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

InfoSec Newsletter

SEP-OCT, 2019

InfoSec CONCEPT 3 page

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 2019

CREDITS

Honorary Professor. N Balakrishnan
(IISc, Bangalore)
Prof. Sukumar Nandi
(IIT, Guwahati)
Prof. V Kamakoti (IIT, Madras)
Prof. M S Gaur (SVNIT, Jaipur)

Design & Technical Team
Ch A S Murty
K Indra Veni
K Indra Keerthi
P S S Bharadwaj

Action Group Members
HoD (HRD), MeitY
Shri.Sitaram Chamarthy (TCS)
Prof. M S Gaur (MNIT, Jaipur)
Prof. Dr.Dhiren R Patel
(NIT Surat)
Representative of Chairman
(CBSE)
CEO, DSCI (NASSCOM)
Representative of Prasar Bharati,
Member of I & B
Shri U Rama Mohan Rao
(SP, Cyber Crimes, CID,
Hyderabad, Andhra Pradesh)
Shri S K Vyas, MeitY

Compiled by
G V Raghunathan
Ch A S Murty

From C-DAC
E Magesh, Director

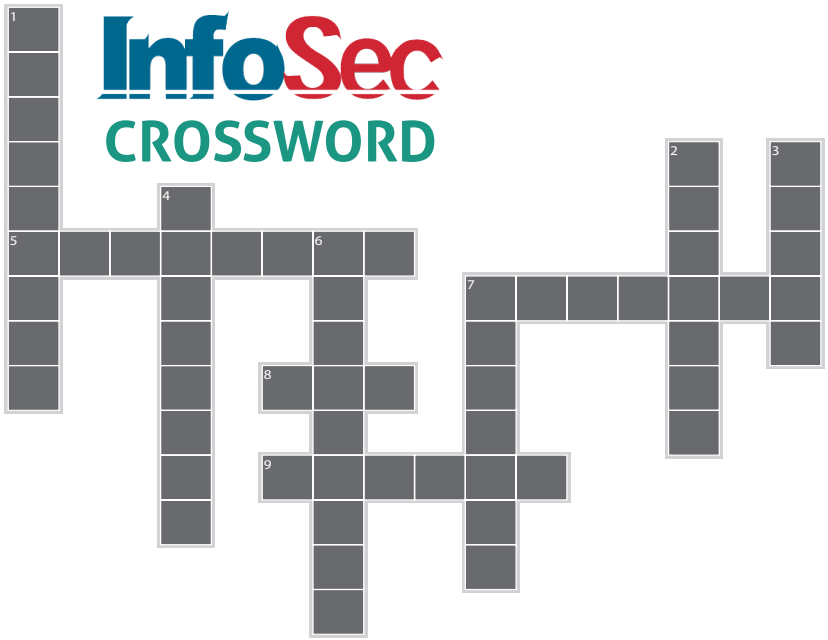
Acknowledgement
HRD Division
Ministry of Electronics &
Information Technology

Supported by
For Virus Alerts,Incident & Vulnerability Reporting
certin
Handling Computer Security Incidents

InfoSec CONTEST

1. Many scammers use _____of sellers to dupe people visiting online classified Web sites.
   a) urgency b) carefulness
   c) both a and b d) None the above
2. Job offer doesn't mention details regarding _____ and the job is offered right away.
   a) contact b) experience
   c) qualifications d) both b & c
3. A genuine job portal/website displays the _____of the website owner who is offering the work from home package.
   a) address b) phone number
   c) name d) all the above
4. Online matrimony sites are the ideal mix of Indian traditional values and latest _____ to explore and find a perfect match.
   a)Traditional b)Scams
   c) Technology d) All the above
5. Matrimonial sites come under _____in IT Act 2000.
   a) Intermediary b) Freedom of expression
   c) Privacy and Surveillance d) None of the above

InfoSec CROSSWORD



Across

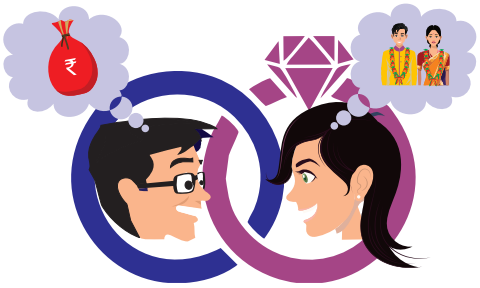
5. Before accepting any online job offer, one must do a complete
7. While you rely on online ways to find your life partner , do a thorough _____check.
8. _____ has a feature wherein an individual or a merchant can send the user a request to collect money.
9. Classified scams work differently depending on who is the_____.

Down

1. Know that there is no need to _____a transaction if money is being transferred to your account, through any payment system
2. Do a Google search for _____ about the website /job portal to find if there is any complaints/ negative reviews about the website/ job portal.
3. Never indulge in _____business with people you met online
4. Most matrimonial websites adds a _____batch of profiles that are checked by their team.
6. If you are the victim of fraud, file a _____with relevant Authorities
7. Be suspicious, when the online job offer asks an individual to make a

ONLINE SCAMS

ONLINE MATRIMONIAL FRAUDS



Over two decades, online matrimonial sites have gained popularity in India where most marriages are still arranged by parents. The whole traditional matchmaking process changed and was set aside when the wave of online matrimony's came into existence. Online matrimony sites are the ideal mix of Indian traditional values and latest technology for Indian bachelors to explore and find a perfect match for a lifetime. This boosted the demand for cyber services, like Matrimony.com Ltd., Jeevansathi.com and Shaadi.com, which operate searchable databases of marriage material. But, matrimonial sites are not completely safe. If you do not take certain precautions, there are chances that you may end up in regret. There has been a rise in the number of people who are cheated through matrimonial sites.

Modus operandi of online matrimonial frauds

- With the minimum KYC procedures to register in online matrimonial websites the fraudster, initially creates a fake profile with attractive descriptions. In most of the cases the person poses to be settled or working abroad, thus making actual meeting difficult.
- Later they look for gullible profiles to fall in their trick. In most cases the targets are widows or divorced while some are elderly women looking for life partners. Also they look for targets who are economically sound.
- Later, phone numbers, email addresses are shared to increase personal communication and gain trust. once the communication is established the fraudsters delete the profiles in the online matrimonial website and only communicate through phones, emails or phone messengers.
- After gaining trust, money is demanded on various pretexts like customs clearance of costly gifts or as conversion charges for foreign currency, government clearance for diamonds, gold or inherited wealth. All this money is asked as online transfer and the person never meets the victim.
- Once they receives the money they never respond to the victim and makes it difficult to trace.

How to save yourself from online matrimony fraud?

Explore the various available online matrimonial websites

Do a good Google search about the available online matrimonial platforms. check for reviews from registered users and find a suitable one. Also, Most matrimonial websites adds a verified batch of profiles that are checked by their team. If you see a verified batch, you can take go forward with the person without thinking much.

Check out how genuine the website is, before you register. Make sure the site has good reviews from registered members.

Do a profile check

While you rely on online ways to find your life partner it is extremely important that you take this responsibility and do a thorough profile check. Check each and every detail carefully. Do a proper check on current and permanent address, their education and work place etc.. At any point you think there is a mismatch, feel free to question the other person.

Once you decide to go ahead, find out whether details given about the individual's qualification, job, family background and such details are indeed true to avoid regrets at a latter stage.

Verify details mentioned in the profile you are interested, and do a profile check in social media platforms for further information about the person. If you do not find details on any social media, it is a red flag

Meet personally before you take a step forward

If after chatting online and over the phone for a while, if you feel comfortable enough to meet them, go for it. Even if you have your trust in them, set up a meeting at a restaurant or coffee shop along with your family member or close friends.

Slow and steady wins the race

Marriage is a lifetime decision and you cannot take a chance here. life is not a race, ensure you take things slow. If you feel the other person is forcing you to take things forward quickly, be stern to take a back step.

Do not share any personal or revealing photographs or videos

Never indulge in money business

No genuine person would ask you to lend money at a early stage of a relationship. It is better to get into any financial transactions unless you are double sure.

If the person demands money or property citing various reasons , report to the site

Be alert to the Red flags that can help you identify Online Matrimonial Fraudsters :

- Are not willing to show their face, reluctant to come on video chat, profile photo may not theirs, reluctant to meet in persons
- Ask for money transfer, citing some emergency, initially a small sum and later a large amount
- May not have social profile or have few friends on social media
- Hesitate to share family/ workplace details
- Express "love" too quickly even before fully understanding each other
- The profile looks too good to be true for that person to express interest to you
- They call from multiple numbers. They usually don't give a number to call back. Even if they give a number, they don't pick up when you call. Later, they call you back from a new number
- Sound inconsistent or confusing when you ask for personal details
- Are in a mad rush for early marriage, without a valid reason
- Request for deletion of your profile immediately after getting in touch with you
- Ask for email user name/ password or credit card/ bank account details
- Come up with false stories to gain sympathy

Finding a life partner is not easy. It might take time to meet the one you are waiting for. But, do not let yourself in any kind of pit just because things are not going right. The key to finding love and happiness online is to 'Stay alert'.

ONLINE JOB SCAMS

Scammers have become extremely tricky and smart these days, making it difficult to determine whether a job offer is fake or a legitimate one. The main motive behind these scams is to extract hard-earned money from the candidates and disappear. Naive young people, who are on the lookout for jobs, are increasingly falling prey to online job scams, who promise with quick money and lucrative employment. At the peak of frustration and agony when one does not have a job, he may fall into such traps. They are taking advantage of the psychological weakness of the individuals and target people belonging to the following groups:

- People with minimal educational qualifications
- People with degree from not so popular colleges
- Housewives with household responsibilities, who are unable to step out to work
- Physically challenged and elderly people who are unable to go out to work

People, belonging to these categories, are gullible and fall prey to false promises made by the scammers, because they are seeing the dream, of a good job and making money. Also, it can be seen that many of these scammers advertise on well-known sites and thus people fail to realise that they are being cheated. These scamsters 'offer' jobs to people, claiming to be from major MNCs while offering attractive packages and ask them to send in some cash or share bank account details to complete formalities.

Example: Let's see what happened with Veena, a native of Jaipur who lost about 7500 INR to an online job fraud.

Veena registered with *****.com, a very popular job search portal was frustrated and was in rigorous search for job. One fine day she receives a call from a number claiming to be from *****.com and telling her that her profile had been shortlisted for a job. She was made to take an online test after a payment of Rs. 1500 via Paytm. When she did not clear the test, she asked for a refund. And as professionally as it happened, they asked her for the card details of the card she had used on Paytm to give them that money.

since she was badly in need for money she provided all her credentials. Another 6000 INR is withdrawn, this time leaving her with no money. They ignored her thereafter leaving her no options.

How this scam works?

- The scammer contacts you by email, letter or phone and offers you a job that requires very little effort for high returns, or a guaranteed way to make money quickly. You may even come across false job opportunities on classified ad websites.
- To accept the job you will be asked to pay an upfront. If you pay the fee you may not get the job that you were promised.
- Or they may give you a task to complete to get the job. On completion of your work, the scammer will refuse to pay you for some or all of your work, using excuses such as the work not being up to the required standard.
- Another type of job opportunity scam asks you to use your bank account to receive and pass on payments for a foreign company. The scammers promise you a percentage commission for each payment you pass on. This is likely to be a form of money laundering which is a criminal offence. If you provide your account details the scammer may use them to steal your money or commit other fraudulent activities.

How to determine if a job offer is scam ?

There are some indications and signs to ensure the possibility of an online job offer being a scam. Some of them are:

- **Asking to make an initial payment:**
  The first obvious reason to get suspicious is, when the online job offer asks an individual to make a payment. even if they ask for a small amount, think that the amount may be small for one individual, but when taken from a large group, the scammers can make a huge amount.
- **Deceptive names:**
  The scammers try and include a word in the name which may indicate that they are, part of the Government or some prestigious MNC. No matter what the name is, one needs to get it checked thoroughly.
- **Job offer comes suddenly:**
  No details regarding educational qualifications or experience are asked and the job is offered right away.
- **The pay offered is too good to be true:**
  Good jobs are hard to find

Before accepting any online job offer, one must do a complete research. Don't let the company to hurry up any process. Before giving any personal information like bank A/c number, credit card number, Pan card number etc. one must clear the doubt and the genuineness of the company.

Steps to follow before you submit your complaint to cyber cell

There are number of things you need to note before you submit your complaints. Here are some of the points you need to follow:

- 1 Before you submit your complaint to cyber cell police, you must confirm that the website you have paid to is a fake website/ fake job portal.
- 2 Most of the job portals/ website who demand money for registration for work from home job are fake. So if you paid, there are great chances that portal/ website is fake.
- 3 A genuine job portal/website displays the name of the website owner who is offering the work from home package. If you can't find the contact details of the website owner/ job portal, then the chances are more that its fake. Once you get the contact details, try to find the details are fake or not
- 4 If the website provide the work of online surveys, copy paste, form filling etc. and offer huge money as return then mostly it's a fake website/job portal.
- 5 Do a Google search for reviews about the website /job portal to find if there is any complaints/ negative reviews about the website/ job portal.

THROUGH ONLINE CLASSIFIED MARKET PLACE

Online classifieds like Quikr, OLX and others, a online portal which facilitates a convenient marketplace for buying and selling all kinds of items. If you are advertising your items for sale through online classifieds portal, beware of scammers posing as genuine buyers. Scammers may make up stories such as needing your help to pay an agent or upfront costs like transportation or insurance. They may promise you reimbursement for these costs. Scammers will pose as genuine sellers and post fake ads on classifieds websites and may also approach you through email or on social media portals. The ad may even include pictures and other details – often copied from a genuine seller's ad. In order to lure a number of victims in a hurry, the scammer advertises the item at a low price, often much lower than comparable items advertised on the same site.

How Do Classified Scams Work?

Scammers usually start out by setting up fake accounts on classified websites. They might also set up fake social media accounts, and – quite rarely – a fake website. Sometimes, the scammer might even contact the victim on the platform if they notice them posting an ad that they are looking for a certain item or service.

The scammer will usually refuse to engage in direct contact with the victim other than just emailing/ messaging them. They will claim to be unavailable to meet face-to-face or chat over the phone. In terms of payment methods, the scammer will try to convince the victim to use alternative options, such as Prepaid cards, UPI payments/Net banking, Cryptocurrencies.

The scammer might also try to get the victim to share their personal and financial data with them – usually under the guise of getting them to prove they are a legit buyer/seller. Besides that, in severe situations, the scammer might ask the victim to meet up face-to-face, but instead of a populated area, it will be a more secluded place. They might also ask the victim to come alone.

If the victim goes ahead with the payment, they will likely lose the money as well as the product(s) they were selling. In case they also share their personal/financial info with the scammer, they will be exposed to identity theft. Basically, the scammer will either use their info in future scams, or sell it off on the deep web.

Classified scams work differently depending on who is being targeted.

Distance Buyer's Scam, How the scam works?

The primary motive of the scammer is to dupe the victim of as much cash as he can. So he claims to be living in a distant location that has very high rates for shipping packages. Let's see strategy played by the scammers .The buyer (the scammer) contacts the seller (the victim) and shows an interest in the item for sale and ask for personal contact number. Once he receives the personal number, He states that he is living abroad, and informs the seller to ship the item to his location if the deal goes through. The (buyer) scammer then reassures the seller that the shipping charges would be taken care of. Scammer also informs that he will send over a representative from a private courier service to collect the item and the shipping charges.

This 'representative' is also in on the scam who arrives at the seller's location to collect the item and the shipping charges. The representative hands over the fake courier details to the seller and even sends a fake email that contains the same details. The scammer will ensure to be in contact with the seller to gain trust and assures him that he will receive the money for the item as well as the shipping charges. But the seller won't receive the money for the product nor the shipping charges.

There are a few variations of this scam, but the overall strategy played by the scammers remains the same. In some cases, the seller may even receive a fake email from a bank. This email request to provide the courier details to approve and release money which have been received from the buyer. This further convinces the seller that this is a legitimate deal.

CASE 1:

Selling:

Samsung S4: Case study of the 'Distance Buyer's Scam'

Punith (name changed) recently experienced this type of scam but fortunately, he recognized the scam and thus saved himself from being duped. The exact sequence of events that he went through was as follows:

- Punith put an add to sell his Samsung S4 on sale in one of the online classified portal. He then received an enquiry for the device from a person residing in the United States – Maria Andriano.
- Maria showed her interest to buy the product and informed the seller that she wanted the phone for her son living in South Africa and asked Punith to ship the phone there directly. While the cost of the phone was listed around the Rs. 6,000, the shipping charges to South Africa were almost double that amount. Maria ensured to pay this amount.
- Maria contacted Punith once more after a couple of days to let him know that she had sent the amount due for the phone and the courier charges to Punith via ***** Bank.
- Punith then received an email from *****Bank within 24 hours, saying that the said amount has been transferred and would be released to Punith once he provides them with the shipping details and courier number.
- Fortunately Punith, was able to identify the scam and save his money.

Be careful and cautions towards such online classified frauds

Think and use common sense, that no bank or courier company would ever send a message or email stating they are holding the money for you and will transfer it once they receive the courier details of the shipped product from you.

Scammers trick Sellers by misuse of the "request money" feature in UPI

Many scammers use urgency and carefulness of sellers to dupe people visiting online classified Web sites where numerous individuals buy and sell goods to get the best price. UPI has a feature wherein an individual or a merchant can send the user a request to collect money. The user needs to authorize the transaction using a security PIN. This PIN is like an ATM PIN and not a uniquely generated one-time password OTP. This is the first and most common variation of misuse of the "request money" feature in UPI at present. The scam starts here. The caller will try to send the money via UPI to book the product. Instead of sending money to you, the caller will request money from you on UPI. The caller might even get an OTP generated for approving the payment from your account instead of his, Let see a similar case studies.

CASE 1:

Listed her ad in online classifieds portal , her Alertness , saved her from getting duped

- Meera (name changed) was shifting her house. She had put an advertisement on one of the online classified portal to sell her furniture.
- An interested buyer called and asked if he could transfer half the money to her account right away, to which she agreed. Instead of sending her money, the buyer sent a request to collect Rs 10,000 from her. He immediately called and asked her to approve it.
- she was alert and realised the trick. He was trying to defraud by making her transfer Rs 10,000 to him.

CASE 1:

Listed an ad in online classified portal for sale of window AC and ended up losing ₹50,000

- Abhinav, decided to replace his window air conditioner (AC) with a split AC, to sell off he listed his window AC on an online classifieds portal for sale. Immediately Abhinav got a call from a prospective buyer.
- Abhinav tried to ascertain the identity of the person through Truecaller. "
- The buyer (scammer) told Abhinav that he was going to transfer him the money right away and his son would come later and collect the AC.
- The buyer (scammer) told Abhinav to enter his UPI (Unified Payment Interface) ID in the UPI app on his phone. immediately, he got a message from his bank, informing him that his bank account was debited.
- He called the buyer (scammer) to figure out what happened and was told that something went wrong and should try doing it again. He tried again, and then again. After the third attempt, he realized he was getting duped.
- What he was entering was not his UPI ID but his UPI PIN, authorizing payment to the scammer. But by then, Abhinav had lost ₹50,000, over the three transactions.
- The Scammer calling you does not use the term 'OTP' instead says that it is a code that you need to share to complete the transaction (though the message does mention OTP)

VIRUS ALERTS

CERT-In Advisory CIAD-2019-0030
Use after free Vulnerability in Apple products (Sock Puppet)

Software Affected
Apple macOS Mojave 10.14.6
Apple iOS 12.4.1

Overview
This vulnerability has been reported Apple products which could allow a remote attacker to execute arbitrary code on the targeted system.

Description
This use after free vulnerability exists in the XNU kernel of iOS and macOS due to improper memory management.
Successful exploitation of this vulnerability could allow a remote attacker to execute arbitrary code with system privileges on the affected systems and allowing the jailbreak of the devices.

Solution
Apply appropriate security updates as mentioned in the Apple Security Advisory

For more details visit:
https://cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2019-0031

CERT-In Advisory CIAD-2019-0031
Multiple Vulnerabilities in Apple iOS

Software Affected
Apple iOS versions 13,13.1 &iPadOS 13.1 and prior

Overview
Multiple vulnerabilities have been reported in Apple iOS which could allow an attacker to execute arbitrary code, cause denial of service conditions (DoS), obtain potentially sensitive information, bypass security controls, spoof a URL and cause cross site scripting on the targeted system.

Description
These vulnerabilities are caused due to logic issue in the display of notification, memory corruption in the core audio component, an error in face ID component, out-of-bound read, improper state management and improper permission validation while executing commands.

A remote attacker could exploit these vulnerabilities by persuading a user to open a specially crafted web content or malicious application. Successful exploitation of these vulnerabilities could allow an attacker to execute arbitrary code, cause denial of service conditions (DoS), obtain potentially sensitive information, bypass security controls, spoof a URL and cause cross site scripting on the targeted system.

For more details visit:
https://cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2019-0031

CERT-In Vulnerability Note CIVN-2019-0170
Vulnerability in Linux

Software Affected
Linux kernel through 5.3.6

Overview
Vulnerability has been reported in Linux which could allow an attacker to access sensitive information on a targeted system.

Description
This vulnerability exists due to Realtek Wi-Fi chips model in Linux devices. An attacker could exploit this vulnerability by rtlwifi driver that mainly supports the Realtek Wi-Fi chips model used in Linux devices.

Successful exploitation of this vulnerability could allow an attacker to compromise a system using nearby Wi-Fi devices.

For more details visit:
https://cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES01&VLCODE=CIVN-2019-0170

CERT-In Vulnerability Note CIVN-2019-0168
Multiple vulnerabilities in SQL Server Management Studio

Software Affected
SQL Server Management Studio 18.3
SQL Server Management Studio 18.3.1

Overview
Multiple vulnerabilities have been reported in SQL Server Management Studio which could allow remote attacker to improperly enforce permissions on the targeted system.

Description
These vulnerabilities exist in SQL Server Management Studio due to improper enforcement permissions. An attacker could exploit the vulnerability if the attackers credentials allow access to an affected SQL server database.
Successful exploitation of these vulnerabilities could allow an attacker to gain sensitive information.

For more details visit:
https://cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES01&VLCODE=CIVN-2019-0168

WORKSHOPS


@Ahmedabad


@Ahmedabad


@Ahmedabad


@Tamilnadu


@Lucknow


@Delhi


@Bhopal


@Bhopal

@Bhopal

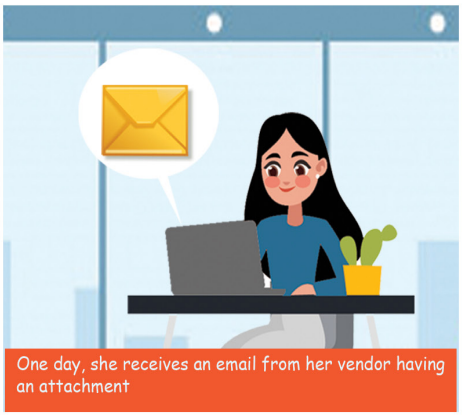
Release of a Book on "FakeThings" by Dr. Jaydeep Mishra, Joint Secretary, MeitY, Prof. R K Shyamsunder, IIT Bombay, Prof. Sukumar Nandi, IIT Guwahati, Smt. Ramavedasri, DSCI, Prof. Manoj Gour, IIT Jammu, Shri SK Vyas, OSD to Secretary, MeitY during a meeting at MEITY,Delhi


@Bhilai

Request for workshop
https://isea-pmu.in/requestFor-Workshop/

Short Story on Ransomware

Alisha is an entrepreneur. Her company has 50 employees & 60 systems



One day, she receives an email from her vendor having an attachment

Alisha downloads the attachment. Her antivirus was not updated, so no alerts

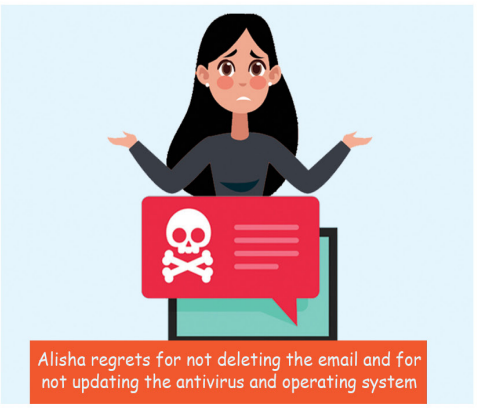
Upon opening the file, her system gets locked and all files are encrypted. unable to access

An alert message on screen demands Rs.One lakh to be paid in bitcoin to unlock the screen

Alisha makes payment to the bitcoin wallet address mentioned

The hacker didnt send the private key. the files remain encrypted and inaccessible

Her company's manager tell alisha that the received mail was a phishing email with ransomware



Alisha regrets for not deleting the email and for not updating the antivirus and operating system

For queries on Information Security
Call us to Toll Free No.

1800 425 6235

For details on
Cyber Crime Cells in India and Cyber Crime Reporting Portal
visit https://www.infosecawareness.in

Threats to your system

A computer system threat refers to anything that has the potential to cause serious harm to a computer system. It can be loss or corruption of data or physical damage to the hardware

Guidelines to protect your system

To protect against viruses, Trojans, worms, etc. use anti-virus software

Scan all email attachments and files before downloading them to your system

Maintain strong unique passwords for all of your accounts

Do not click on Web links sent by someone you do not know

Beware of suspicious emails and phone calls requesting confidential information

For more details / queries on Cyber Security visit or call us to our Toll free number

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

www.InfoSecawareness.in

1800 425 6235

For Virus Alerts,Incident & Vulnerability Reporting
certin Handling Computer Security Incidents
http://cert-in.org.in/

www.cyberswachhtakendra.gov.in

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)