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

InfoSec Newsletter

Nov-Dec 2017

Online Gaming Safety

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

सी डैक CDAC
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 Pahal (V & GP), Via Ragasnna guda, Maheshwaram (M), Ranga Reddy District, Hyderabad - 501510.Telangana(India)
Nalanda Building, No. 1 Shivabagh Satyam Theatre Road, Ameerpet, Hyderabad - 500016, Telangana (India)

CREDITS

Message from
E Magesh
Director
CDAC, Hyderabad

Online games have taken the computer world by storm. Gaming has always been and remains a prime driver for children to use Computer technology. In the past 10 years, it has grown as quickly as the Internet, and can now be found in tens of millions of homes. Along with the Internets phenomenal growth comes plenty of adolescent growing pains, these pains mostly concern problematic and pervasive computer security issues.

With the availability of different platforms that range from personal computers and consoles to handhelds, smartphones and tablets, the number of people that play games around the world have made the gaming industry one of the fastest growing industries on the planet. Its popularity and market size makes game platforms and individual users ideal targets for cybercriminals who see it as a platform for stealing user information, invading privacy, or spreading malicious content and malware.

Information security awareness is the need of the hour as more and more children are getting addicted to the online gaming technology and their future depends on how safe they can use them. Children acquire varied skills naturally while growing up in this environment. Online gaming accounts will also invariably contain personal information besides the user's login credentials, such as the player's name, birthdate, address, mobile number, email address for verification, social network ID, and even a linked credit card account. This information is ultimately more valuable , as it could either be sold in cyber criminal underground markets, or used to further invade the victim's privacy by accessing email and other online accounts.

The current edition of the newsletter will help the readers understand the complete scenarios of Online Gaming and the tips to be safe. Making children sensitive to the safe use of Internet, safe use of technology, secure computing environment and the need for individual protection. It is expected, that once the knowledge in Information / cyber security is provide to the all, who will create a safe and supportive environment for themselves to use Internet safely by which we can create a better cyber aware society.

Online Gaming safety for Children

Online Gaming is a fun and social way to spend time, encouraging teamwork and developing skills. Children see the online gaming world as a virtual playground.

These days Gaming consoles operate same way as a computer—children can log online, put on a headset, turn on a webcam, and talk to and play with any of the millions of gamers around the world.

Many online games have associated online communities, making online games a form of social activity beyond single-player games.

Online gaming can be a fun way for kids to connect with others, but it's important for them to understand the risks and know how to handle certain situations.

HERE ARE SOME SAFETY TIPS FOR ONLINE GAMING:

- Children should select games for enjoyment and make sure they're appropriate for their age.
- Some online games are abusing the fear around the challenge to encourage others to self-harm and carry out various dares and post the results online under the guise of some game challenge. Stop playing such games and inform your parents/ elders. Children should understand the pain their parents will go through if they hurt themselves.
- Some games let children play and chat with any strangers in the world. Be cautious as children might come across offensive language and bullying.
- Children should avoid giving out personal details that could identify them or their location.
- If children experience Online grooming by strangers who aim to take advantage of their naiveness and the inability to protect themselves from dangers, stop interaction and inform parents.
- Play any game for limited time period, only look for games that are educational and stimulating.
- Children should be aware that there are some games which encourage players to buy extra elements during the game without realising the risk involved before they begin to play the game.
- In extreme cases bullying can be used as a tactic to win games. Children may find themselves either bullying or being bullied. Avoid those games and inform your elders.

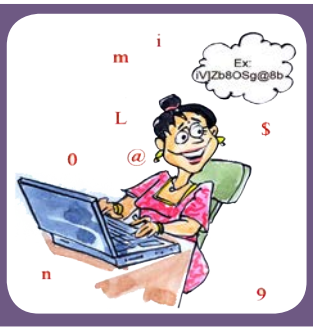
ISEA, Supported by MeitY, Government of India

Keep your device uptodate :

All Internet-enabled devices need to be kept up to date to protect them from malware and other threats. Security protections are built in and updated on a regular basis. Take time to make sure all the mobile devices in your house have the latest protections. Before you start playing, be sure your computer/gaming system has the latest operating system and software, including anti-virus protection, web browsers and apps.

Have a strong password :

A strong password should be at least 12 characters long with alpha numeric special characters, think about strong and easy to remember passwords which are hard to guess.



Protect your personal information :

Never reveal your real name, location, gender, age, or any other personal information. Keep your user name vague and use an avatar rather than an actual picture of yourself.

Do not use voice chat and web-cam while playing an online game for safety

- Always maintain a time limit for yourself while playing online games with the permission from your elders/parents
- Never accept downloads from strangers which may include malware/cheat programs that may claim to help you perform better in the game.
- Do not meet a stranger from your gaming world in person. People are not always who they say they are. Be aware of the risks, practice good judgment and feel free to take advice from parents/elders.
- Never feel pressurized into doing anything to which you feel uncomfortable. If you are feeling worried, cancel the game/chat and speak to an adult you trust.
- What you do online has the potential to affect everyone – at home, at school and around the world. Practicing good online habits, will benefit the Global digital community.

SAFETY TIPS FOR PARENTS/ TEACHERS

One of the most important duty of a parent/ teacher is to keep their kids safe, basically protect them from any kind of danger online or offline. A parent should be able to find out about the various dangers that a child can face and then find out what to do to protect them from those dangers.

HERE ARE SOME SAFETY TIPS FOR ONLINE GAMING:

- One of the best things that you can do to keep your kids safe while playing online games is by your own participation in the game. Spend your time with your children and join them in some of their games to find out why children find them so much fun and also helps to keep their gaming experience healthy.
- Use parental controls on all the devices used by your child. Monitor the screen time and keep an eye on his/her online activities, because it is a good way to help/ teach them about how to deal with other people online and also allows them to have fun in a safe and secure way.
- Discuss with children who they play with online, who they meet and talk to and what kind of language is being used in live chat . Make sure your child knows that many of the gaming sites often have ways of reporting abusive chat and excluding anti-social players. You can teach your child about what they should do if they come across cyberbullies.
- Make sure that your child is using an appropriate screen name for the game, to avoid revealing of any personal information and harassment of your child.
- Especially for younger children, change the settings on your tablet or smartphone to 'airplane' mode so that they can play the game offline without making accidental purchases or connecting with someone they don't know.
- Teach your children to protect themselves and remind them not to share personal information and also to keep gaming friends in the game only rather than adding them to their other social networks.
- If they are using an online gaming feature like live voice chat, they really shouldn't talk to people whom they don't know to avoid any harassment.
- Read each game's advice for parents and play the game yourself to help you understand more about the game, your child is playing and its appropriateness.
- Make sure your child knows how to block abusive comments and report content that worries them.
- Teach them to respect others online and think about comments before they post them.
- Teach them how to use secure and legal sites to download music and games. Advise them to Check attachments and pop ups for viruses before they click or download anything.

- Create the trust and make sure your child knows that they can come to the parents/teachers if they're upset by something they have seen online while monitoring their internet use.
- If your child comes to you with an issue, stay calm and listen without judging them and don't threaten to take away their devices.
- Advise your child to tackle peer pressure by explaining them that if you are bullied online or someone sending inappropriate images, it will be reported to school authorities or even to the police .
- Talk to them about how much time they spend online and make sure that there is a balance against other activities.
- Make sure your child knows not to share personal information like phone number, email address, social networking ID's online.
- Advice children that some apps have gained a reputation for being potentially risky for children because of the types of technology they use and the types of communities that have formed around them.
- Advice children to talk only to real life friends whom they know physically & family members on social media sites and in chatrooms.
- Use privacy settings wherever they exist to keep their information private.
- Use secured Public WiFi and use filters to avoid inappropriate content.
- Be sensitive and praise children when they share their online experiences with you.
- Teach children the ethical behaviour on Internet, frame the Internet rules for your home.

Tips for Schools

- Ensure that children do not bring and use any gadgets during school hours.
- Ensure that children are sensitized about the pros and cons of the internet from time to time.
- Teachers need to keep an eye on falling grades and social behaviour of the students.
- Monitor the behaviour of each and every child.
- Look for anti-social behaviour and talk to such children who don't interact with other children or are aloof.
- Anything suspicious or alarming, inform the school authorities immediately.
- Teach good net etiquette and ethics.
- Create awareness on cyber safety and security for children by instructing them to visit www.infosecawareness.in, conducting workshops, displaying posters, having tips for safety and security.

Always ensure you have effective and updated antivirus/antispyware software and firewall running before you start downloading.

Close all the important applications in order to be safe if something goes wrong while downloading.

Enable firewalls & set auto-scan in antivirus to actively scan all the files you download.

Scan all the files after you download whether fromwebsites or links received from e-mails


Beware of
BLUE WHALE CHALLENGE
For more details visit :
http://infosecawareness.in/Know-About-Blue-Whale-Suicide-Game
SUICIDE GAME
DAY 50
DAY 5
Never click links/game notifications received through social networking sites.
Limit your social network posts only to your friends
Never share private information like age, place in public domain
Always discuss with your parents for better advice
ISEA, Supported by MeitY, Government of India

InfoSec QUIZ

1. The action or practice of playing video games or role-playing games on the Internet is called as
   A. Online gaming
   B. Online Chatting
   C. Browsing
   D. None of the above

2. Stealing someone's identity online, usually by phishing when they provide personal information like bank account details is known as
   A. Information threat
   B. Identity theft
   C. Data theft
   D. None of the above

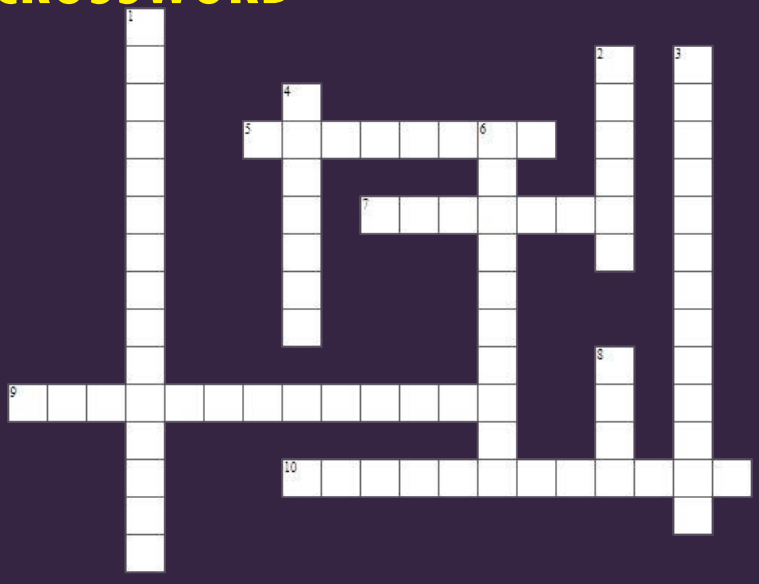
3. The best way to behave on the net/online is
   A. Netiquette
   B. Etiquette
   C. Ethical
   D. None of the above

4. Making a fake version of an Original site is known as
   A. Phishing
   B. Spoofing
   C. Morphing
   D. None of the above

5. A type of malware that replicates itself so it can spread to other computers is called as
   A. Worm
   B. Threat
   C. Malware
   D. None of the above

6. _____ is the state of being certain of remaining safe and unthreaten
   A. Security
   B. Cyberbullying
   C. Virus
   D. None of the above

InfoSec CROSSWORD



Down

1. _____Settings on a computer or phone that parents can change to determine what content their kids can see and how long they can spend online.
2. _____is Someone who uses code to change or modify an existing website
3. _____can be a challenging topic to talk about it, but it doesn't have to be.
4. _____a type of software that spies on you, stealing your data and passwords.
6. The best way to behave on the net/online is
8. A type of malware that replicates itself so it can spread to other computers is called as

Logon to www.infosecawareness.in/contest to participate in InfoSec Contest and win prizes

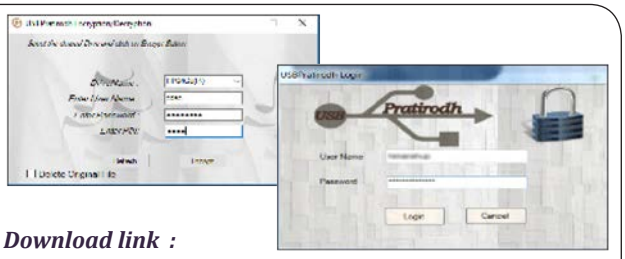
Across

5. Making a fake version of an Original site is known as
7. _____is a Social media platform where users share videos in the form of sketches, vlogs, or freeform content.
9. Stealing someone's identity online, usually by phishing when they provide personal information like bank account details is known as
10. The action or practice of playing video games or role-playing games on the Internet is called as

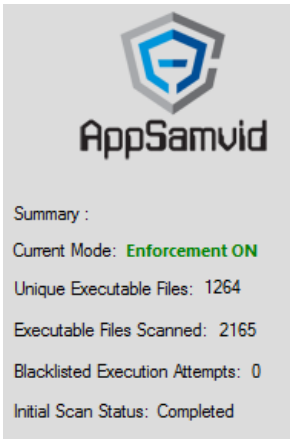
USB PRATIRODH

Standalone Version

USB Pratirodh controls the usage of removable storage media like pen drive, external hard drives, cell phones, and other supported USB mass storage devices. Only authenticated users can access the removable storage media.



Download link :
https://www.cdac.in/index.aspx?id=cs_eps_usb_pra35



AppSamvid

Application Whitelisting Software

AppSamvid is application whitelisting software for Microsoft Windows based operating systems. Whitelisting allows only the pre-approved files to execute on operating system. This is in contrast to traditional signature based antivirus software approach of blacklisting the virus files. Whitelisting has the advantage over blacklisting as it does not require frequent virus definition updates. AppSamvid can work for Microsoft Windows XP SP2 and above operating systems. AppSamvid can protect operating system against computer malware (such as Viruses and Trojans).

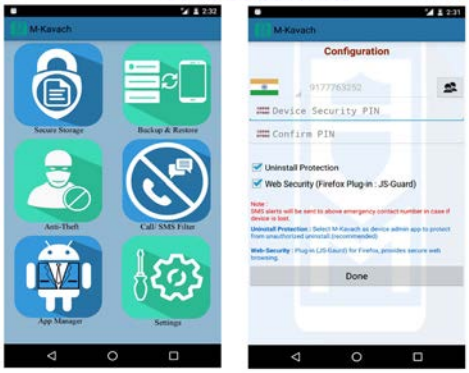
Download link : https://www.cdac.in/appsamvid

MKavach

Mobile Device Security Solution

M-Kavach is a comprehensive mobile device security solution for Android devices addressing various threats related to mobile phones. It addresses threats related to misuse of resources such as WiFi, Bluetooth, Camera & Mobile-Data by preventing unauthorized access to these resources and protects against JavaScript Malware. Users can restrict the access to critical applications like mobile wallets, social media apps etc and also block unwanted Calls & SMS. It also helps the users in tracking SIM card changes on the device in case of device loss/theft and provides an option to remotely wipe Contacts/Call-Logs & Factory Reset the device.

Some Screenshots



Download from Google Playstore

Browser JS Guard

Protects from JavaScript based Threats

In the recent times, most of the systems connected to Internet are getting infected with malware and some of these systems are even becoming zombies for the attacker. When user knowingly or unknowingly visits a malware website, his system gets infected. Attackers do this by exploiting vulnerabilities in web browser and it is possible to acquire control over the underlying Operating System. Once attacker compromises the user's web browser, he can instruct the browser to visit the attacker's website by using number of redirections. During the process, user's web browser downloads the malware without the intervention of the user. Once the malware is downloaded, it would be placed in the file system and responds as per the instructions of the attacker. These types of attacks mostly happen through JavaScript and malicious HTML tags. Browser JSGuard detects and defends from such attacks made through the web browser. It blocks access to the harmful, inappropriate and dangerous websites that may contain malicious content.

Download link :
https://addons.mozilla.org/en-US/firefox/addon/browser-jsguard/
https://chrome.google.com/webstore/detail/browserjsguard/ncpkigeklafkopcelcegambndlhkcbhb

BAD RABBIT RANSOMWARE

A large scale ransomware campaign dubbed "bad rabbit" is reported spreading. Initial information indicates genuine sites were compromised [watering hole style attack] and that directed victims to a fake Flash update that downloaded the malicious Bad Rabbit executable.

User action is required for the dropper(630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed8496fcbb97a558d0da) to start the infection, which contains the BAD RABBIT ransomware component. Bad Rabbit ransomware uses DiskCryptor, an open source full drive encryption software, to encrypt files on infected computers with RSA 2048 keys. The ransomware targets MBR also rendering the system unusable. The malware is capable to laterally move via open SMB shares, with hardcoded list of credentials to drop malware, and also uses Mimikatz post-exploitation tool to dump credentials from the affected systems.

Open source reports say that Bad Rabbit leverages EternalRomance [MS17-010] also to propagate in the internal network apart from the windows legitimate features [SVCCTL: the remote service management,SMB2,SMB,NTLMSSP authentication brute force,WMI].

IOCs:

URLS

- 1dnscontrol[.]com/index.php - fake Flash download URI
- 1dnscontrol[.]com/flash_install.php - fake Flash download URI
- 185[.]149[.]120[.]3/scholargoogle/ - URI called out to from watering hole sites
- caforssztxqzf2nm.onion

WATERING HOLE SITES:

- Fontanka[.]ru - Referrer to 1dnscontrol[.]com
- Adblibri[.]ro - Referrer to 1dnscontrol[.]com
- Spbvoditel[.]ru - Referrer to 1dnscontrol[.]com
- Grupovo[.]bg - Referrer to 1dnscontrol[.]com
- sinematurk[.]com - Referrer to 1dnscontrol[.]com
- argumenti[.]ru - Referrer to 1dnscontrol[.]com

HASHES:

- 630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed-8496fcbb97a558d0da - fake flash installer
- 8ebc97e05c8e1073bda2efb6f4d00ad7e789260a-fa2c276f0c72740b838a0a93 - C:\Windows\dispci.exe associated with DiskCryptor
- 682ADCB55FE4649F7B22505A54A9DBC454B4090FC2B-B84AF7DB5B0908F3B7806 - C:\Windows\cscc.dat (x32 diskcryptor drv) associated with DiskCryptor
- 0b2f863f4119dc88a22c-c97c0a136c88a0127cb026751303b045f7322a8972f6 - associated with DiskCryptor
- 579FD8A0385482FB-4C789561A30B09F25671E86422F40EF5C-CA2036B28F99648 - C:\Windows\infpub.dat [malicious DLL with some similarities to Nyetya]
- 2f8c54f9fa8e47596a3beff0031f85360e56840c77f-71c6a573ace6f46412035 - Mimikatz x86
- 301b905eb98d8d6bb559c04bbda26628a942b2c-4107c07a02e8f753bdcfe347c - Mimikatz x64

SCHEDULED TASKS NAMES:

- viserion_
- rhaegal
- drogon

MITIGATION /COUNTERMEASURES:

- Block the execution of files c:\windows\infpub.dat and c:\Windows\cscc.dat.
- Secure use of WMI by authorizing WMI users and setting permissions / Disable or limit remote WMI and file sharing.
- Configure access controls, including file, directory, and network share permissions with the principle of least privilege in mind.
- Block remote execution through PSEXEC.
- Enable Anti-ransomware folder protection feature added in Windows 10 v1709 *https://blogs.technet.microsoft.com/mmpc/2017/10/23/stopping-ransomware-where-it-counts-protecting-your-data-with-controlled-folder-access/*
- Consider deploying Microsoft LAPS[Local Administrator Password Solution]" which ensures that each domain-joined host in an organisation has unique Local Administrator credentials, preventing ransomware from using the extracted credentials to spread laterally *https://technet.microsoft.com/en-us/mt227395.aspx*

CERT-In Vulnerability Note CIVN-2017-0163

Remote Users Bypass Security Restriction Vulnerability in Red Hat Enterprise Linux

Software Affected

- Red Hat Enterprise Linux Server 6 x86_64
- Red Hat Enterprise Linux Server 6 i386
- Red Hat Enterprise Linux Workstation 6 x86_64
- Red Hat Enterprise Linux Workstation 6 i386
- Red Hat Enterprise Linux Desktop 6 x86_64
- Red Hat Enterprise Linux Desktop 6 i386
- Red Hat Enterprise Linux for IBM z Systems 6 s390x
- Red Hat Enterprise Linux for Power, big endian 6 ppc64
- Red Hat Enterprise Linux for Scientific Computing 6 x86_64

Overview

A Vulnerability has been reported in Apache HTTPD on Red Hat Enterprise Linux which could be exploited by a remote attacker to bypass security controls on the targeted system.

Description

This vulnerability exists in Apache HTTPD on Red Hat Enterprise Linux due to improper parse comments in the "Allow" and "Deny" Configuration lines.

Successful exploitation of this vulnerability could allow the attacker to access an ostensibly restricted HTTP resource.

Solution

Apply appropriate Security fixes as mentioned in the following Red Hat advisory.
https://access.redhat.com/errata/RHSA-2017:2972

Vendor Information

Redhat
https://access.redhat.com/errata/RHSA-2017:2972
References

Redhat
https://access.redhat.com/errata/RHSA-2017:2972
Securitytracker
https://securitytracker.com/id/1039633

CVE Name

CVE-2017-12171

CERT-In Vulnerability Note CIVN-2017-0164

SQL Injection Vulnerability in WordPress

Software Affected

- WordPress 4.8.2 and earlier.

Overview

A vulnerability has been reported in WordPress, which could be exploited by remote attacker to conduct an SQL injection attack on a targeted system.

Description

1. SQL injection Vulnerability (CVE-2017-14723)

This vulnerability exists due to insufficient security restrictions and improper processing of user-supplied input by the affected application. A remote attacker could exploit this vulnerability by submitting crafted queries to the affected application.
Successful exploitation of this vulnerability could allow an attacker to conduct an SQL injection attack, which could be used to access sensitive information on the system.

Solution

Apply appropriate fixes as issued by vendor in the following link
https://wordpress.org/

Vendor Information

WordPress
https://wordpress.org/news/2017/10/wordpress-4-8-3-security-release/

References

WordPress
https://wordpress.org/news/2017/10/wordpress-4-8-3-security-release/
Cisco
https://tools.cisco.com/security/center/viewAlert.x?alertId=55744
Security Tracker
https://www.securitytracker.com/id/1039553
Security Focus
http://www.securityfocus.com/bid/100912

CVE Name

CVE-2017-14723

Beware of Malicious Mobile Apps

InfoSec NEWS ALERTS

Published in Times of India on 6th April 2017

Your apps could be secretly stealing data

Smartphone apps that we regularly use to organise lunch dates, make convenient online purchases and communicate the most intimate details are mining our data by secretly colluding with each other, a new study warns.

Researchers conducted the first ever large-scale and systematic study of exactly how the trusty apps on Android phones are able to talk to one another and trade information.

"Researchers were aware that apps may talk to one another in some way, shape, or form," said Gang Wang, Assistant Professor at Virginia Tech University in the US.

"What this study shows undeniably with real-world evidence over and over again is that app behaviour, whether it is intentional or not, can pose a security breach depending on the kinds of apps you have on your phone," said Wang.

The types of threats fall into two major categories, either a malware app that is specifically designed to launch a cyberattack or apps that simply allow for collusion and privilege escalation, researchers said.

In the latter category, it is not possible to quantify the intention of the developer, so collusion, while still a security breach, can in many cases is unintentional, they said. In order to run the programmes to test pairs of apps, the team developed a tool called DIALDroid to perform their massive inter-app security analysis.

"Of the apps we studied, we found thousands of pairs of apps that could potentially leak sensitive phone or personal information and allow unauthorised apps to gain access to privileged data," said Daphne Yao, Assistant Professor at Virginia Tech.

The team studied a whopping 110,150 apps over three years including 100,206 of Google Play's most popular apps and 9,994 malware apps from Virus Share, a private collection of malware app samples.

The set up for cybersecurity leaks works when a seemingly innocuous sender app like that handy and ubiquitous flashlight app works in tandem with a receiver app to divulge a user's information such as contacts, geolocation, or provide access to the web. The team found that the biggest security risks were some of the least utilitarian. —*PTI*

Tips to Protect your data on your Mobile:

- Do not click on download links received through e-mail, SMS, Whatsapp from unknown senders
- Do not click on pop-up ads or 'click bait' posts on social media
- Download the APP only from trusted sources and read "Terms and conditions"
- Do not allow App's to access the data in your mobile
- Disable automatic downloads and always keep an updated antivirus solution installed
- Always check reviews of the applications that you are using
- Update the mobile operating system or firmware regularly

Uninstall the malicious apps from your Android/IOS Mobile

- First tap on the Clear cache button to remove the cache.
- Next, tap on the Clear data button to remove the app data from your Android phone.
- Finally tap on the Uninstall button to remove the malicious app.

Scan your device with Mobile Antivirus

- There are virus, malware, spyware which affect your mobiles
- Regularly scan your mobile for any malware
- Reset your mobile to factory setting after taking backup of important data

Scan & verify all the applications being used, Uninstall all the unused applications

Beware of CyberBullying

InfoSec NEWS ALERTS

Published in http://www.dnaindia.com on 3rd July 2017

Priyanka (name changed) was in for a shock recently when she logged into her LinkedIn account. She had received a thread of messages from someone named Dr Arjun Pandey, Head of Research and Development at the Sajjan India Limited. The man had sent her increasingly lewd messages on the network meant for professionals.

Speaking to DNA, Priyanka revealed that she did not file an FIR against the man since she had no faith in the system. "Filing a complaint against the man will be very troublesome for me. I would be making multiple trips to the police station while taking care of my family. I'm not even sure whether the cops would be able to help," she said.

"If I take any action against this man, my own career might be affected. I am not losing my fire but I have lost faith in the system," she added.

From homes to workplaces to streets to the internet, harassment seems to have become a of part of women's lives. The advancement in technology has opened up new avenues where women can be victimised, even on professional networking sites.

Section 67 under the IT Act of the Indian Penal Code (IPC) deals with publishing or transmitting obscene material in electronic form, material containing sexually explicit acts, material depicting children in sexually explicit acts, and preservation and retention of information by intermediaries.

Shares 3

Tips

Block the Bully if you receive strange messages

Never let anyone have access to your passwords

Think very carefully before posting/ sharing photos of yourself Online

Save and take print out of any bullying messages, posts, pictures or videos you received or seen

Don't ignore if you see cyberbullying going on, report it to your parents, teachers, higherups & police

Don't Suffer- Speak out- Together let us Stop CYBERBULLYING

Do's & Don'ts

Do's

- Take action immediately if you are bullied talk to/inform your parent/teacher for help.
- Intervene immediately. It is ok to get another adult to help.
- Understand that all types of bullying are unacceptable and such behavior is subject to disciplinary action.
- Meet any immediate medical or mental health needs.
- Model respectful behavior and never send/forward mean or hurtful text messages to any one.

Don'ts

- Do not send photos and videos of others without their permission to try and embarrass.
- Do not spread rumors or lies about anyone via e-mails or social networking sites or text messages.
- Don't think you can work it out without adult help.
- Don't force other children to say publicly what they saw.
- Don't question the children involved in front of others.

Section 67 of IT Act: Publishing of information which is obscene in electronic form

ISEA, Supported by MeitY, Government of India

Master trainer program @Gurgaon

Awareness program @Ghaziabad

@NRLDC Delhi

@NIRD Hyderabad

Awareness for Teachers @Jaipur

Govt. official training @Medak

Awareness program@ IIT Madras

Awareness for Students @ Haryana

Awareness program@ Noida

Awareness program@ Punjab

@ ONGC Rajamundry

Govt. Official training@Dharamshala

@ Parwanoo, Himachal Pradesh

Awareness Program in National Network All India Radio@Delhi

Master trainer program@ Jaipur

Awareness@Tamilnadu

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

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 etc.,

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.

Ministry of Electronics and Information Technology (MeitY)
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)