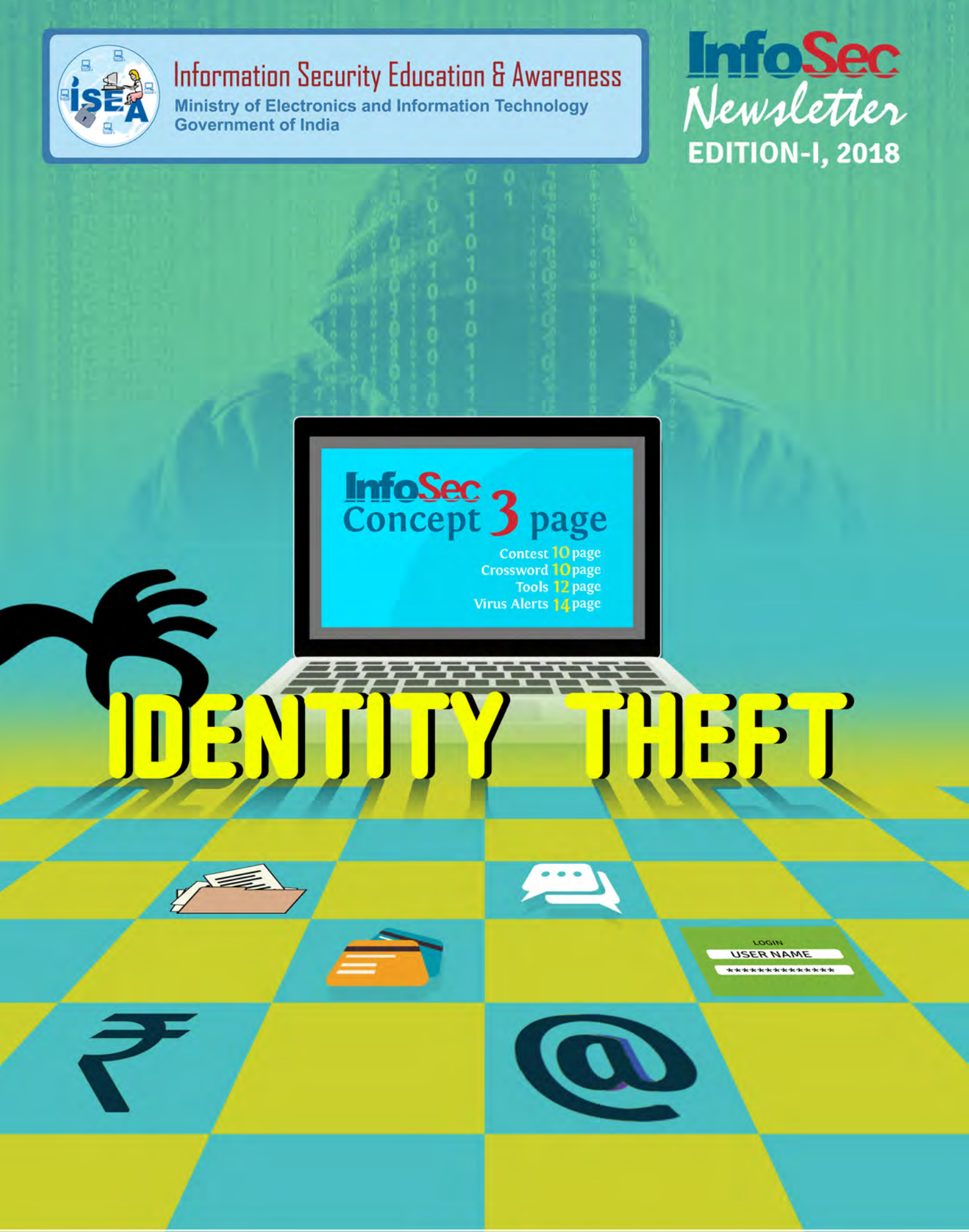
Information Security Education & Awareness
Ministry of Electronics and Information Technology
Government of India

InfoSec Newsletter

EDITION-I, 2018



For Virus Alerts,Incident & Vulnerability Reporting
cert-in 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

EDITION - I, 2018

CREDITS

Supported by

For Virus Alerts,Incident & Vulnerability Reporting

certin
Handling Computer Security Incidents

Message from

E Magesh

Director, C-DAC Hyderabad

With internet and technology having a impressive growth and India moving to a digital era , lot of concerns come up in the minds of people. The reach of Internet is expanded that every device we use , makes us vulnerable to identity theft. Identity theft is a major concern of the society which is fast growing problem in India and else where. It can be defined as an act where someone uses your identity for their own benefit. Over the years Identity theft has risen to affect millions of people all over the world and the numbers are increasing day by day.The vast amounts of personal data that is available either online or through data breaches is only making it easier for the fraudster.

The current edition of the newsletter will help readers to understand the complete scenario of Identity theft and how to be safe. The rise of the internet has forced us to seek easy-access communications at the expense of personal safety & security. Life has been made easier by replacing physical transactions with digital ones. Each Individual must focus on educating on good cyber-security behaviors and raise awareness on the social engineering techniques employed by fraudsters.

This newsletter on Identity theft will help prevent you from becoming a victim of cyber thieves. However, as cyber thieves become more sophisticated, you should know ways to safeguard your personal information. 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 all stake holders.

Connect us with /informationsecurityawareness

Follow us at /infosecawa

Subscribe us at /informationsecurityawareness

Follow us at /infosec_awareness

IDENTITY THEFT

We are all part of digital movement that is transforming India into a digitally empowered society. In this digital world, we need to ensure that every citizen is safe and his/her interest including the interest of the family is secure in all aspects.

Every device/ technology you come across, which makes your life easier and happier can put your digital identity at danger. Identity theft is one of the fastest growing problem which is effecting millions in India as well as in the world which requires immediate attention. In this scenario, it is essential that every individual is fully aware of various aspects of Identity theft.

What do you mean by your Identity and what is Identity Theft and various ways/methods to protect one's Identity ?

Identity-answers to the question who you are? In general context, it can be your social identifying information or employment details and digital social identifying characteristics in the world. Personal Identifying information includes, Name, Phone Number, Email-ID, Date of birth, Address, Identity card number, Permanent account number, Aadhaar card number, Voter ID, Credit/Debit card details, Medicare Number, Passport details, Travel details, Iris scan, Fingerprints, Voice sample etc.

"Identity Theft is illegally using another person's personal identifying information like name address etc., as well as financial information like credit/debit card details in order to make purchases or borrow money, open a new account or commit a crime without that person's permission"

How Identity theft can happen?

We know that identity thieves can misuse our identity for fraudulent activities. We put across different ways the theft can happen, how cyber criminals exploit the different vulnerabilities to steal individual's identity.

1

We come across survey forms given in restaurants and lucky draw coupons at shopping malls/movie theaters requesting personal information. Generally, this information is sold to many parties for money. We may carelessly speak in public places with our friends and family. People may be watching us from nearby location, and listening to our conversation. If you give out personal information like over the telephone, the potential thieves overhear your conversation and may use for fraudulent activities.

2

We often get calls regarding products and we may wonder how they get our phone number. Many organizations sell these phone numbers to consultants for money. For example, after shopping at super markets and medical stores and retail chains in malls, these outlets insist on giving our phone number, saying that it is for add-on points which can be used for the next purchase. This can be misused leading to Identity theft.

3

Stealing of personal information can happen through malware. Malware can be sent through mail/SMS/WhatsApp link. Malwares can be in different forms like Viruses, Spyware, Rootkits, Remote Access Tools.

4

Personal information from credit/debit and other smart payment cards (like shopping, gift cards etc.) can be read though RFID (Radio Frequency Identification) device without even physical contact with the card.

5

Very often, we receive messages promising some benefit in the form of cash prize/ lottery/job offers through email/WhatsApp/SMS. They send mails with logos similar to the original websites making them feel like authorized one. They may ask us to click on a link which redirects to another page, where we are asked to give our personal sensitive information like banking details. We may get excited by some offer we received and may click on the link. This may result in loss of money, if you reveal your banking information through such links.

6

Criminals may access your private information from online shopping portals, e-commerce sites and online bank accounts and use that information against you or for self-benefit. Identity thief casually go through different profiles in social media through a fake account. From the profiles they select a few gullible targets for attacking. They send 'friend' request to initiate a relationship and try to gain trust through chatting. After gaining trust they get hold of sensitive personal information from the potential targets.

7

Criminals try to retrieve information from computer servers that is not secured or monitored properly. They may access routers, through ports which are configured improperly or opened unknowingly, or have weak password which are vulnerable to identity thefts.

With enough identifying information about an individual, a criminal can take over that individual's identity to conduct a wide range of fraudulent activities/crimes. These include,

- Submitting false applications for loans and credit cards and making withdrawals from bank accounts resulting multiple range of debts in victim's name without the knowledge of victim.
- Making fake online accounts in social media and may also try to defame any individual in the social networking sites.
- Forgery of the documents of an individual's identity to get the benefits like obtaining new phone connections.
- PAN card and Medical Insurance Information can be used by thieves to file a tax return or claim fraudulent tax return, get medical discounted benefits using your name.
- Use children's personal information to avail government benefits.
- Can use your driving license/Passport/Aadhaar Information to avail benefits on behalf of your name.

DO's:

- ✓ Protect your personal data.
- ✓ Monitor your financial accounts for any suspicious activity on a regular basis – this includes bank accounts, credit card statements
- ✓ Enable two factor authentication for authorisation.
- ✓ Be aware of onlookers when using your credit/debit card and entering your PIN number.
- ✓ Update anti-virus and encrypt internet connection to save from malware and perform quick scan while downloading from E-mail.
- ✓ Do transact only with trusted companies/websites.
- ✓ Regularly check all your online accounts and social networking accounts for any unauthorized use.
- ✓ Limit upload of personal information in social networking sites.
- ✓ Always read and check privacy policies.
- ✓ Do online shopping only through sites that have secure payment gateways.
- ✓ Send password protect documents over the internet.
- ✓ Take immediate by informing the concern authorities if you think your personal information has been misused.

Don'ts

- × Don't provide personal information about you or your family members over the phone or internet unless you initiate the contact.
- × Don't throw unteared documents with your personal information in the dustbin.
- × Don't share your personal data or leave it unprotected.
- × Don't carry all your Identity cards (like Aadhaar card/PAN card/Medical Insurance Number) in your wallet.
- × Don't Send financial information through email or website without the 'http**s**://' prefix in the URL.
- × Don't download email attachments from anonymous mails/unknown senders.
- × Don't respond to exciting job offers/gift offers through mails.

TYPES OF IDENTITY THEFT

Phishing
Phishing is a form of Identity theft that frequently occurs on the web. The term refers to techniques implemented by a criminal to fish personal information. The purpose is to use this information to commit identity theft and other types of fraud.

Stealing
Identity thief tries to get personal information through Electronic wallets, purses or using other sources. Identity theft can happen through the photocopies of ID proof documents handed over to strangers for various purposes.

Pharming
Hackers who redirect a legitimate website's traffic to an imposter website, where they trick the consumer into thinking they are on the legitimate site and try to get you to either purchase their product or divulge your personal information.

Child Identity theft:
Personal Information of a child is used by criminals to apply for government benefits, open bank and credit card accounts and apply for loan.

Skimming
Special electronic devices are inserted in ATM and credit and debit card processing machines to obtain credit and debit card details.

Dumpster Diving
It is a way of getting hold of invoices, financial records or other documents containing personal information from the dustbin.

Tax Identity Theft
PAN card number which is personal information of an individual is stolen for the purpose of filing fraudulent tax return in the victim's name and also in 'unauthorized' transactions, purchase of luxury cars, etc.

Medical Identity Theft
Personal Information like Name or Medicare Number stolen to submit fraudulent claims to Medicare and other health insurers without your authorization.

Pretexting
Fraudsters use false pretenses to obtain your personal information from financial institutions, telephone companies, and other sources.

Identity theft where Identity Cards are involved.

ID proof's like Aadhaar card, PAN card, Driving License and Medical Insurance Number may be asked by some business organization or anyone else. It is best to give this information only when you initiate the phone call, the email or the application with the organization concerned. Keep a list of phone numbers to call in case you find yourself as a victim of identity theft. When we lose our major ID proofs by any means it is better to report to agency concerned immediately. The Organizations associated, for Driving license -Regional transport office (RTO), for PAN card - Income Tax Department, and for Voter ID - Election commission can be contacted for the reissue of lost ID card.

Punishment for Identity Theft

Information Technology Act, 2000(Amendment 2008) ,66C. - Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one Lakh.

Identity theft can happen to anyone at any point of time. It can take many forms and shapes. It can cause a potential damage to your social identity and loss of your hard earned money. We are always cautious to protect ourselves and our family in the physical world. In the same way, since we all are aware that the cyber world is as good as physical world with similar risks existing, we should take extra steps to protect ourselves and our family as well as our valuables which we have earned. Your identity is your responsibility. With respect to the current state of cyber world where we cannot put a stop to this problem, it is always better to protect ourselves from these crimes.

Steps to be taken if Identity theft had taken place

If you feel an identity theft had taken place, then what are the possible steps to be taken to mitigate the situation

STEP 1

Ascertain the type of identity theft that has taken place on your identity.

STEP 2

File a complaint in a written document showing the details of theft happened on your identity

STEP 3

Report your identity theft to the police station concerned and register a complaint and also submit a copy to the concern banks/ financial institutions.

It is always advisable to keep a copy of all the document pertaining to your identity at a safe place. File complaint based on the copies of the identity cards safely preserved.

If necessary, the following documents are to be submitted in the local police station

- A copy of your identity theft report
- A government issued ID with a photo
- Proof of your address
- Any other proof of your identity theft
- After reporting make sure you take a copy of the police report

What are the further steps that can be taken?

- Once we identify ourselves as a victim of identity theft, it is better to intimate the bank to close any of the new accounts that are opened on your identity without your knowledge. Also intimate the bank to remove the bogus charges from your account which are being charged on you for the actions of the identity thief.
- Make sure that your credit/debit account reports are corrected by intimating the bank.

Other possible steps that can be taken?

- Immediately report to the authority concerned on misuse of any identity card.
- Stop debit collectors from trying to collect debits you don't own.
- Apply for re issue of Identity card to the authority concerned.
- Take efforts to clear your identity from the criminal charges that are occurred by seeking the help of Law

InfoSec NEWS ALERTS

CASE STUDIES

Case 1: Identity theft on Instagram

In recent times, social networking application -- Instagram which also features video-sharing and chatting options that are often linked to Facebook and Twitter, has gained immense popularity among smartphone users. The Chennai city police received a complaint on identity theft based on Instagram, which is a popular photo-sharing network.

According to the police, a young girl has petitioned that her personal Instagram account has been duplicated by an unknown person and is being misused online. It is suspected that it was a work of a prankster who lifted the photographs posted by the girl using screenshots and a duplicate account had been created on Instagram.

The suspect has added ('following' in Instagram terms) a few friends through the duplicated account and started chatting with them. After learning about it from one of her friends, the girl decided to lodge a complaint with the office of the police commissioner. Though there has been a steady flow of complaints regarding derogatory Facebook posts and profile duplication. This complaint pertaining to Instagram was the first.

Case 2: Student arrested for hacking WhatsApp accounts

Nashik police have arrested a college student from Rajasthan for allegedly hacking 31 WhatsApp accounts and sending obscene messages through these. The accused, was arrested from Jasol in Barmer district of Rajasthan.

Most of the complaints have come from women. The accused hacked accounts by managing to get hold of one-time-password (OTP) issued for account verification. According to police, the accused has sent obscene messages from the hacked account to others on the victim's contact list.

Case 3: Identity theft pertaining to online dating/matrimonial websites

Now a day's marriage proposals have taken a new face through matrimonial websites, through which online dating/chatting have become common. Many register their profile with fake photos and salary details. They exchange phone numbers /e-mail id/family details. These could be misused.

Case 4: Identity theft pertaining to banking operations

Though banks have been regularly providing various alerts through Email and SMS as they never ask any sensitive/confidential information over the telephone or through email, etc. But a senior citizen from Mumbai still got misled, when some female misrepresented as a Bank Executive and asked for various details of the Debit Card. The account got debited of Rs 70000 immediately.

Case 5: Identity theft that can happen through social media

The technology can put us at the risk of cybercrimes. Now-a-days it is difficult to find an internet user who is not active in social media. With the reach of smart phones, social media is in easy reach of an individual at any point of time.

So Identity thieves after finding their target, scans through the social networking sites. This gives them an idea of your regular activities as well as your friends and other Interests. This helps them to trap others. Very often high profile government officers are targeted for their sensitive information.

An Indian Army Officer met someone at coffee shop from rival army unknowingly. She was trapped with the information from Social media. The meeting was caught in video and with that she was blackmailed to get sensitive Information of the Indian Army.

Case 6: Identity theft that can happen through online taxi booking apps

Online taxi booking has reduced the hurdle of travel to a large extent. To register we need to provide our personal information which includes name, mobile number, e-mail. While booking a taxi/cab our mobile number is shared to the driver to whom the trip is assigned. The driver uses the information from the app and calls to confirm the pickup location. But generally the drivers use a different number other than their registered number with the app. The driver may steal your mobile number and may misuse it.

Case 7: Identity theft relating to fake weight loss/beauty apps/travel and hotel booking apps

Social media is flooded with advertisements of fake weight loss/ beauty apps. They give free trial for a month/week and ask to pre-register with personal banking details promising to send notification mail once your trail period is expired, which may or may not happen. Travel and hotel booking apps offer attractive discounts to attract people to download and register in their app. Seeing the offers many book the travel tickets and end up with loss of money as there was no ticket/hotel booked in their name. Be aware

InfoSec QUIZ

1. Stealing wallets, purses, mail, or using other sources to gather personal information is called as
   a)Theft b) Dumpster diving c) Pharming d) Vishing

2. Sifting through garbage to find invoices, financial records or other documents containing personal information
   a)Theft b) DumpsterDiving c) Pharming d) Vishing

3. _____is Creating Fraudulent Web sites that look legitimate in order to collect personal information from consumers.
   a)Phishing b) Pharming c) Vishing d) Skimming

4. _____ is Gathering personal information from forms that are linked from e-mails or pop-ups. Reputable companies will never solicit personal information through unsecured e-mail or through the internet.
   a)Phishing b) Pharming c) Vishing d) Skimming

5. _____is Special electronic devices are inserted in ATM and credit and debit card processing machines to obtain credit and debit card numbers.
   a)Phishing b) Pharming c) Vishing d) Skimming

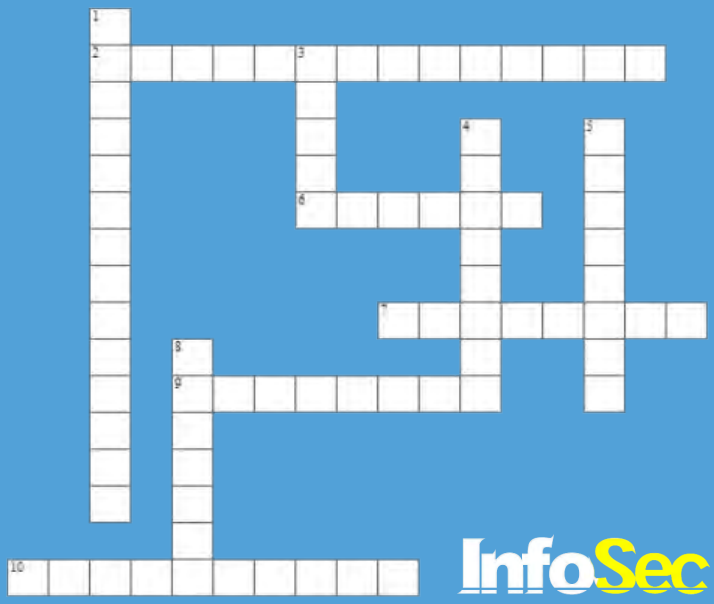
6. _____ is an Identity Frauds use false pretenses to obtain your personal information from financial institutions, telephone companies, and other sources.
   a)Phishing b)Pretexting c) Pharming d) Skimming

7. _____ is the state of being certain of remaining safe and unthreatened.
   Theft b) Trojan c) Security d) Malware

8. Collection of personal information and effectively posing as another individual is known as
   a)Identitytheft b) onlinethreat c) both a and b d) None of these

9. What is the name of the application program that gathers the user information and send it to someone else through internet is _____
   a)Spyware b) Trojan c) Worm d) None of these

10. A program that performs a useful task while simultaneously allowing destructive acts is a _____
    a)Spyware b) Trojan c) Worm d) None of these



InfoSec CROSSWORD

Across

2. Sifting through garbage to find invoices, financial records or other documents containing personal information is called as
6. A program that performs a useful task while simultaneously allowing destructive acts is called
7. _____is special electronic device which are inserted in ATM and credit, debit card processing machines to obtain credit and debit card numbers.
9. _____is Gathering personal information from forms that are linked from e-mails or pop-ups.
10. _____is an Identity Frauds use false pretenses to obtain your personal information from financial institutions, telephone companies, and other sources

Down

1. Collection of personal information and effectively posing as another individual is known as
3. Stealing wallets, purses, mail, or using other sources to gather personal information is known as
4. is Creating Fraudulent Web sites that look legitimate in order to collect personal information from consumers.
5. is the state of being certain of remaining safe and unthreatened
8. What is the name of the application program that gathers the user information and send it to someone else through internet is called a

Logon to
www.digitalsuraksha.in
www.infosecawareness.in
to participate in
InfoSec Contest and win Prizes

INFORMATION SECURITY AWARENESS WORKSHOP

@ Bhopal

@ Madhya Pradesh

@ IIIT Bhubaneswar

@ Indore

@ Madhya Pradesh

@ IIIT Bhubaneswar

@ Telangana

Govt. Official@ Hyderabad

With the introduction of smartphones, people have started using them to do a variety of tasks such as shopping, internet surfing, banking, payment of bills, photography and interaction on social media. This means there is a lot of sensitive data that can be found on a person's phone. Not only should this sensitive data be protected from being misused but your personal information must also be protected from hackers.

While smartphone apps can help you with a variety of everyday tasks, they can also protect your phone from identity theft and hackers and help you keep your personal data from falling into the wrong hands. Here are some of the best Android apps to protect you from identity fraud.

Identity Guard

It's common for hacking victims to be totally oblivious to the fact that their personal details have been stolen. You can say goodbye to those worries by simply installing the Identity Guard app for Android. It provides real-time alerts as soon as it notices any unusual activity on any of your accounts. It also maintains your personal credit report and notifies you of any significant changes. It also provides you alerts for any change of address so that your mails or posts are not delivered to the wrong place.

Link to download the identity guard on your identity guard
https://play.google.com/store/apps/details?id=com.intersections.identityguard&hl=en

Credit Karma

Keeping a good check on your monthly credit reports is the best way to know whether your credit cards or your personal details have been misused by someone or not. Credit Karma has ties with two major credit bureau and provides totally free-of-charge credit report on a daily basis. Credit Karma also features special notifications for any significant changes in the credit reports and also provides tools and recommendation to the user to organize their information and keep it safe from attackers.

Download link for credit karma
https://play.google.com/store/apps/details?id=com.ckreport.techniquehighscore&hl=en

Life Lock

The amazing Life Lock app not only keeps your personal details organized but can also help you keep your financial information safe. You can keep the information from your credit cards and other loyalty cards organized in a digitized format, so you don't need to carry them whenever you want to go shopping. In addition to this, users get a theft and data protection service as soon as you register for the app, which will provide you with regular alerts each time your accounts are accessed. It also offers a protection service in case you lose your wallet and provide you a monthly report of your credit score which seems to be a plausible reason to install this app

Download link for Life Lock
https://itunes.apple.com/us/app/lifelock-id-theft-protection/id1087187361?mt=8

Credit Sesame

Credit cards and personal loans are some of the most susceptible areas for identity-related frauds. When your personal details are compromised, there is a high chance that they will be used to create a fraudulent account or transaction in your name. So keeping a check on your credit reports is a great way to notice any irregularities. Credit Sesame provides you a free of charge credit score and also monitors your credit cards. It also provides you with several tips and advice to help you save money and lower your expenses.

Link to download the identity guard on your identity guard
https://play.google.com/store/apps/details?id=com.creditsesame&hl=en

Log Dog

With so many accounts on various websites and social media platforms, it is certainly hard to keep a track of all the accounts. This can also be a major problem when your details get stolen by a malicious hacker and you cannot tell where the information was taken from. To solve this problem you can install the Log Dog app, which is basically a security system that alerts you as soon as it senses an unusual activity on your accounts. This not only helps you keep a track of all your online accounts, but also helps you in taking quick action in case your details are compromised.

Download link for Log Dog
https://play.google.com/store/apps/details?id=com.logdog.websecurity&hl=en

Secret Control – Anti-theft

Getting your phone stolen is not only a big blow for your access, but also compromises your personal data. As most people use smartphones to store and manage their personal data, accidental loss or theft can leave your details at the mercy of others. To prevent this one simply needs to install the Secret Control app that helps you keep your smartphone from being stolen or lost. It contains a password protected screen-lock, phone finder, anti-theft alarm with motion sensors and notifications if the phone's Sim card is removed or changed.

Download link for secret control
https://play.google.com/store/apps/details?id=com.majesticappsco.secretcontrol&hl=en

Alerts for Identity Theft

In addition to installing tools on your computer to protect yourself follow the below alerts:

- When entering sensitive information (bank account numbers, credit card information, social security number, mother's maiden name) online look for "shttp://" or "https://" in the address line of your browser. This means information is being sent securely.
- Never click on a link in an email directing you to a Web site. Manually type the Web site address into your browser to be sure you are not misdirected.
- To prevent pharming, use anti-virus and anti-spyware software and be sure to keep them up to date.
- Don't give out personal information unless you've initiated the contact or are sure with whom you are dealing.
- Look for Web site privacy policies for maintaining accuracy, access, security, and control of personal information collected by the site, how the information will be used, and whether it will be provided to third parties.

CERT-In Vulnerability Note CIVN-2018-0032
Denial of Service Vulnerability in ISC BIND
Software Affected
ISC BIND version 9.10.6-S1 through 9.10.6-S2
ISC BIND versions 9.10.5-S1 through 9.10.5-S4

Overview
A vulnerability has been reported in ISC BIND which could be exploited by a remote attacker to cause a denial of service (DoS) condition on the targeted system.

Description
TThis vulnerability exists in ISC BIND due to improper handling of malformed packets by the affected software when a SERVFAIL rcode is selected erroneously instead of a FORMERR rcode. A remote attacker could exploit this vulnerability by sending a malformed packet to a targeted system when the SERVFAIL cache feature is enabled leading to an assertion failure in badcache.c

Successful exploitation of this vulnerability could lead to a denial of service condition on the targeted system.

For more details please visit http://cert-in.org.in/

Android Banker Trojan
Virus Type: Banking Trojan
It has been reported that a malicious application targeting various banking and payment apps [including Indian banks] has been circulating. The malicious application is masquerading as Flash Player which is being offered via third party app stores, possibly when the users are being directed from compromised servers or after clicking on ads. The application is instructed to steal banking credentials, intercept SMSs, displaying an overlay screen (to capture details) on top of legitimate apps, steal sensitive data to attacker controlled servers, among others.

Note: Adobe Flash player is in-built in Android Mobile browsers since Android Version 4.1 and official versions are not being offered for download in Google Play.

Once successfully installed via side-loading and being granted administrative privileges on the system, it listens for command from the c2 server and keeps track of the installed applications. If the targeted payment applications [the complete list can be seen from the link in the reference section] found, the app shows a fake notification on behalf of the targeted banking app with the app's icon. If the user clicks on the notification leads to a phishing page of the targeted bank to steal the user's confidential.

Up on receiving specific commands from the C2 server, the app can do activities in the background like intercept SMS's to thwart OTP based authentication, can collect all the contacts and SMS on the device and siphon off to the C2 server, can send specific SMS on the mobile contacts, can send IP/GPS location etc.

CERT-In Vulnerability Note CIVN-2018-0031
Security Bypass vulnerability in Apache Tomcat
Software Affected
Apache Tomcat versions 7.0.0 to 7.0.84
Apache Tomcat versions 8.0.0.RC1 to 8.0.49
Apache Tomcat versions 8.5.0 to 8.5.27
Apache Tomcat versions 9.0.0.M1 to 9.0.4

Overview
A vulnerability has been reported in ISC BIND which could be exploited by a remote attacker to cause a denial of service (DoS) condition on the targeted system.

Description
The vulnerability is due to improper handling of security constraints on a URL containing a character sequence of double quotes surrounded by empty space ("") that maps to the context root of a web application.

Successful exploitation of this vulnerability could allow a remote attacker to bypass security restriction on the targeted system.

Mirai Botnet affecting IoT devices

It has been observed that the variants of a new malware named as "Mirai" targeting Internet of Things(IoT) devices such as printers, video camera, routers, smart TVs are spreading. The malware is capable of scanning the network devices or Internet of Things and try to compromise these systems especially those protected with defaults credentials or hardcoded username passwords.

The malware is capable of performing the following function:

- Compromise IoT systems with default username and passwords
- Create botnets of the compromised devices.
- Use compromise devices to launch DDoS attacks.
- Make network connections to receive commands from launch further attacks.

It is also reported that the malware resides in memory of the infected device and can be wiped out by simply rebooting of the compromised device. However, the malware scans the vulnerable devices constantly leading to the re-infection of the rebooted device within minutes of reboot.

It is also reported that the malware resides in memory of the infected device and can be wiped out by simply rebooting of the compromised device. However, the malware scans the vulnerable devices constantly leading to the re-infection of the rebooted device within minutes of reboot.

"Satori" a new variant of Mirai IoT DDoS malware

It has been reported that "Satori" a new variant of Mirai IoT DDoS malware, is spreading like a worm recently. Satori, the new variant of Mirai is different from all previous variants as it does not use a Telnet port scanner instead it will scan TCP ports 37215 and 52869 on random IP addresses. It is employed with two new exploits which is targeting TCP ports 37215 and 52869. One of the exploit works on TCP port 52869 of IoT devices/routers, exploiting the vulnerability [CVE-2014-8361] in miniigd SOAP service in Realtek SDK.

For more details visit:
http://www.cyberswachhtakendra.gov.in/alerts/mirai.html

Android Banker Trojan

It has been reported that a malicious application targeting various banking and payment apps [including Indian banks] has been circulating. The malicious application is masquerading as Flash Player which is being offered via third party app stores, possibly when the users are being directed from compromised servers or after clicking on ads. The application is instructed to steal banking credentials, intercept SMSs, displaying an overlay screen (to capture details) on top of legitimate apps,steal sensitive data to attacker controlled servers, among others.

Note:
Adobe Flash player is in-built in Android Mobile browsers since Android Version 4.1 and official versions are not being offered for download in Google Play.

Once successfully installed via side-loading and being granted administrative privileges on the system, it listens for command from the c2 server and keeps track of the installed applications. If the targeted payment applications [the complete list can be seen from the link in the reference section] found, the app shows a fake notification on behalf of the targeted banking app with the app's icon. If the user clicks on the notification leads to a phishing page of the targeted bank to steal the user's confidential.

Up on receiving specific commands from the C2 server, the app can do activities in the background like intercept SMS's to thwart OTP based authentication, can collect all the contacts and SMS on the device and siphon off to the C2 server, can send specific SMS on the mobile contacts, can send IP/GPS location etc.

android.permission.READ_CONTACTS	to read the user's contacts data.
android.permission.INTERNET	to open network sockets.
android.permission.WAKE_LOCK	PowerManagerWakeLocks to keep processor from sleeping or screen from dimming.
android.permission.READ_PHONE_STATE	read only access to phone state.
android.permission.RECEIVE_SMS	to receive SMS messages.
android.permission.READ_SMS	to read SMS messages.
android.permission.WRITE_SMS	write to SMS messages stored phone or SIM card. Malicious apps may delete messages
android.permission.ACCESS_NETWORK_STATE	access information about networks.
android.permission.CALL_PHONE	to initiate a phone call without going through the Dialer user interface for the user to confirm the call.
android.permission.SEND_SMS	to send SMS messages.
android.permission.ACCESS_FINE_LOCATION	Allows an app to access precise location.
android.permission.PACKAGE_USAGE_STATS	to collect component usage statistics
android.permission.SYSTEM_ALERT_WINDOW	Allows an app to create windows using the type TYPE_SYSTEM_ALERT, shown on top of all other apps.
android.permission.SEND_RESPOND_VIA_MESSAGE	(Phone) to send a request to other applications to handle the respond-via-message action during incoming calls.

For more details visit:
http://www.cyberswachhtakendra.gov.in/alerts/AndroidBankerTrojan.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

between 10.00 AM to 6.00 PM
or give us a missed call
we will call you back within 24 hrs

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)