Information Security
Education & Awareness
www.isea.gov.in

For more details visit :
www.
InfoSec
awareness.in

ONLINE SAFETY TIPS FOR CHILDREN

@ Home

#Stay safe #Keep Learning, #Be aware

Programme by : Ministry of Electronics & Information Technology(MeitY), Govt. of India

Supported by : Ministry of Home Affairs (MHA), Govt. of India

certin
http://cert-in.org.in/

www.
cyberswachhtakendra.
gov.in

CYBER DOST

Cyber Safe GIRL

DSCI
PROMOTING DATA PROTECTION

END NOW
ADVOCACY ON DIGITAL SAFETY

For more details / queries on
Cyber Security
Call us on our Toll free No.
1800 425 6235

Implemented by
सी-डैक
CDAC

Information Security Education and Awareness (ISEA) Project Phase-II

Programme by
Ministry of Electronics and Information Technology
Government of India

Children of all ages enjoy using digital devices and gadgets and Internet Technology at home. Due to lockdown, Schools are urged to conduct online classes, so young children attending classes online. Children also play games, talk to other family members, watch videos, share messages and even learn to use voice enabled tech devices like Alexa and Siri to find out about their world

Problem Impact Tip

Attending Class Room Sessions Online

Children may not have a tendency to understand the impact of not meeting teachers in person.

Online Education may create "monologue and not a real dialogue" in the learning environment

Put more effort to build relationship with your teachers and classmates in online environment

Online Courses usually have deadlines of assignments, tests, homework etc.

You need to pursue a lot of content and have a better time management.

Develop self-discipline and self-direction to do assignments, practice tests, home work etc.

Online courses typically require a greater amount of reading and assignments than traditional classes

Invest more time to prove and master the subject

While accessing content in Internet, some advertisements may attract you with free offers for your content.

Clicking such websites may attract malware to your systems.

Never click on links while accessing web pages. Copy and paste the link is the best practice to be followed.

The following are the good practices to be followed while using content available on Internet.

- Follow Internet Ethics
- Follow Copyrights of the content
- Always give reference(s)of web site, in case you have taken content from respective website
- There are a number of practice exercises for your subject on the Internet. Utilize them to become as master in the subject.

Online Games at Home

As children, most of you enjoy playing games online or offline. Virtual reality games are incredibly popular among students. It is a perfect way to get rid of stress, exhausting assignments, and boredom. Considering the current situation most likely you might be looking for free online games to spend your idle time.

Did You Know ?

Some of the online educational games provide multiple examples of concepts, motivation, hand and eye coordination, improved motor skills, memory, Quick thinking and decision making(important to make a right decision but also do that quickly to speed up your competitors), Improving problem-solving skills(most of the modern online games have a strategy that must be recognized by the player to win a game), Development of teamwork and cooperation skills (Many modern online games can be played in pairs, groups, teams).

Children who play online games online feel overwhelmed or excited by the type of gaming content they interact with. These online games with challenges and levels makes them spend more time to cross the level or win a challenge. Certain games even makes them exposed to a culture of violence. Online gaming is the favorite hub for online predators and cyber bullies to find their targets.

There are lots of instances that might stop your game from having fun, and expose you to the darker sides like:

- being bullied or hurt
- not able to stop (gaming addiction)
- Privacy issues
- hidden charges and malwares
- getting in trouble with your parents for spending more time on online games.

As children you may not be aware of the dangers posed by the online world. Here are few dangers and simple tips to stay safe online.

Cyber bullying

Cyber bullying can happen in online gaming platforms and Cyber bullies target gullible players directly with hurtful and harmful messages, or by spamming chat windows with derogatory comments.

Cyber bullying can affect children in everyday life and may become a constant source of distress and worry

- Don't blame yourself when you are bullied with bad comments
- Make use of the features like "block" chat and messages from unknown users
- Read about the game's terms of service and report for any violations.

Cyber bullies conquer or capture needed targets in online games before the other players can get hold them just for annoying them; or create chain groups to block them in entering high-level challenges. There are some people who play online video games for the sheer "satisfaction" of harassing other players.

This can create distress among children and they may try to retaliate in the same manner out of anger.

- Do a good research on content ratings and choose age appropriate games for your kids
- Enable parental control features or devices to block inappropriate messages from strangers or chat rooms.

Some of you may think it is okay to send harassing messages to their opponents in the online gaming world.

Bullying for fun and in any form can put children in trouble as it is considered as a criminal offence.

- Don't be a bully and avoid joining the chain of bullies
- If someone you know is being bullied, help him to take action.

Gaming Addiction

When you are not able to get off the tablet, gaming console or computer when your parents call or for any other needs, you may need to realize the fact that you are getting "addicted" or you are "overusing online games."

Increased aggressive thoughts and aggressive behaviors, particularly in children, Less or No social interactions. it can also lead to poorer mental health and cognitive functioning including poorer impulse control and Physical and Psychological issues.

- Engage yourself in a digital detox that may help you to get rid of addiction.
- Set rules of screen time and follow them to avoid getting addicted to online games

---

- Engage yourself in activities like playing online games together to help children in avoiding cyber risks

Did you Know ?

'Gaming disorder' is in the WHO's International Classification of Diseases and is defined "by impaired control over gaming, increasing priority given to gaming over other activities to the extent that gaming takes precedence over other interests and daily activities, and continuation or escalation of gaming despite the occurrence of negative consequences."

Privacy Problems

Certain online games request permissions to access microphone and webcams

Webcams being a popular hacking target can be controlled remotely by attackers and can be used to exploit.

Ensure that all webcams you use is in "off" state and make use of physical shields in case of built-in camera like a cover or even a piece of opaque tape.

Follow these tips to ensure privacy while connecting online using webcams.

- *Use your webcam only to talk to people you know*
- *Anything you broadcast can never be taken back, and it is available for anyone to see*
- *Unplug webcam when you are not using it*
- *Don't do anything on your webcam that you are uncomfortable with*
- *Predators can hack into your webcam and see what you are doing without your knowing*

Online gaming being evolved with social media allows cyber criminals to manipulate your conversations.

These cyber criminals may try to interact with you personally using chat windows and then start sending personal messages that ask for more details like phone number and emails to get in touch with you or use this information against you.

- Never give away any personal information and use proxy names for usernames
- Avoid using personal information for passwords and maintain different passwords for different accounts.

Online Predators

Online predators try to lure and groom younger children online. They force younger children to send inappropriate messages, webcam chats or even face-to-face meetings that could lead to sexual exploitation.

Through online games these online predators try to build a kind relationship with you by acting as your defender, teammate and ally. After defeating a tough opponent or exploring a new level of a game, predators make their bond stronger with victims and tend to believe

- Keep in mind that people are not always who they say they are.
- Don't talk to anyone who wants to get too personal.
- If someone is flattering you online, you should be wary

How online predators befriend their target

Different types of online predators

Sex Offenders:
These predators are interested in having an explicit online and potentially physical relationship with a child

Sextortioners
Sextortion is a new online epidemic and involves getting teens to send explicit photos, then blackmailing them to send more.

Pornographers
Predators who do not want to meet children offline, only look and collect photos, might not even think what they are doing is wrong.

Hidden Fees

Dangerous online games have many forms and tricks. Some online games give you some content for free, however, for full game features, functions and access app purchases is required.

They offer subscriptions, expanded functionality, virtual currencies, weaponry, special abilities or other accessories through app purchases which popup while you are playing the games.

Online games require users to attach a credit card to their gaming profile. Their card is automatically charged whenever users purchase new items or services.

Once children start playing the game, they may be so involved that they want to reach higher levels for this they may knowingly or unknowingly try to unlock the paid features by using in-app purchases.

- Never give your card number for any free online games. Adjust privacy settings to notify you before you make any app purchases.
- It is a good practice to regularly check your credit card bills to make sure you are not being charged for purchases you did not approve.

Most App stores will have legitimate app uploaded the malicious version. Malware can be hosted by or simply masquerade as a legitimate app.

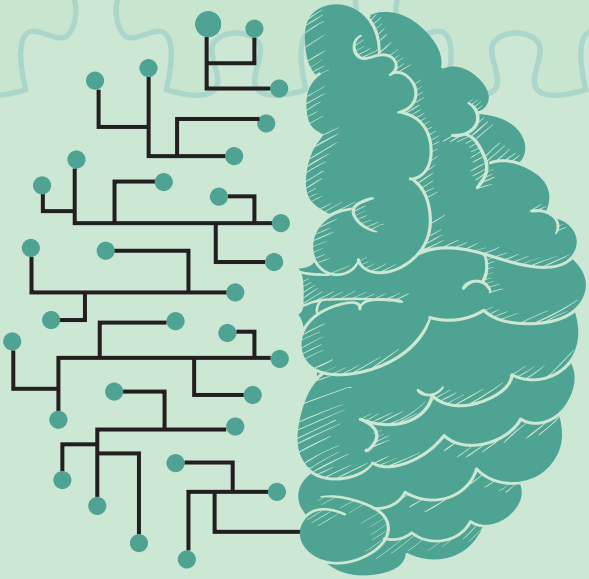
These malwares are designed to infiltrate your device without your knowledge. Adware, spyware, viruses, botnets, Trojans, worms, rootkits and ransomware all fall under the definition of malware

- Pay attention to recent reviews and news stories
- Research the game developers as well as the vendor or marketplace
- Use your cyber security software to scan the files when you download them to your computer or mobile device

Information Security Education & Awareness
www.isea.gov.in

For more details visit :
www.InfoSecawareness.in

Fun with memory games



Memory games can help to improve your child memory while enjoying fun learning activities online. Try everything from remembering patterns to being a detective, matching pictures, following cups, remembering foods, finding numbers, completing sequences and more.

For more information, please visit: www.infosecawarenees.in

Programme by : Ministry of Electronics & Information Technology(MeitY), Govt. of India

Supported by : Ministry of Home Affairs (MHA), Govt. of India

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

www.cyberswachhtakendra.gov.in

CYBER DOST

Cyber Safe GIRL

END NOW FOUNDATION
ADVOCACY ON CYBER SAFETY

For more details / queries on Cyber Security
Call us on our Toll free No.
1800 425 6235

Implemented by
सी-डैक
CDAC

Impersonation

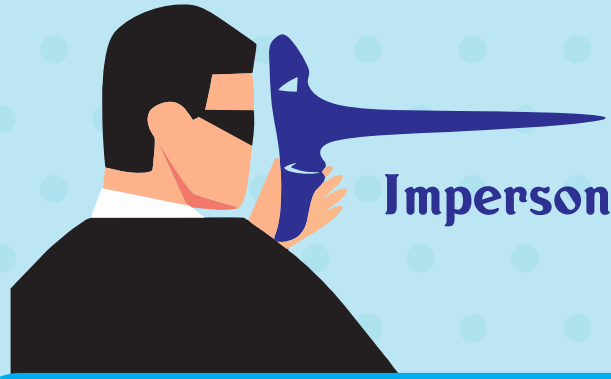
Impersonation - an act of pretending to be another person

Scams done by impersonation are called Impersonation scams.

Children may be inclined towards entertainment means inside the house i.e by using digital devices and Internet. keeping this in view cyber criminals target children and try to trick them through social media, online games and messaging platforms.

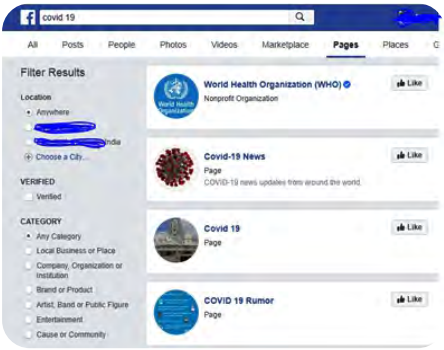
Cyber criminals may use impersonation to trick on the internet users in different ways

- Impersonated profiles in social media
- Impersonated online games



Impersonated profiles social media

Impersonators create fake profiles of well-known people in various fields like sports, actors, singers, Pages about latest issues, etc., For Example: Eager to know the status of COVID- 19, most of us search for the latest updates in social media .



When you search for COVID- 19 updates on facebook, you may end up with a list of profiles with the name COVID- 19. You may feel confused to about which page to follow for genuine updates.

But the official and verified page are highlighted and have a blue tick mark as shown in the figure above. Most of the social media platforms have the feature of blue tick mark to make the users aware of the verified profiles/ groups.

Be careful and wary while following COVID 19 updates or while following your favorite stars in social media platforms as you may end up following the wrong page with wrong information

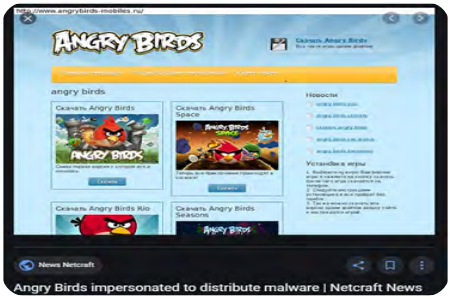
Look for verified profiles to follow any updates on COVID 19

Impersonated Online Games

During the lock down time of COVID-19 most children look for free games online to spend their leisure time.

There are chances that you may come across in free game links which may end up compromising the security.

For example when you do a google search for most loved and popular games, you may notice that there are multiple options of the same game as shown in figure below.



These game links have impersonated the game of angry birds by using the title of the game and the game itself to a great extent .Many impersonated game apps appear to be legitimate.

These games generally carry malwares that can infect your system.

Take assistance of an adult (Parents) to choose and download the right games.

Information Security Education & Awareness
www.isea.gov.in

For more details visit :
www.InfoSecawareness.in

Audio stories for kids

Many online stores with audible range of audio books for children have made its subscription free, especially for children during COVID- 19 lockdown period. During this lockdown, help your child in listening to the classic stories that you may come across by accessing this audio books

For more information, please visit: www.infosecawarenees.in

Programme by : Ministry of Electronics & Information Technology(MeitY), Govt. of India

Supported by : Ministry of Home Affairs (MHA), Govt. of India

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

www.cyberswachhtakendra.gov.in

CYBER DOST

Cyber Safe GIRL

END NOW FOUNDATION
ADVOCACY ON CYBER SAFETY

For more details / queries on Cyber Security
Call us on our Toll free No.
1800 425 6235

Implemented by
सी-डैक
CDAC

Blogging

Blogging is one of the best ways to project ones creativity with a larger audience. It is also useful to share your knowledge in a particular field to position yourself with the competitors in the same field.

Blogs are also an excellent way to build a brand value of your talent.

Posting valuable information in blogs may also help others to learn. It always help in enhancing the educational experience.

Did you Know ?

Over time, blogging evolved into a powerful medium for sharing news, opinions, entertainment, and educational content. Almost everyone today has a personal blog of some sort, whether they keep it private and allow access only to certain people or publish for the whole world to see.

Another method of blogging is video blogging or "vlogging" for short. Vlogging usually happens on a video-sharing platform, like YouTube, where vloggers upload videos that range in topics just like written blogs do.

Interestingly, some of the most popular YouTube channels are the ones featuring children, often supervised and managed by their parents. There are many you tube channels successfully running with many likes and subscriptions

Before you start blogging or v-logging, Let's see, what are the online risks involved in blogging so that you can be safe to blog.

Lets see, How does blogging risk your privacy and safety and also your family privacy ?

Your Blog Itself

You might think that your blog is an unlikely target, but consider the following common motivations for attackers. if you post against any individual, organization, country, your site could be targeted by them

If you blog about anything controversial (current issues, religion, politics, etc.), you may be targeted just for that

Always post right / reliable information common for all in global network. It also helps in reaching as many in Internet.

Follow Internet/ Security ethics to secure your information on blog. One of Internet ethics is avoid using bad or rude language while posting content into blogs

Your site could be targeted just for the fun or challenge of it. Also if you post against any individual, organization, country, your site could be targeted by them

Joke on one blog can have serious emotional and psychological effects on the victim.

Your Personal Privacy & Financial Safety while blogging

Your blog registration :If you have registered your blog, your personal information may be made public for the world to see by default.

The attackers may have enough information on your identity to open fake profile in your name, and spread fake news in your name.

Check the possibility of proxy details at domain registration to avoid threats to your blog.

Restrict personal information in blogs ...may be your proxy name would do the purpose of branding for your blog

Your Personal Safety: As a blogger, your own personal security may sometimes be at risk. The recent surveys show that cyber bullying can also happen to bloggers too. emotional and psychological effects and can ruin the experience of blogging putting your safety at risk.

Cyber bullying or Harassment via comments or in discussion forum of your blogs can have serious emotional and psychological effects and can ruin the experience of blogging putting your safety at risk.

Tell the person to stop, Save the evidence and don't hesitate to reach out for help

Ways to secure your Personal Data as a Blogger

It is true that when it comes to harassment, the victim is never to blame – but there are steps you can take to mitigate the risk of blogging and protect yourself from those with ill intentions.

Use domain privacy

When registering a domain, it is better to use domain privacy. Instead of listing your personal address and contact information in the public database, your host's information will be listed

Create a separate e-mail ID to for creating your own blog

It is a smart to have a mailing address that is separate from your personal email to secure your financial accounts

Secure and backup your website

To protect your site against hackers and malware, it is smart to make sure it is secure and you have a recent backup available to restore if anything goes wrong.

Use unique, secure passwords for every site

Stay safe by using unique, secure passwords for every single account. A password manager service helps.

Use a Separate phone number

As a blogger, you may periodically have the need to give out your phone number to various services, apps, or even clients you deal with. Instead of handing out your home phone or cell phone number, get a separate phone number to give out instead.

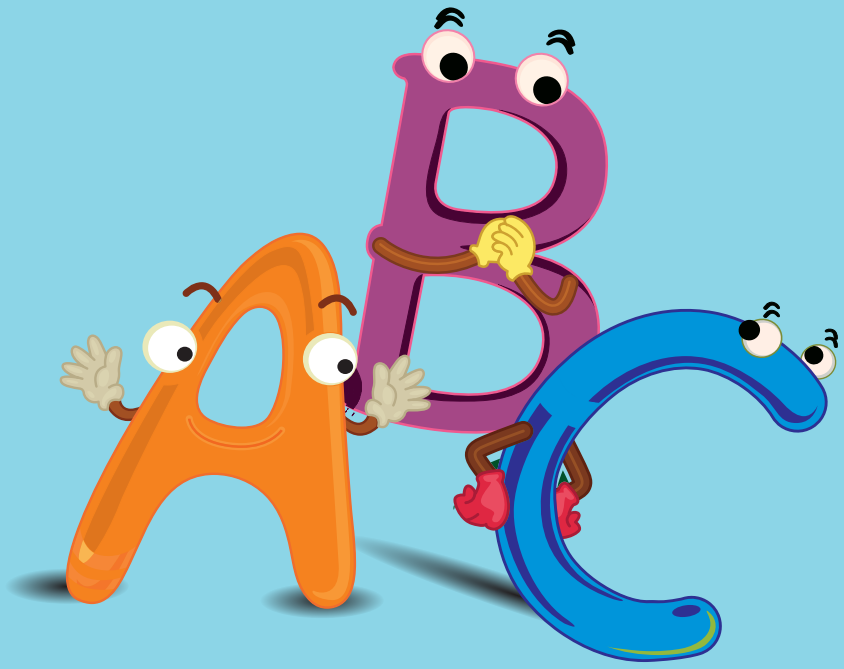
Be careful what you blog about

Be very careful about sharing personal identifying details in your blog posts, including your specific schedule, location, names or details about your family and friends, etc. When sharing stories, consider fudging the details a bit – change dates, names, times, locations, etc.

Information Security Education & Awareness
www.isea.gov.in

For more details visit :
www.InfoSecawareness.in

Fun with Words



Look out for online games or make picture cards which can help to improve your child's vocabulary. These pictures or cards are presented to the player to make a word out of it where the child has to select from a choice of letters to come up with a word. Also can consider interactive puzzles with short animation illustrating the definition and the child has to solve the puzzle to find the word.

For more information, please visit: www.infosecawarenees.in

Programme by : Ministry of Electronics & Information Technology(MeitY), Govt. of India

Supported by : Ministry of Home Affairs (MHA), Govt. of India

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

www.cyberswachhtakendra.gov.in

Cyber Safe GIRL

END NOW FOUNDATION
ADVOCACY ON CYBER SAFETY

For more details / queries on Cyber Security
Call us on our Toll free No.
1800 425 6235

Implemented by
सी-डैक
CDAC

Social Networking during Social Distancing

Social distancing is a public-health protection measure intended to reduce and slow transmission of disease by reducing the probability of contact between people carrying an infection and others who are not infected.

The Corona virus or covid-19 being infectious disease spreading rapidly forced a nationwide lockdown to enforce social distancing in order to stop the spread of the virus and forced people to stay home.

Stay Safe at Social Media @ Home:

To get connected during social distancing, social networking sites are now a primary source for communicating, news/information and keeping in touch with friends and family.

For getting connected, you may tend to share photos, post updates and reveal all sorts of personal information. The visible trail you leave behind might seem meaningless at first.

If your personal information falls into the hands of identity thieves, you may become victim of identity theft.

Remember to post responsibly, to avoid leaving an online identity trail you might later regret.

Social Media is major source of networking, news, information, advertisements, knowledge sharing, playing games etc.,

The lockdown or #StayHome period have shown an increased use of these social media like Facebook, Twitter, Instagram, TikTok, Youtube etc., as people are spending most of the time only on these mediums, the maximum data consuming /using for these applications.

Personal information updated in social media sites could be stolen by cyber criminals, putting your identity at risk.

When you update your status with your whereabouts on a regular basis, you could tip someone off to your routine, and invite real-life threats like robberies, break-ins or stalking.

Avoid Regular updates of your day to day activities in social media

Cyber criminals send emails and messages with links posing as someone you know or could be part of a phishing attack trying to trick you to collect your personal information. These links may contain malware that infects your computer/PC or Mobile.

You could end up giving your login details to hackers and online thieves or your desktop or laptop can get encrypted with Ransomware by downloading an attachment, or clicking a link that hosts a drive-by malware.

Don't click the links which you are getting through social networking sites. If you want to visit the site then directly visit the original websites.

Geotagged photos are photos that have geographical information, like your current location, added to them

Geo-tags can expose where you live, when you are traveling and even what car you drive, which could make you a target for robbery.

Disable geo-tagging feature in your Smartphone's and digital cameras as it automatically geo-tags all your photos unless you turn it off.

Deactivate location services in your phone.

Apps deleted from your account or smart phone may not be fully deleted and may sometimes track your activities

The creator of the app may still have access to your information.

Regularly check applications accessing your messages, camera, contacts and other critical services in your mobile settings.

Hidden files can be traced through specific tools, be cautious while installing apps

You may come across unknown people sharing c interest, If you add "friends" you don't know you may end up in cyber threats like cyber bulling or online harassment

When you add someone unknown to your social network you give access to your personal information, pictures and other details.

Before accepting a friend or follow a request from an unknown person, just go through that person's profile. If you feel the profile is genuine and you would like to get to know the person, then accept the request or else give it a second thought.

Spare some time to change your default privacy settings. Do not post your friends information on networking sites, which may put them at risk.

If you don't have a strong password, others could gain access to your profile and pose as you – and potentially send out spam or fake posts that may damage your reputation

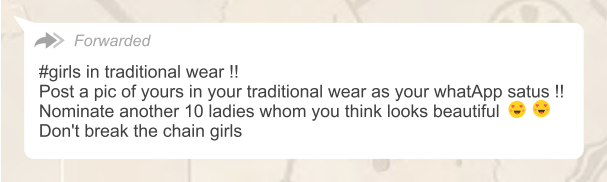
Cyber criminals could gain access to any account with password recovery option available and use any saved information for cyber attacks.

Never share your password with anyone. Use different passwords for different accounts

Social Media Applications / Messengers @Home:

The various messaging apps like WhatsApp, Telegram, FB Messenger, WeChat etc., has shown an increase in usage and the amount of data sharing has drastically increased as most of them including children are using these applications for sharing information, communicate with friends, relatives and their fellow colleagues.

The social media challenges have increased these days, because of the Covid-19 outbreak lockdown, most of the users are online and accepting different types are challenges which are shared by their friends and fellow users in Facebook, Twitter, Instragram and WhatsApp and actively taking part in these type of challenges.



Example : Like sharing your friends picture and tagging other friends whom they want to challenge other friends by sharing their childhood picture, present picture, a picture with a dress code, activity challenge etc., this may lead to unnecessary problems to you and your friends too.

These kind of challenges are made/created by marketing companies to observe the behavior of the users in social media, how people are responding to it. Participating these challenges will also lead to loss of your personal data, identity theft etc.,

Avoid participating in challenges thrown by unknown people. Never share too much personal information like your likes, dislikes, personal photographs, your children pictures, whereabouts etc.,
Never tag your friends or family members in these kind of challenges without their permission.

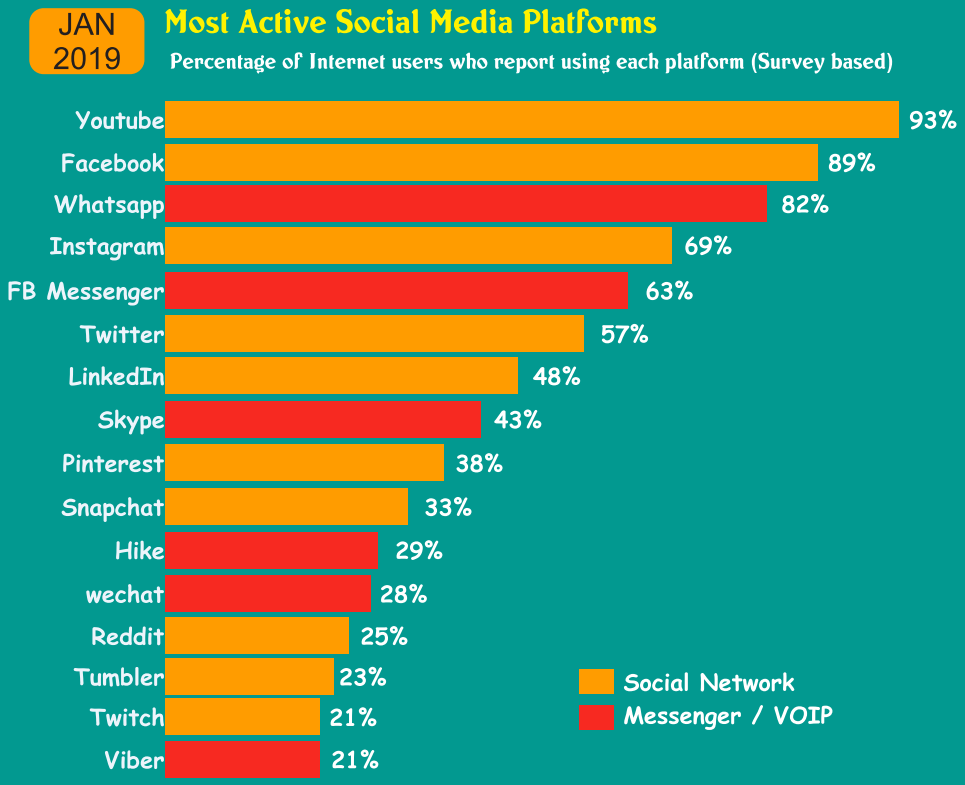
Information Security
Education & Awareness
www.isea.gov.in

www.
InfoSec
awareness.in

Fun with science experiments

Children are born scientists. They always keep experimenting with something, whether they throw glass of water on the floor, blowing bubbles in the bathwater, or stacking blocks into an intricate tower only to destroy it and so on. Similarly you can do some amazing, hands-on science experiments at home using stuff you probably have lying around the house. Many websites provide information regarding simple experiments that can be done at home by kids with the minimum resources.

Below are the few examples of usage of these social media/ messenger application usage:



This picture shows current Active Social media platforms:

Source : https://www.messengerpeople.com/messaging-apps-in-india/

Behavior of the users:

The purpose of Social Media

JAN 2019

Social Media Behaviours

How Internet users engage with social media (survey based)

Visited or used a social network or messaging service in the past month	Actively engaged with or contributed to social media in the past month	Average amount of time per dat spent using social media	Average number of social media accounts per internet user	Percentage of internet users who use social media for work purposes

Behavior of the users: The purpose of Social Media

Source : https://www.messengerpeople.com/messaging-apps-in-india/

Use of Social Media:

JAN 2019

Mobiles Activities

Percentage of Internet users oerforming each activity on a mobile phone each month (survey based)

Percentage of Internet users using mobile messagers	Percentage of Internet users using watching videos on mobile	Percentage of Internet users using playing games on mobile	Percentage of Internet users using mobile banking	Percentage of Internet users using mobile map services

Behavior of the users: Use of Social Media

Source : https://www.messengerpeople.com/messaging-apps-in-india/

Fake Messages

In times of crisis, misinformation or fake news is spreading at an alarming rate creating panic among people on social media platforms. In most of the cases, people actually share fake news just for fun and entertainment.

Fake news spread with a motto of fun

Fake news spread with a motto of fun like few viral fake stories like 'all of it started with bat soup' and celebrities getting tested positive for example like Ronaldo, the pope etc.,.' were created just for fun.

This is an clear example of spreading fake news just for fun.

Fans who believed Ronaldo to be sick and might have shared the post and spread the fake news in social media and given a chance they will be thrilled to shake his hand; Actually he maintained self quarantine as his team-mate tested positive for Coronavirus

Make use of the various fact check websites to check the news circulating in social media platforms

Also there was another fake news spread claiming

Cristiano Ronaldo plans to turn his hotels in Portugal into hospitals for people infected by Coronavirus..... is also fake.

Fake news that can create panic

Fake News works on the fact that, when someone receives any message, most of them first evaluate the information by first comparing with what we are told or have read with our existing beliefs: if it fits, we tend to accept the information.

Fake news takes advantage of reinforcing the prejudices, for example: drinkers believe that alcohol is a cure.

Overcome the initial reaction to fight against fake news. Recognize that whoever is addressing is not trying to manipulate your thoughts.

Use Fact checking websites to know the true news.

Fake news that can create panic, fear inevitably leads to panic, speculation, and the spread of misinformation – and there's a lot of fear in the world right now.

Here are few examples of fake news :

Also there was another fake news spread claiming

Example 1: In India, Twitter timelines and WhatsApp forwards are chock-full of claims that coronavirus can be treated by homoeopathic drugs promoted by the ministry of AYUSH (Ayurveda, yoga & naturopathy, Unani, Siddha, Sowa Rigpa and homoeopathy). Even a fake public advisory was released claiming that homoeopathic drugs can be used for the prevention of infection.

Reference: https://thelogicalindian.com/fact-check/ayush-ministry-coronavirus-20013

However, it was later confirmed as false news by the fact-checking website AltNews. There are no vaccines available to cure coronavirus infection, according to the World Health Organisation (WHO).

Do an online search about the supposed causes, effects, or cures for Covid-19, if you come across any such news..Look out for well-recognised and authorised sources.

Example 2: Fake news with tag line 'Home made remedies to cure coronavirus' like the example given below. In times of such pandemics, the impact of people believing each and every piece of information found online can have severe consequences.

Reference: https://inc42.com/buzz/are-social-media-cos-doing-enough-to-curb-fake-news-around-coronavirus/

Information Security Education & Awareness
www.isea.gov.in

www.InfoSec awareness.in

Fun With Artificial Intelligence (AI)

With schools temporarily shut down and outdoor activities prohibited, artificial intelligence (AI) can offer a solution. Several activities anchored around AI for example: Eliza, a chatbot therapist (https://web.njit.edu/~ronkowit/eliza.html) or similar other AI tools, can keep children engaged, entertained and also help them learn.

For more information, please visit: www.infosecawarenees.in

Programme by : Ministry of Electronics & Information Technology(MeitY), Govt. of India

Supported by : Ministry of Home Affairs (MHA), Govt. of India

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

www.cyberswachhtakendra.gov.in

Cyber Safe GIRL

END NOW FOUNDATION ADVOCACY ON CYBER SAFETY

For more details / queries on Cyber Security Call us on our Toll free No.
1800 425 6235

Implemented by
सी-डैक CDAC

Children should know to detect fake news and photos

The different forms of misleading information that your child might encounter include:

- Hoaxes such as the Momo Challenge and the oft-reported stories
- User-generated 'factual' content in internet searches which are not correct and may be accepted by many children.
- News outlets that have a political bias.
- Blogs and vlogs, such as on YouTube, where a person's opinions are presented as fact.
- Outdated information, for example news stories dating back several years.
- Social media, where people often share stories without checking if they are true.

Fun with Online learning:
Look out for free educational learning sites, with massive online learning resources like creative and inspiring videos, math's and science practice questions, materials/books etc., can be downloaded for free.

Fun with coding for kids:
Basic programming has become an essential skill for grown-ups and children alike. The benefits of picking up this skill, especially for kids, are huge: Learning how to build simple websites and games helps kids refine their design, logic, and problem-solving abilities. It also allows them to express ideas and creativity in unique ways. Choose one of the 'teaching coding apps' which are free for your child to spend the lockdown period effectively.

There are lots of cool, interactive ways for children to enjoy the lockdown period ....

How to spot fake news

- **Look closely at the source.** Fake news creators are good at what they do. While some content has detectable errors, others are sophisticated and strangely persuasive. So, take a closer look. Test credibility by asking:
  - *Where is the information coming from?*
  - *is the author of article an expert on the topic, and is the website legitemate ?*
  - *Are studies, infographics, and quotes appropriately attributed?*
  - *Is the URL legitimate (cnn.comvs. cnn.com.co)?*
  - *Are there red flags such as unknown author, all capital letters, misspellings, or grammar errors?*
- **Be discerning with viral content.** Often a story will go viral because when it is unbelievable. So pause before you share. Google the story's headline to see if the story appears in other reliable publications.
- **Pay attention to publish dates, context.** Some viral news items may not be entirely false, just intentionally shared out of context. Fake news creators often pull headlines or stories from the past and present them as current news to fit the desired narrative.
- **Beware of click-bait headlines.** A lot of fake news is carefully designed with user behavior in mind.
- A juicy headline leads to a false news story packed with even more fake links that take you to a product page or, worse, download malware onto your computer, putting your data and privacy at risk.
- **Verify information.** It takes extra effort, but plenty of sites exist that can help you verify a piece of information. Before sharing that a piece of content, check it out on sites like:
  - *Snopes.com*
  - *Factcheck.com*
  - *Politifact.org*
  - *Opensecrets.org*
  - *Truthorfiction.com*
  - *Hoaxslayer.com*

Supported by

सत्यमेव जयते
गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

mygov
मेरी सरकार

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

CYBER DOST

NIC एनआईसी
National Informatics Centre


Subscribe us at
/c/InformationSecurityEducationandAwareness


Follow us at
/InfoSecAwa


Connect us with
/infosecawareness


Follow us at
/infosec_awareness

About ISEA

Looking at the growing importance for the Information Security, Ministry of Electronics & Information Technology has identified this as a critical area. Information Security Education and Awareness (ISEA) Project was formulated and launched by the Govt. of India. One of the activities under this programme is to spread Information Security Awareness among children, teachers, home users, IT and non-IT professionals throughout the country. C-DAC Hyderabad has been assigned the responsibility of executing this project by Ministry of Electronics & Information Technology, Government of India. As part of this activity C-DAC, Hyderabad has been preparing Information Security Awareness material, coordinating with Participating Institutes (PI's) in organizing the various Information Security Awareness events all over India.

To Share Tips / Latest News, mail us to
isea@cdac.in

ISEA Whatsapp Number for Incident Reporting
+91 9490771800
between 9.00 AM to 5.30 PM

For queries on Information security
Call us on Toll Free No.
1800 425 6235

सत्यमेव जयते
Ministry of Electronics &
Information Technology,
Government of India

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 Raviryal (V & GP), Via Ragaanna guda, Maheshwaram (M), Ranga Reddy District, Hyderabad – 501510. Tel: 9248920201.