children's' welfare. We are privileged to inform you that this time your school has been shortlisted for availing the **donation of Rs. 2.5 lacs**. **Today is the last date for Registration**. Registration link is given below.

www.fakelink.com/onlineregistration.html

Regards,
Secretary & Trustee
ABC Charitable Trast

Mrs. Talwar, principal of XYZ School was very excited to see the mail and in no time clicked the link.

SCAM THROUGH FAKE EMAIL... CONTD

http://www.fakelink.com/onlineregistration.html

SCHOOL REGISTRATION FOR DONATION

Name of the School -

Principal

First Name | Last Name

Teacher-in-charge

First Name | Last Name

Address of the School -

School Identification Number -

Bank Account Number of School -

IFSC Code -

SAVE and NEXT

Mrs. Talwar filled up all the details and proceeded further.

http://www.fakelink.com/onlinepayment.aspx

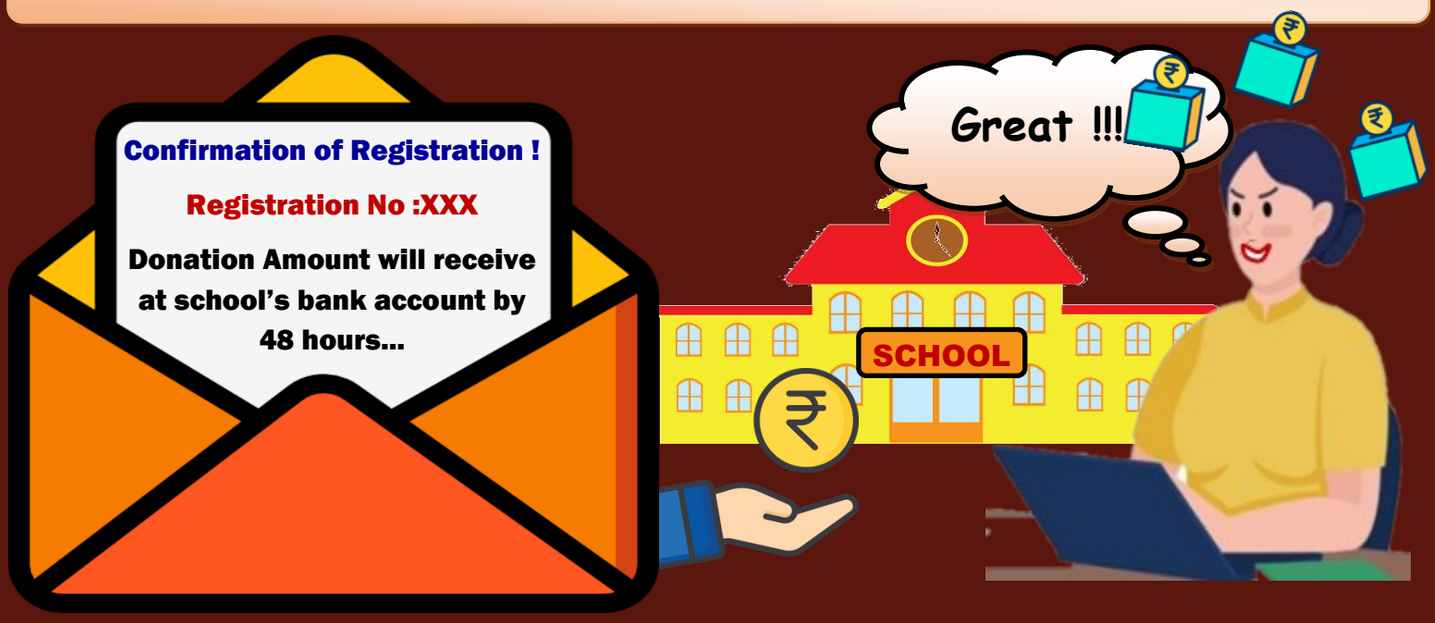
For First Time Registration, please pay Rs.20000/- as Security Deposit which will be refunded to school along with the Donation Amount.

Choose payment option

PROCEED TO PAY

Mrs. Talwar paid the amount of Rs.20000 through card and received a confirmation email of registration.

SCAM THROUGH FAKE EMAIL... CONTD



After few days, Mrs. Talwar checked the bank account of the school. But no amount was received as donation. She tried contacting through mail but Nattu deactivated the sender email account. After that she found an official website of ABC Charitable Trust. After making direct communication with the secretary she realized that she has been duped via fake Phishing Email.

Know the Signs of Phishing Email

Mismatch between sender's name and email address

Unofficial domain of email sender

From: **ABC Charitable Trust** <*abc420@hotmail.com*>
To: **Tanya Talwar** <*principal@xyz.edu*>
Subject: Avail Donation of Rs. 2.5 lacs !

Eye-catchy subject

Respected Principal,

We are a Non Profitable Trust that works under **State Government Educational Wellfare Committee**. We provide funds for devlopment of educational institutions and also for children's' welfare. We are privileged to inform you that this time your school has been shortlisted for availing the **donation of Rs. 2.5 lacs**. **Today is the last date for Registration**. Registration link is given below.

Contains Spelling mistake

www.fakelink.com/onlineregistration.html

Urgency to Respond

Regards,
Secretary & Trustee
ABC Charitable Trast

Include malicious link

PHISHING SCAMS

Signs of PHISHING !!

UCO Bank never asks for sensitive information like Aadhaar Number, Password, OTP, Card Number, Expiry Date, CVV, PIN etc. over Email / SMS / Phone Call

WHAT SCAMMERS NEED FROM YOU ?

- Passwords
- Financial Information
- Identity
- Money

BEWARE OF

- Suspicious Email Senders
- Unknown Links
- Attachments

AVOID PHISHING EMAILS !

Follow the Flowchart

Be Cyber Smart

Received Email from External Source?

No

Carry on

Yes

Contain a link?

Contain an attachment?

Ask for sensitive information?

No

No

No

Yes

Don't be Quick

Think Before You Click

Know the sender?

Carry on

No

Yes

Can you verify the sender?

100% sure about sender?

No

Yes

Yes

Report to the Respective Authority & delete the mail

- Hover over links to see destination
- Call a known phone number and ask about the message
- Visit trusted website to validate the info

Carry on

Don't take the bait... Stay Aware, Stay Safe

रियलिटी शो के नाम पर साइबर धोखाधड़ी

नट्टू फिल्मी सितारों की नकल बहुत अच्छे से करता था। एक दिन उसने अमिताभ बच्चन की आवाज की नक़ल के साथ एक ऑडियो संदेश रिकॉर्ड किया।

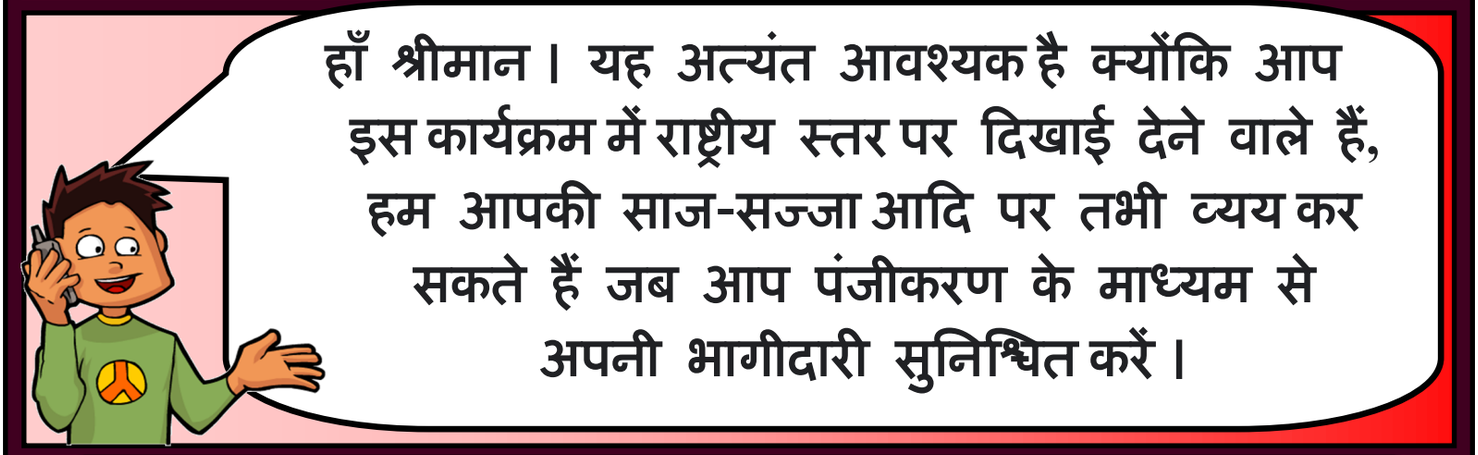
क्या आप "कौन बनेगा करोड़पति ?" खेलने का अवसर चाहते हैं? अगर हाँ तो 878XXXXX985 पर संपर्क करें।

चिंटू नाम के एक लड़के ने बड़े उत्साह से उस नंबर पर कॉल किया।

हेलो। मुझे अभी-अभी क्विज़ शो में भाग लेने के संबंध में एक संदेश प्राप्त हुआ है।

हाँ श्रीमान चिंटू जी, बधाई हो । आपको "कौन बनेगा करोड़पति ?" खेलने के लिए चुना गया है। क्या आप पंजीकरण करना चाहेंगे ?

रियलिटी शो के नाम पर साइबर धोखाधड़ी... जारी

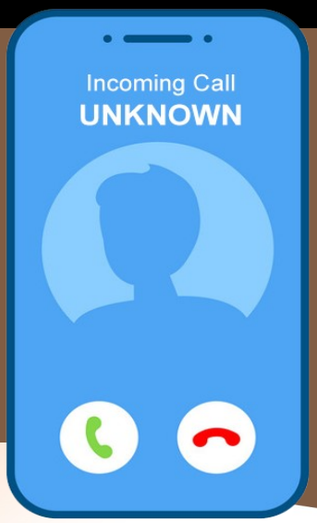


चिंटू ने नट्टू के निर्देशानुसार भुगतान किया जिसके पश्चात नट्टू ने कॉल काट दिया। चिंटू ने उसे कॉल करने की बहुत कोशिश की लेकिन नंबर स्विच ऑफ आता रहा। उसे जल्द ही एहसास हो गया कि फर्जी कार्यक्रम के नाम पर उसे ठगा जा चुका है।

साइबर सुरक्षा युक्तियाँ:

1. लुभावने ऑफर वाले अंजान कॉलर पर भरोसा न करें, हो सकता है कि वे आपका विश्वास जीतने के लिए चर्चित हस्तियों का रूप धारण कर रहा हो।
2. रियलिटी शो चैनल की आधिकारिक वेबसाइट पर जाकर देखें कि क्या वास्तव में ऐसा कोई प्रस्ताव दिया गया है।

Phishing through Phone Calls & SMS

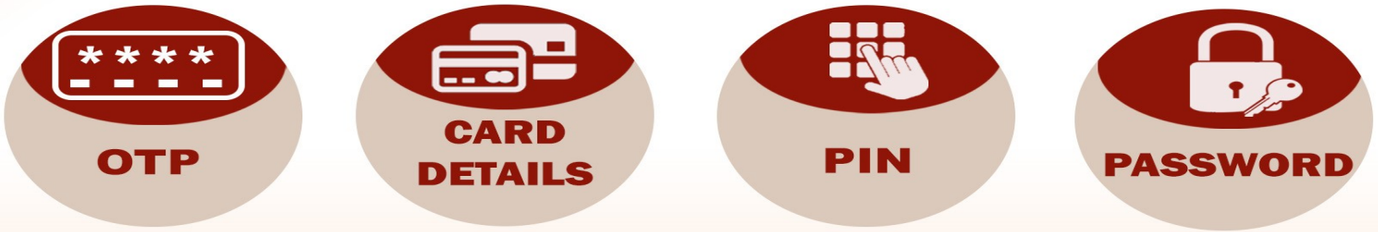


Unsolicited Calls !

STAY ALERT..

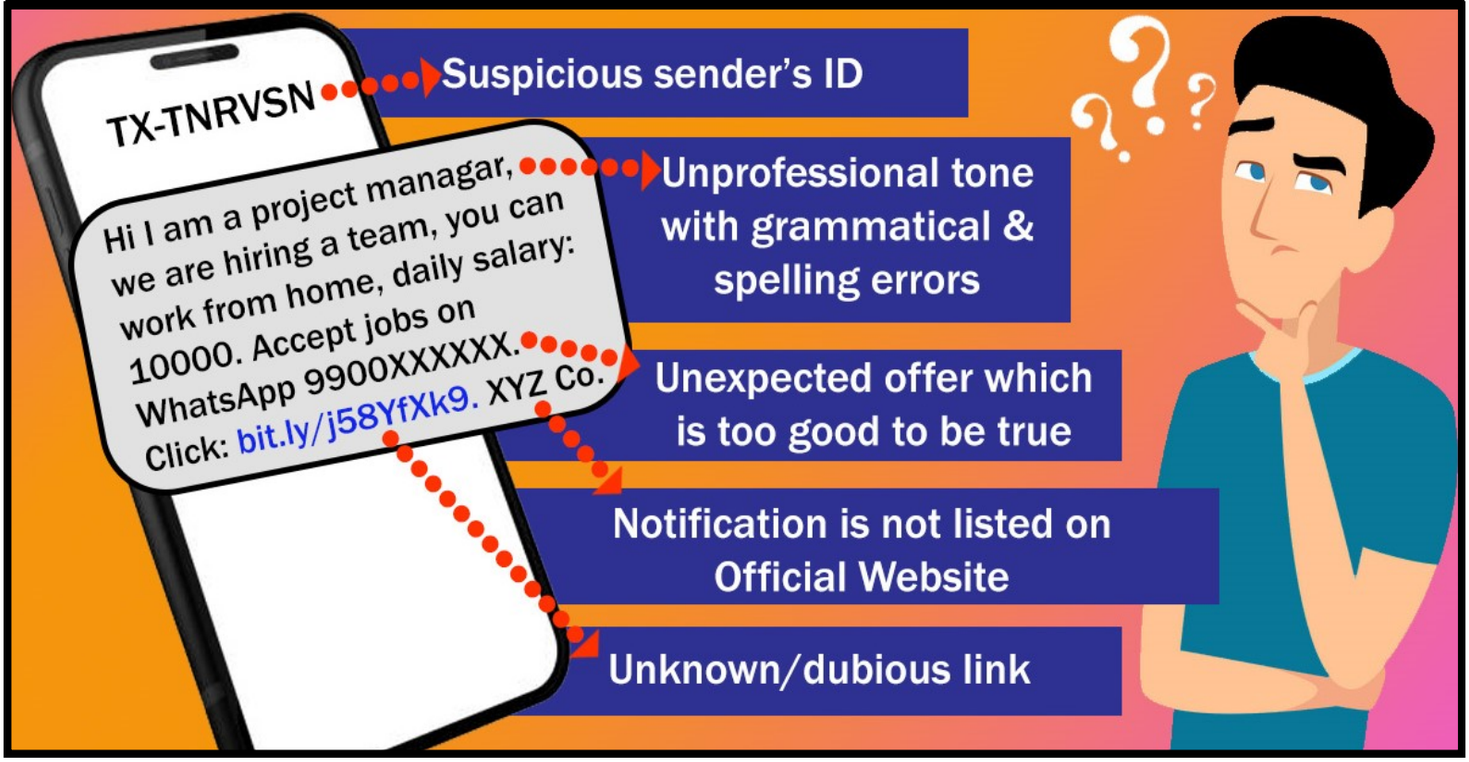
Always be careful of unsolicited phone calls/emails/SMSs asking for personal or sensitive information.

DO NOT SHARE YOUR



WITH ANYONE

HOW TO SPOT A FAKE MESSAGE ??



Let's take a BREAK...

Crossword Zone

Crossword 1

	Down
1	Fraudulent phone calls purporting to be
2	Phishing through SMS / Text message

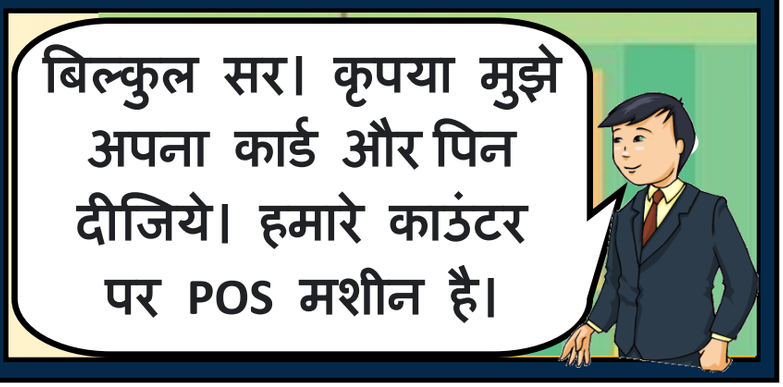
	Across
3	Email targeting to a group of people working in a same department
4	Unauthorized entry into restricted places by following someone

कार्ड के जरिये साइबर धोखाधड़ी

एक दिन नट्टू ने कुछ पैसे देकर एक रेस्टोरेंट के वेटर से दोस्ती कर ली और दोनों ने मिलकर वहां आने वाले ग्राहकों को ठगने की योजना बनाई।

ग्राहक ने खाना ऑर्डर किया और खाना खत्म करने के बाद वेटर को बुलाया।

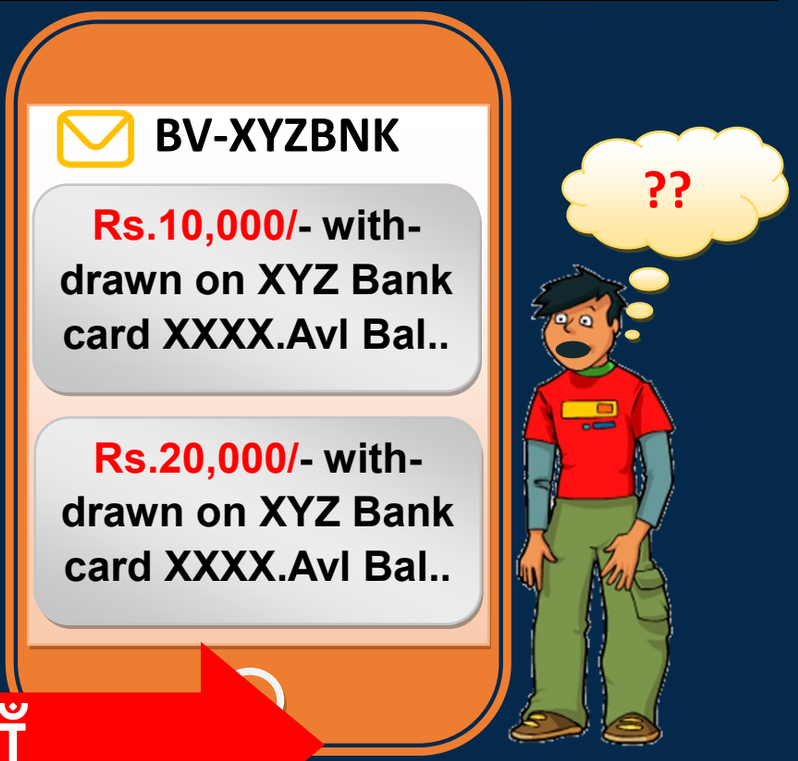
वेटर ने बिल दिया।



कार्ड के जरिये साइबर धोखाधड़ी... जारी

ग्राहक ने अपना कार्ड वेटर को दे दिया और पिन भी बता दिया।

नट्टू ने उस कार्ड का इस्तेमाल करके कई बार ग्राहक के खाते से पैसे निकाल लिए।
बहुत से ट्रांसक्शन मैसेज देखकर उसे एहसास हुआ की उसके कार्ड का गलत इस्तेमाल हुआ है।



साइबर सुरक्षा युक्तियाँ

अपना कार्ड अपरिचित व्यक्तियों को न दें।
अपनी आंखों के सामने पीओएस मशीन मँगवाकर भुगतान करें ।

POS मशीन के माध्यम से भुगतान करते समय, अपना पिन साझा न करें या इसे मुख से न बोलें, बल्कि मशीन में गुप्त रूप से अंकित करें।

ATM SAFETY

TYPES OF ATM FRAUD

SAFETY PRECAUTIONS

Cover keypad while entering your ATM PIN

Do not share your ATM PIN and ATM Card with anyone

Don't ask strangers for help

Keep records of your transactions

Check ATM for any fraudulent devices attached

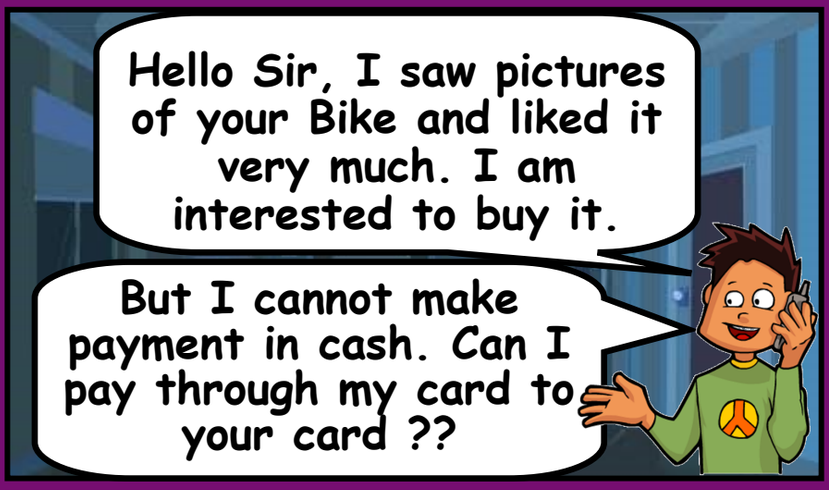
Before leaving, make sure your transaction cycle is complete

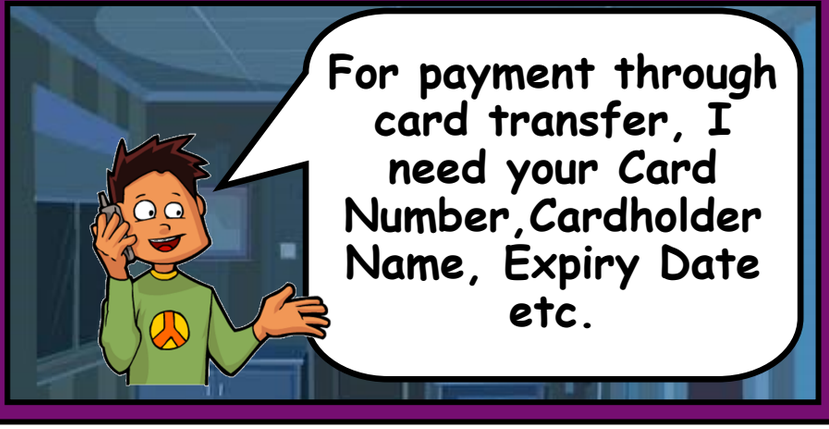
PROTECT YOUR ATM CARD AS IF IT IS CASH.

STAY AWARE. STAY SAFE.

ONLINE MARKETPLACE SCAM

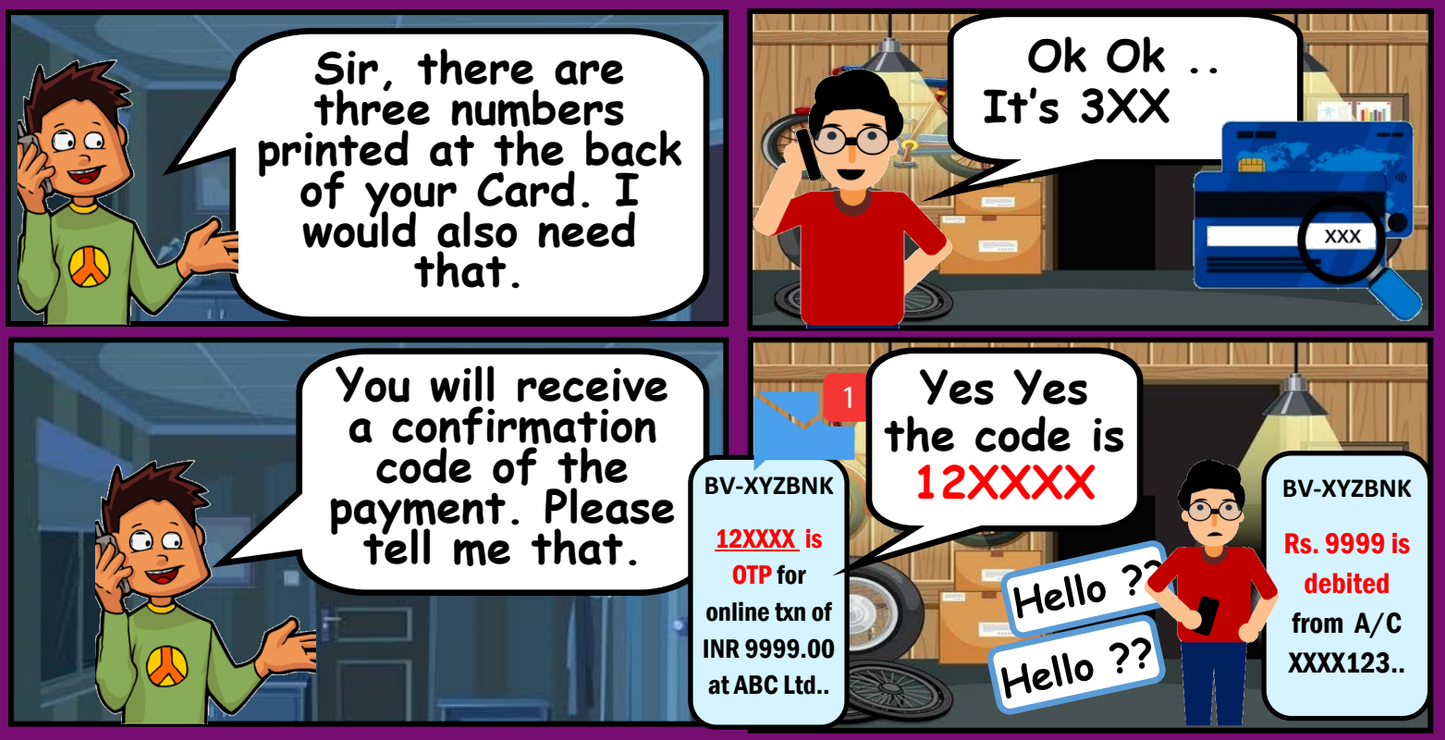
Golu was looking to sell his bike online. He clicked pictures of his bike and started posting them with his contact details on random online marketplace websites.





Golu readily gave Nattu all his card details.

ONLINE MARKETPLACE SCAM... CONTD



Golu was shocked to learn that instead of receiving money, Rs.9999 was debited from his account. Soon he realized that he has been duped via fake call and tricked to share sensitive information.

HOW TO AVOID SUCH SCAMS

- ✖ *Never share card number, cardholder name, expiry date, CVV, PIN, OTP etc. with anyone under any circumstances*
- ✖ *Most of the OTP messages mention the reason for generation of the OTP. Read every message carefully before taking any action*
- ✖ *Avoid responding Calls / Emails / Links / Messages from unknown sources & do not share personal / sensitive information with strangers or on any unknown / untrusted website*
- ✔ *Always use trusted websites & Apps and check customers reviews, ratings etc. before buying / reselling products*

PASSWORD SECURITY

Passwords are the first line of defense against cyber criminals. Weak passwords are easy to hack. Protect your device and secure your information with a strong password.

How Fraudsters get Passwords ?

Visual Hacking or Shoulder Surfing

Email Phishing

Guessing from publicly shared information

Insecure practices

Password cracker like Brute Force, Dictionary attacks

Use combination of lowercase and uppercase letters, numbers & special characters

Never use personal information or common words for making password

Make password atleast eight characters long

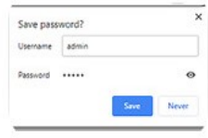
Do not share password with anyone

Use unique and different passwords for different accounts and devices

Never store password in any devices

Memorize your password

Avoid using password Auto-save function over internet



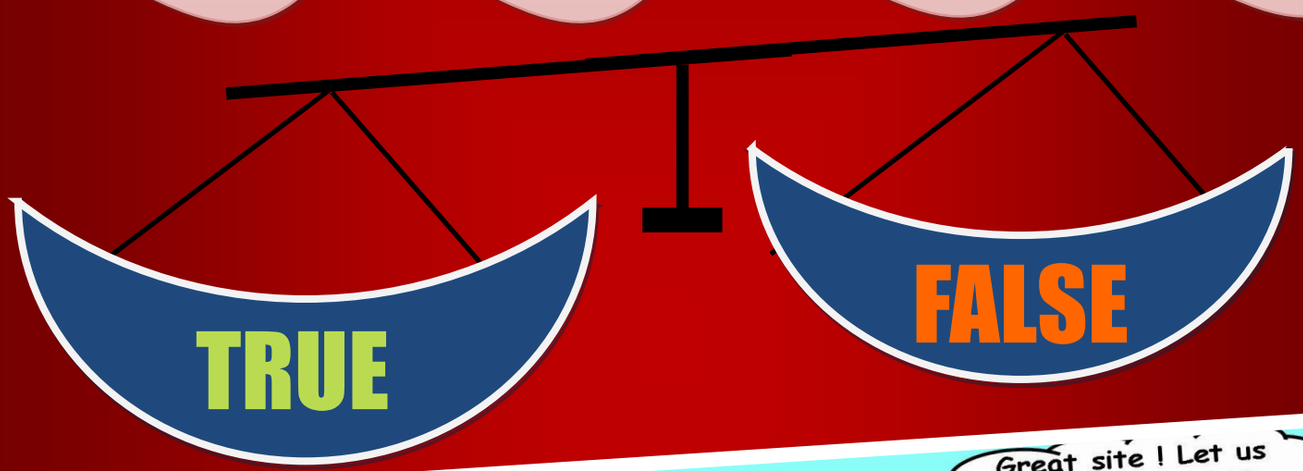
Change password frequently

Do not let anyone watch you typing your password

IS IT TRUE OR FALSE

Avoid doing transaction while being connected to a public Wi-Fi.

Always save your password / PIN in your phone contacts.



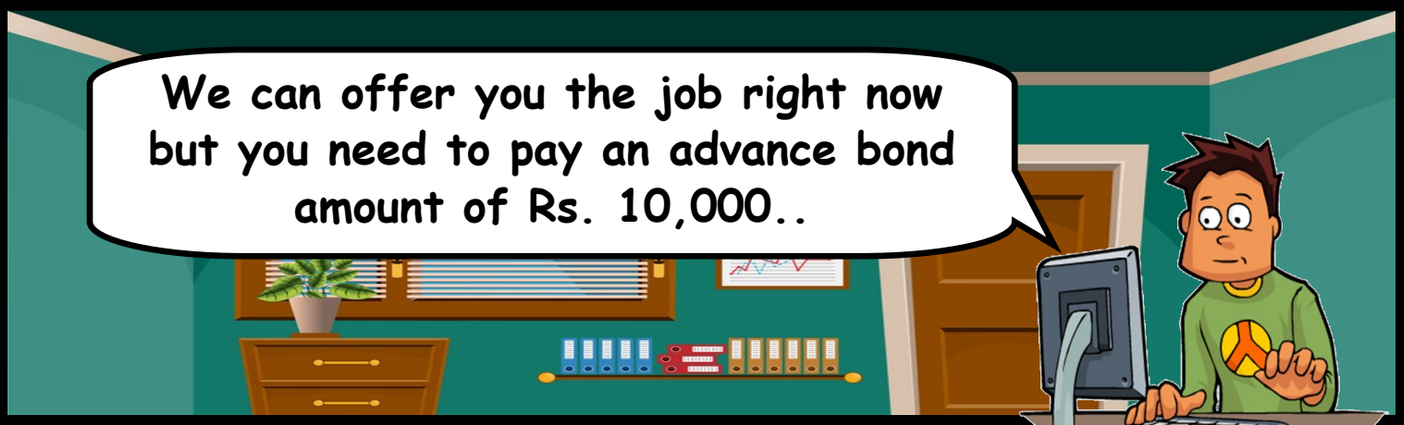
FAKE JOB OFFER SCAM

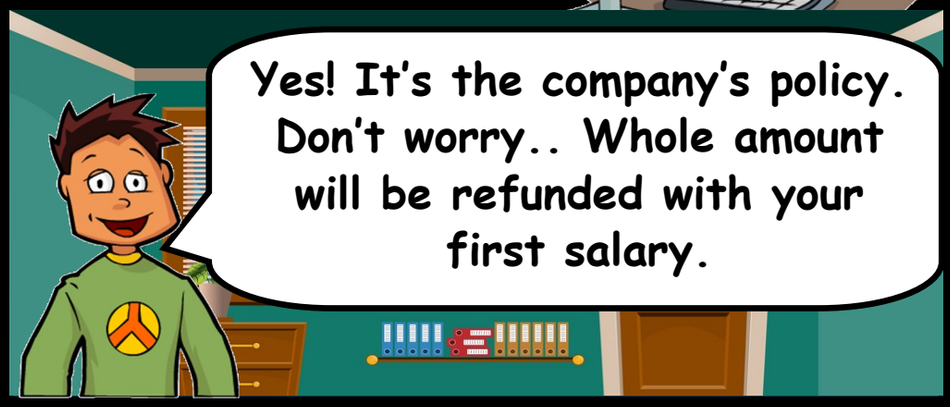
Once Nattu created a fake profile on a job cum social networking app. He impersonated as an HR executive and mentioned under his profile that he hires folks.

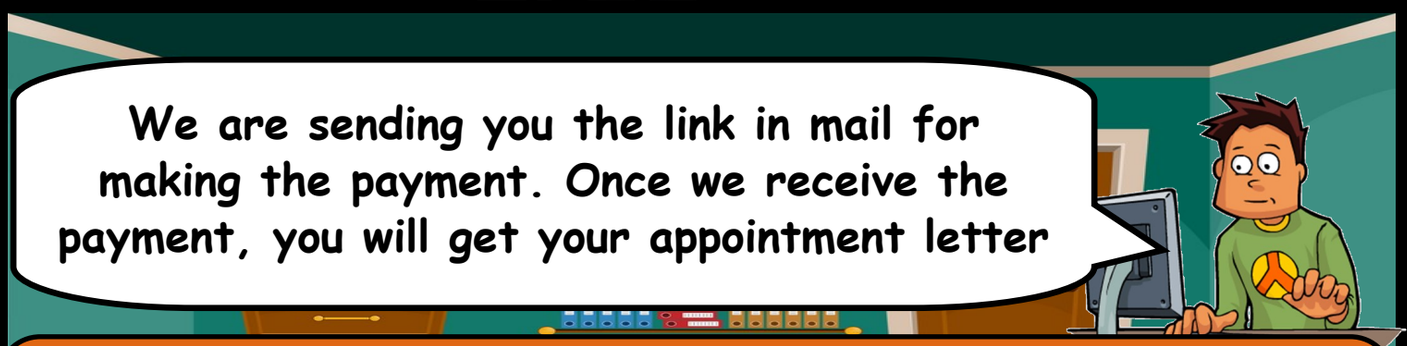
Soon he started getting requests from multiple job aspirants. He targeted one of them named Chiku who had sent him message personally in the inbox.

Chiku immediately shared his resume.

FAKE JOB OFFER SCAM... CONTD







Chiku immediately paid the amount. After few hours when he did not receive any mail from the company, he thought of sending the message to the HR executive. To his surprise, the profile was deleted !!

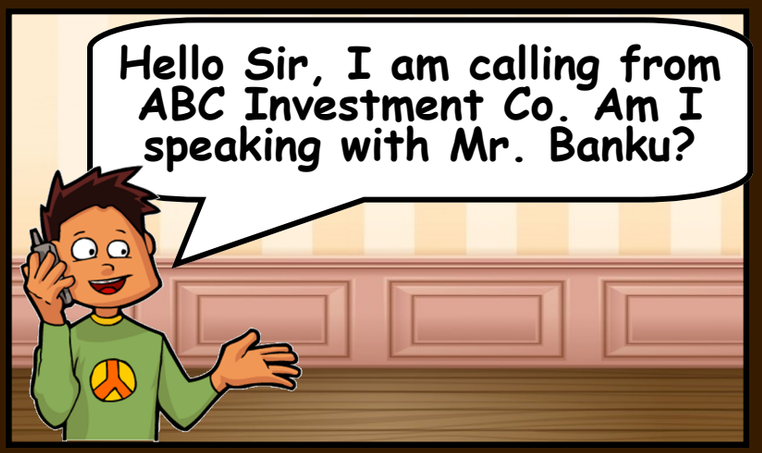
LESSONS TO LEARN

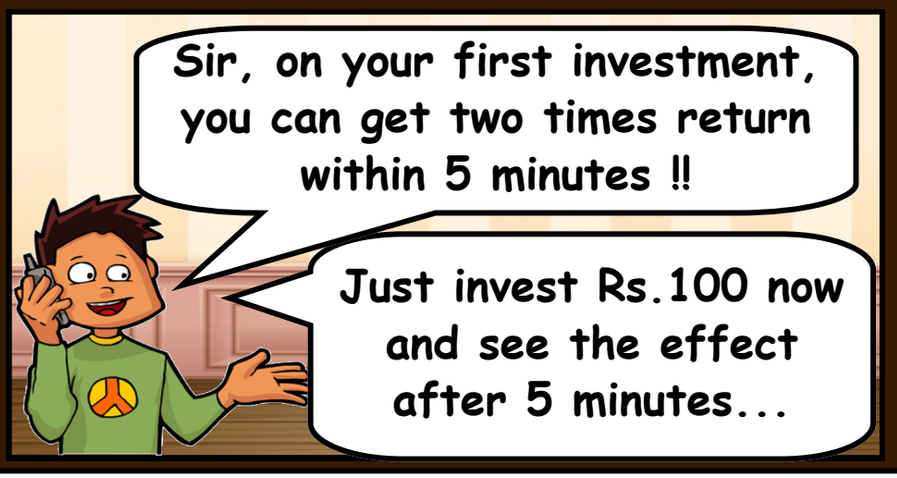
✖ Do not trust random job advertisements or social media profiles of recruiters

✔ Verify the authenticity of the job openings from companies' official website

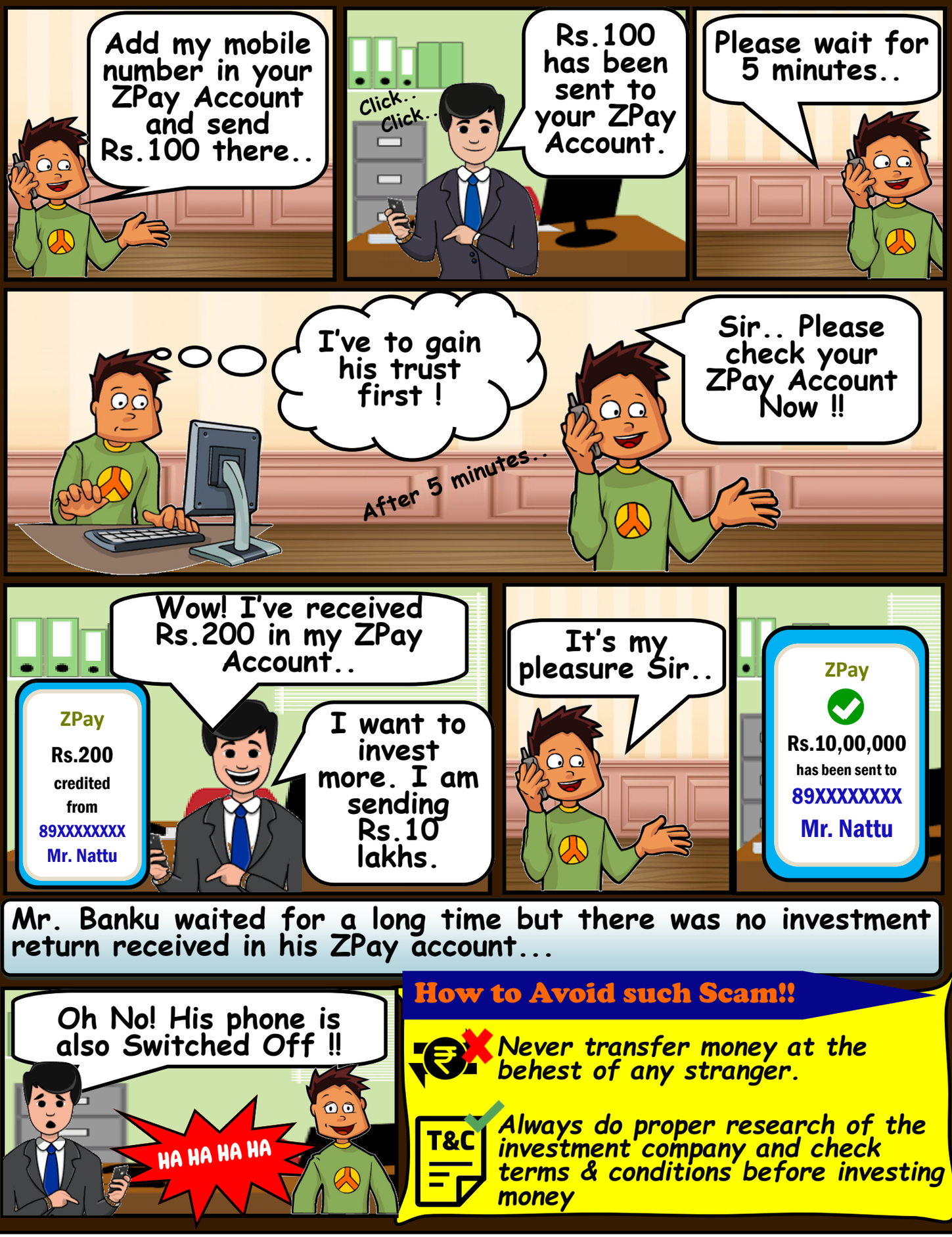
FAKE INVESTMENT OFFER

One day Nattu decided to pull a scam for a large chunk of money. He was looking for ideas when suddenly his eyes fell on a mutual fund investment article. He searched for people who were at senior executive positions in different companies.





FAKE INVESTMENT OFFER... CONTD



LOAN SCAMS

Beware of Online Loan Scams !

Warning signs of Online Loan Fraud

- Offers interest free loans or very low interest rate on loans
- Offers loan without Credit Score
- Lender is not registered with the govt. / RBI approved
- No physical address or contact details of the lender mentioned
- Demands for advance payment in the name of processing and other charges
- Gives limited period offers which creates an urgency to make decisions quickly

How to Avoid Online Loan Fraud

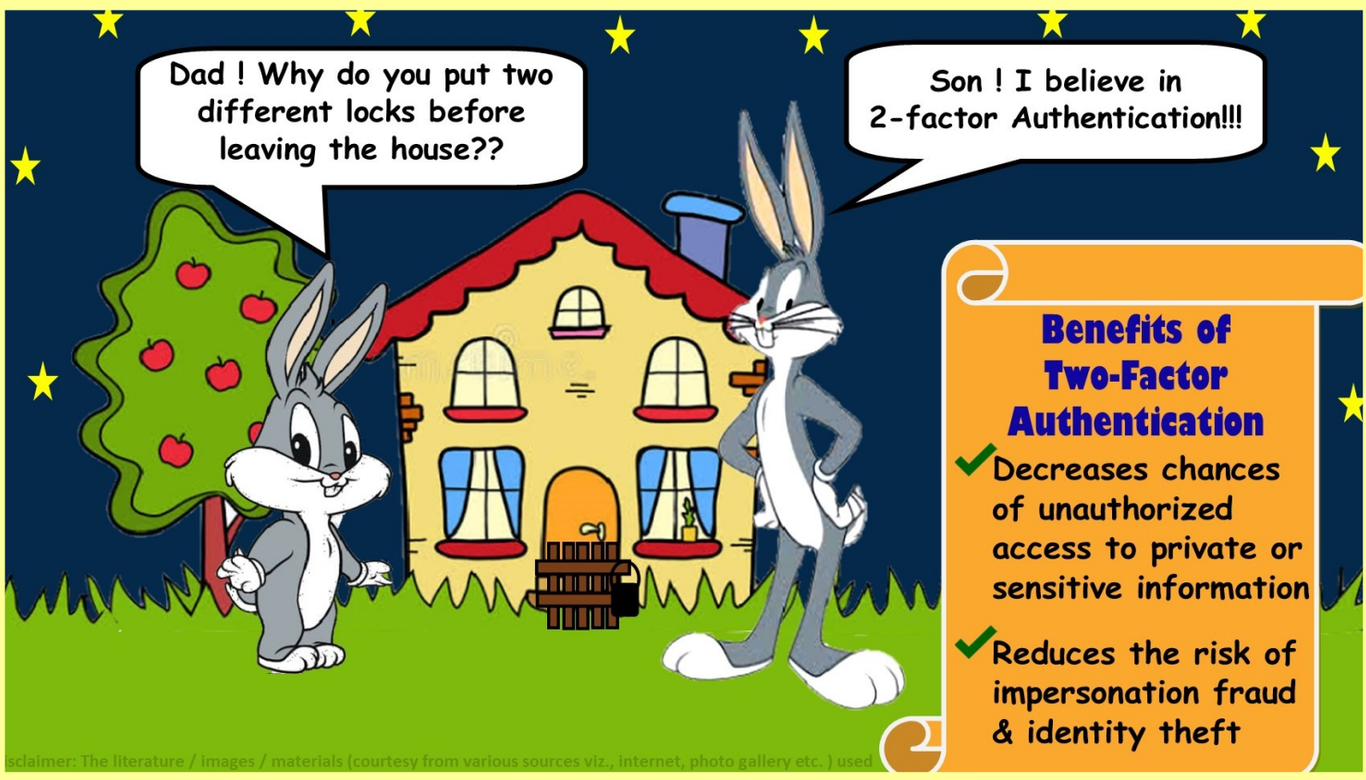
- Do proper research on the lender before availing a loan
- Stay away from lenders who ask for any advance payment
- Do not provide personal or financial information over phone or email
- Avoid Offers Which are too Good be True. Providing attractive deals is a trick used by fraudsters to attract people.
- Never click on any external link received through emails, SMSs, WhatsApp for an instant Loan Approval.
- Avoid clicking on Pop-up Advertisements promises for sanctioning quick & hassle free loans

To apply loan from UCO Bank, visit to your nearest Branch or refer official website www.ucobank.com

LETS TRY THIS...

Arrange the given LETTERS to guess the name of Malware

1. N T A R J O
2. R B O A C D K O
3. R D W A A E
4. T R I K O T O



Beware of these UPI scams

- Fake Offers
- Phishing Links
- Request Money
- QR Code Scams
- Remote Screen Monitoring
- Scams using UPI PIN & OTP

SALIENT FEATURES OF BHIM UPI APP

Balance enquiry

'Scan and Pay' using QR code

Used by customers of any Bank

Request Money

Instant Money Transfer

set "Virtual Payment Address (VPA)"

SAFETY TIPS WHILE USING BHIM UPI APP

- Never disclose confidential details like your UPI pin, passwords, or card number to anyone.
- Use UPI PIN only for making payments, not for receiving money.
- Do not download unverified third-party apps. Download the BHIM App from Official App stores.
- Do not scan QR code received from unidentified sources. QR code needs to be scanned only for making payments.
- Do not accept fund transfer requests from unidentified or unknown ids on UPI.
- Check UPI address before doing any transaction. Never respond to unverified messages or calls.

PAYMENT SCAM FOR MERCHANTS

One day Nattu went to a grocery store. After doing his shopping he went to the billing counter.

Nattu pretended to scan the QR in front of the shopkeeper but in reality he had created a fake payment confirmation page in which he entered the amount 5000. It displayed a message "Rs.5000 payment done". Nattu showed it to the Shopkeeper.

PAYMENT SCAM FOR MERCHANTS... CONTD

At night when the Shopkeeper was matching the total item sold with the total balance. He found out that the bill was not paid for few of the items. When he checked he found out all the items were bought by Nattu.

SAFETY PRACTICES TO AVOID PAYMENT FRAUD

Never rely on any screenshot messages shown by customer as payment confirmation

Before letting a customer go, strictly verify the completion of transaction through official App

After receiving payment through Digital means, always check or reconcile your Wallet or Bank Account statement

Make use of sound speakers that says "Payment Received of Rs.XXXX" after every transaction

DIGITAL / e-WALLET SAFETY

ADVANTAGES OF USING e-WALLET

Hassle-free Virtual Wallet

Quick Fund Transfer

Multiple Services at a time

SAFETY PRECAUTIONS

Enable biometric login or use a unique and different password for your Digital Wallet Application

Do not save your card information while doing transaction

Lock your device with multiple layers of security such as Passcode, pattern lock, Biometric locks etc

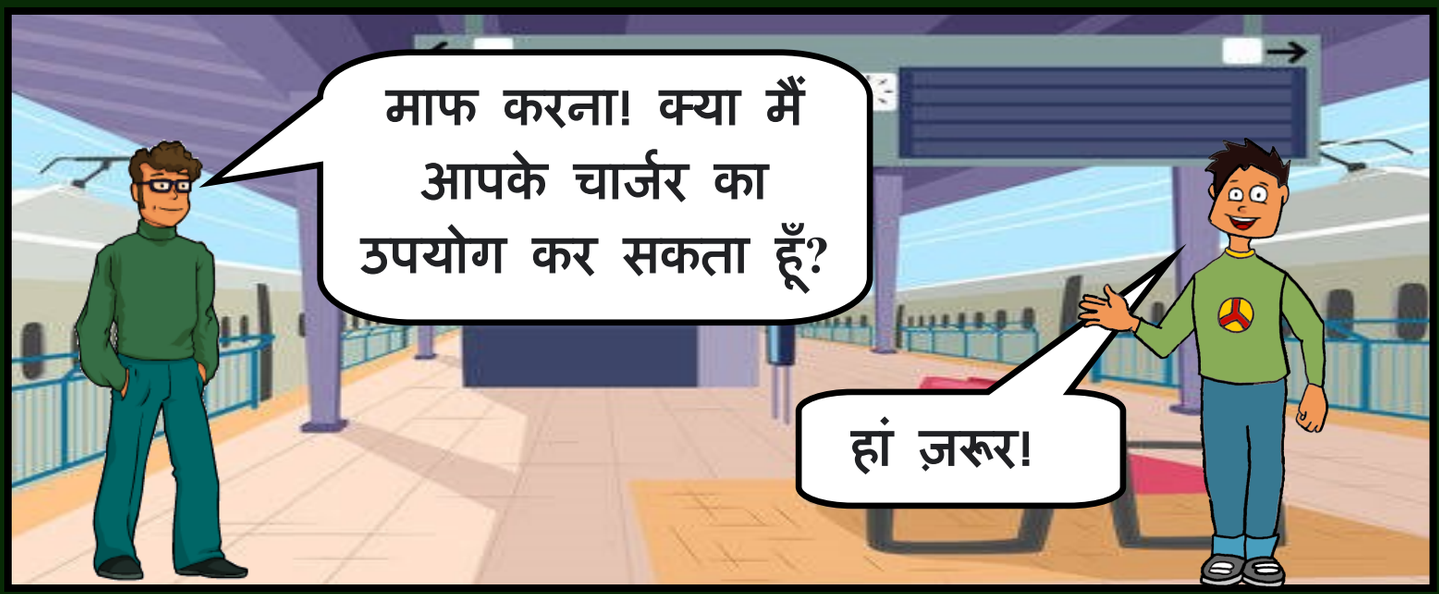
Avoid using public wi-fi networks while doing transactions through e-Wallet. Choose trusted & secure network conection

Do not download Apps from unsolicited links received through Emails & SMSs. Install apps from verified trusted sources

Never share e-Wallet PIN / Passwords and other Private / Sensitive information with anyone

जूस-जैकिंग फ्रॉड

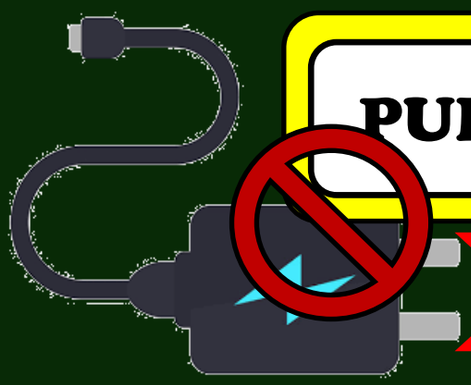
एक दिन रिंकू को अपनी ट्रेन पकड़ने में देर हो रही थी इसलिए वह अपना फोन चार्जर ले जाना भूल गया। उसने रेल्वे स्टेशन के चार्जिंग प्वाइंट पर एक चार्जर लटका देखा। उसके ठीक बगल में एक आदमी (नट्टू) खड़ा था।



जैसे ही रिंकू ने चार्जर इंजेक्ट किया, उसका फोन स्पाईवेयर सहित वायरस से भर गया। अगले कुछ दिनों के दौरान, नट्टू को रिंकू के बैंक विवरण सहित सभी संवेदनशील जानकारी प्राप्त हुई जो उसके फोन में थी।

जूस-जैकिंग फ्रॉड... जारी

कुछ दिनों बाद रिंकू को मैसेज आया कि उसके खाते से 30,000 रुपये डेबिट हो गए हैं। रिंकू को समझ नहीं आ रहा था कि क्या हो गया है।



PUBLIC CHARGING STATION

साइबर सुरक्षा युक्तियाँ:

✘ अपने फोन को कभी भी अनजान चार्जर से चार्ज न करें, खासकर सार्वजनिक स्थानों के चार्जिंग पॉइंट पर।

✘ उन लोगों पर भरोसा न करें जो आपको अपना चार्जर उधार देने की पेशकश करते हैं। वे आपके सभी संवेदनशील डेटा को निकाल सकते हैं।

✔ भरोसेमंद कंपनियों के चार्जिंग केबल का इस्तेमाल करें। एडॉप्टर और चार्जिंग केबल के ब्रांड को हमेशा सत्यापित करें।

MOBILE DEVICE SECURITY

Types of Mobile Malwares

Mobile Adware
serves advertisements on mobile device and tracks user behaviour

Mobile Ransomware
locks devices, makes files inaccessible or encrypts files unless a ransom is paid

Remote Access Tools
access the device remotely and take complete control of the device

Mobile Banking Trojan
looks like legitimate banking apps but aims to steal financial credentials

SMS Trojan
uses the SMS of a mobile device to send and intercept messages

Mobile Spyware
records the action of users without the user's knowledge

BEST PRACTICES

स्क्रीन शेयरिंग धोखाधड़ी

एक दिन नट्टू ने रिमोट स्क्रीन शेयरिंग ऐप के जरिए एक घोटाला करने का सोंचा। उसने बेतरतीब रूप से लोगों को फोन करना शुरू कर दिया और उसका कॉल नीता के पास पहुंचा।

हेलो ! मैं टेलीकॉम कंपनी से कॉल कर रहा हूं। हमें आपको यह बताते हुए खुशी हो रही है कि आपने छह महीने का अनलिमिटेड कॉल और डेटा रिचार्ज जीता है।

आपको बस एक ऐप इंस्टॉल करके ऑफर को भुनाना होगा।

पर मेरे पास पहले से ही XYZ टेलीकॉम ऐप है।

मैम, वह पुराना संस्करण है। मैं आपको नवीनतम संस्करण डाउनलोड करने के लिए एक लिंक भेज रहा हूं।

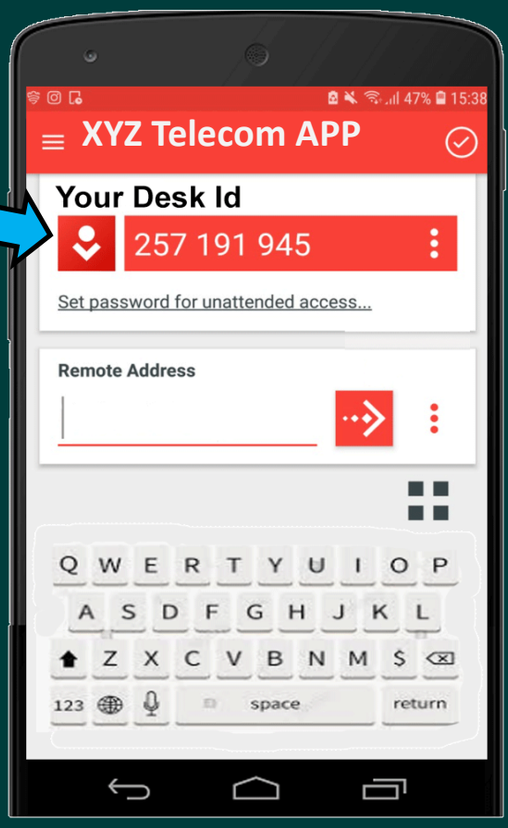
XXXX55

To download new version of XYZ App click the below link

bit.ly/85Khf9i

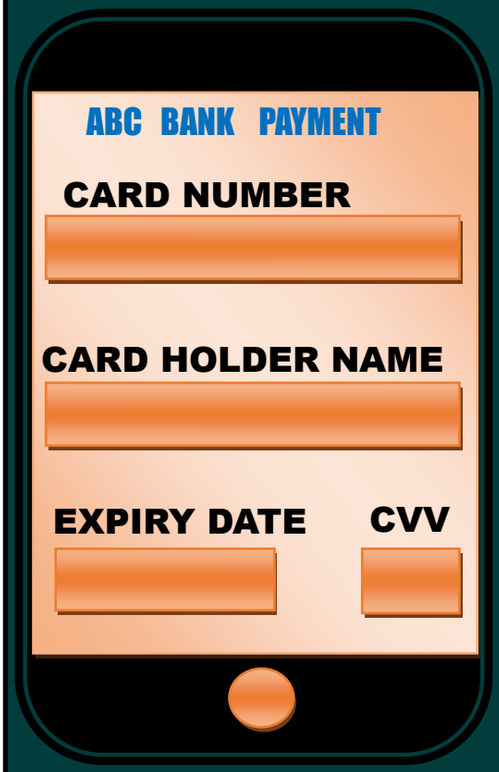
स्क्रीन शेयरिंग धोखाधड़ी... जारी

नीता ने तुरंत उस लिंक पर क्लिक करके ऐप डाउनलोड किया।



नट्टू ने नीता के मोबाइल पर सफलतापूर्वक रीमोट स्क्रीन शेयरिंग ऐप इंस्टॉल करवा लिया और अब वह आसानी से नीता के मोबाइल की निर्देशिका, तथा संदेशों को पढ़ सकता था।

स्क्रीन शेयरिंग धोखाधड़ी... जारी



जैसे ही नीता ने भुगतान करने के दौरान अपने कार्ड का विवरण डाला, नट्टू ने स्क्रीन शेयरिंग ऐप के ज़रिए कार्ड संबंधित एवं OTP जैसी सारी जानकारी हासिल कर ली और उसका इस्तेमाल करके नीता के अकाउंट से सारे पैसे निकाल लिए। जल्द ही नीता को एहसास हुआ की उसके साथ फ़र्ज़ी टेलीकॉम एप्लीकेशन के जरिये साइबर धोखाधड़ी हुई है।

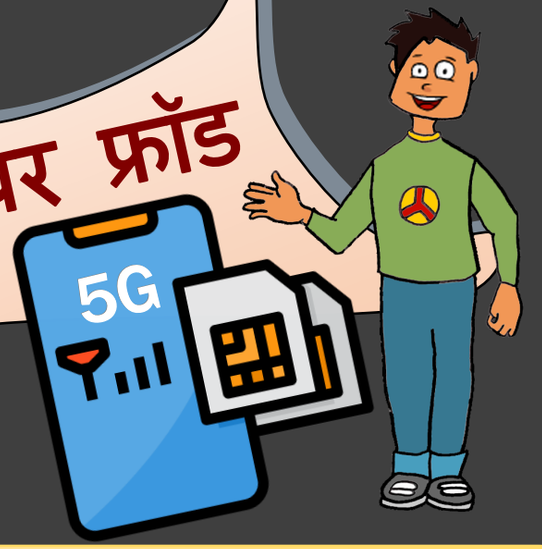
साइबर सुरक्षा युक्तियाँ

✗ किसी अनजान कॉलर के कहने पर कोई एप्लिकेशन डाउनलोड न करें।

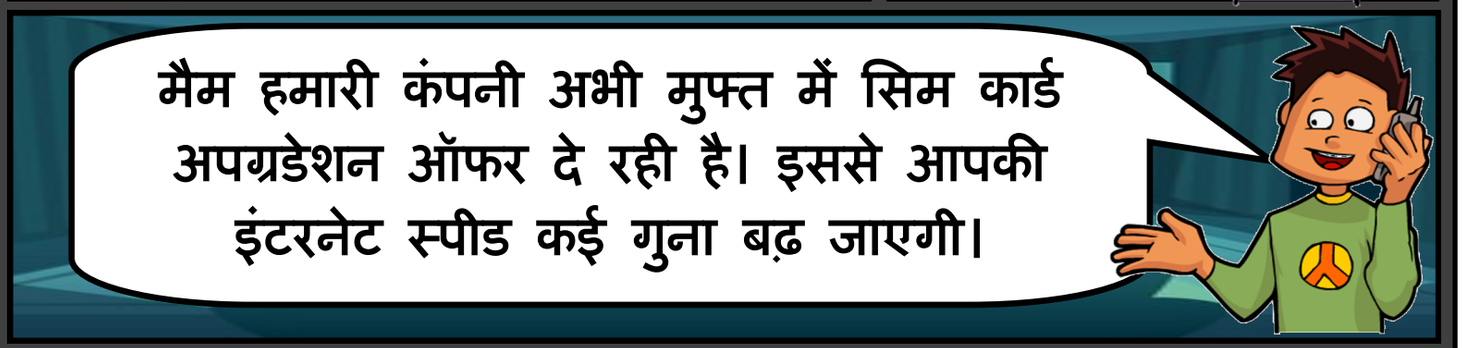
✗ कोड, ओटीपी, पासवर्ड या कोई अन्य संवेदनशील जानकारी किसी के साथ साझा न करें।

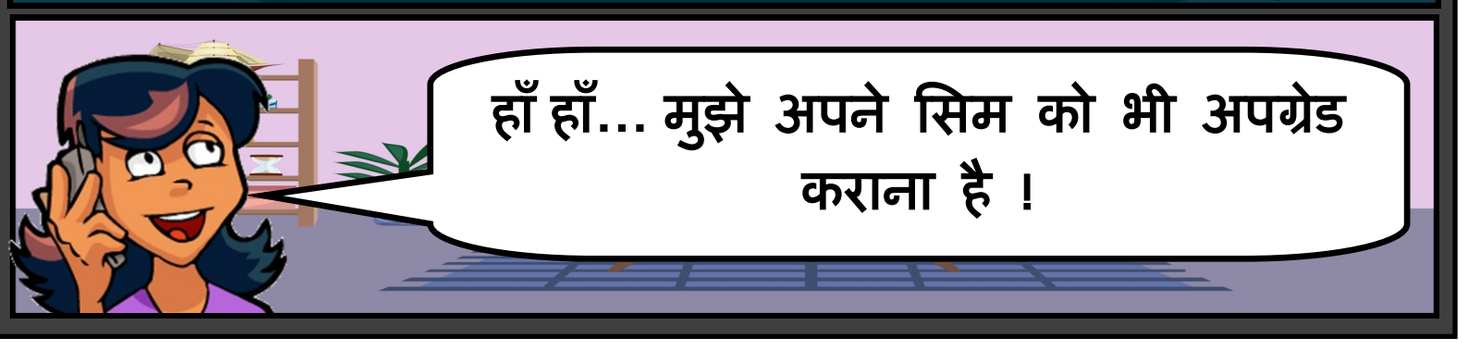
✓ किसी भी ऑफ़र संबंधी जानकारी के लिए हमेशा कंपनी के ऑफिसियल ऐप को फॉलो करें।

सिम कार्ड अपग्रेडेशन के नाम पर फ्रॉड

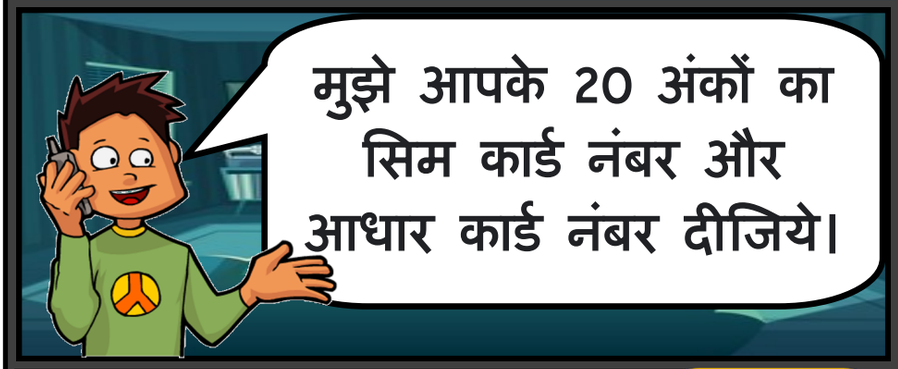


एक दिन नट्टू ने किसी तरह कुछ टेलीकॉम ग्राहकों की मोबाइल नंबर हासिल किया और उन्हें एक-एक करके कॉल करना शुरू कर दिया। जोया नाम के एक ग्राहक ने फोन उठाया।





सिम कार्ड अपग्रेडेशन के नाम पर फ्रॉड... जारी



जोया ने नट्टू द्वारा पूछी गई सारी जानकारी दे दी।

कुछ समय बाद, अचानक जोया के फोन का नेटवर्क चला गया। नट्टू ने जोया के सिम को अपने पास रखे खाली/ब्लैंक सिम में परिवर्तित कर लिया। अब जोया का फोन कॉल्स, मेसेज सब कुछ नट्टू के पास आने लगा। फिर नट्टू ने टेक्स्ट मैसेज और OTP के जरिये जोया की बैंकिंग क्रेडेंशियल्स भी हासिल कर ली और जोया के अकाउंट से पैसा गायब करना शुरू कर दिया।

साइबर सुरक्षा युक्तियाँ:

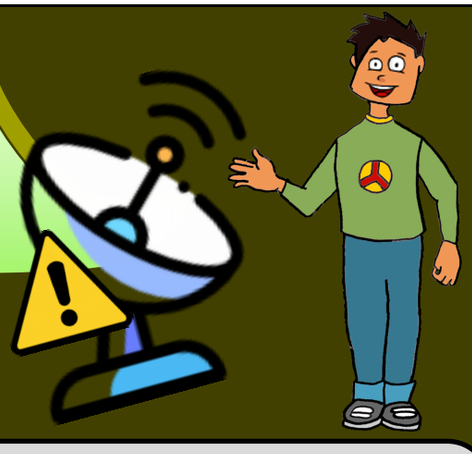
✗ सिम कार्ड अपग्रेडेशन के लिए किसी अनजान कॉल / मैसेज / लिंक पर भरोसा न करें।

✓ सिम कार्ड की स्थिति सत्यापित करने के लिए हमेशा अपने टेलीकॉम कंपनी से सीधे संपर्क करें।

Pick the ODD one out !

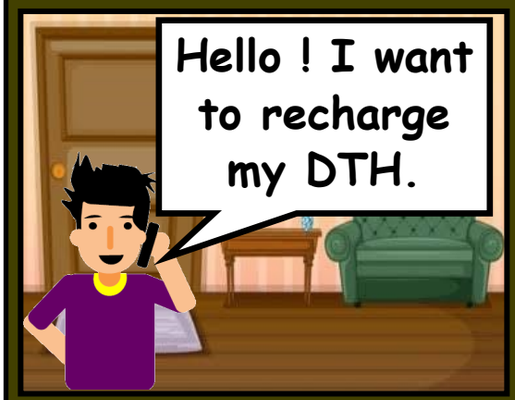
Confidentiality	Linux	Rootkit
Availability	IOS	Spyware
Integrity	Windows	Keylodger
Consistency	C++	kaspersky

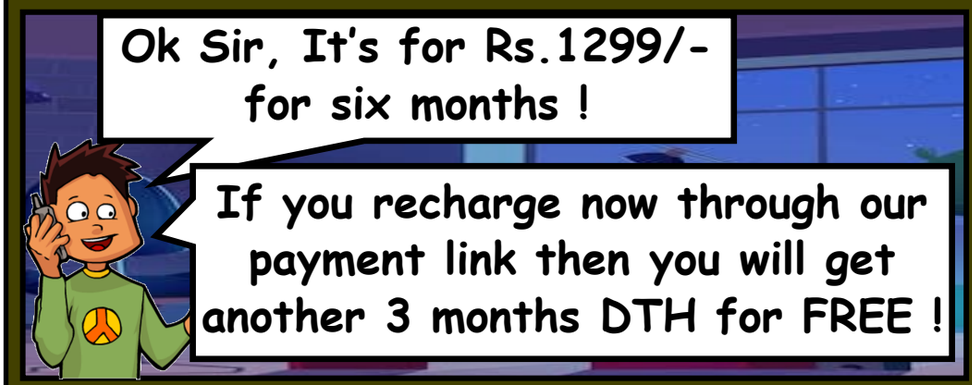
DTH RECHARGE FRAUD



Nattu created many fake online forums for online recharge of DTH services and was waiting for people to fall prey.

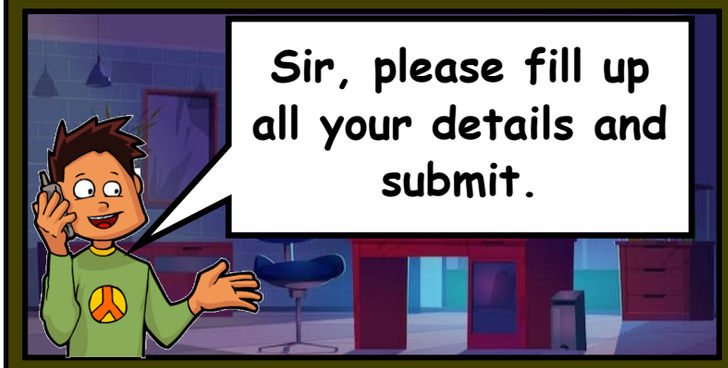
Meanwhile, Rinku was watching news on TV when suddenly his DTH plan got expired. He searched for contact number of DTH recharge provider on Search Engine (Google) and fell for the portal created by Nattu. He called the displayed number.

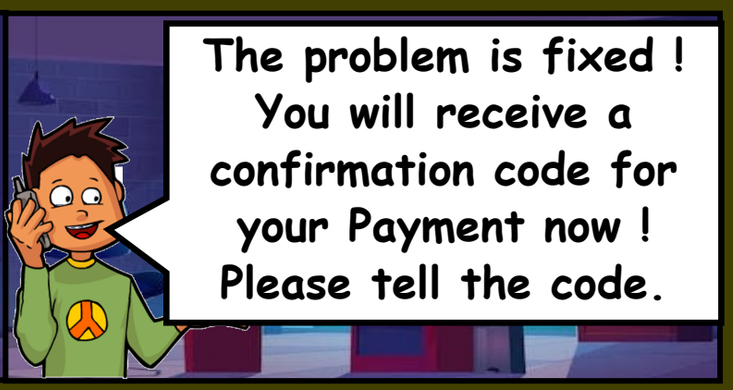


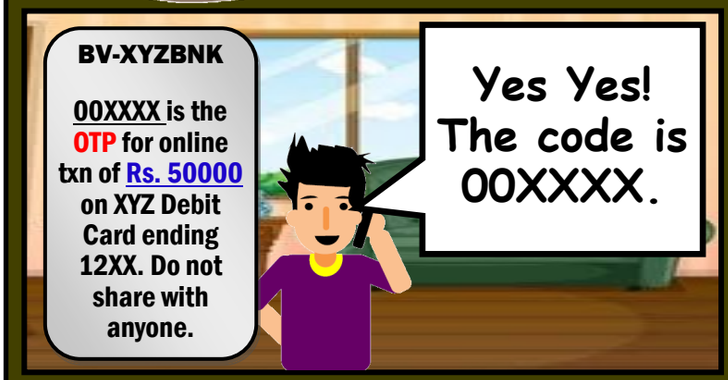


Rinku clicked on the link sent by Nattu which led him to a fake form asking to fill up all the personal and financial details like Card number, Expiry date, CVV code etc.

DTH RECHARGE FRAUD... CONTD







Rinku waited for a long time but the DTH was still not recharged. Meanwhile, he got a message from his Bank that Rs.50000 has been deducted from his account. Soon he realized that he has been scammed in the name of fake DTH recharge.

Points to Remember!!

Don't do random searches over search engine to find customer care numbers, rather visit the official website/Apps of that particular company.

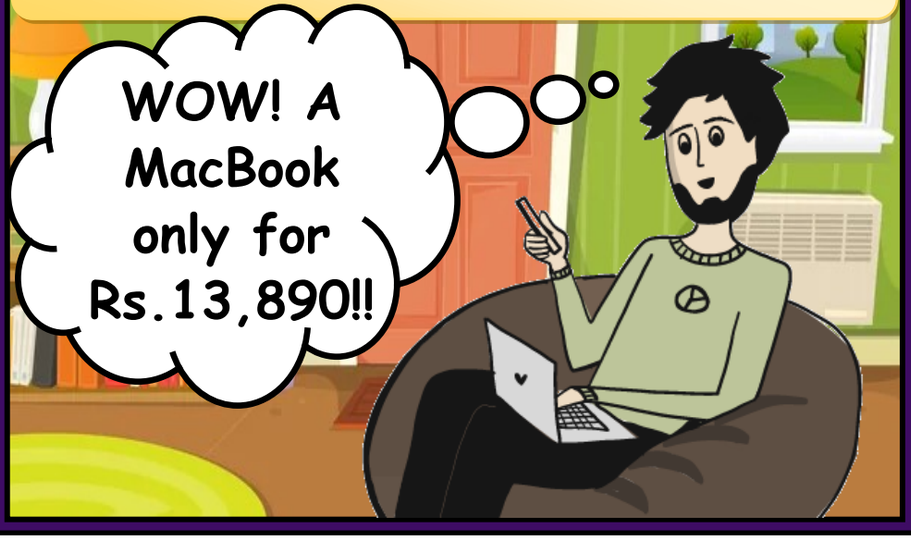
Do not share your OTP with anyone. Most of the OTP messages mention the reason for generation of the OTP. Read every message carefully before taking any action.


Beware of
FAKE CUSTOMER CARE NUMBER
in search results
Do not search Bank's Customer Care Number randomly in search engines
Search Customer Care Numbers from Bank's Official Website only (www.ucobank.com)
Stay Vigilant...
Stay Safe
Contact UCO Bank only on: 1800 103 0123
Write to us at: uco.custcare@ucobank.co.in
Follow us on:
UCOBankOfficial
Official.UCOBank
Official.ucobank
UCO BANK
UCO Bank Official

FAKE E-COMMERCE WEBSITE

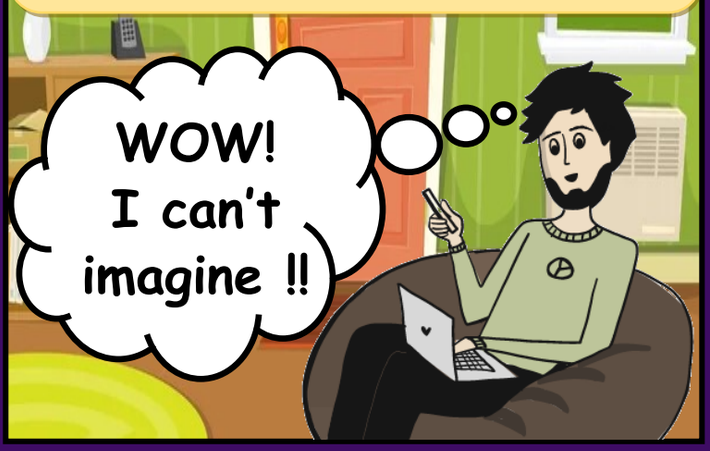
One day Nattu created a fake shopping website and posted its link on multiple social networking sites.

Jeetu, a social media freak, while scrolling his social media feeds, saw the advertisement and fell for it.

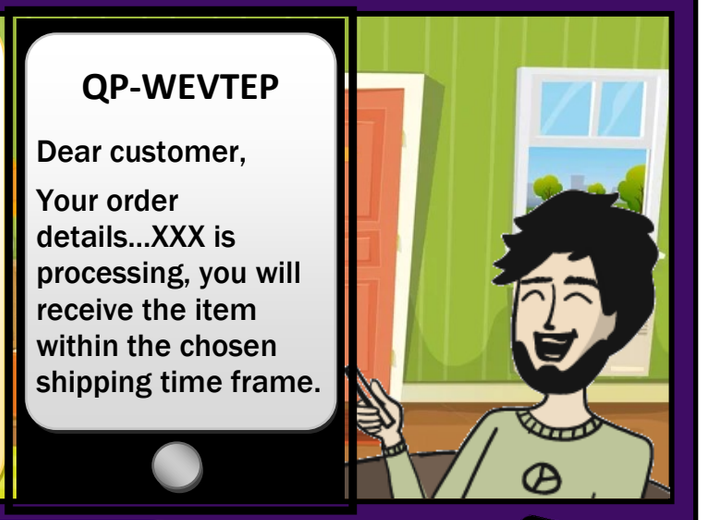


FAKE E-COMMERCE WEBSITE... CONTD

He immediately clicked on the Ad and was mesmerized to see all the versions of MacBook at an unbelievably low price.



All the offers were expiring soon, so he finally decided to buy a MacBook. He didn't find the 'Cash on Delivery' option for payment. Soon, he completed the purchase by making card payment and got a confirmation message.



Few days past but Jeetu did not receive his order. There was no means through which he could contact anyone. He tried to find the shopping website at the internet but Nattu had already deleted the website. Soon he realized that he has been duped through fake advertisement and shopping website.

ONLINE SHOPPING

SAFETY MEASURES

Do online shopping from known and trusted stores. Do proper research on the online seller.

Always check website URL address, spelling, 's' after 'http', lock sign etc.

Before buying, read customers reviews & ratings, shipping terms and return policy etc from the portal.

Preferably opt for 'Cash-on-delivery' payment option for first time purchase.

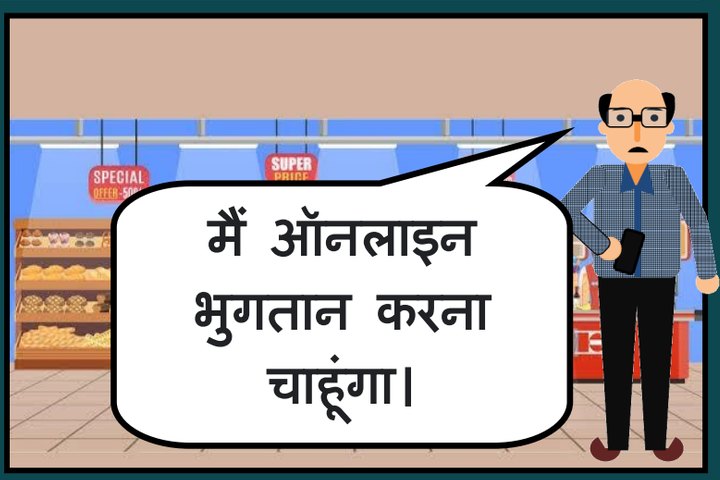
Never save Debit / Credit card details and password in the website.

Always logout from the website after completing financial transaction.

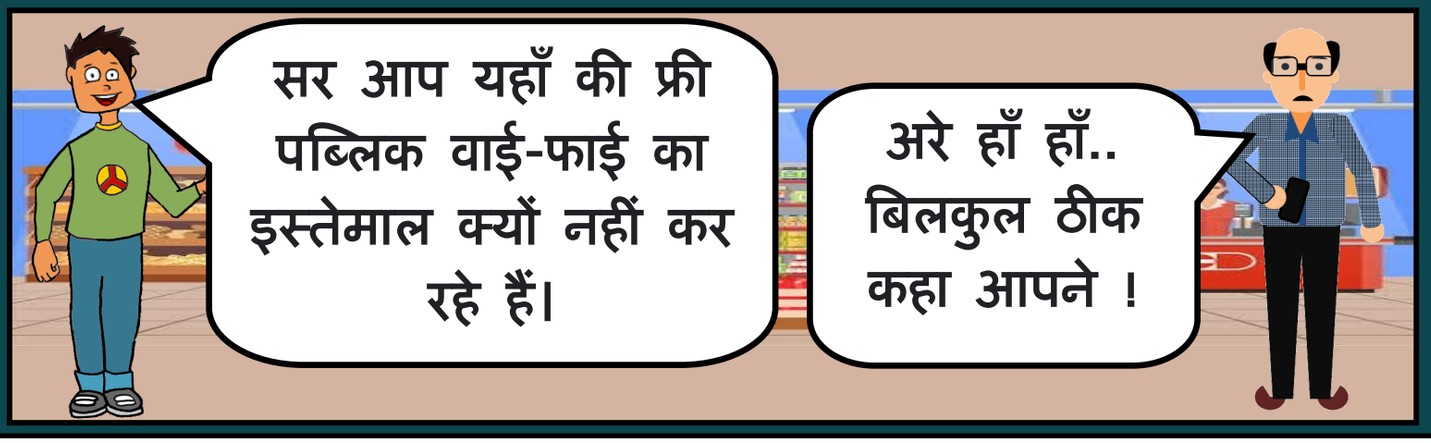
SEE YOURSELF IN CYBER

पब्लिक वाई-फाई का इस्तेमाल कर धोखाधड़ी

अपने किराने की खरीदारी के बाद गुप्ताजी बिलिंग काउंटर पर गए।



जब गुप्ताजी ने ऑनलाइन भुगतान करने का प्रयास किया, तो कुछ नेटवर्क समस्या होने के कारण वह भुगतान नहीं कर सकें। नट्टू उनके ठीक पीछे खड़ा था।



पब्लिक वाई-फाई का इस्तेमाल कर धोखाधड़ी... जारी

गुप्ताजी ने तुरंत पब्लिक वाई-फाई से कनेक्ट किया और अपना ऑनलाइन भुगतान पूरा किया। नट्टू ने पहले से ही स्टोर का पब्लिक वाई-फाई नेटवर्क हैक कर लिया था।

नट्टू ने डेटा इनटरसेप्शन द्वारा गुप्ताजी की सारी संवेदनशील जानकारी जैसे ईमेल, यूजरनेम, पासवर्ड, कार्ड नंबर आदि हासिल कर ली।

एक दिन के बाद, गुप्ताजी को लगातार दो संदेश मिले कि उनके खाते से 20,000 रुपये और 25,000 रुपये डेबिट हो गए हैं।

साइबर सुरक्षा युक्तियाँ:

✘ वित्तीय लेनदेन करते समय कभी भी सार्वजनिक वाई-फाई का उपयोग न करें।

✓ कभी भी अपने मोबाइल को किसी खुले सार्वजनिक नेटवर्क से न जोड़ें। हमेशा सुरक्षित और विश्वसनीय नेटवर्क कनेक्शन का ही उपयोग करें।

ENSURE SAFE BROWSING

Always check for "s" after "http" or green lock at the beginning of URL

Keep your Browsers & Operating System up-to-date

Disable the "Remember Password" option from Browser

Frequently clear browsing history, cookies, temporary files etc.

SAFE DOWNLOAD TIPS

- ✗ Never download cracked or pirated software and files
- ✓ Download only from reputable sites and sources
- ✗ Avoid downloading files with malicious extensions like ".exe", ".scr" etc.
- ✓ Read user feedback, reviews, ratings etc. before downloading software

CHECK YOUR AWARENESS

Which of the following is a sign of phishing email?

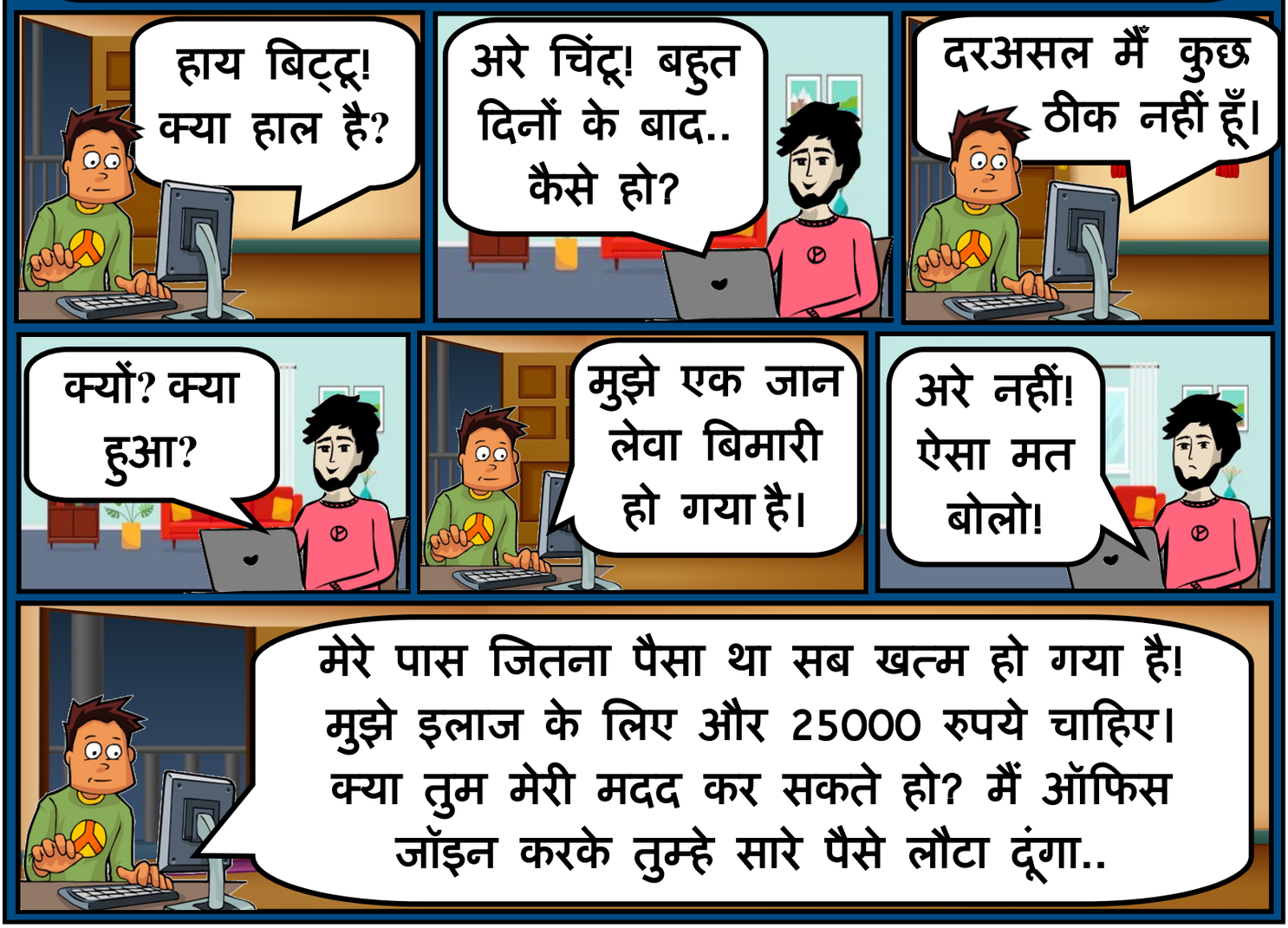
A. Misspelling
B. Wrong Grammar
C. Threat/ Urgency
D. All of the Above

Which attack will make a network inaccessible for it's intended user?

A. DOS Attack
B. Man in the Middle
C. Juice-Jacking
D. Phishing

फर्जी सोशल मीडिया प्रोफाइल

एक दिन नट्टू ने अपने एक पड़ोसी चिंटू का फर्जी अकाउंट बनाया और सोशल नेटवर्किंग साइट पर उनके सभी दोस्तों को फ्रेंड रिक्वेस्ट भेजने लगा। उनमें से कुछ ने फ्रेंड रिक्वेस्ट स्वीकार कर लिया। नट्टू ने उन्हें एक-एक करके मैसेज करना शुरू किया और आखिर में बिट्टू नाम के एक दोस्त ने जवाब दिया।



फर्जी सोशल मीडिया प्रोफाइल... जारी

बिट्टू ने तुरंत उसके दिए गए अकाउंट पर पैसा भेज दिया। फिर कुछ दिन बाद उसने चिंटू के नंबर पर कॉल करके उसके ईलाज के बारे में पूछा।

चिंटू और बिट्टू को जल्द ही एहसास हुआ कि ये किसी जालसाज़ (नट्टू) का काम हैं, जिन्होंने सोशल मीडिया पर फर्जी प्रोफाइल से बिट्टू को ठगा है।

साइबर सुरक्षा युक्तियाँ:

- ✓ अगर सोशल मीडिया पर आपका दोस्त मदद मांग रहा है, तो आर्थिक मदद देने से पहले व्यक्तिगत रूप से उससे संपर्क करने का प्रयास करें।
- ✓ सोशल मीडिया पर अपनी प्रोफ़ाइल, मित्र सूची और अन्य संवेदनशील जानकारी को निजी बनाएं।

BE SOCIAL BUT BE SAFE

Block profiles from public searches

Log out after each session

Never share credentials with anyone

Never mention home or work address

Never accept friend requests from strangers

Never click on suspicious links

Keep the profile privacy settings at the most restricted levels

Limit your share & be cautious about what you are sharing

SAFETY PRACTICES AT WORKPLACE

FOLLOW CLEAN DESK & CLEAR SCREEN PRACTICES TO BUILD CYBER SECURE WORK CULTURE

Don't leave sensitive documents lying around. Store them securely

Securely dispose of all sensitive & confidential data

Always keep devices password protected

Shut down computers, printers etc. before leaving office

Lock your PC when not in use by ⊞ + L key

Clear sensitive documents from Printer immediately after printing

Protect Your Information

Shred / destroy sensitive or confidential documents before disposal

साइबर धोखाधड़ी की रिपोर्ट कैसे करें?

भारत सरकार का

साइबर क्राइम हेल्पलाइन नंबर

155260

अब यह है

1930

यदि आप साइबर अपराध के शिकार हैं,

तो **1930** डायल करें

और अपनी शिकायत

https://cybercrime.gov.in

पर दर्ज करें

शिकायतकर्ता निम्नलिखित जानकारी प्रदान करें

- ⇒ मोबाइल नंबर
- ⇒ बैंक का नाम और खाता संख्या जिससे पैसे डेबिट हुए हैं
- ⇒ लेन-देन का विवरण (आईडी और लेन-देन की तारीख)
- ⇒ कार्ड का उपयोग करके की गई धोखाधड़ी के मामले में डेबिट/ क्रेडिट कार्ड नंबर
- ⇒ लेन-देन का स्क्रीन शॉट या धोखाधड़ी से संबंधित कोई अन्य छवि

शिकायत की रिपोर्ट करने के बाद, शिकायतकर्ता को एसएमएस / मेल के माध्यम से एक सिस्टम जनरेटेड लॉग-इन आईडी प्राप्त होगी। उपरोक्त लॉग-इन आईडी का उपयोग करते हुए, 24 घंटे के भीतर राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (www.cybercrime.gov.in) पर शिकायत पंजीकरण पूरा करना होगा।

www.InfoSec awareness.in

Brochure

National Cyber Security Awareness Month

October, 2022

www.isea.gov.in

WHAT TO DO WHEN YOUR E-MAIL ACCOUNT IS HACKED ?

1. Check to see which devices have recently connected to your account
2. Reset your password and make sure that it is strong and hard to guess
3. Report the incident to the e-mail site
4. Notify everyone on your contact list that your email has been compromised
5. If you don't mind losing the e-mail address, the best thing to do is close it down and open a new one
6. Enable 2-step verification to protect your account from unauthorized access due to a compromised password
7. Scan your computer for malware and check what else has been compromised
8. Remember the security questions with answers at the time of registration

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: Ministry of Electronics and Information Technology; certin; Cyber Swachhta Kendra

Supported by: NIC National Informatics Centre; साइबर स्वच्छता केन्द्र CYBER SWACHHTA KENDRA Botnet Cleaning and Malware Analysis Centre www.cyberswachhtakendra.gov.in; Cyber Safe Girl; I4C; NCERT

Implemented by: CDAC

www.InfoSecawareness.in

Poster

National Cyber Security Awareness Month

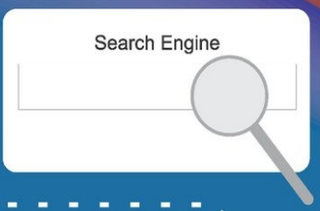
October, 2022

www.isea.gov.in

HOW TO IDENTIFY FAKE WEBSITES

1 Type the website address into a search engine and review the results

The address bar contains a vital information. Always check the url before browsing / buying / registering



2 Look at the website's connection type

Make sure the website connects securely over http (https, not http)

HTTPS : GOOD HTTP: BAD

3 Verify website certificate "and" trust seals

Always check for SSL Certification, to confirm its legitimacy. Trust seals are commonly placed on homepages, login pages, and checkout pages.

4 Look for bad English on the site

If you notice a large number of poorly-spelled (or missing) words, generally bad grammar, or awkward phrasing, you should question the site's reliability

5 Watch out for invasive advertising

If your selected site has a stunningly large number of ads crowding the page, or ads that automatically play audio, it's probably not a credible site

Report incidents related to cyber frauds on www.cybercrime.gov.in or call on 1930

For more information visit: www.isea.gov.in and www.infosecawareness.in

Programme by: इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY; certin; CYBER DOST; NIC एनआईसी National Informatics Centre

Supported by: साइबर स्वच्छता केन्द्र CYBER SWACHHTA KENDRA Botnet Cleaning and Malware Analysis Centre www.cyberswachhtakendra.gov.in; CYBER SAFE GIRL

Implemented by: सी-डैक CDAC; एन सी ई आर टी NCERT

PUZZLE ANSWERS

Crossword Zone

Guess the name of Malware

Sl. No	Words
1.	TROJAN
2.	BACKDOOR
3.	ADWARE
4.	ROOTKIT

PUZZLE ANSWERS

Check your Awareness

Q1. Which of the following is a sign of phishing email?	Q2. Which attack will make a network inaccessible for it's intended user?
Answer: All of the above	Answer: DOS Attack

True or False

Avoid doing transaction while being connected to a public Wi-Fi.
TRUE

Always save your password/ PIN in your phone contacts.
FALSE

Pick the ODD one out!

Answers	Consistency	C++	Kaspersky
Explanation	The three CIA triad are considered to be Confidentiality, Integrity and Availability	Linux, IOS, Windows are all operating system whereas C++ is a Programming Language	Rootkit, Spyware, Keylogger are all malwares whereas Kaspersky is an android anti-malware software.

कंप्यूटर सुरक्षा दिवस प्रतिज्ञा

मैं :

- सुरक्षा के लिए व्यक्तिगत जिम्मेदारी लूँगा और सही सुरक्षा उपायों का उपयोग करूँगा
- इंटरनेट से जुड़ने से पहले उसके जोखिमों के बारे में सोच-विचार करूँगा
- अपने कंप्यूटर या लैपटॉप को स्वयं उपस्थित नहीं रहने पर लॉक रखूँगा
- सुरक्षा सुविधाओं को सक्रिय करके जैसे पासवर्ड आदि का उपयोग कर अपने मोबाइल डिवाइस को सुरक्षित रखूँगा
- कठिन पासवर्ड का उपयोग करूँगा और प्रत्येक खाते के लिए अलग पासवर्ड बनाऊँगा
- अपने पासवर्ड को कभी साझा नहीं करूँगा
- अपने बैंक की नीति का पालन करूँगा और सभी सुरक्षा घटनाओं की तुरंत रिपोर्ट करूँगा
- किसी भी अनुचित प्रकटीकरण से संवेदनशील डेटा को सुरक्षित रखूँगा
- सोशल मीडिया पर कभी भी व्यक्तिगत, संवेदनशील या गैर-सार्वजनिक जानकारी पोस्ट नहीं करूँगा
- अपने परिवार, दोस्तों, सहकर्मियों और समुदाय के बीच सही सुरक्षा उपायों के बारे में जागरूकता बढ़ाऊंगा

Computer Security Day Pledge

I will:

- take personal responsibility for security and use good security practices
- pause and think about the risks before I connect to the Internet
- lock my computer or laptop when unattended
- protect my mobile device by activating security features such as using a password
- use strong passwords and create a separate one for each account
- never share my password
- follow my Bank's policy and promptly report all security incidents
- safeguard sensitive data from any inappropriate disclosure
- never post personal, sensitive, or non-public information on social media
- raise awareness of good security practices among my family, friends, colleagues, and community

WE ARE THE PILLARS TO CREATE A CYBER SECURE ENVIRONMENT

STAY VIGILANT ! BE CYBERAWARE !

CYBER SECURITY IS A SHARED RESPONSIBILITY

Let's raise awareness among our fellow colleagues, stake holders and citizens of our country reaffirming India's commitment in promotion of integrity and probity in public life through citizen participation

IF YOU CHANGE NOTHING, NOTHING CHANGES..

यूको बैंक
(भारत सरकार का उपक्रम)

UCO BANK
(A Govt. of India Undertaking)

सम्मान आपके विश्वास का

Honours Your Trust