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

सी डैक
CDAC

Newsletter
NOV-DEC 2015

HOW STRONG IS YOUR PASSWORD ?

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

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
Nalanda Building, No. 1 Shivabagh Satyam Theatre Road, Ameerpet, Hyderabad - 500016, Telangana (India)
Plot No. 6 & 7, Hardware Park, Sy No. 1/1, Srisailam Highway, Pahadi Shareef Via Keshavagiri (Post), Hyderabad - 500005, Telangana(India)
E-mail : isea@cdac.in

InfoSec

Newsletter

Nov- Dec 2015

Credits

For Virus Alerts,Incident & Vulnerability Reporting

certin
Handling Computer Security Incidents

InfoSec Quiz

1. It is one of the malware
   (a)gossips (b)threat (c)vulnerability (d)ransomware

2. We can click on the links received from known or unknown emails ID's
   (a)True (b)False

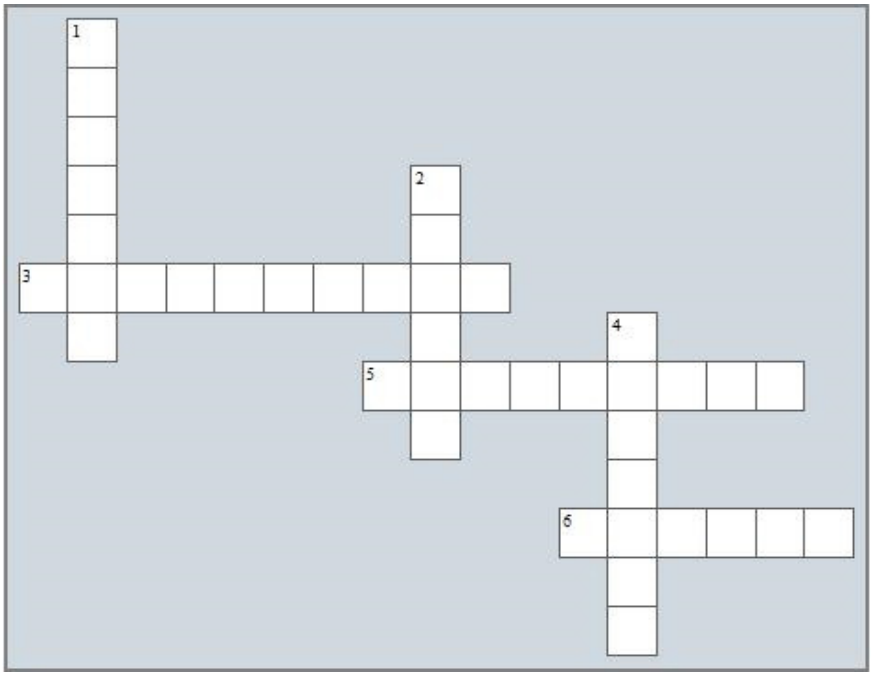
3. We can copy the content available over internet and we cannot be sued for copyright violations
   (a)True (b)False

4. A Hacked computer can be used to
   (a)Infect other systems (b)Harm your system by malware
   (c)Help your system with latest updates (d)Both a and b

5. My email is private and no one can look into it
   (a)True (b)False

logon to
www.infosecawareness.in/contest
to participate in Infosec Contest and **WIN PRIZES**

InfoSec Crossword



Across
3. Uses an algorithm that transforms information and making it unreadable & inaccessible to anyone except for those who have the appropriate credentials
5. Restrict network activity to known applications, and prevent malicious people and programs from exploiting holes in operating systems and other software applications
6. Ensures that the information you need is there when you need it and it can recovered if the information is damaged in the system.

Down
1. It is one of the methods of social engineering
2. The information stored on client computer by a webserver is called a
4. _____ is harmful software, usually installed without your knowledge

InfoSec Guess Tip

Guess the Tip which best suits the cartoon by logging in to
http://www.infosecawareness.in

InfoSec Tip

All Wi-Fi equipment support some form of encryption,so enable them.

Wi-Fi Security

Internet users are widely using Wi-Fi devices to access Internet. Every year millions of Wi-Fi devices are sold in the market. Out of these most of the wireless devices are vulnerable in their default configuration mode. Since end users are not fully aware of security levels to be set on these devices, these get rendered vulnerable. By taking advantage of these unsecured Wi-Fi devices terrorists and hackers fulfill their needs.

Tips for securing Wireless Communications

- **Always use strong password for encryption**
  A strong password should have atleast 15 characters with uppercase letters, lowercase letters, numbers and symbols. Also it is recommended to change the encryption key frequently so that it makes difficult for the cracker to break the encryption key. Do not use WEP for encryption, rather use WPA/WPA2.
  Restrict access to the Access Point based on MAC address
  In order to allow authorized users to connect to the Access Point, wireless clients should be provided access based on MAC address.
- **Change the default username and Password of the Access Point**
  Most of the users do not change the default passwords while configuring the Access Point. But it is recommended to keep a strong password, as this default password information can be known from product manufacturers.
- **Do not broadcast your network name**
  SSID information is used to identify a Access Point in the network and also the wireless clients connect to the network using this information. Hence, in order to allow authorized users to connect to the network, the information should not be provided in public.
- **Disable DHCP service**
  When the number of users accessing the Access Point is less, it is recommended to disable the DHCP service. As this may make the attackers easy to connect to the network once they get associated with the Access Point.
- **Shutdown the Access Point when not in use**
  Hackers try to brute force the password to break the keys, so it is good practice to turnoff the Access points during extended periods of Non-use. For more details visit

ABOUT PASSWORDS

Password is a key or a Secret word or a string of characters which is used to protect your assets or information from others in the cyber world. It is used for authentication, to prove our identity or to gain access to our own resources. It should be kept secret to prevent access by unauthorized users.

In social networking sites like Facebook, Orkut, and LinkedIn each of which is studded with answers to commonly used security questions such as favourite place, school, college, etc..

Importance of Passwords

- Password represents the identity of an individual for a system.
- A password helps individuals in protecting personal information from being viewed by unauthorized users. Hence it is important to secure passwords.
- Password acts like a barrier between the users and his personal information

Possible Vulnerabilities with Passwords are

- Passwords shared with other persons, might be misused.
- Passwords can be forgotten
- Stolen password can be used by an unauthorized user who may collect your personal information
- Easy Passwords such as name, date of birth, mobile numbers could be guessed by anybody and misuse them
- If you use same password for all accounts, It would be easy for the hackers to crack all account passwords

"You are responsible for safeguarding your ID and password."

"Never write your passwords on paper or anywhere else for referring"

Various Techniques used by hackers/crackers to retrieve your passwords

Shoulder Surfing

One way of stealing the password is standing behind an individual and look over their shoulder to read their password while they are typing it. Shoulder Surfing is a direct observation technique, such as looking over someone's shoulder to get passwords, PINs, other sensitive personal information and even overhearing your conversation when you give your credit-card number over the phone.

Shoulder surfing is easily done in crowded places. It's comparatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM, or use a calling card at a public pay phone. It can also be done long distance with the help of binoculars or other vision-enhancing devices.

Your confidential information will be at risk if your passwords are observed by Shoulder Surfers. They can use your password information for logging into your account and they may do harm to your information.

Beware of shoulder surfing Make sure you donot use remember password option in browser

Writing your passwords on papers or storing it on hard disk

Strangers search for papers or the disk for passwords where they have been written.

"Children donot write the passwords on any paper or on any disk drive to store it. Memorizing is the best way to store them"

Brutal force attacks

Another way of stealing the password is through guesses. Hackers try all the possible combinations with the help of personal information of an individual. They will try with the person's name, pet name (nickname), numbers (date of birth, phone numbers), school name... etc.. When there are large numbers of combinations of passwords the hackers use fast processors and some software tools to crack the password. This method of cracking password is known as **"Brute force attack".**

"Do not use a password that represents your personal information like nicknames, phone numbers, date of birth, etc.."

Dictionary attacks

Hackers also try with all possible dictionary words to crack your password with the help of some software tools. This is called a "Dictionary attack".

"Children donot use dictionary words (like animal, plants, birds or meanings) while creating the passwords for login accounts"

"Children should not give their passwords to their friends or to anyone through online chatting, e-mails or even through phone conversations"

Sharing your passwords with strangers

Sharing the passwords with unknown persons (strangers) may also lead to loss of your personal information. They can use your login information and can get access to your information. The operating system does not know who is logging into the system, it will just allow any person who enters the credential information into the login page. Strangers, after getting access to your information, can do anything with it. They can copy, modify or delete it.

blank passwords

Weak and blank passwords are one of the easiest ways for attackers to crack your system.

Strong and easiest to remember Password

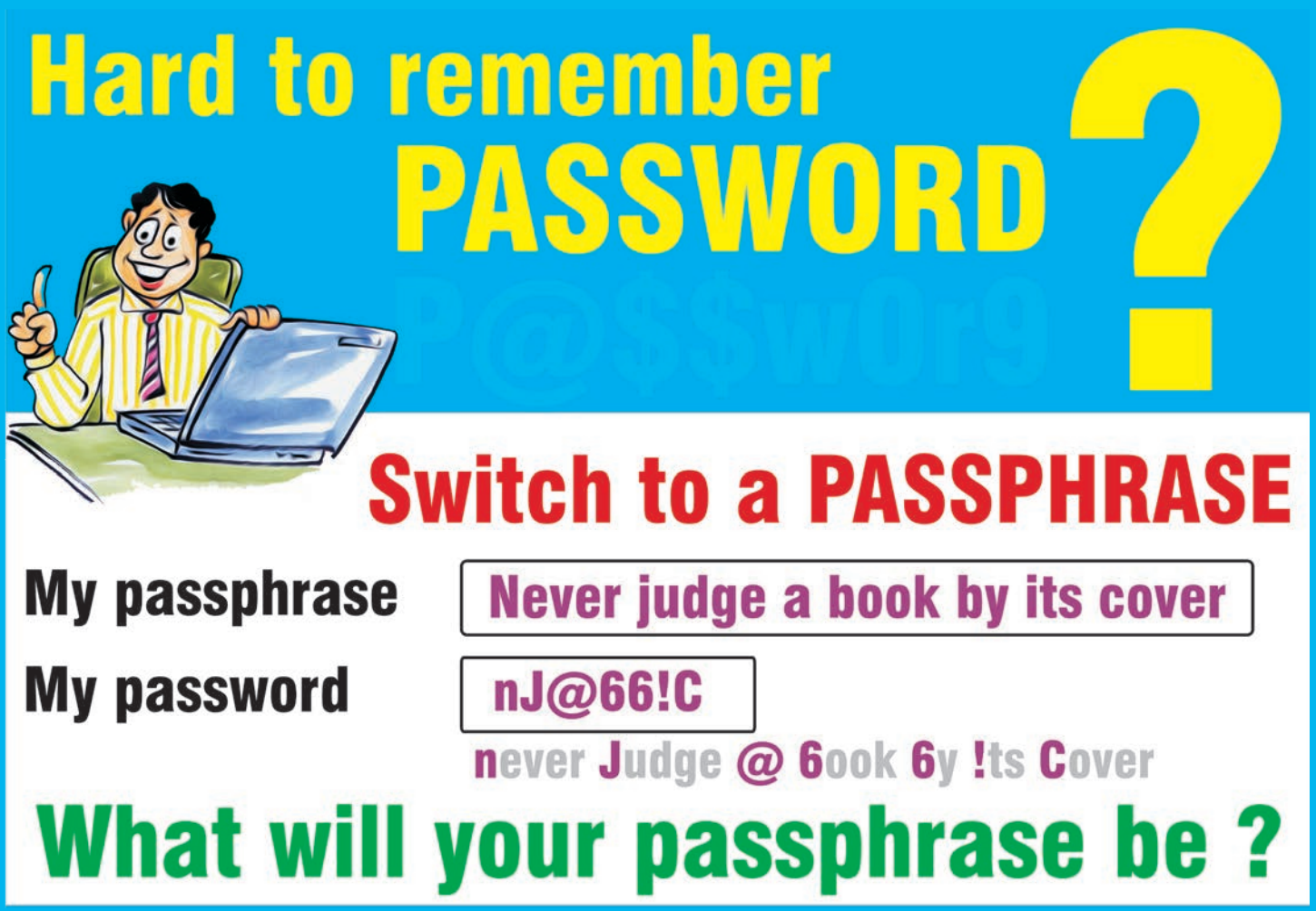
A strong Password should have combinations of Alphabets, Numbers and Characters such as c.!@*^&)(~@. Remembering these passwords are very difficult.

Things to be remembered while creating Strong Passwords

- Use at least 8 characters or more to create a password. The more number of characters we use, the more secure is our password.
- Use various combinations of characters while creating a password. For example, create a password consisting of a combination of lowercase, uppercase, numbers and special characters etc..
- Avoid using the words from dictionary. They can be cracked easily.
- Create a password such that it can be remembered. This avoids the need to write passwords somewhere, which is not advisable.
- A password must be difficult to guess.
- Change the password frequently at least 2 weeks once

Guidelines for maintaining a good password

- Change the password once in two weeks or when you suspect someone knows the password.
- Do not use a password that was used earlier.
- Be careful while entering a password when someone is sitting beside you.
- Store the passwords on computer with the help of an encryption utility.
- Do not use the name of things located around you as passwords for your account.



Passpet

Convenient Password Management and Phishing Protection

Passpet makes logging in to websites easier: just click a button to fill in your username and password. You only need to memorize one secret, and Passpet will generate a different password for each site. Even if there is a break-in at one site, your other accounts and passwords are safe. Passpet protects you from attackers who try to fool you into revealing passwords because each password is generated only for the site where you originally established it.

Passpet was presented in a paper published at SOUPS 2006 (the Symposium on Usable Privacy and Security).

Here are a few ways Passpet improves on previous password helper tools:

- You click a button instead of typing in your password.
- Impostors can't get you to give away your passwords, because you never type them in.
- The button you click is personalized, which makes it hard for impostors to fool you with a fake login.
- You can change your password for an individual site whenever you want.
- Your passwords are never saved in a file anywhere.
- You can use your passwords to log in from more than one computer.
- Someone who steals one of your passwords would have to do a lot of work to guess your other passwords, and you can make it take as much work as you want.
- You can inhibit attacks by choosing a trickier password, or just by waiting longer.

The Passpet source code is released as open source under the Apache 2.0 License.

Source code: passpet-2007-04-08.zip
Source repository: http://zesty.ca/passpet/darcs
Firefox 1.5 extension: passpet.xpi

How to Use Passpet

Passpet appears on your Firefox toolbar as an animal icon. Everyone gets a randomly chosen animal with a randomly chosen name, so the Passpet button is hard for an impostor to imitate. When you first start Firefox, your Passpet is asleep. To awaken it, click on it and enter your master secret.

Home - Vulnerability Notes

CERT-In Vulnerability Note CIVN-2015-0265

Cisco ASA Software DHCPv6 Relay Denial of Service Vulnerability

Original Issue Date:October 27, 2015

Severity Rating: HIGH

Solution

Apply appropriate updates as mentioned in CISCO advisory
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151021-asa-dhcp1

Vendor Information

CISCO
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151021-asa-dhcp1

References

CISCO
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151021-asa-dhcp1

Security Tracker
http://www.securitytracker.com/id/1033912

CVE Name
CVE-2015-6324

Disclaimer
The information provided herein is on "as is" basis, without warranty of any kind.

Software Affected

- Cisco ASA software version 9.2(1)

Overview

A vulnerability has been reported in Cisco Adaptive Security Appliance (ASA) which could allow an unauthenticated remote attacker to cause an affected device to reload.

Description

This vulnerability occurs due to insufficient validation of DHCPv6 packets. A remote attacker could exploit this vulnerability by sending specially crafted DHCPv6 packets to an interface on the targeted device that is configured with the DHCPv6 relay feature.

Successful exploitation of this vulnerability could allow a remote attacker to cause an affected device to reload.

http://cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES01&VLCODE=CIVN-2015-0265

Home - Vulnerability Notes

CERT-In Vulnerability Note CIVN-2015-0264

Cisco ASA Software DNS Denial of Service Vulnerability

Original Issue Date:October 27, 2015

Severity Rating: HIGH

Solution

Apply appropriate updates as mentioned in CISCO advisory
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151021-asa-dns1

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151021-asa-dns2

Vendor Information

CISCO
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151021-asa-dns1
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151021-asa-dns2

References

CISCO
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151021-asa-dns1
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151021-asa-dns2

Security Tracker
http://www.securitytracker.com/id/1033913

CVE Name
CVE-2015-6325
CVE-2015-6326

Disclaimer
The information provided herein is on "as is" basis, without warranty of any kind.

Software Affected

- Cisco ASA software version 9.2(1)

Overview

A vulnerability has been reported in Cisco Adaptive Security Appliance (ASA) which could allow an unauthenticated remote attacker to cause an affected device to reload.

Description

This vulnerability occurs due to improper processing of DNS packets. A remote attacker could exploit this vulnerability by sending a specially crafted request to the affected Cisco ASA device to generate a DNS request packet and the attacker needs to spoof the reply packet with a crafted response.

Successful exploitation of this vulnerability could allow a remote attacker to cause an affected device to reload.

http://cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES01&VLCODE=CIVN-2015-0264

InfoSec WORKSHOPS

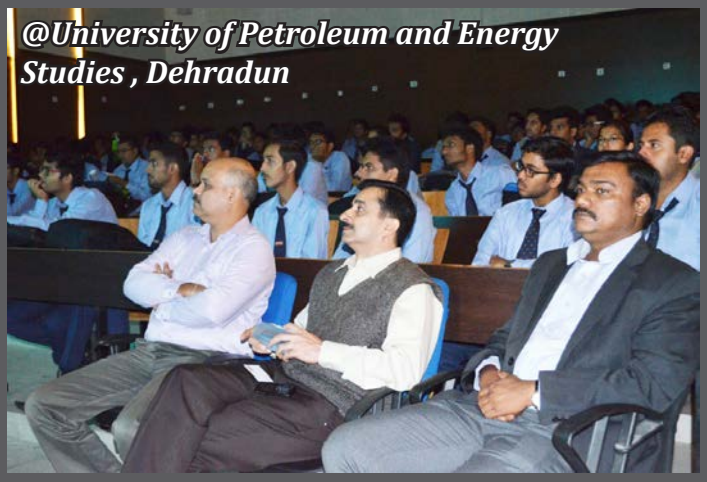

@Srikrishna Vidya Mandir, Visakapatnam


@Ministry of Civil Aviation, Delhi


@Amrutha college of Engineering, Bangalore


@College of Airwarfare, Hyderabad


@Airforce, Begumpet


@University of Petroleum and Energy Studies , Dehradun


@University of Petroleum and Energy Studies , Dehradun


@DOOM University, Dehradhun

To conduct workshop on "Information Security Awareness" at your place

Click Request for a Workshop at http://isea-pmu.in/

CARD CHEATS

Desi crooks top in fraud cases

Homegrown cheats beat Nigerians at fake card game

K. K. ABDUL RAHOOF | DC
HYDERABAD, NOV. 16

Homegrown debit cards scammers have overtaken Nigerian cons.

The crooks have safe havens in Jamtara and Dumka districts of Jharkhand, where even the police can't reach. When Hyderabad cyber crime police analysed more than 150 cases of debit card frauds, they found that maximum calls had been made by frauds from these two districts and other parts of Jharkhand.

They usually call up citizen in the city pretending to be bank managers or UDAI officials and extract debit card details including One Time Passwords (OTP) before looting victims' money by making online purchases and recharges. City cyber cops, who have been able to catch only one of the accused so far, say the Jharkhand police do not cooperate.

"There was spurt of complaints, in which the victims said that they got calls from people claiming to be bank managers. The callers asked them to upgrade their debit cards or else the cards would be blocked. The victims were then asked to provide the name, card number, and CVV, and OTP in order to upgrade the card. Believing them, the users provided the details only to find out a few minutes later that they had been looted," said Hyderabad Cyber Crime inspector Mr V.P. Tiwari.

"As part of the investigation, when we verified the callers' phone numbers, and online purchases and recharges, we found that most calls had originated from Jharkhand," said Mr Tiwari, adding that attempts were made to arrest the suspects, but they were not successful. In June this year, a team of cyber cops went to apprehend the gang, but they managed to arrest only one person, who was working for the main gang. All the other address that they traced were fake. "We could have done better if we had got adequate support from the Jharkhand police. But they do not cooperate," said another cyber crime official.

The Jharkhand gang is suspected to have bought SIM cards in bulk using fake IDs and are running secret call centers accessing, bank account holders' profiles from disgruntled bank employees.

"We are not blaming the victims, but despite various attempts to educate people, many do not understand that they should never disclose their debit card details to anyone. Bank officials will never call asking for debit card details," said a senior Cyber Crime official.

FAKE BANK OFFICIALS

- **SCAMMERS USUALLY** call up citizen in the city pretending to be bank managers or UDAI officials and extract debit card details including One Time Passwords (OTP) before looting victims
- **DESPITE VARIOUS** attempts to educate people, many do not understand that they should never disclose their debit card details to anyone. Bank officials will never call asking for debit card details, said an official

http://epaper.deccanchronicle.com/articledetailpage.aspx?id=4118651

Fraudsters use 'duplicate' email to dupe ONGC, Saudi company

MOHAMED THAVER
MUMBAI, OCTOBER 13

IN ONE of the biggest cyber crimes in Mumbai, the Oil and Natural Gas Corporation Limited (ONGC) lost Rs 197 crore after cyber criminals duplicated the public sector firm's official e-mail address with minor changes and used it to convince a Saudi Arabia-based client to transfer payments to their account.

The fraud was committed on the premise that the company making the payment would not notice a minor change in the e-mail address of the ONGC representative, with whom they had been communicating. While ONGC communicated with the company from patel_dv@ongc.co.in, the fraudsters duped the company by communicating with them from patel_dv@ognc.co.in.

According to the BKC cyber police team probing the case, ONGC had an order to deliver 36,000 metric tonnes of Naphtha — flammable liquid hydrocarbon mixtures — to Saudi Aramco, an oil company based in Dhahran. On September 7, ONGC dispatched the order, worth Rs 100.15 crore, from Hazira port in Surat. According to the police, the company usually transferred payments to ONGC's State Bank of India (SBI) account, but did not do so this time.

"ONGC was to send a second batch of naphtha to Aramco on September 22. However, since they had not received the earlier payment, they enquired with the Saudi-based company," an officer said. On being told that the delay was on account of public holidays and bank holidays, ONGC dispatched the second batch of Naptha worth Rs 97 crore on September 22. Again, ONGC e-mailed a scanned copy of the tax invoice with its SBI account number to the company.

Again, no payments were received in the ONGC account. What finally set alarm bells ringing was an e-mail ONGC received on October 7 from Aramco stating that the money had been transferred to a new account. When the PSU contacted Aramco, they were told the company had merely followed up on ONGC's request to deposit the money into an account in Bangkok Bank Public Company Limited. "ONGC had never made such a request," the officer said.

As soon as an official complaint was registered on October 10, Additional Commissioner of Police K M M Prasanna instructed the cyber crime police station to probe the matter on priority. During investigations, police found that someone aware of the e-mail communication between ONGC and Aramco regarding the transfer of a large sum of money had created an e-mail ID similar to an official ONGC email ID.

"The communication from ONGC was done using the e-mail ID patel_dv@ongc.co.in. The fraudsters merely created an e-mail address patel_dv@ognc.co.in," said senior police inspector S Mahadik. Using this ID, the fraudsters began to communicate with Aramco, and as the second email ID appeared almost identical to the original, Aramco officials did not notice the difference. The fraudsters then sent an e-mail asking for the payment to be deposited to a Bangkok-based account. Officers of the BKC cyber police station said an FIR has been registered under Sections 419 (cheating by impersonation), 420 (cheating), 465 (forgery), 468 (forgery for purpose of cheating), 471 (using a forged document) of the Indian Penal Code and Sections 66 C (punishment for identity theft) and D (cheating by impersonation using computer resource) of the Information Technology Act. ONGC was unavailable for comment.

E-MAIL ID TWEAKED

CYBER CRIMINALS duplicated the public sector firm's official e-mail address with minor changes and used it to convince a Saudi Arabia-based client to transfer payments to their account

WHILE ONGC used the ID patel_dv@ongc.co.in to communicate with its client, fraudsters used patel_dv@ognc.co.in

The Indian EXPRESS epaper editions Wed, 14 October 2015
epaper.indianexpress.com/c/7056027

httpepaper.indianexpress.com613449Indian-Express-Mumbai14-October-2015#page19

Post against Virbhadra: Youth's arrest sparks row

TRIBUNE NEWS SERVICE

MANDI, NOVEMBER 8

Various political parties have condemned the arrest of local journalist for allegedly making objectionable comments against Chief Minister Virbhadra Singh on a Facebook post.

The Aam Aadmi Party, the CPM and the BJP also demanded the cancellation of the FIR registered against him.

On the complaint of district Congress leader Puran Chand, the Sadar police on Thursday registered a case against Rajneesh Sharma and detained him for questioning. In the complaint, the Congress leader had alleged that Sharma had posted a comment on his Facebook account with an intention to defame Virbhadra Singh.

Praveen Sharma, media coordinator, BJP, said intolerance was at its peak in the state. A Chief Parliamentary Secretary was making offensive statements against the Prime Minister, but no case was registered against him. Sharma said state Youth Congress president and Chief Minister's son Vikramaditya Singh had led an attack on the BJP office in Shimla and a BJP worker had lost an eye in the incident, but no arrest had been made in the case.

CPM district president Bhupender Singh said criticism on the social media was a common practice. Instead of arresting the journalist, the authorities should have released him after issuing a warning.

In a letter to the Chief Minister, the district AAP unit had stated that it was sad to see that a scribe of Mandi had been framed and then arrested for posting allegedly objectionable comments on the social networking site.

District AAP spokesperson Lawan Thakur said the act of the Congress had sent a wrong message among the users of Facebook and other social networking sites.

"India has constitutionally guaranteed the Right to Freedom of Expression and Speech to its citizens and this act is being seen as violation of the rights," he said.

"The act of framing the scribe and arresting is being seen an act to silence the dissenting voice for posting some adverse remarks on the social networking sites," he said.

AAP condemned the act of the senior Congressman of Mandi on whose behest the press reporter was framed.

AAP would always stand for the freedom of speech and always raise its voice against the forces who wanted to silence the voices of dissent, he said.

Intolerance at its peak: BJP

- A Chief Parliamentary Secretary was making offensive statements against the Prime Minister, but no case was registered against him
- State Youth Congress president and Chief Minister's son Vikramaditya Singh had led an attack on the BJP office in Shimla and a BJP worker had lost an eye in the incident, but no arrest had been made in the case

The Tribune (Himachal Edition) Mon, 09 November 2015
epaper.tribuneindia.com/c/7243318

http://epaper.tribuneindia.com/635403/Himachal-Edition/HE_09_November_2015#page/2/1

CRIMES ON THE WEB

More FIRs make cyber cell cops the busiest officers

Two inspectors are investigation officers in 100 cases each

MOHAMED THAVER
MUMBAI, NOVEMBER 24

POLICE INSPECTOR Kalpana Gadekar's desk at the Bandra-Kurla Complex (BKC) cyber police station is covered with paperwork. The pages — all in official ink — will form part of several chargesheets. Among the cases are an identity crime in which a man created a fake profile on Facebook in the name of a woman to defame her, a bank fraud in which Romanian nationals attached skimmers to ATMs, and the big catch of people who duped people on the pretext of giving them jobs by getting their data from online portals.

While Gadekar, who investigated the Jiah Khan abetment to suicide case before it was transferred to the CBI, has had assistance from juniors to compile the chargesheets, there are fears if she would remember the intricate technical details of the case that defence lawyers tend to stick on to. The fears are valid.

She is currently the investigating officer (IO) in 100 cases (30 cases from last year) at the cyber police station.

Three cubicles to her left, inspector Ravi Sardesai, an old hand at handling cyber crimes, also bears the same cross — both are IOs of nearly 100 cases each, a number shocking even by the skewed yardstick by which the nearly 55,000-strong overburdened Mumbai Police operates.

Inspector-level officers have complained of excess work when they are IOs of over 15 cases at a time. Gadekar and Sardesai are probably the busiest officers in the Mumbai Police.

As per Section 78 of the Information Technology (IT) Act, only an officer of the rank of police inspector (PI) — earlier an assistant commissioner of police — or above can probe a case where sections of the IT Act have been invoked to prevent misuse of the Act. The BKC cyber police station currently has three PI-level officers and above — Gadekar, Sardesai and senior PI Sudhir Mahadik.

This still was not a hindrance till earlier this year when the cyber police station would only accept applications in most cases and register FIRs in a few cases citing limited manpower. In 2013, there were 40 FIRs through the year and last year it was around 60, which worked out to a maximum of 15-20 cases for each of the three IOs.

This year, however, said an IPS officer, in order to portray the actual workload encountered by the cyber police so as to get approval for hiring more men, coupled with the criticism of them not registering FIRs, they decided to register FIRs in all complaints.

As a result, the tally of FIRs went up rapidly.

Additional Commissioner of Police (Crime) K M M Prasanna said the BKC cyber police station had registered 208 FIRs till November 15 this year, nearly five times the 2013 figure and more than three times the FIRs registered in 2014. "For the current year, the three officers have nearly 70 cases each, besides 30 each from last year...," he said.

Sources said the bulk of the cases had Gadekar and Sardesai as IOs due to additional responsibilities on their senior Mahadik.

In order to tackle this problem, the Mumbai Police sent a recommendation earlier this year asking for amendment to Section 78 of the IT Act and allow officers of police sub-inspector (PSI) rank and above to probe cases. The cyber police station has three PSIs, eight APIs, which coupled with the three PIs, will take the count of officers to 14 instead of three if the proposal is accepted.

While the other officers at the police station do help the three PIs with major chunks of the investigation, when these 100 cases go for trial the IO concerned will have to depose in each case. "If every alternate day these officers will have to go to court for deposing, when will they be able to investigate these cases. Also, having so many cases will impact the quality of the probe," said a senior officer.

The only hope for these officers is that the amendment to IT Act comes through or more PI-level officers are given to the cyber police station. "Since the IT Act is a central Act, the amendments will have to happen at the Central government level, which could be a long and winding process," said the officer.

Tushar Mahajan, Under Secretary, Home, however, has communicated to the Mumbai Police recently that a committee had been set up to look into the amendments into the IT Act.

The Indian EXPRESS epaper editions Wed, 25 November 2015
epaper.indianexpress.com/c/7404152

httpepaper.indianexpress.com648579Indian-Express-Mumbai25-November-2015#page4

Biz man conned of ₹88 lakh

Victim falls prey to cyber crime, deposits money into fake account

DC CORRESPONDENT
BENGALURU, NOV. 17

A businessman fell victim to a cyber crime and lost a whopping ₹ 88 lakh recently. He had deposited the amount into a bank account number given by the cyber criminals, who had hacked the email account of a Chinese company from which the businessmen had intended to buy machinery.

The victim, Mr Hayath Khan of Jindal Aluminium Ltd in Dobbspet near Nelamangala, has filed a complaint with the cyber crime police. The police said that Mr Khan was in touch with the Chinese company to buy some machines for his industry.

"He had made several transactions with the company over the last five years and had purchased machines from them. In September, he had placed an order for some machines, and the deal was struck through emails. The company had asked him to pay 10 per cent of the total amount for the machines to be exported," the police said.

"In one of the mails, it was mentioned that the bank account number had been changed and that he had to deposit ₹88 lakh as advance into the new account number given. The complainant made the payments in a few installments from September 11 to 30. Some of them were made through RTGS, while others were done through IDBI Bank on K.G. Road. But even after making the payment, he did not receive the machines. Finally, he contacted the company over phone and was shocked to hear that the company had not changed its bank account number and that they had not received any money from him," the police said.

The complainant later checked with the bank and learnt that the money had been credited into a bank account in England. "Preliminary probe established that the email account of the Chinese company has been hacked. The company officials too have been informed about their email being hacked. We have written to the IDBI bank seeking information on the bank account into which the money was credited. We have sought the name of the bank and where it is located in England," the police said.

"As the matter involves other countries, we have decided to take the help of Interpol," the police said.

> Preliminary probe established that the email account of the Chinese company has been hacked. The company officials too have been informed about their email being hacked. We have written to the IDBI bank seeking information on the bank account into which the money was credited. We have sought the name of the bank and where it is located in England
>
> — The police

http://epaper.deccanchronicle.com/articledetailpage.aspx?id=4126773

For any queries on Information Security

Call us on Toll Free No.

1800 425 6235

between 10 A M to 6 P M

or give us a missed call, we will call back within 24 hrs

To share tips / Latest news mail us to

pmu-isea@cdac.in

Follow us on Facebook

https://www.facebook.com/infosecawareness

Follow us on Youtube

https://www.youtube.com/channel/UCWPBKQryyVvydUy4rYsbBfA

Follow us on twitter

https://twitter.com/CDAC_ISEA

For more details visit

www.infosecawareness.in

Centre for Development of Advanced Computing (C-DAC), a Scientific Society of Department of Electronics and Information Technology, Ministry of Communications & Information Technology, Government of India, is primarily an R&D institution involved in design, development and deployment of Advanced Electronics and Information Technology Solutions, including the celebrated PARAM series of Supercomputers. The C-DAC, Hyderabad is working in R&D with a focus on system level programming, web technologies and embedded programming in the application domains of Network Security, e-learning, Ubiquitous Computing, India Development Gateway (www.indg.in), Supply Chain Management and Wireless Sensor Networks.

Department of Electronics & Information Technology,
Ministry of Comunications & Information Technology,
Government of India

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

Nalanda Building, No. 1 Shivabagh Satyam Theatre Road, Ameerpet, Hyderabad - 500016, Telangana (India)

Plot No. 6 & 7, Hardware Park, Sy No. 1/1, Srisailam Highway, Pahadi Shareef Via Keshavagiri (Post), Hyderabad - 500005, Telangana(India)