Information Security Education & Awareness
Ministry of Electronics and Information Technology
Government of India

InfoSec Newsletter

SEP-OCT, 2018

InfoSec
CONCEPT 3 page

CYBER THREATS IN FINANCIAL TRANSACTIONS

For Virus Alerts,Incident & Vulnerability Reporting
certin Handling Computer Security Incidents
www.cyberswachhtakendra.gov.in

सी डैक CDAC
www.cdac.in

प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
संचार एवं सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Communications and Information Technology, Government of India
Plot No. 6 & 7, Hardware Park, Sy No. 1/1,Srisailam Highway, Pahadi Shareef Via Keshavagiri (Post)
Hyderabad - 501510 , Telangana(India)

InfoSec Newsletter
SEP-OCT, 2018

CREDITS

Supported by

For Virus Alerts,Incident & Vulnerability Reporting

certin
Handling Computer Security Incidents

Message from
E Magesh
Director, C-DAC Hyderabad

Securing your hard earned money is a prime task to everyone.

With the bloom of digitalization in India, there has been manifold increase in the digital transactions in India by touching almost one lakh crore rupees a month. At the same time there is a significant jump in the number of financial frauds and the value, making it a major concern to the people in India and elsewhere.

Each day fraudsters devise new methods to execute frauds. Financial fraud both online and offline can impact the individual with direct financial loss leading to emotional and psychological stress. The current edition of newsletter will help the readers to understand the complete scenario of financial frauds and how to secure your money. With the advent of low-cost Internet services, it can be seen that the more number of the population accessing online services more proactively.

Most of the Physical money transactions are replaced by online transactions. With this there is a need to raise awareness among people on the types of financial frauds and methods employed by fraudsters to commit fraud.C-DAC Hyderabad, being the coordinating center for creating mass awareness on Information Security under the purview of ISEA Project Phase II, is glad to release this newsletter on such an important topic, which is of interest for most of the stake holders.

Connect us with /informationsecurityawareness
Follow us at /infosecawa
Subscribe us at /informationsecurityawareness
Follow us at /infosec_awareness

To conduct Information Security Awareness Workshop at your Institution, please submit "Request for Workshop " in the website **isea.gov.in**

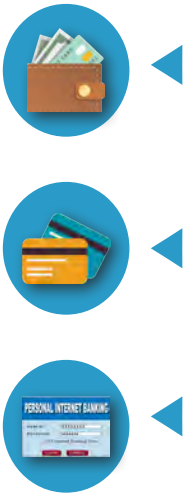
Financial security has different meaning to different individuals. But basically it is deep rooted feeling giving individuals a peace of mind that, "Everything will be good". The world of finance including financial transactions and investments has moved into a new phase where Internet plays a key role

InfoSec CONCEPT

CYBER THREATS IN FINANCIAL TRANSACTIONS

Electronic devices like smart phones, computer, laptop, tablet, POS machines, ATM etc..., are used to for online means of banking and investments. Most of these devices have become an integral part of an individual's life resulting in online means of banking and investments overtaking the traditional banking methodology. As all of us are aware that Internet also has a negative side which puts all means of online financial transactions at high risk.

Cybercriminals rely on the vulnerabilities present in Internet to seize your hard earned money. Due to this it is a necessity to take extra step to secure your hard earned money and investments. To get an insight to this, let us look at case of common banking fraud where the victim lost money from his bank account without his knowledge. It happened so, that the victim had received a mail from a stranger saying that he won a lottery. To credit the money to his bank account the victim was asked to click on a link where he had to fill his banking details. The victim shared the information on the link thinking that it is genuine. The link was used to divulge information pertaining to the bank account of the victim. With the information received, the cybercriminal could easily withdraw money from his bank account through illegal online transactions. This can happen with anyone of us any time if we are not aware and and take necessary precautions.



Major challenge lies in identifing cyber-attack, when it happens. In the present scenario wherein the life of an individual, technology plays a vital role, it is better to be aware of aspects like how to detect, how to protect and how to recover from cyber threats in financial sector?

With increase in online scams most of us are flooded with lot of questions in his mind like is my money safe online? What are the cyber security threats that can affect the savings of an individual transacted digitally in financial institutions? How can I assure safety to my investment?

Keeping all this in mind, there is a need to learn about cyber issues present in the cyber world to protect yourself and your money.

This newsletter is prepared to create awareness of the different types on online financial frauds that can happen to you. Each type of fraud is explained with a case study for better understanding of what actually happens. What are different methods used by cyber criminals to perform the fraud and what is the impact of financial fraud on an individual and the various precautions to be taken to prevent yourself being a victim of financial fraud.

HOW FINANCIAL FRAUDS HAPPEN ?

Cyber criminals employ various methods to attain the sensitive personal information to execute fraud. Few methods used by cyber criminals are Phishing, Smishing, Vishing, Skimming, SIM Swapping fraud, Fraudulent policy applications, Payment hijacking, Malware, DDos attack, Man in the middle Attack, Ransomware, Business email Compromise.

IMPACT OF ONLINE FINANCIAL FRAUD ON AN INDIVIDUAL

The first thing that comes to mind when we talk about 'impact of online financial fraud on an individual' is the direct financial loss. Victims often pass through wide range of emotional and psychological impacts of fraud. Many panick, and feel angry, freightened, anxious, ashamed and blame themselves after they are cheated. They even feel vulnerable, lonely, violated and depressed and in the most extreme cases, suicidal, as a result of the fraud they experienced.

These emotional and psychological impacts relate to both the stress of financial loss and also the loss of self-confidence that followed the fraud. The experience also may affect relationships with others, making it difficult for victims to trust others. It can be summerised as

- becoming a financial fraud victim carries emotional as well as financial costs;
- Financial and emotional costs vary across fraud categories; and
- Individual personality traits influence the victims' perceptions of impact.

TYPES OF FINANCIAL FRAUDS

BANKING AND OTHER FINANCIAL TRANSACTIONS RELATED FRAUDS

e-Wallet Fraud

e-Wallet, a facility introduced by banks to use money for commercial transactions, is now the new target for cyber criminals. Hackers and fraudsters are targeting wallets as there is minimum Know Your Customer compliance. In e-Wallets the crucial security protection of OTP is being bypassed.

"Let us go through a case study which was reported on e-Wallet fraud."

With the increase in e-payments and e-Wallet transactions, the chances of frauds and scams have also increased. One such case of fraud was reported by times of India which happened in December 2017 at Mumbai.

A fraudster has allegedly been gathering as much as Rs 91 lakh, by taking advantage of a technical glitch in e-Wallet online payment system of Gurgoan based firm in September 2017.

The fraudster transferred Rs 91 lakh through 1850 transactions to his bank account. The "technical glitch", which was detected by the end of an internal

audit in September after lasting for three months, had cost the e-Wallet company over Rs 19.6 crore.

After that the company filed a complaint, an FIR was registered at police station concerned under sections 406 (breach of trust) and 420 (cheating) of IPC. He was arrested by Police as he did not refund the money, despite a notice being issued to him by police.

https://timesofindia.indiatimes.com/city/gurgaon/bank-manager-arrested-for-e-Wallet-fraud/articleshow/62200961.cms

Credit/Debit card fraud

It is the fraudulent use of a credit or debit card account through the theft of the account holder's card number, card details and personal information, through a wide variety of methods in order to perform unauthorized transactions.

Fraudsters use different techniques to find out the details of your card. They may make up an excuse to see your card when you are using it to buy something or withdraw cash.

Let us go through a case study which was reported on 'Credit card gift scam'

On July 12th 2018 Times of India reported a case where, 30 scamsters held for Rs 5 crore credit card gift fraud. Here, one of the scamster managed to recruit 22 telecallers. His associates had collected data of SBI credit card holders like name, mobile number and city name.

The rest of the accused were hitred as team leaders. The call centre employees called customers pretending to be SBI bank employees and obtain card number, expiry date, CVV, OTP numbers. The accused targeted people in metropolitan cities who could easily speak English or Hindi.

The Manager of SBI Cards and Payment Services Pvt Ltd.,, after receiving several complaints from the customers who lost money from SBI Card, lodged Police complaint. Police arrested the accused and seized material including papers containing data, Rs. 80 lakh cash and an Hyndai creta.

https://timesofindia.indiatimes.com/city/hyderabad/30-scamsters-held-for-rs-5-crore-credit-card-gift-fraud-most-from-delhi-1-from-hyderabad/articleshow/64957139.cms

Insurance frauds

With money transactions and online financial investments having a steep rise, there is an increase in frauds in online insurance as well. Frauds are committed in short span of time by different means like opening fake account, social engineering, remote access, and payment hijacking.

Let us go through a case study which was reported on Insurance fraud. Woman Declares Herself 'Dead' To Claim Insurance Money, Arrested

On November 2017 Indian express reported a false Insurance claim made by an insurance holder where a 35-year-old woman has been arrested for allegedly declaring herself "dead" in a bid to fraudulently claim Rs. 1 crore from a private insurance company with aid from her husband. Their plan was foiled by officials of the firm who found that the claimant was alive. The woman's husband, a real estate agent who allegedly submitted "fake" documents declaring that his policy-holder wife had died. The accused had taken the insurance policy coverage of Rs. 1 crore in 2012 and used to pay Rs. 11,800 towards the annual premium.

Later, he submitted the insurance claim stating that his wife had died due to chest pain. It was found during verification that fake documents of death of another woman was submitted, along with fake medical records, fake certificates pertaining to a graveyard and also a death certificate from the civic body.

However, the insurance company official found that the policy-holder woman was alive and subsequently approached the police.

A case was registered and the woman was arrested in the last week of September 2017 on charges of cheating and forgery under relevant sections of the IPC.

The investigator said another private insurance company had also lodged a complaint accusing the couple of using a similar modus operandi in order to claim insurance policy amount and that case is also under investigation.

http://indianexpress.com/article/cities/hyderabad/woman-declares-herself-dead-to-claim-insurance-money-held-4955830/

OTHER TYPES OF FRAUDS

Mutual fund fraud

In mutual fund all transactions are done digitally. With the rise in cybercrime it has become a concern for every investor. It becomes easier for anyone to set up a fake website and offer to sell you schemes that promise high returns in a short span of time. Once the 'website' collects details of your bank account and other KYC forms through phishing / vishing, they can easily rob you of your life-savings. There have been instances where people claiming to be brokers or agents have taken cheques from investors and invested them in funds of their own.

Let us go through a case study which was reported on Mutual fund fraud, 'The third party scam'

Business today on September 2010 reported a third party scam in Mutual funds. A Retired couple was leading happy retirement life as there was no financial worries thinking their investments were in safe hands. Everything was shattered when he applied for redemption of some of the mutual funds. The retired civil engineer felt the ground beneath him slip when he was told by three mutual funds that there was no account of the Rs 82.8 lakh he had invested over the years.

A shocked civil engineer showed the receipts that, the relationship executive of a brokerage firm had given him. These turned out to be fake - colour prints taken on an inkjet printer. Using a mix of subterfuge, forgery and loopholes in mutual fund rules, the broker allegedly managed to defraud the couple of Rs 82.8 lakh invested in various schemes of three mutual funds. These were LIC mutual fund (Rs 44.8 lakh), TATA mutual fund (Rs 28 lakh) and Fortis mutual fund (Rs10 lakh).The victim feels cheated of his life savings.

https://www.businesstoday.in/moneytoday/mutual-fund/the-thirdparty-scam/story/8846.html

https://www.financierworldwide.com/qa-cyber-security-and-technology-risk-for-investment-funds/#.WrKkhNR96Ko

Dos

- ✓ Always keep your device updated, locked & protected with a strong password.
- ✓ Beware of unsolicited calls, texts or emails asking for sensitive financial information.
- ✓ Download applications on your devices from authentic apps stores with good reviews only.
- ✓ Ensure authenticity of applications by validating from links on bank websites.
- ✓ Always verify and install authentic e-wallet Apps
- ✓ Ensure your phone number is protected with a PIN.
- ✓ Make sure the beneficiary's mobile number is correct before transactions
- ✓ Use only verified and trusted browsers & HTTPS secured websites for payments.
- ✓ Ensure you change passwords frequently and promptly if compromised.
- ✓ Ensure that you securely dispose of receipts and statements.

Donts

- × Refrain from clicking suspicious links received in SMS or email.
- × Steer clear of using jailbroken or rooted devices for mobile banking.
- × Never handover your device to strangers.
- × Avoid using a common password for all wallets.
- × Refrain from opening wi-fi or unverified services for making payments.
- × Do not scan untrusted QR codes.
- × Avoid transacting through public devices and on unsecure/open networks.
- × Never allow merchants to store your card information.
- × Do not leave your credit or debit card with anyone.
- × Never share or write down your UPI M-PIN.
- × Refrain from transferring money without verifying the recipient first.
- × Never allow merchants to store your biometrics and card details.
- × Avoid giving away your Aadhaar and personal details

SECURE:
'S' for Security for citizens, **'E'** for Economic development, **'C'** for Connectivity in the region, **'U'** for Unity, **'R'** for Respect of sovereignty and integrity, and **'E'** for Environment protection.

Reference: *https://www.msn.com/en-in/sports/ipl-videos/pm-modi-at-asian-summit-sco-bats-for-secure/vp-AAyrwVr*

Shri Narendra Modi
Hon'ble Prime Minister
@Asian Summit SCO, Bats For 'SECURE'

Best practices to avoid Financial Frauds

- Never handover your device to strangers
- Avoid using open Wi-Fi for making payments
- Disclose your banking details only in secure payment websites
- Keep a watch on transaction logs and alerts
- Always verify and install authentic e-wallet Apps
- Immediately block your SIM if your device gets lost or stolen
- Report promptly the theft or loss of your card on the toll free numbers
- Ensure that you securely dispose your payment receipts & bank statements
- Use strong passwords and change frequently
- Refrain from clicking suspicious links received in SMS or email

InfoSec QUIZ

1. __a facility introduced by banks to use money for commercial transactions
   a)APY b) Mutual funds c) E wallet d) PMAY

2. ___is a patented secure keyboard
   a)ONkey b) MePIN c) Startoken d) EndPointLock

3. E wallet fraud case registered an offence under____of the IPC
   a) 419 and 420 b) 500 c) 506 and 508 d) 292

4. ____allows you to protect any app with your fingerprint.
   a) FingerSecurity b) MePIN
   c) Abhay d) Star token

5. Steer clear of using _____devices for mobile banking..
   a)Secure b) Jailbroken c) Offline d) unattended

6. Fraudsters try to collect your bank account and other KYC forms through_____
   a) Malware b) Phishing/vishing
   c) Skimming d) DDos attack

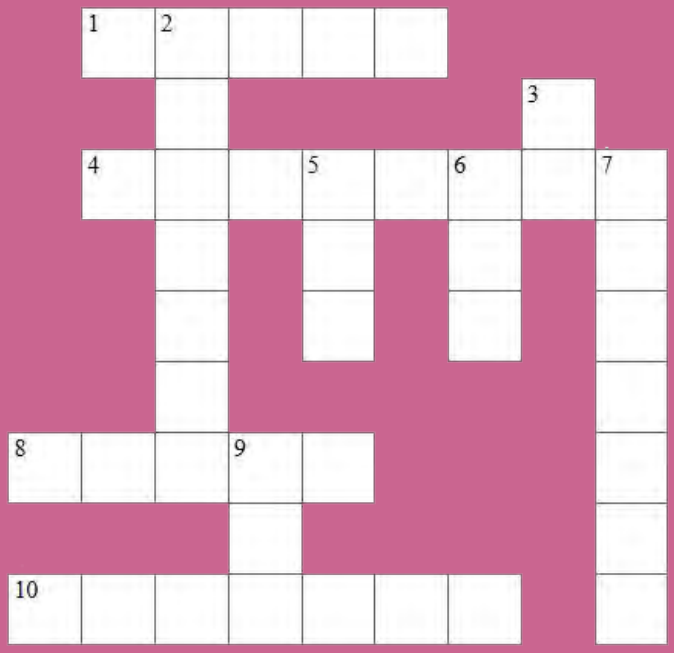
7. Immediately ____ if your device gets lost or stolen and inform respective bank/wallet organization & police officials
   a) Block your SIM b) lock your phone
   c) lock your account d) reset your device offline

8. Keep a watch on____and alerts
   a) Transaction logs b) Password
   c) Login time d) Address details

9. A _____ is a carefully shaped financial scam that's completely illegal
   a) Mutual fund b) Debit card fraud
   c) Credit card fraud d) Ponzi schemes

10. A financial fraud victim carries _____ as well as financial costs
    a) Emotional b) Pride c) Happiness d) Excited

InfoSec CONTEST



InfoSec CROSSWORD

Across

1. _____is a smart security key for online services.
4. Avoid using a common _____for all wallets
8. Use only verified and trusted browsers & ____ secured websites for payments
10. What techniques was used by cybercriminals to commit e wallet fraud

Down

2. _____ is a facility introduced by banks to use money for commercial transactions
3. Avoid scanning un-trusted ____ codes
5. Secure OTP is an OTP generation App from
6. E-wallets the crucial security protection of OTP is being bypassed
7. In mutual fund all transactions are done _____
9. Ensure your phone number is protected with a_____

Logon to

www.infosecawareness.in

to participate in
InfoSec Contest and win Prizes

INFORMATION SECURITY AWARENESS WORKSHOP

@ Gujarat

@ Goa

@ Maharashtra

@ Mumbai

@ Ahmedabad

@ Patna

@Kanpur

@Goa

CYBER FRAUDS DUPE MUMBAI-BASED FIRM OF OVER RS 20 LAKH

Aug 22, 2018

A senior accounting executive of a manufacturing company fell victim to a debit card fraud. According to the police, Rs 50,000 was allegedly siphoned off from his savings account and withdrawn in Bengaluru.

According to the police, the incident took place on July 21 when the victim, identified as Deepak, received a text message on his phone, informing that a transaction of Rs 50,000 had been conducted on his account.

Deepak, who works as a senior accounting executive in a manufacturing company in Khandsa, said, "I was returning from office and had boarded a bus for my house when I received a text message, at 5.47pm. Another message read that the user ID and password for my account had been changed, even though I did not register for online transactions with the bank."

Deepak said that he approached the bank on July 23 and also filed a police complaint. The investigating officer, requesting anonymity, said that according to the bank statement, the amount had been withdrawn from an account in Bengaluru and the police are trying to trace the accused.A case has been registered at the Cyber Crime police station under Section 420 (cheating) of the Indian Penal Code and Section 66 of the Information Technology (amendment) Act 2008, said police.

On August 18, a banking professional had lodged a complaint with the police alleging that Rs 67,000 was fraudulently withdrawn from her bank account in four transactions, after she received a text message asking her to claim her reward points.

https://www.hindustantimes.com/gurugram/accounting-executive-of-manufacturing-firm-from-gurugram-duped-of-rs-50-000/story-IHppmOA5uzddBeEPlKgA2I.html

ACCOUNTING EXECUTIVE OF MANUFACTURING FIRM FROM GURUGRAM DUPED OF RS 50,000

August 19, 2018

According to Powai police that registered an FIR, this is a case of a Man-In-The-Middle (MITM) scam, where fraudsters intercept the company's communication, impersonate the hacked parties and get money transferred to their own accounts.

An engineering company in Mumbai along with its Canada-based client were targeted by cyber criminals, who made fraudulent transfers to the tune of over Rs 20 lakh from their accounts. No arrests have been made in the case as yet.

An officer linked to the case said the Chandivali-based company, which dealt in furnace and foundry equipment, had contacted a German company to supply them hardware related to crane parts in April this year. The company normally places orders through e-mail.

The firm contacted the German company in November last year. The two companies kept communicating through emails and in February this year, the Chandivali company placed an order for some crane parts. The German company confirmed the order and asked them to make an initial payment of 30 per cent of the total amount — 5,940 euros (Rs 4.89 lakh), an officer said.

The company made a payment of Rs 4.89 lakh in April and the rest of the payment of Rs 11.24 lakh in June this year. However, within a few weeks the complainant's company received an invoice from the German company. "Having made the payment already, the complainant was taken aback and informed the German company of having already made the payment.

https://indianexpress.com/article/cities/mumbai/unit-to-fight-crime-against-women-lacks-special-training-and-basic-infrastructure-5380513/

GOVT DEVELOPS ONLINE GAME TO COUNTER CYBER CRIMES AGAINST CHILDREN

September 23, 2018

New Delhi: The government has launched its own game application for children in a bid to counter incidents of cyber crimes against children due to dangerous games like 'blue whale' and 'momo' challenges.

The 'cyber trivia' app would have a set of multiple choice questions and children would rewarded points based on their answers, the National Commission for Protection of Child Rights said. "It is an attempt to teach these children in a fun way what should be done if they are contacted by a stranger on the Internet who might ask for their pictures or ask them to do things," said Yashwant Jain, a member of the NCPCR.

The game has been developed amid rising cases of suicide by children due to challenges like 'blue whale' and 'momo'.

"The children these days outsmart even their parents. They do not understand the dangers the cyber world poses and teaching them about it would not help them understand the dangers as online games would do. That is the reason we decided to develop this game," Jain told PTI. The blue whale and momo challenges led to suicides of several children in India as well as world over.

According to advisory issued by the government, in these games, the creators seek out their victims who are in depression and send them an invitation to join. The basis of the challenge is that an anonymous "group administrator", otherwise known as "the curator," hands out tasks to selected "players" that must be completed, documented and posted during a period.

https://www.news18.com/news/india/govt-develops-online-game-to-counter-cyber-crimes-against-children-1886417.html

NOW, GOVT OFFERS OFFLINE TOOLS FOR YOUR AADHAAR VERIFICATION

October 3, 2018

Bid To Counter Surveillance & Data Leak Fears

New Delhi: In a bid to assuage fears over surveillance, breach of privacy and data farming, the government is promoting offline verification tools for Aadhaar such as QR codes and a paperless KYC that will not require sharing of biometrics or involve UIDAI servers for authentication.

The KYC process will not even need users to reveal their Aadhaar numbers, the collection of which has often been subject to controversies over potential data mining and tracking. The offline processes will fulfil the Supreme Co- urt's order ruling out biometrics-based Aadhaar authentication for private companies.

The offline KYC processes can be used by service providers, including the government, and will be in addition to other IDs such as driving li-

Aadhaar offers downloadable offline eKYC which is a digitally signed secure document. It contains as much demographic info as you want, with five options. Apart from name and address, other demographics like gender, date of birth, mobile, email and photo are optional

It can be verified offline and electronically transferred to a service provider. It can be in an electronic or printed format. Much more reliable than other forms of ID.

Advantage of both QR code and paperless eKYC is that there is no submission of biometrics and authentication through UIDAI server, addressing fears of data tracking and collection and safeguarding individual privacy cences, ration and electoral photo cards, passports and PAN cards. The government hopes reliability of offline Aadhaar KYC will make it popular while providing options for fintech firms disadvantaged by being denied ac- cess to UIDAI authentication.

The QR codes, which include three options, can be downloaded and printed from the Unique Identification Authority of India site.

https://www.pressreader.com/india/the-times-of-india-mumbai-edition/20181003/281479277354671

MEPIN SECURE AUTHENTICATOR

MePIN is a smart security key for online services. It can help you to protect yourself against password phishing and hacking. It can be used for 2-step verify passwords with a simple tap, PIN code or fingerprint and no manual passcodes needed. It can also authorize online transactions (payments, account changes, etc). Sign up and sign in to online services without the use of passwords at all. Keep in touch with the services and avoid e-mail overload. MePIN does not use or save usernames and passwords. It is built on Public Key Infrastructure (PKI), where each device is identified with its own secure private key

https://play.google.com/store/apps/details?id=com.mepin.android3

ENDPOINTLOCK

EndPointLock is a patented secure keyboard, which produces keystroke encryption for Android mobile devices, protecting user credentials, passwords and online transactions. The EndpointLock is the most powerful must-have security tool that every mobile user needs to be secure. Mobile devices are now replacing the home and corporate desktop computers. In this new role, the mobile device has become a focal point for the hacker looking to breach your online transactions and corporate network, therefore protecting these mobile devices is critical. It actually encrypts Password logins, Mobile Banking, Mobile Shopping, Credit Cards entries, Health-Care information. It supports Android Phones & Tablets.

https://play.google.com/store/apps/details?id=com.endpointlock

FINGERSECURITY

FingerSecurity allows you to protect any app with your fingerprint. FingerSecurity has many options to make your life easier and more secure. FingerSecurity will only work on Android devices with a fingerprint sensor. Even when your device has a fingerprint sensor it is still possible that your device is not supported due to limitations of the device.This app uses the Device Administrator permission, as an opt-in option, to prevent the app from being uninstalled. Protect notifications of protected apps. Automatically protect new apps.

- Protect any app with your fingerprint
- Widget for fast enabling/disabling
- Set timeouts to allow a short switch between apps
- Unlock multiple apps at ones
- Use your alternative password or pin code to unlock apps when your fingerprint is not recognized
- FingerSecurity can't be uninstalled or killed
- Automatically protect new apps
- Use your favorite image as background
- Use fake crash dialog
- Automatically unlock your apps at specific locations
- Only allow specific people(fingerprints) to unlock an app
- Protect notifications of protected apps
- Detect intruders by taking a picture of them

https://play.google.com/store/apps/details?id=com.rickclephas.fingersecurity

STARTOKEN – NG

StarToken NG is the official mobile banking app from Bank of India. StarToken NG, the next generation secure digital banking app, allows convenient access to digital banking services of Bank of India from your Android phones while maintaining the strictest security standards. Install, Activate and Enjoy worry-free banking with intuitive user experience and watertight security from REL-ID . Quick Banking featuring your frequently used banking services such as Balance Inquiry, Mini Statement, Self-Link Fund Transfer, Third-Party Fund Transfer, NEFT etc. It can also search for nearby ATM or Branch. Transaction authorization for seamless retail commerce experience.

https://play.google.com/store/apps/details?id=com.uniken.r2fa4a.boi

SBI SECURE OTP

SBI Secure OTP is an OTP generation App for verifying transactions done through State Bank Internet Banking and State Bank Anywhere App. You can generate OTP in two modes. Online OTP in which Internet connection (via SIM or Wi-fi) is required for generating OTP. Offline OTP in which OTP is generated in the absence of Wi-fi, Mobile network or SIM card. One time registration with your INB credentials is required for using the App. Service provider independent, hassle free OTP service is now available to you.

https://play.google.com/store/apps/details?id=com.sbi.SBISecure

ABHAY

Abhay by IDBI Bank Ltd provides IDBI Bank customers instant, anywhere control of their Debit Cards. Key Features & Functionality include On logging-in to the application, all valid Debit cards issued to the customer will be displayed. Each card can be controlled independently. Switch the card On/Off (Temporary Activation/Deactivation). Set a daily transaction limit in Rupees for ATM & POS. Display last 10 transactions in the account linked to the card with description. Customer can enable/disable international transactions. In case of emergency, Customer can Hot-list the card (Permanent Deactivation of card) .

Key Features & Functionality:

1. On logging-in to the application, all valid Debit cards issued to the customer will be displayed.
2. Each card can be controlled independently.
3. Switch the card On/Off (Temporary Activation/Deactivation).
4. Set a daily transaction limit in Rupees for ATM & POS.
5. Display last 10 transactions in the account linked to the card with description.
6. Customer can view loyalty points accumulated.
7. Customer can enable/disable international transactions
8. In case of emergency, Customer can Hot-list the card (Permanent Deactivation of card)
9. Customer can view the balance available for the primary account.
10. Customer can use the Language option (Hindi or English).

https://play.google.com/store/apps/details?id=com.idbibank.abhay_card

CERT-In Advisory CIAD-2018-0025
Multiple Vulnerabilities in Apple Safari

Software Affected

Apple Safari versions prior to 12.0

Description

The vulnerabilities are due to the access control error in various components within WebKit and Safari component. A remote attacker could exploit this vulnerability by creating a specially crafted content or persuading a user to click a link which may lead to malicious website to spoof the user interface and obtain auto-filled data in Safari.

Successful exploitation of this vulnerability could allow the attacker to lead user interface spoofing, preventing user to delete browsing history items and obtain potentially sensitive information on the targeted system.

For more details visit :
https://cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2018-0025

CERT-In Advisory CIAD-2018-0026
"Wiretapping" attacks in ATMs

Systems Affected

ATMs

Description

Each day there are new reports of attacks on ATMs around the world and criminals continue to vary and modify their attacks and attempt to bypass the protections in place.
A card skimming attack is defined as "the unauthorized capture of magnetic stripe information by modifying the hardware or software of a payment device, or through the use of a separate card reader". Skimming is often accompanied with the covert capture of customer PIN data.

For more details visit :
https://cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2018-0026

CERT-In Advisory CIAD-2018-0027
Facebook Security Breach

Description

On 28 September 2018, Facebook Inc published a security update regarding a data breach that affected almost 50 million users account.

The attackers exploited a vulnerability in Facebook's "View As" feature to gain unauthorized access of user accounts that lets users see what their own profile looks like to someone others profile. The attackers used Facebook's APIs to access personnel details of user account.

This vulnerability allowed attackers to steal the user's access tokens, which they could then use to gain access to the Facebook account and other third-party websites that the user had logged into using his/her Facebook credentials.

The attackers could leverage the vulnerability to access the personal information stored in user's Facebook accounts, using such information, scams and phishing attempts could look more credible.

Facebook has also reset the access tokens of the 50 million user accounts that were affected and another 40 million accounts that have been subject to a "View As" look-up in the last year. After they have logged back in, people will get a notification at the top of their News Feed explaining what happened.

For more details visit :
https://cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2018-0027

Magniber ransomware

It has been reported that ransomware named "Magniber" is spreading. Magniber Ransomware is being distributed through malvertisements, compromised websites which make the victim to land on the Magnitude exploit kit page.

Malicious Activity:

- First victim is landed on the Magnitude exploit page with the help of obfuscated java script along with a Base64 encoded VBScript as shown in Figure1.
- Now attacker try to exploit the vulnerability (CVE-2018-8174) present in VBScript engine with the help of internet explorer. This vbscipt then executes the shell code.
- The shell code just act as simple downloader for downloading the obfuscated payload. This obfuscated payload contains the Magniber ransomware in packed form, which it unpack and try to inject it into the legitimate process.
- Finally the ransomware start encrypting all the files with a unique key and add the .dyaaghemy extension to all the encrypted files.
- While encrypting the files, Magniber will also create a ransom note and links to a URL (which contains the victim actual ID) of TOR decryption service to decrypt its files.

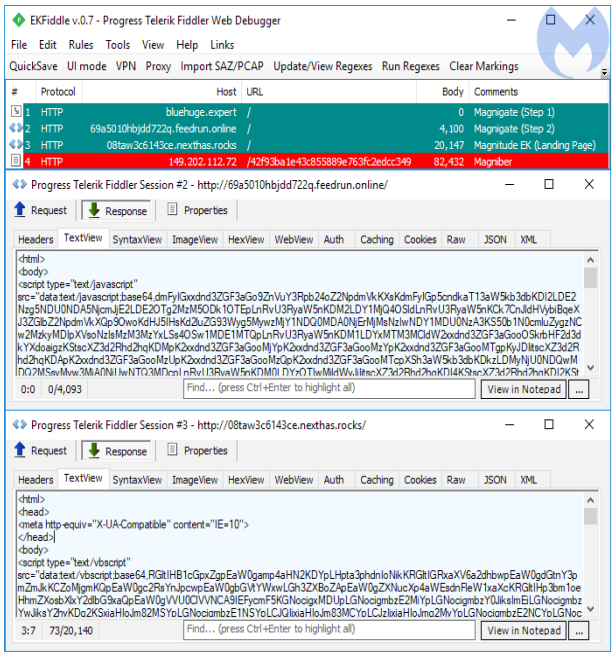


Figure 1. Traffic view of a Magniber infection (source: Malware bytes)

For more details visit :
https://www.cyberswachhtakendra.gov.in/alerts/MagniberRansomware.

Emotet Trojan

Emotet is banking Trojan which stole the sensitive information from the victim computer. The modes of spreading is unscrupulous phishing emails with malicious attachments or links pointing to malicious documents. Once emotet infect the victim system, it starts building the connection with its C2 server and send all the sensitive data, credentials to the attacker controlled C2 server[s].

Malicious activity:-

- Once victim open the malicious document, it ask for enabling the macro, which will invoke power shell to execute a script present in doc file to download the Emotet from the c2 server.
- After Emotet downloaded, it checks whether it is running in sandboxing environment or not. If it finds that it is running in a sandbox then it will not proceed further, else it will execute further.

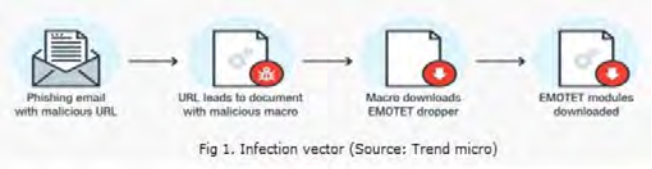


Fig 1. Infection vector (Source: Trend micro)

- Now emotet act as dropper and download other banking malware names as Zeus Panda banker, Trickbot or Iced ID on the victim machine.
- Emotet also download the different module for performing malicious activities like Banking module for performing authorized transaction, Distributed denial of service (DDoS) module, Spam module for propagation across the network, Email client info stealer module, Browser info stealer module, Personal Storage Table (PST) info stealer module as shown in figure2.
- Finally Emotet start performing malicious activity based upon the module it download like performing authorized transaction, stealing victim credentials, communication with C2 etc. Emotet maintains its persistence via changing the registry Run key.

For more details visit :
https://www.cyberswachhtakendra.gov.in/alerts/emotet.html

To Share Tips / Latest News, mail us to

isea@cdac.in

About ISEA

Looking at the growing importance for the Information Security, Ministry of Electronics & Information Technology has identified this as a critical area. Information Security Education and Awareness (ISEA) Project was formulated and launched by the Govt. of India. One of the activities under this programme is to spread Information Security Awareness among children, teachers, home users, IT and non-IT professionals throughout the country. C-DAC Hyderabad has been assigned the responsibility of executing this project by Ministry of Electronics & Information Technology, Government of India. As part of this activity C-DAC, Hyderabad has been preparing Information Security Awareness material, coordinating with Participating Institutes (PI's) in organizing the various Information Security Awareness events all over India.

About C-DAC

C-DAC established its Hyderabad Centre in the year 1999 to work in Research, Development and Training activities embracing the latest Hardware & Software Technologies. The centre is a Knowledge Centre with the components of Knowledge Creation, Knowledge Dissemination and Knowledge Application to grow in the areas of Research & Development, Training and Business respectively. The R & D areas of the centre are e-Security, Embedded Systems, Ubiquitous Computing, e-Learning and ICT for Rural Development. The centre has developed over a period of time a number of products and solutions and has established a number of labs in cutting edge technologies. In line with these R&D strengths, the centre also offers Post Graduate level diploma courses. Centre is also actively involved in organizing faculty training programs. The centre regularly conducts skill based training and information security awareness programmes. InDG portal is hosted and maintained to facilitate rural development through provision of relevant information, products and services in local languages.

BOOK POST

For queries on Information security

Call us on Toll Free No.

1800 425 6235

ISEA Whatsapp Number for Incident Reporting

+91 9490771800

Between 9.00 AM to 5.30 PM

Subscribe us on

https://www.youtube.com/c/InformationSecurityEducationandAwareness

Follow us on

https://twitter.com/InfoSecAwa

Connect us with

https://www.facebook.com/infosecawareness

Ministry of Electronics & Information Technology
Government of India

सी डैक
CDAC
www.cdac.in

प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Electronics and Information Technology, Government of India
Plot No. 6 & 7, Hardware Park, Sy No. 1/1, Srisailam Highway, Pahadi Shareef Via Keshavagiri (Post), Hyderabad - 501510, Telangana(India)
Nalanda Building, No. 1 Shivabagh Satyam Theatre Road, Ameerpet, Hyderabad - 500016, Telangana (India)