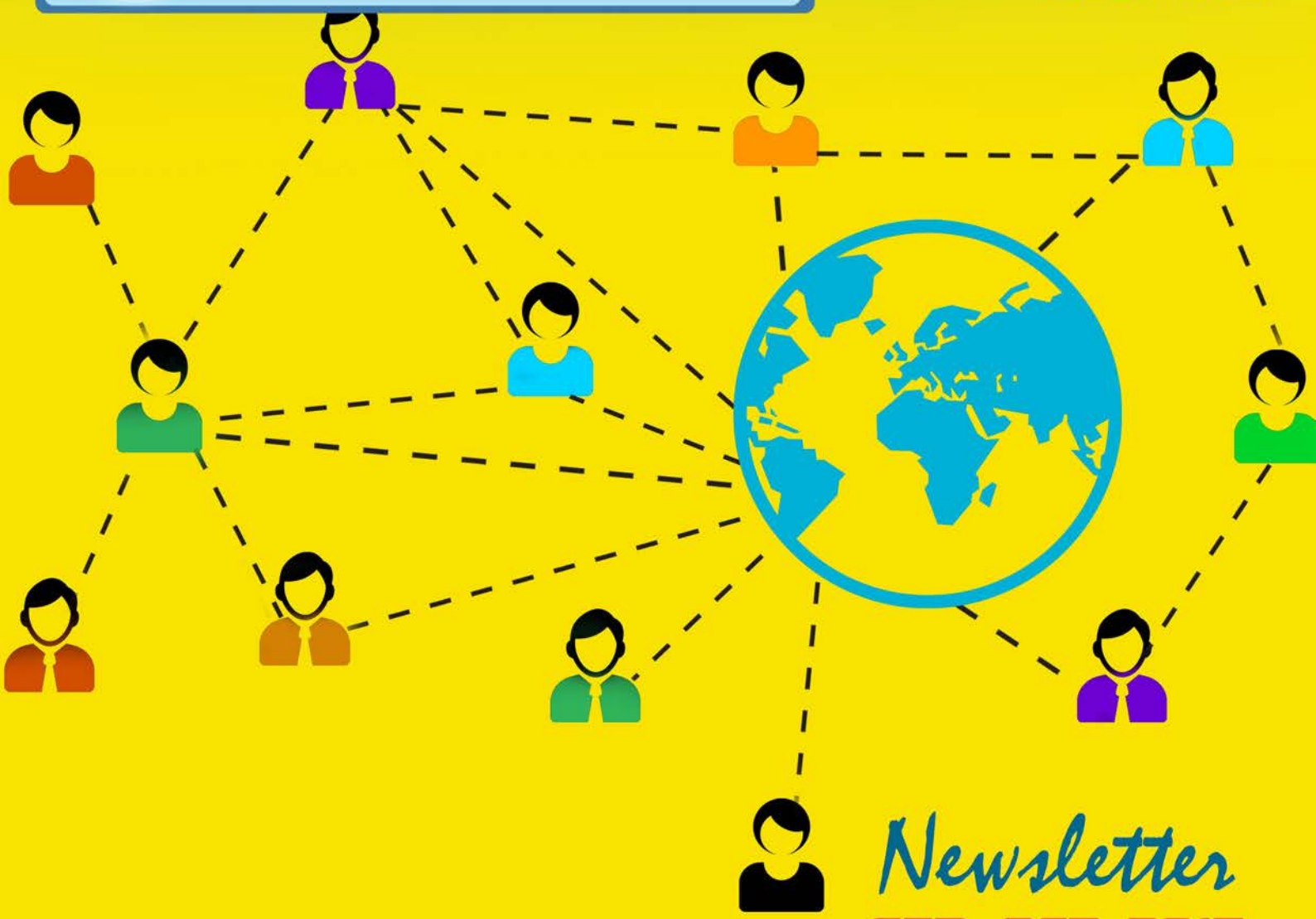
Information Security Education & Awareness
Department of Electronics and Information Technology
Ministry of Communications and Information Technology
Government of India



# Newsletter

SEP-OCT 2015

InfoSec CONCEPT Page 4 - 8

InfoSec Page
TOOLS 9
ALERTS 10
NEWS 11

# RISKS IN SOCIAL NETWORKING SITES

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

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 SEP - OCT 2015

## CREDITS



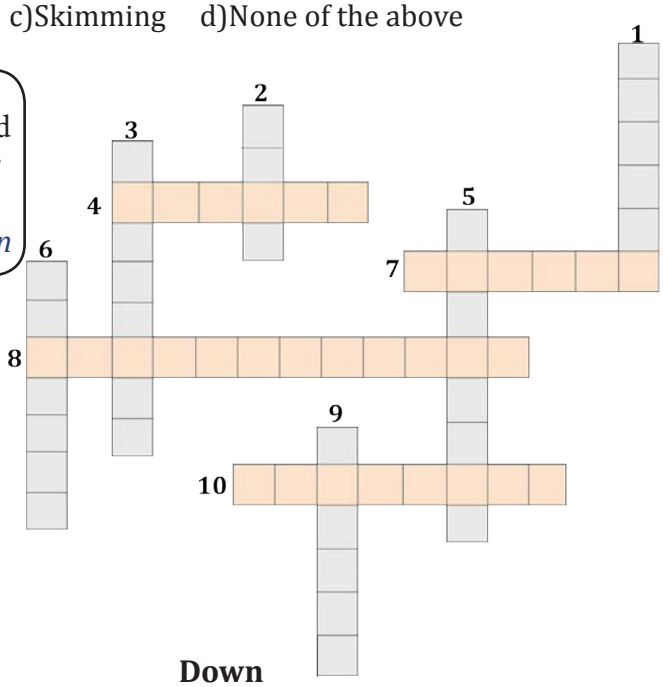
For Virus Alerts, Incident & Vulnerability Reporting
certin
Handling Computer Security Incidents

Comments and feedback mail us at
***pmu-isea@cdac.in***

## InfoSec QUIZ

1. Which of the following is used for secure exchange of email is
   a) HTTPS b) HTTP c) SSL d) www
2. Social engineering is a con-artist or some one makes you to reveal personal information
   a)true b)False
3. Skimming is terminology given to
   a) Theft of Internet banking information
   b) Theft of Credit/Debit card information
   c) It is one type of Social Engineering
   d) Both b & c
4. ___is an attack which targets the specific high profile executives in the businesses or targeting upper management in the corporate.
   a)Whaling b)Phishing c)Baiting d)Vishing
5. It is one of the methods of social engineering
   a)baiting b)Virus c)Skimming d)None of the above

For previous answers of quiz and crossword and *to participate in Infosec Contest and win prizes* *www.infosecawareness.in*




## InfoSec CROSSWORD

**Across**

4. ____ is a course of action, guiding principle, or procedure considered expedient prudent or advantageous
7. A computer overtaken by a hacker and used to perform malicious tasks
8. This is a malicious technique of tricking Web users into revealing confidential information or taking control of their computer While clicking on seemingly Innocuous web pages.
10. A security tool that protects an individual computer or even an entire network from unauthorized attempts to access your system.

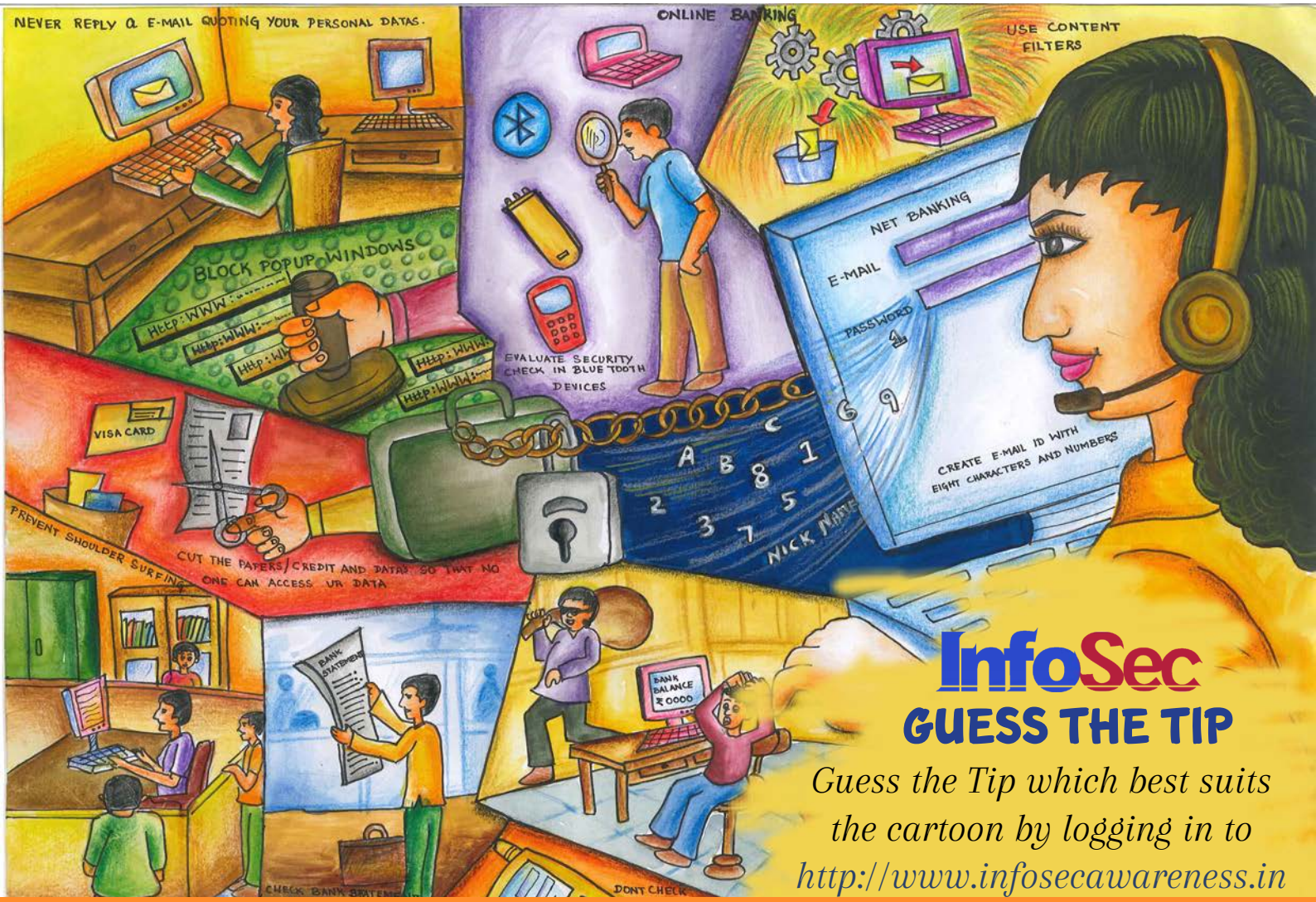
**Down**

1. A form of spyware that enters your computer from an Internet download.
2. A new term for spam messages being sent to lnstant message addresses.
3. Forging an e-mail or instant message address to make It appear as If It came from someone or somewhere other than the true source.
5. The transfer of data from one computer (or server) to another computer.
6. A person who enjoys exploring the details of computers and how to stretch their capabilities.
4. A violation or Infraction, as or a law, a legal obligation,or a promise.

InfoSec TIP

# Be aware of Loan Frauds


- Some of the culprits advertise in the news papers stating that they offer loans to the individuals on low rate of interest and furnishes a cell number, which is taken on furnishing wrong address documents.
- The culprit sends some fake certificates to the individuals stating that he has been sanctioned a loan and asks them to deposit certain amount in bank account. The individual deposits the amount in fake accounts for the purpose of registration, tax's, advocate fee, etc.,
- So be aware of such fake certificates
- Don't believe advertisements of finance companies stating that they will sanction loans with low interest rate.




## InfoSec GUESS THE TIP

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

**For more details visit :**

**www.InfoSec awareness.in**

**For any queries on Information Security**

**Call us on Tool Free No.**

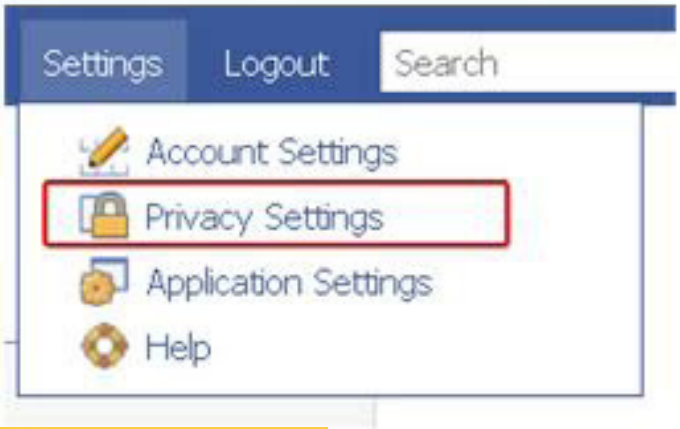
**1800 425 6235**

**between 10 A M to 6 P M**
**or give us a missed call, we will call back within 24 hrs**

Social networking is the grouping of individuals into specific groups, like small communities who share interests and/or activities, or who are interested in exploring the interests and activities of others. Although social networking is possible in person, especially in the workplace, schools, colleges and universities, it is most popular online. This is because unlike most high schools, colleges, or workplaces, the Internet is filled with millions of individuals who are looking to meet other people, to share first-hand information and experiences about interests like cooking, golfing, gardening, developing friendships professional alliances, finding employment, business-to-business marketing and even groups sharing information about baking cookies. The topics and interests are as varied and rich as the story of our universe

The other side of Social Network is security and privacy issues and is entirely treated as two different issues. As security issue, the third person gains unauthorized access to the information of protected resources and the privacy issues is someone can gain access to confidential information by simply watching you what you type your password. But both types of breaches are often intertwined on social networks, especially since anyone who breaches network and opens the door to easy access to private information belonging to any user. The reason behind Social network security and privacy lapses exist because of the amounts of information the sites process each and every day that end up making it much easier to exploit a single flaw in the system. Features that invite user participation - messages, invitations, photos, open platform applications, etc., are often the avenues used to gain access to private information.

*Take advantage of the privacy settings available in social networking sites*




**A social network is a social structure made of nodes (which are generally individuals or organizations) that are tied by one or more specific types of interdependency, such as values, visions, ideas, financial exchange, friendship, dislike, conflict or trade.**

# RISKS
# SOCIAL

## Social Networking Risks and Challenges

Social networking has become most popular activity in today's Internet world, with billions of people across the world are using this media to meet old friends, making new friends, to collect and share information, social networking while being a popular media has several disadvantages associated with it. These sites can be trapped by scammers or hackers leading to loss of confidentiality and identity theft, of the users. Social Networking sites are becoming very popular especially among the growing kids. These sites expose the kids to various risks like online bullying, disclosure of personal information, cyber-stalking, access to inappropriate content, online grooming, child abuse, etc. In addition there are many more risks like fake profiles with false information, malicious application, spam, and fake links which leads to phishing attacks etc.,

## Illegal content:

In General, anybody who access social networking or media sites may not deliberately seek out inappropriate content and may inadvertently access content while undertaking online access or searches or they may seek it out or be referred content by others.


The content may include sexually explicit messages, images, sexual abuse, violence, criminal activity or accidents, video clips, extreme political views, potentially used in the radicalization of vulnerable members of the community, based on race, religion, sexual preference or other social/ cultural factors. They may also exposes to online advertising which promotes adult content.

The illegal content on the sites like, images of child abuse and unlawful hate speech, pornography or sexual content, violence, or other content with adult themes which may be inappropriate for young people may be displayed. They might also discover content through their smart phones that may be blocked by home and school internet filters.

# IN

# L NETWORKING SITES

**Social networks are fun to use, helpful for job hunting, and great for keeping in touch with friends, business contacts and relatives**

## Spam

As we all know that spam is usually unwanted e-mail advertising about a product sent to list of e-mails or group of e-mail addresses. Similarly spammers are sending the unwanted mails or messages to the billions of users of social networking sites which are free to gather the personal information of the unsuspecting users.


**Social spam** is unwanted spam content appearing on social networks and any website with user-generated content (comments, chat, etc.). It can be manifested in many ways, including bulk messages, insults, hate speech, malicious links, fraudulent reviews, fake friends, and personally identifiable information. Bulk messages in social networking sites are a set of comments repeated multiple times with the same or very similar text. These messages, also called as spam-bombs, can come in the form of one spammer sending out duplicate messages to a group of people in a short period of time, or many active spam accounts simultaneously posting duplicate messages.

### Abusive, vulgar, or irreverent language:

User-submitted comments that contain swear words or slurs are classified as profanity or abusive or vulgar or irrelevant language. Common techniques include "cloaking" works by using symbols and numbers in place of letters. These bad words are still recognizable by the human eye, though are often missed by website monitors due to the misspelling.

### Insults:

User -submitted insults are comments that contain mildly or strongly insulting language against a specific person or persons. These comments range from mild name calling to severe bullying. Online bullies often use insults in their interactions, referred to as cyber bullying. Hiding behind a screen name allows users to say mean, insulting comments with anonymity; these bullies rarely take responsibility for their comments and actions.

### Threats:

User-submitted threats of violence are comments that contain mild or strong threats of physical violence against a person or group. It may also quickly turn into a stream of racism and provoke to insulting comments, and threats against others. This is a more serious example of social spam.

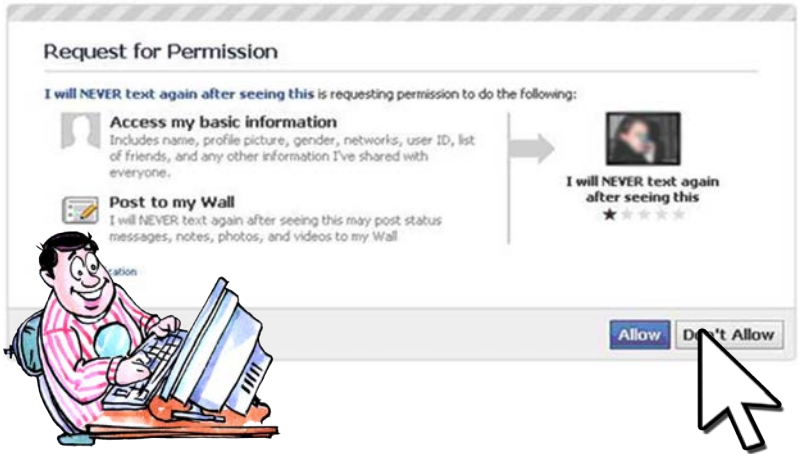
### Hate speech:

User-submitted hate speech is a comment that contains strongly offensive content directed against people of a specific race, gender, sexual orientation, etc.

### Malicious links:

User-submitted comments can include malicious links that will inappropriately harm, mislead, or otherwise damage a user or computer. These links are most commonly found on video entertainment sites, such as Youtube. What happens when you click on malicious links can range from downloading malware to your device, to directing you to sites designed to steal your personal information, to drawing unaware users into participating in concealed advertising campaigns.

Malware can be very dangerous to the user, and can manifest in several forms: virus, worm, spyware, Trojan Horse, or adware. Malicious application might come through different application while using or installing software's. Similarly, the clicking on the social networking application starts the application installation process or link to view the video, etc. In order to fulfill its intended operation the application requests for some elevated privileges from the user like access to my basic information, update on my wall, post on my wall, etc




# Malicious applications may come in many ways... never allow them

**Fraudulent Reviews:**
Reviews of a product or service or movie or story from users that never actually used/viewed it. These are often solicited by the proprietor of the product or service, who contracts out positive reviews, "reviews-for-hire". Some companies are attempting to tackle this problem by warning users that not all reviews are genuine

**Fake Friends:**
Fake friends occur when several fake accounts connect or become "friends". These users or spam boats often try to gain credibility by following verified accounts, such as those of popular celebrities and public figures. If that account owner follows the spammer back, it legitimizes the spam account, enabling it to do more damage.

**Personally identifiable information:**
User-submitted comments that inappropriately display full names, physical addresses, email addresses, phone numbers, or credit card numbers are considered leaks of personally identifiable information.

---

**Phishing:**
Phishing attack is creation of fake site just similar to original site. Similarly these days even social network phishing has come in different flavors just like phishing attacks on banks and popular trading websites. Social networking phishing has come up with fake mails and messages like offering some specialized themes, updating the profile, updating the security application/features etc. In order to see the updates the user needs to follow a link and log in, through which the credentials are taken by the attacker. The linked page is a fake copy of the original login page, focused on stealing user account credentials

**Click jacking:**
Generally, click jacking is a malicious technique of tricking Web users like phishing into revealing confidential information or taking control of their computer while clicking on seemingly innocuous Web pages. Vulnerability across a variety of browsers and platforms, a click jacking takes the form of embedded code or script that can run without the user's knowledge. The same is followed in the social networking domain. The objective behind such an attack is that users can be tricked into clicking in the links, icons, buttons etc, which could trigger running of processes at the background without the knowledge of the user

**Conduct:**
This relates to how people behave online, this may include bullying or victimization (behaviors such as spreading rumors, excluding peers from one's social group, and withdrawing friendship or acceptance) and potentially risky behaviors (which may include for example, divulging personal information, posting sexually provocative photographs, lying about real age or arranging to meet face-to-face with people whome the previously met online) Networking sites are third party application program interface (API) which allows for easy theft of private information and it gives developers access to more information like addresses, pictures than needed to test the applications.


## Guidelines for Social networking:

- ***Don't give or post any personal information like your name, address of the school / home, phone numbers, age, sex, credit card details***
  - *The information which was posted by you online can be seen by everyone who is online because internet is the world's biggest information exchange tool. Many people who are having access to the site which you are using can access your profile and get all the information what you have posted. The persons who is having access to your profile may include good persons like your friends, parents, teachers and also bad persons like strangers/hackers.*
- ***Be aware that the information you give in the sites could also put you at risk of victimization***
  - *Never give out your password to anyone other than to your parent or guardian*
  - *Change your password frequently, and avoid clicking links that purport to send you back to the social network site. Instead, type the site's address directly into your browser (or follow a bookmark you've previously saved) to get back to your account*
  - *When you are choosing a Social Networking site, privacy issues should be considered*
  - *While accepting the friends on Social Networking sites, be selective. Only add people as friends to your site if you know them in real life*
  - *Never meet in person with anyone whom you met on Social Networking site because some of the people may not be who they say they are online.*
  - *Take your parents' permission if you want to meet the person whom you met in the networking site*
  - *Most of the Social Networking web sites enable users to set privacy controls for who has the ability to view the information. So try to use such facilities*
  - *Do not post anything which may harm your family credibility*
  - *Never post photographs, videos and any other sensitive information to unknown persons in Social network sites*
  - *If you think that your social networking account details have been compromised or stolen, report your suspicions to the networking site support team immediately.*
  - *Never respond to harassing or rude comments which are posted on your profile.*
  - *Delete any unwanted messages or friends who continuously leave inappropriate comments and immediately report those comments to the networking site support team.*
  - *Do not post your friends information in networking sites, which may possibly put them at risk. Protect your friends by not posting the group photos, school names, locations, ages, sex...etc*
  - *Avoid posting the plans and activities which you are going to do in networking sites*
  - *Check the privacy settings of the Social Networking sites and set the settings in such a way that the people can only be added as your friend if you approve them also set the settings in such a way that the people can only view your profile if you have approved them as a friend.*

**2.206 BILLION** active users in social media

**1.925 BILLION** users utilise their mobiles for Social Media platforms

**1 MILLION** active mobile social users are added per day

**365 MILLION** active mobile social users have been added in one year

**1/2 MILLION** new users added in facebook, and 6 new profiles every second

*http://www.socialmediatoday.com/social-networks/kadie-regan/2015-08-10/10-amazing-social-media-growth-stats-2015*

**51%** of children of 8-17 years have an online profile

**63%** of 8 to 17-year-olds with a profile use Bebo

**59%** of 8 to 17-year-olds use social networks to make new friends

**36%** of parents say they set no rules for their children's use of social networks

**43%** of children say their parents set no rules for use of social networks

# MailWasher

## Free Spam Blocker


MailWasher is the ultimate free spam blocker. Not only is MailWasher very simple to use, it quickly sorts your spam email from your good email so you get only the email you want.

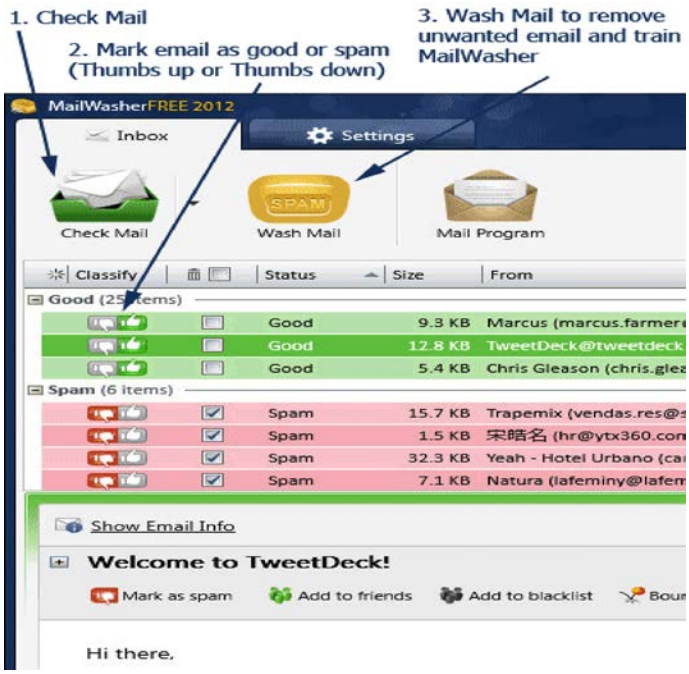
One of the benefits of MailWasher is it lets you view all your email on the server before it gets to your computer. This ensures you don't get spam, viruses and other harmful emails on to your computer, instead they are deleted off the server so you can download only the good remaining email.

### Some of the notable features of MailWasher are listed below:

- Delete unwanted e-mails before you download to your computer. You'll be able to see who the email is from, the subject, and the attachment. This will enable you to decide if you want to delete the email or keep it. A great way to stop viruses, large attachments or to just delete unnecessary emails from getting to your computer.

- **Preview.** Easily preview the message in your email to see what the sender has to say before downloading it to your computer. This ensures you won't download any nasty emails to your computer. Additionally, spam is marked in a red color, and your good email is marked as a green color for quick analysis.

- **Anti spam tools.** Comprehensive anti spam tools ranging from your personal friends list and blacklist, customizable filters, external blacklists, bayesian spam filtering which quickly learns to distinguish your spam and good email and email virus filtering.
  - **Friends List.** Add your friends email addresses to MailWasher and they will always be recognised. You can even hide your friends from the screen so the spam is easy to recognise.
  - Bounce back unwanted e-mails so it looks as if your email address is not valid. This will make the sender think your address is no longer active so your name can be removed from their list. This unique feature is great for privacy and it couldn't be simpler!
  - **Filtering.** Effective filtering to automatically spot spam, plus it uses a customisable list of blacklisted e-mail senders and/or regular expressions to filter out potential spammer addresses and messages.
  - **Bayesian spam filtering.** This clever type of spam filtering learns which of your email is spam and which is not very quickly and accurately.
- **Recycle bin.** If you accidentally delete an email, you can restore it back to your email account.



MailWasher is so simple to use, just leave it running and 'wash' your mail when you want to.

MailWasher comes in two versions, a free version and a pro version. The two programs are identical except the pro version has some extra goodies:

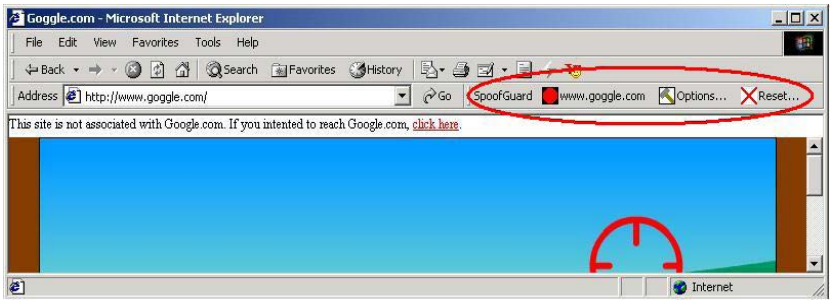
- The free version limits you to using 1 email account, where as the pro version lets you use unlimited email accounts.
- The pro version lets you auto delete spam, the free version does not let you.
- The pro version uses a real time spam blocking service called FirstAlert! which helps block known spam and trains MailWasher's spam filters.
- The pro version includes 7 day a week email support, and 5 day a week phone support
- All future updates are free with the pro version
- The pro vesion does not have the advertising banner.

***http://www.mailwasher.net/free-spam-blocker***


SpoofGuard is a tool to help prevent a form of malicious attack called "web spoofing" or "phishing." Phishing attacks usually involve deceptive e-mail that appears to come from a popular commercial site. The email explains that the recipient has an account problem, or some other reason to visit the commercial site and log in. However, the link in the email sends the user to a malicious "spoof" site that collects user information such as account names, passwords, and credit card numbers. Once your user information is collected by a "spoof:" site, criminals may log into your account or cause other damage.

SpoofGuard is a browser plug in that is compatible with Microsoft Internet Explore. SpoofGuard places a traffic light in your browser toolbar that turns from green to yellow to red as you navigate to a spoof site. If you try to enter sensitive information into a form from a spoof site, SpoofGuard will save your data and warn you. SpoofGuard warnings occur when alarm indicators reach a level that depends on parameters that are set by the user.

## The toolbar




The SpoofGuard Toolbar has three buttons. The first, the Settings Button, brings up the Settings dialog. The second, the Status Button, displays the current domain (in case it is otherwise obscured) and a brief representation of the status (as a green, yellow or red light). The Status Button brings up a status message when pressed. The third, the Reset Button, removes all data collected by SpoofGuard (image hashes and password hashes), but will not clear the user's Internet Explorer History.

***https://crypto.stanford.edu/SpoofGuard/***

# FB crook from Bholanagar nabbed

■ After sending friend requests from fake Facebook accounts, Majid would lure young girls

K.K. ABDUL RAHOOF | DC
HYDERABAD, SEPT.11

A BTech student from Banjara Hills has been arrested for exploiting girl students after luring them to send him their nude pictures.

Abdul Majid, 21, a resident of Bholanagar, extracted money from one victim and tried to exploit others in different ways. Posing as a girl, he used six fake accounts to start conversations with the victims. In one-and-a-half years, he had contacted 200 girls from international schools and other posh institutions in Hyderabad, and secured nude pictures of as many as 80 victims. The cyber crime police arrested Majid after a parent approached them.

Majid, who is in his Third Year B. Tech Computer Science, only targeted girls studying in Class VIII to Intermediate. He threatened and blackmailed most of his victims. However, none of them told this to their parents or approached the police till this week.

From the fake accounts, he would chat with the victims, pretending to be a girl and tell them that "she" was new to the city and had no friends here.

According to Cyberabad commissioner of police C.V. Anand, after sending friend requests from his fake account, Majid would lure the victims through chatting. "Most girls accepted the friend request thinking it was a girl. And he would build up the conversation cunningly with the victims, and then start chatting about sexual encounters. He would ask if they had such experiences. If they, too, start chatting explicitly about their experiences, he would take screenshots of the conversation and tell them that he would upload the same on their Facebook wall. He would then ask for nude photos, and if the victim refused, he would threaten to send the chat history to their parents," said Mr Anand.

The complainant, Janani Rao and her mother, Swati Prabhu with Cyberabad Commissioner of Police, C.V. Anand (top), Abdul Majid (right) —DECCAN CHRONICLE

**The girls would realise that it was a man behind the account once he started threatening them. By then, the victims would have shared their personal experiences and even phone numbers**

—Md Riyazuddin, *Cyberabad cyber Crime inspector*

"They would only realise that it was a man behind the account once he started threatening them. By then, the victims would have shared their personal experiences and even phone numbers. He also called up several victims over phone and threatened them," said Cyberabad Cyber Crime inspector Md Riyazuddin.

The investigation officials, who checked the chat history, found that one victim had begged him not to ask for more money. "It stated that she had already paid more than ₹80,000 to him, and she couldn't pay him anymore," said an official. Majid also made several unsuccessful attempts to extort money from other victims.

Police suspect that he also wanted to sexually exploit his victims. He has been sent to judicial remand.

**BEWARE**

MAJID, WHO IS IN HIS THIRD YEAR B. TECH COMPUTER SCIENCE, ONLY TARGETED GIRLS STUDYING IN CLASS VIII TO INTERMEDIATE.

**200**

Girls from international schools and other posh instititions in Hyderabad befriended him. Majid secured nude pictures of as many as 80 victims

POLICE SUSPECT THAT HE ALSO WANTED TO SEXUALLY EXPLOIT HIS VICTIMS.

## Formal chat turns into personal chat

DC CORRESPONDENT
HYDERABAD, SEPT.11

Janani Rao (17) from Banjara Hills got three Facebook friend requests from unknown girls, whose bio indicated that they were Intermediate students in Hyderabad.

After she accepted one of the requests, the "girl" started chatting with her. The formal chats soon turned into personal chats, and then it took a shocking turn.

The "girl" claimed that a man possessed obscene videos of Janani, and he was going to upload it on the Internet. "The girl said she was ready to help me to stop the guy from uploading the video. In return she asked me for my nude photos. I was shocked. I was sure that no such video existed, and I got suspicious about why this girl would ask for my nude photos," said Janani, who is an Intermediate student.

"The girl then started threatening me saying she was the daughter of an IG, and I would be booked under false cases if I didn't obey her," she added.

Janani informed her mother about the whole episode. After a while, she got a call from a person who claimed to be a police inspector from Madhapur. "He wanted to talk to my mother, and wanted my Facebook password. He told my mother that some explicit content had been shared on my FB account. We became suspicious and did not give any details. Later, we approached the police," said Janani.

After police arrested cyber stalker Majid, Janani and her mother, Ms Swati Prabhu, understood that it was he who was trying to blackmail them. "It was good that my daughter told me before it took a horrible turn. We also made a quick decision to approach the police. I would suggest all teenagers to open up to their parents if they get into trouble online," said Ms Prabhu.

**THE SIX FAKE ACCOUNTS USED BY MAJID TO LURE GIRLS ARE IN THE NAMES OF**

- Vedika Chopra
- Rishika Lodani
- Jhanvi Bhatia
- Kherti Verma
- Tanvi Vaidyum
- Shriya Chitturi

**PARENTS CAN CONTACT THE COPS REGARDING THE CASE AT:**

9490617437, 9491030428

***http://epaper.deccanchronicle.com/articledetailpage.aspx?id=3671890***

*In Social Networking always check the authenticity of the person before you accept a request*

*Think twice before posting pictures of you, or your family members, or your friends on the Internet*

*Report abuse like spam, harassment, stalking etc., to the concerned authorities.*

Congratulates
Mrs. Swathi Prabhu and Ms. Janani for their bold step to complain about the Internet Fraud

# Girls target in 90 cyber cases

## Morphing and impersonations were the main methods to target victims

DC CORRESPONDENT
HYDERABAD, SEPT. 13

Insulting the modesty of women, sexual exploitation, and blackmailing are motives of a large section of cyber criminals in Telangana.

Last year, the motives in 90 cases were to insult the modesty of women and in 24 cases, it was sexual exploitation, shows NCRB data. In as many as 35 cases, the accused were trying to blackmail women.

The Telangana police had arrested five "distinct sexual freaks" in different cases, according to the data. Majority of the victims in these cases were targeted on Facebook. Morphing and impersonations were the main methods used.

The cyber criminals who were arrested for targeting women believed that they could get away with the offences thinking that they were anonymous in the cyber world. Most of them were also using fake profiles on Facebook to attack their victims.

"They strongly believed that the victims or police could never identify them or catch them since they had anonymity in cyber space. A few of them were also intelligent enough to tap into WiFi facilities of others and browse. However, since we have cyber experts tracking them, they cannot remain anonymous for a long time," said a senior cyber crime police official from Cyberabad.

While many offenders seek sexual gratification by targeting women Facebook users, a lion's share of the offenders are also out there to defame their victims by creating fake profiles of their targets and flooding them with obscene content before sending friend requests to the victims' relatives. Some also put up mobile phone numbers of victims on Facebook mentioning them as call girls.

Shockingly in many cases, the predators lurk in the neighbourhood or are from the same family. As per NCRB, as many as 25 offenders arrested by the Telangana police last year were friends, relatives and neighbours of the victims.

Senior police officials say that there is still a strong reluctance among women to approach the police. Many victims do not even discuss it with their kin even after being harassed online for many months. In the recent case of Abdul Majid, who extracted naked photos of around 80 teenaged girls, none of the victims came out till this week, police officials say.

Cyber crime officials promise that they protect the identity of the victims completely, so the latter need not fear any trouble after lodging a complaint.


***http://epaper.deccanchronicle.com/articledetailpage.aspx?id=3686418***

# Cyber crook used free Wi-Fi to trap

DC CORRESPONDENT
HYDERABAD, SEPT. 12

Cyber stalker Abdul Majid, under arrest for exploiting around hundred girls online, was using Wi-Fi facility of a business establishment near his house without the knowledge of its owner, to lure his victim, police said Saturday.

Majid lost interest in studies after he started trapping girls on the social network, and there were several backlogs in his exam record. He told police that he tried to befriend some girls on Facebook from his original account a year and a half ago, but nobody accepted his friend request.

Then he started creating fake accounts of girls to make matters easy for him.

Police said his father ran a small betel shop near his house in Bholanagar. Next to that was another business establishment. Majid used to sit near his father's shop and access the Wi-Fi set up by the company for its internal use. He somehow managed to get the password and kept on accessing it via his smartphone.

Majid, now in his third year B Tech Computer Science, failed in most of his semester exams in the second year and the current year. Since he belonged to a poor family, his education expenses were covered under a state scheme.

He had few friends in his locality and he generally kept himself aloof from others. He also maintained utmost secrecy about what he was doing. "We are yet to ascertain if he had shared the nude photographs of his victims with anyone. Usually, he does not brag about what he does on Facebook, unlike other youths", said an official investigating the case.

Majid however used to save all the naked photographs he managed to get from his victims. "We are verifying if he had uploaded the photos on any website," police said.

Meanwhile, more victims of Majid contacted cyber crime police after his arrest news came out. He has been sent to judicial custody.

# Nigerian gang cons bizman over BMW car sale, busted

DC CORRESPONDENT
HYDERABAD, NOV. 27

A Mumbai-based, five-member gang run by Nigerian nationals fleeced a businessman from LB Nagar by promising to sell him a BMW car imported from the US. The fraudsters, claiming to be US consulate officials, put up a car sale advertisement on *quikr.com* and convinced the victim, Sheik Jeelani Basha, by sending him customs receipts, etc. A Mumbai-based woman and a West Godavari native, a part of the gang, posed as Mumbai custom officials and took lakhs of rupees from him.

Cybercrime sleuths of Cyberabad have busted the gang in Mumbai, which is suspected to be involved in a Nigerian lottery scam, RBI scam and other fraudulent activities.

The accused have been identified as Talla Mojesh alias Venkat, a native of West Godavari and currently settled in Mumbai; Pascal Emmanuel alias George Frideric, 34; Paul Osemweigie, 43; Oluikpe Sunday Onyegbula, 29; and Sajida Abdul Hamid, a Mumbai native.

Cyberabad Additional DCP of Crime B. Srinivas Reddy revealed that the fraudsters had looted ₹18.63 lakh as car price, demurrage charges, other customs clearance charges, etc. The woman member in the gang, Sajida, pretending as a customs official, contacted the victim frequently over phone and made him deposit money in various bank accounts.

The businessman, Mr Shaik Jeelani Basha, who runs a building and interior designing firm, jumped at the opportunity of buying the car priced at ₹14 lakh on the online platform, as the rate appeared lower. "After Mr Basha responded to the online ad, Emmanuel contacted him, introducing himself as a Dr George Frideric, working with the US consulate and wanting to sell his car as he was leaving for the US soon. After clinching the deal, he asked the victim to deposit ₹1.5 lakh in a bank account as demurrage charges and sent some fake receipts in return. As the victim got convinced, other gang members, pretending to be customs officials, made him deposit more money in various accounts, citing different charges," said Mr Srinivas Reddy.

Basha realised he was being duped as they asked more money from him. He later approached the police and lodged a complaint

***http://epaper.deccanchronicle.com/articledetailpage.aspx?id=3678411***

By simply guessing your phone number, which is easily done, hackers can get access to all your Facebook data

# FB hole threatens data security

ANDREW GRIFFIN

A SIMPLE hack could give criminals access to all your Facebook data — just by guessing your mobile number. The names, location, images and more data of users can be gathered by just guessing a phone number — a relatively straightforward process. That data could then be stolen and sold on, for use in crime and identity theft.

The hack exploits a tool that's intended to let anyone find a Facebook user by putting their phone number into a search box. But Reza Moaiandin, technical director at Salt Agency, has found that using a computer to automatically put in numbers can let people scrape a huge amount of data on Facebook users easily.

By gathering up an entire country's possible combinations and putting them through the search box, hackers can pick up all Facebook user IDs of people using those numbers. That can then be put into Facebook's GraphQL, the tool Facebook uses to organise its data, to pick up all the information that the site has on those people.

All of that information is publicly available. But Moaiandin points out that collecting all of that data on a large scale means that it can be easily sold on — and potentially combined with other stolen data to find out much more about the people involved.

The "Who can find me?" setting that decides whether people should be able to locate people using a phone number is turned to "Everyone/public", though it can be switched off to avoid being liable to the hack.

A spokesperson for Facebook said, "The privacy of people who use Facebook is important to us. We have strict rules that govern how developers may use our APIs to build their products, and in this instance, all the information being returned is already designated to be public.

"Everyone who uses Facebook has control of the information they share, including information on their profile and who can look them up by phone number. Our privacy basics tool has a series of helpful guides that explain how people can quickly and easily decide what information they share and with whom they want to share it." But Moaiandin says, Facebook should go further by "limiting the requests from a single user, and detecting patterns, before moving on to pre-encrypting all of its data".

Moaiandin said he had found the loophole by mistake: "I wasn't even searching for flaws in Facebook's security when I came across it", he writes in his blog. He found the flaws a few months ago and decided to release it to the public when trying to tell Facebook failed as "an attempt to catch Facebook's attention to get this issue fixed". — *The Independent*


***http://www.tribuneindia.com/news/trends/fb-hole-threatens-data-security/136834.html***

Privacy and security are major concerns that are under threat due to jailbreaking, which permits root access to Apple's iOS file system

# Jailbreak is living dangerously

VAIBHAV SHARMA

THE first thing you do when you buy an iPhone is to accept that you will now have to live inside Apple's walled garden. You won't be able to 'sideload' apps or use an App Store that isn't Apple's, change the default browser, customise the layout and so on — that's unless you decide to jailbreak.

Jailbreaking essentially frees you of Apple's limitations in how much access to underlying code each app has, and you can as a result completely overhaul the look, feel and functionality of your iOS device. It permits root access to the iOS file system, allowing the download of additional applications, extensions, and themes that are unavailable through the official App Store. Each method of jailbreaking takes advantage of a software exploit that Apple then works hard to fix in the next release. While jailbreaking voids your warranty, it isn't hard to reverse should you run into a problem, just restore your iPhone via iTunes and your phone is as good as new. This has prompted a large number of people to jailbreak their devices, especially on the advice of the thousands of small mobile phone repair shops that are scattered throughout the country. Needless to say, pirating apps is only possible if you jailbreak, and these stores are happy to install hundreds of paid apps and games for a small fee. Other than pirated apps and customisation, another 'advantage' of going down this route is being able to bypass carrier restrictions such as enabling a hotspot.

That said, is it really worth the trouble? The answer to that question, especially in 2015, is a resounding no. With each iOS release, the software has become better, and a lot of the key iOS tribulations are now history. Airdrop makes sending files via bluetooth possible, otherwise there are faster apps like Xender that even let you share files with android users. Multi-tasking is better and apps can now talk to each other. App prices have come down, and there is even a special 'Ten Rupee' section in the App Store.

But more than all of that, the reason you should stay away from jailbreaking is privacy and security. When you jailbreak, you trust someone else's code to run on your phone, and yet do nothing malicious. That is a very high level of faith, and a pirated game that you got hold off in a remote corner of the internet isn't worth that trust. The app could well and truly install a second virtually invisible app that has a blank icon and resides inside the 'Newsstand' section that no one uses, and yet steal photos, GPS data, keypresses and contact information without making a fuss. While jailbreaking, you also sacrifice stability and the ability to install the latest software as it becomes available, as Apple obviously patches the exploit that let the jailbreak happen in the first place.

On Android, 'rooting' is analogous to jailbreaking. However, since customisation options are already aplenty, and because you can sideload apps, the lure to 'root' the device is small. That said, if you do go down that road as an Android user, the same pitfalls await you.



***http://www.tribuneindia.com/news/trends/jailbreak-is-living-dangerously/136835.html***

## CERT-In Vulnerability Note CIVN-2015-0220

### GnuTLS ServerKeyExchange MD5 Signature Vulnerability

Original Issue Date:August 28, 2015

Severity Rating: MEDIUM

### Software Affected

- GnuTLS versions prior to 3.3
- GnuTLS versions prior to 3.4

**Solution**

Upgrade to GnuTLS 3.3.15 or 3.4.1. Vendor advisory is available at
http://www.gnutls.org/security.html

**Vendor Information**

**GnuTLS**
http://www.gnutls.org/security.html#GNUTLS-SA-2015-2

**References**

**Cisco**
http://tools.cisco.com/security/center/viewAlert.x?alertId=40511

**Disclaimer**

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

### Overview

A vulnerability has been reported in GnuTLS which could be exploited by a remote attacker to conduct cryptographic attack.

### Description

This vulnerability exists due to improper authentication of ServerKeyExchange and ClientCertificateVerify messages. A remote attacker could exploit this vulnerability by sending MD5 signatures during a message exchange between a GnuTLS client and GnuTLS server.

Successful exploitation of this vulnerability could allow the attacker to conduct cryptographic attack.

***http://cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES01&VLCODE=-CIVN-2015-0220***

## CERT-In Vulnerability Note CIVN-2015-0221

### Denial of Service vulnerability in GnuTLS

Original Issue Date:August 28, 2015

Severity Rating: MEDIUM

### Software Affected

- GnuTLS versions prior to 3.3.17
- GnuTLS versions prior to 3.4.4

**Solution**

Upgrade to GnuTLS 3.3.17 or 3.4.4. Vendor advisory is available at
http://www.gnutls.org/security.html

**Vendor Information**

**GnuTLS**
http://www.gnutls.org/security.html#GNUTLS-SA-2015-3

**References**

**Cisco**
http://tools.cisco.com/security/center/viewAlert.x?alertId=40512

**CVE Name**
CVE-2015-6251

**Disclaimer**

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

### Overview

A vulnerability has been reported in GnuTLS which could be exploited by a remote attacker to conduct Denial of Service (DOS) condition.

### Description

This vulnerability exists in the _gnutls_x509_dn_to_string() function in GnuTLS due to improper validation of user-supplied input processed by an application utilizing the affected GnuTLS library. A remote attacker could exploit this vulnerability by sending crafted certificate with long DistinguishedName (DN) entries to a targeted system.

Successful exploitation of this vulnerability could allow the attacker to cause Denial of Service (DoS) condition.

***http://cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES01&VLCODE=-CIVN-2015-0221***

For any queries on Information Security

Call us on Tool 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/infosecawarenesss*

# National Level Painting/Drawing Competition on Information/Cyber Security Awareness

For VII to XI standard students

**Where to send:**

C-DAC, Plot No. 6 & 7, Hardware park, Sy No. 1/1, Srisailam Highway, Pahadi Shareef via, Keshavgiri(Post), Hyderabad-500005, India.
Tel: 040-23737124/125

Last date for entries Nov 30th 2015

The backside of the paintings should carry Name of the student, Father's/Mother's name, Class, School name and address, Signature of the head of School/ Institution, Tel. no. of the school and School stamp

For more details visit
www.infosecawareness.in/contest

**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.


सत्यमेव जयते

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)
E-mail : isea@cdac.in