

# **Be Safe on Cyber Space**

Gajendra Deshpande,  
KLS Gogte Institute of Technology, India

<https://gcdeshpande.github.io>

# Outline of the Talk

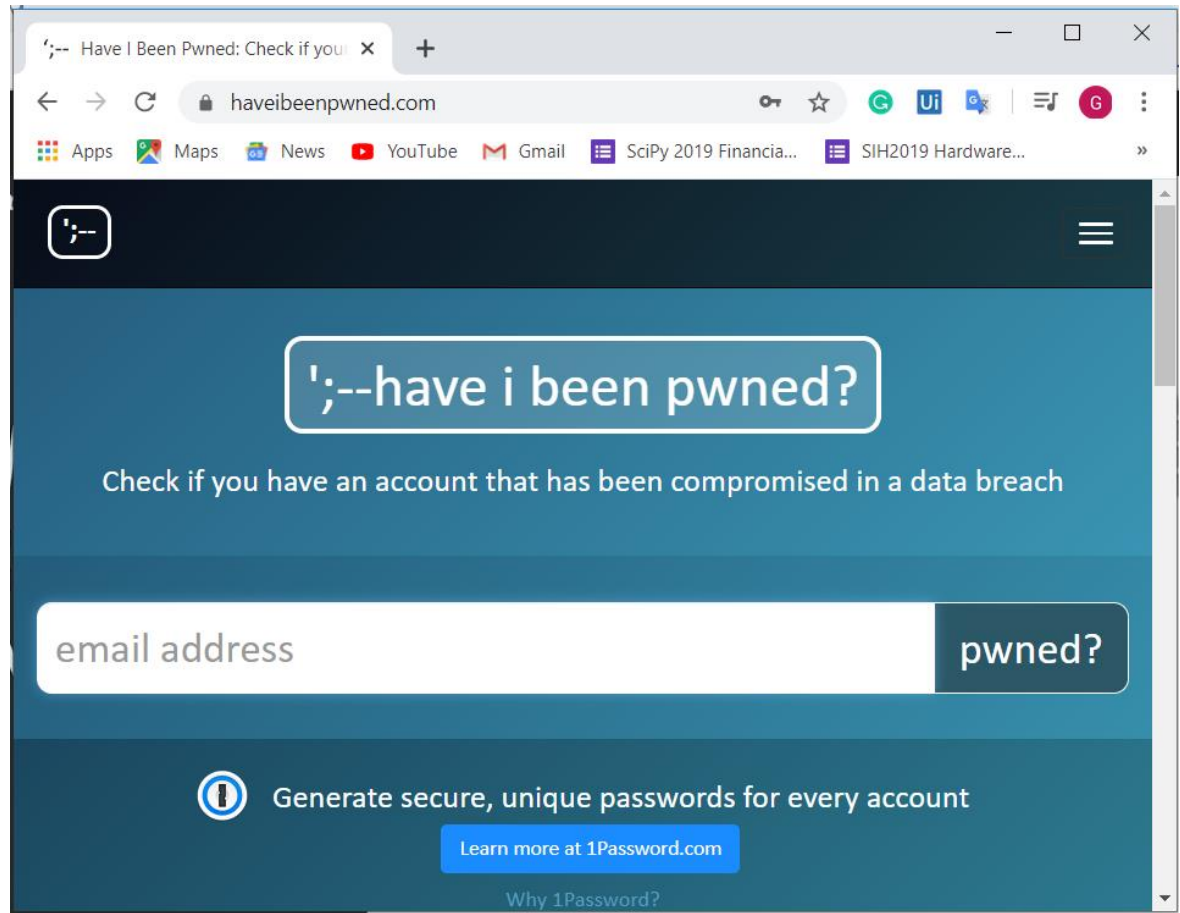
- ▣ Cyber Crime Statistics
- ▣ Passwords: Good and Strong Password
- ▣ E-Mails- Do's and Don't's
- ▣ Social Networking
- ▣ Chatting
- ▣ Safe Downloads
- ▣ ATM Safety Tips

# Cyber Crime Statistics

- The Internet Crime Report for 2019, released by USA's Internet Crime Complaint Centre (IC3) of the Federal Bureau of Investigation, has revealed that India stands third in the world among top 20 countries that are victims of internet crimes.
  - USA-4,67,361; UK-93,796; India-27,248 (2018 data)
- According to RSA report (2015), mobile transactions are rapidly growing and cyber criminals are migrating to less protected 'soft' channels.
- According to report by Norton (2015), an estimated 113 million Indians lost about Rs. 16,558 on an average to cybercrime
- According to an article published in Indian Express on 19<sup>th</sup> November 2016, *Over 55% Millennials in India Hit by Cybercrime.*

# Passwords

- ❑ Strong Password
- ❑ Two Factor Authentication
- ❑ One Time Login
- ❑ Social Engineering




<https://www.haveibeenpwned.com>

# Good and Strong Password

- ❑ Use at least 8 characters or more to create a password. The more number of characters we use, the more secure is our password.
- ❑ Use various combinations of characters while creating a password. For example, create a password consisting of a combination of lowercase, uppercase, numbers and special characters etc..
- ❑ Avoid using the words from dictionary. They can be cracked easily.
- ❑ Create a password such that it can be remembered. This avoids the need to write passwords somewhere, which is not advisable.
- ❑ A password must be difficult to guess.
- ❑ Change the password once in two weeks or when you suspect someone knows the password.
- ❑ Do not use a password that was used earlier.
- ❑ Be careful while entering a password when someone is sitting beside you.
- ❑ Do not use the name of things located around you as passwords for your account.

# E-Mails

STRICTLY AND CONFIDENTIAL.

 This message was identified as junk. We'll delete it after 6 days. [It's not junk](#)



Mr.Sal Kavar <salkavar2@gmail.com>  
Mon 9/14/2020 4:27 PM



Dear friend.

I assume you and your family are in good health. I am the Foreign operations Manager at one of the leading generation bank here in West Africa.

This being a wide world in which it can be difficult to make new acquaintances and because it is virtually impossible to know who is trustworthy and who can be believed, i have decided to repose confidence in you after much fasting and prayer. It is only because of this that I have decided to confide in you and to share with you this confidential business.

In my bank; there resides an overdue and unclaimed sum of \$15.5m, (Fifteen Million Five Hundred Thousand Dollars Only) When the account holder suddenly passed on, he left no beneficiary who would be entitled to the receipt of this fund. For this reason, I have found it expedient to transfer this fund to a trustworthy individual with capacity to act as foreign business partner. Thus i humbly request your assistance to claim this fund.

Upon the transfer of this fund in your account, you will take 45% as your share from the total fund, 10% will be shared to Charity Organizations in both country and 45% will be for me. Please if you are really sure you can handle this project, contact me immediately.

Yours Faithful,  
Mr.Sal Kavar.

Your **AppleID** has been locked - Current changes were made from Ontario. Receipt Order: 57080537



Apple <kuchongmogunielsanahmsmev@feasgea.com>

Tue 10/13/2020 4:35 PM

To: no-reply.41574929@web.appnNetflix.com



Dear Customer

Here your number of cases is : 864846338

We've noticed that some of your account information appears to be missing or incorrect, your iCloud will be blocked until we receive a response from you. We need to verify your account information to continue using iCloud in 24 hours

[Verify your account >](#)

**Apple** Support

---

[Apple ID](#) | [Support](#) | [Privacy Policy](#)

Copyright 2020 **Apple** Inc.

One **Apple** Park Way, Cupertino, CA 95014, United States

All rights reserved.

Activate Windows  
Go to Settings to activate Windows.

# E-Mails – Do's and Don't's

- ❑ Use e-mail filtering software to avoid spam so that only messages from authorized users are received. Most e-Mail providers offer filtering services.
- ❑ Do not open attachments coming from strangers, since they may contain a virus along with the received message.
- ❑ Be careful while downloading attachments from e-Mails into your hard disk. Scan the attachment with updated antivirus software before saving it.
- ❑ Do not send messages with attachments that contain executable code like Word documents with macros, .EXE files and ZIPPED files. We can use Rich Text Format instead of the standard .DOC format. RTF will keep your formatting, but will not include any macros. This may prevent you from sending virus to others if you are already infected by it.
- ❑ Avoid sending personal information through e-Mails.
- ❑ Avoid filling forms that come via e-Mail asking for your personal information. And do not click on links that come via e-Mail.
- ❑ Do not click on the e-Mails that you receive from un trusted users as clicking itself may execute some malicious code and spread into your system.

# Social Networking

- ❑ Everything is permanent and your social profile is an extension of yourself. Be cautious. Be sensible
- ❑ Whatever you post online are permanent (this includes texting!) Private is not always private. The photo you post online is not owned by them anymore. The rights of the photo get transferred to the social channel once it is uploaded.
- ❑ Every choice you make reveals your character.
- ❑ Try to be kind, not popular.
- ❑ Social media should supplement your relationships, not replace them.

# Social Networking – What's not Safe?

- ❑ Share personal information online. Personal information includes full name, date of birth, home address, school address, email, parent's details, etc.,
- ❑ Post pictures of yourself and others online.
- ❑ Talk with strangers online and offline.
- ❑ Share location online to strangers

# Social Networking – Potential Risks

- ❑ Exposure to harmful or inappropriate content (e.g., sex, drugs, violence, etc.)
- ❑ Exposure to dangerous people
- ❑ Cyber bullying, a risk factor for depression and suicide
- ❑ Oversharing personal information
- ❑ Exposure to excessive advertisements
- ❑ Privacy concerns including the collection of data about teen users
- ❑ Identity theft or being hacked
- ❑ Interference with sleep, exercise, homework, or family activities

# Chatting

- ❑ Never open, accept, or download a file in IM from someone you don't know.
- ❑ If the file comes from someone you don't know, don't open it unless you know what the file is.
- ❑ Contact the sender by e-mail, phone, or some other method to confirm that what they sent was not a virus.
- ❑ Visit Microsoft Update to scan your Windows computer and install any high-priority updates that are offered to your PC.
- ❑ If you have Automatic Updates enabled, the updates are delivered to you when they are released, but you have to make sure you install them.
- ❑ Similarly, the concern software patches from Linux OS also need to be updated
- ❑ Use up-to-date version of your Instant Messenger software for a better protection of your computer against viruses and spyware.
- ❑ If you're using MSN Messenger, upgrade to Windows Live Messenger, which will block attachments that might contain malware and allow you to scan attachments for viruses.

# Chatting

- ❑ Similarly for other Instant Messengers like WhatsApp should be upgraded.
- ❑ Like e-mail viruses, instant message viruses are malicious programs that are designed to travel through IM.
- ❑ Spim is a short form of spam over instant messaging, it uses IM platforms to send spam messages over IM. Like e-mail spam messages, a spim message also contains advertisements. It generally contains web links, by clicking to on those links malicious code enters into your PC.
- ❑ Antivirus software can help to detect and remove IM viruses from your computer, only if you keep the antivirus software up-to-date.
- ❑ If you've purchased a subscription from an antivirus software company, your antivirus software may update itself when you're connected to the Internet.
- ❑ Antispyware software can help to protect your computer from spyware and remove any spyware you may already have.
- ❑ If you don't have antispyware software, you can download Windows Defender.

# Safe Downloads

- ❑ While downloading any file close all the applications that are running on your computer, let only one set-up file run at a time of downloading.
- ❑ Close all the important applications in order to be safe if something goes wrong while downloading.
- ❑ Set firewalls, set antivirus to actively scan all the files you download.
- ❑ Scan all the files after you download whether from websites or links received from e-mails.
- ❑ Always use updated antivirus, spam filter and spyware to help detect and remove virus, spyware from the application you want to download.
- ❑ Never download any files like music, video, games and many more from untrusted sites and don't go by the recommendations given by your friends or made by any random website's comments.
- ❑ Check that the URLs are same and always download games, music or videos from the secure websites like which use HTTPS websites instead of HTTP. In the web address, it replaces "http" to https". The https refers to the hypertext transfer protocol secure.

# Safe Downloads

- ❑ Download anything only from trust worthy websites. Don't click links to download anything you see on unauthorized sites.
- ❑ If any dirty words appear on the website just close the window no matter how important it is, because spyware may be installed on your PC from such websites.
- ❑ Check the size of the file before you download, sometimes it shows a very small size but after you click it increases the size of the file.
- ❑ Never believe anything which says click on this link and your computer settings will be changed and your PC can be turned into XBOX and can play unlimited games on your computer.
- ❑ Don't accept anything that offers you free download because that may contain malicious software.
- ❑ Don't click the link or file and let it start download automatically, download the file and save where you want save and then run on the application.

# Safe Downloads

- ❑ Set secure browser settings before you download anything.
- ❑ Read carefully before you click on install or run application. That means read terms and conditions.
- ❑ Don't download anything until you know complete information of the website and know whether it is an original site of an original company.
- ❑ Never download from the links that offer free antivirus or anti spyware software, always download from trusted sites, if you are not sure about the site you are downloading, enter the site into favourite search engine to see anyone posted or reported that it contains unwanted technologies.

# ATM Safety Tips

- ❑ Enable your mobile phone number and e-mail with your banking transactions for timely SMS and e-mail alerts.
- ❑ Your Financial Institution or Bank will never send you an e-mail asking you to enter your Banking details online.
- ❑ Check regularly your credit card or bank account details and keep track of your transactions.
- ❑ Update your details such as change of address for receipt of cheque books, statements, debit /credit cards at the right address.
- ❑ For protecting phishing attacks, your browser should be enabled with phishing filters and never click links in your e-mail for updating and transactions.
- ❑ Keep a strong and easy to remember password and change it regularly .
- ❑ Vishing is a form of phishing, where instead of people receiving an email trying to lure them into giving personal information, the criminal uses a phone call, either live or automated, to attack the bank or credit union customer and get critical information.

# ATM Safety Tips

- ❑ Try to restrict yourself from giving personal information when you receive a call from a Bank or Credit Card Provider.
- ❑ Look for a "no tampering" sign. Crooks often place these to stop anyone curious about a new piece of equipment.
- ❑ Steer clear of a jammed ATM machine that forces customers to use another ATM that has a skimmer attached. Often, the criminal will disable other ATMs in the area to draw users to the one that has the skimming device on it.
- ❑ Customers should check their bank accounts regularly to make sure there are no unusual or unauthorized transactions. Federal law limits loss from ATM fraud and many banks offer additional protection. Consumers should check with their financial institution for details.
- ❑ If you see anything unusual or suspicious around an ATM, or if you find unauthorized ATM transactions on your bank account, immediately notify local law enforcement, as well as your financial institution and/or the establishment where the ATM is located.
- ❑ Always protect your PIN: Don't give the number to anyone, and cover the keypad while you are entering your.

# Secure Your PC

- ❑ Update OS
- ❑ Install an antivirus product and keep up to date
- ❑ Enable Computer Firewall
- ❑ Use Strong Passwords

# Online Banking

- ❑ Never click web links in your e-mail and no bank will ask you to update the accounts through online.
- ❑ Never provide personal information including your passwords, credit card information, account numbers to unknown persons.
- ❑ Never keep username, account name and passwords at one place. Always try to remember passwords.
- ❑ Always use phishing filters at your Internet browser.
- ❑ Do not click any images in the web sites if you are unsure.
- ❑ Confirm whether email is received from bank or not.

# Online Banking

- ❑ Be cautious while providing bank details via online, before proceed further confirm with bank about the email you received. Think that if something is important or urgent why don't bank calling me instead of sending email?
- ❑ Delete all cookies and history file before you perform online trasactions.
- ❑ Always use virtual keyboard while accessing online banking.
- ❑ Delete all the history and cookies once you are done with online transactions.
- ❑ Avoid accessing online banking in cybercafes.

# Copyrights- Do's and Don't's

Copyright refers to a form of intellectual property that gives the author of an original work exclusive right for a certain time period in relative to that work, including its publication, distribution etc. Copyright is described under the umbrella term intellectual property along with rights and trade name.

Or

Copyright refers to laws that authorize the use of the work of a creator, such as author, artist, and many more. This includes copying, distributing, altering and literary and other kind of work. Unless stated in a contract, the author or creator of any work holds the copyright.

# Copyrights- Do's and Don't's

- Copyright can/to apply for any work, it must be an original idea or literature that is put to use. The idea alone cannot be protected by copyright. It is the physical use of that idea, such as a design or a written novel, which is covered under copyright law.
- Copyright also includes for wide range of creativity like intellectual, scientific, artistic form of works which also includes poems, composition of songs, music, videos, dances, sculptures, software, and many more specifically vary by concern authority or jurisdiction.
- Copyright is given to the author according to the law, as soon as he completes his work.
- In order to protect your own work and idea you need to register the work in the copyright office.
- Many copyright law infringing copies of entertainment files e.g. MP3 music files, VCD video files and etc. and software are often shared by P2P software.
- The act of unauthorized uploading of a copyright works for others to download may attract civil or even criminal sanctions. Unauthorized downloading of copyright works entails civil liability.

# Copyrights- Do's and Don't's

- ❑ Do not copy copyrighted software without author's permission.
- ❑ Always respect copyright laws and policies.
- ❑ Computer ethics is set of moral principles that govern the usage of computers.
- ❑ The common issues of computer ethics is violation of copyright issues.
- ❑ Duplicating the copyrighted content without the authors approval accessing personal information of others are some of the examples that violate ethical principles.
- ❑ Be aware of copyright issues while using online information.

# Public Computers

- ❑ Never pass or tell the Cyber Cafe Owner or anyone else in Cyber Cafe about your email and password to check your e-mail. This may sound little bit odd but the surveys saying that small kids or many old aged persons have no idea about the risks of information theft. Username and passwords always be entered by their owners and at most you may request for guidelines to reach login page.
- ❑ If you store or download any personal information on Desktop in cyber cafe make sure you delete all the documents after your done with your work.
- ❑ When surfing the Internet, you always should check about the browser security to avoid risks of exposing personal information such as disabling the option “Remember my ID on this computer”. User ID or Username also should be secured along with password to avoid trail passwords by next user.
- ❑ A keylogger is basically spyware and logs or records your keystrokes so that your username and password are made available to Cyber cafe owner or any Attacker. These records may types into directly into Hacker’s machine or collected afterwards through a file transfer. Some of Cyber Cafes may use Hardware key loggers so that you check that there is an intermediate device between your keyboard and CPU.

# Public Computers

- ❑ Cyber Cafe computers are public computers and shared computers. Your data or communication may be exposed to all users at the same time. So be aware that sensitive information like personal details like username, passwords etc. should be deleted.
- ❑ Whenever you go to Cyber Cafe, you ensure that it has most up to date Anti Virus and Anti spam software. These may help to stop some of the key loggers, Trojans and other malware.
- ❑ Don't leave the computer unattended with sensitive information on the screen.
- ❑ Disable the feature that stores passwords.
- ❑ Don't enter sensitive information into a public computer.
- ❑ Force Cyber Cafe Owner to allocate you a computer loaded with updated antivirus software.
- ❑ Finally, Always make sure to logout properly when you leave Cyber cafe.

# Credit cards- Do's and Don't's

- ❑ Be cautious while using the creditcard.
- ❑ Dont give your credit card pin number to unknown persons.
- ❑ Avoid sending credit card details through e-mails.
- ❑ Dont write pin number on the credit card, try to remember it.

# Credit cards- Do's and Don't's

- ❑ Be cautious while using the credit card.
- ❑ Don't give your credit card pin number to unknown persons.
- ❑ Avoid sending credit card details through e-mails.
- ❑ Don't write pin number on the credit card, try to remember it.

# Mobile Devices- Do's and Don't's

- ❑ Be careful while downloading applications through Bluetooth or as MMS attachments. They may contain some harmful software, which will affect the mobile phone.
- ❑ Keep the Bluetooth connection in an invisible mode, unless you need some user to access your mobile phone or laptops. If an unknown user tries to access the mobile phone or laptop through blue tooth, move away from the coverage area of blue tooth so that it automatically gets disconnected.
- ❑ Avoid downloading the content into mobile phone or laptop from an untrusted source.
- ❑ Delete the MMS message received from an unknown user without opening it.
- ❑ Read the mobile phone's operating instructions carefully mainly regarding the security settings, pin code settings, Bluetooth settings, infrared settings and procedure to download an application. This will help in making your mobile phone secure from malicious programs.
- ❑ Define your own trusted devices that can be connected to mobile phone or laptop through Bluetooth.

# Mobile Devices- Do's and Don't's

- ❑ Activate the pin code request for mobile phone access. Choose a pin, which is unpredictable and which is easy to remember for you.
- ❑ Use the call barring and restriction services provided by operators, to prevent the applications that are not used by you or by your family members.
- ❑ Don't make you mobile phone as a source for your personal data, which is dangerous if it falls in to the hands of strangers. It is advisable not to store important information like credit card and bank cards passwords, etc in a mobile phone.
- ❑ Note the IMEI code of your cell phone and keep it in a safe place. This helps the owner to prevent access to the stolen mobile. The operator can block a phone using the IMEI code.
- ❑ Regularly, backup important data in the mobile phone or laptop by following the instructions in the manual.
- ❑ Use free cleansing tools, which are available in the Internet to make your mobile work normally, when ever it is affected by malicious soft wares.

# Blogging- Do's and Don't's

- ❑ Never give away your personal information into the blogging sites
- ❑ Put reliable information as it reaches entire world and assume what you publish on the web is permanent.
- ❑ Avoid competition with other bloggers.
- ❑ State the terms of use, copy right in blog properly to viewers to protect your blogs.
- ❑ Guide them with other positive examples such as the children are posting their related information.
- ❑ Post anonymously: Manage your blog anonymously or adopt an alias for all online posting. This will help protect you in the event that you draw unwanted attention
- ❑ Avoid personal or identifying details: Avoid any personal or identifying details when posting in your blog. Do not post in advance about locations that you will be or about areas that you live near

# Blogging- Do's and Don't's

- ❑ No photos: Refrain from posting a picture. Photos can invite trouble or unwanted attention.
- ❑ Avoid inappropriate dialogue: Be careful not to engage in dialogue that could be interpreted in a way that it was not intended. Sometimes humorous threads can get out of hand. If the dialogue degrades to an area that makes you uncomfortable, disengage from the dialogue and refrain from further posting. Also when making decisions about individuals online, consider their past posting behaviour and attempt to consider their true intentions
- ❑ Always remember that just because you do not have a dialogue with someone does not mean that they are not reading everything that you write. Many people merely lurk on line and don't engage in comment posting, but do read what is written. Your audience could be much larger than you realize
- ❑ Timeless: Internet content is timeless, and keep in mind that even if you remove content, it might be archived or syndicated. If you do not want something read, do not post it to the Internet. High Schools, Colleges and Employers all search the Internet to discern an individual's history. Sordid details about a late night will not help land a coveted job

# Blogging- Do's and Don't's

- The internet is a haven for all types of predators. Always remember that just because someone says something is true, does not mean that it is. Predators adopt personas of who they think you want them to be. Just as we provide guidelines to young children, adults should be wary and take precautions when posting online as well
- While blogging can be a great outlet and channel, and in some way immortalizing thoughts, it is important that safety is considered and that good blogging practices are followed at all times.



## National Cyber Crime Reporting Portal



!w Feature "Citizen Financial Cyber Fraud Reporting and Management System" has been activated for prevention of money loss in case of Cyber Financial Fraud, For immediate reporting ,Call

HOME

REPORT WOMEN/CHILD RELATED CRIME

REPORT OTHER CYBER CRIME

CYBER VOLUNTEERS NEW

RESOURCES

CONTACT US

HELPLINE

### Filing a Complaint on National Cyber Crime Reporting Portal

This portal is an initiative of Government of India to facilitate victims/complainants to report cyber crime complaints online. This portal caters to complaints pertaining to cyber crimes only with special focus on cyber crimes against women and children. Complaints reported on this portal are dealt by law enforcement agencies/ police based on the information available in the complaints. It is imperative to provide correct and accurate details while filing complaint for prompt action.

Please contact local police in case of an emergency or for reporting crimes other than cyber crimes. National police helpline number is 100. National women helpline number is 181.

Learn about cyber crime

File a complaint

Media Gallery

Cyber Awareness

Internet Safety Tips for Kids

Tweets by @Cyberdost

Activate Windows  
Go to Settings to activate Windows

Browser tabs: ADSA, W3Schools, JavaScript, jQuery, Advice, Cyber Crime, cyber Safe, brochure 3, Job Fraud, final.cdr, New browser, Cyber Security, You are, Mobile, Info X, Live stream.

Address bar: <https://www.infosecawareness.in>

Toll Free Number : 1800 425 6235

Select Language: A- A A+

Search

Children Student Women Family Police Teacher Govt Employee System/Network Admin

# InfoSec depot 2019

Download now

- INDULGE WITH ISEA
- YOU & ME
- FOREFRONT
- GO MOBILE
- SOCIAL MEDIA SECURITY
- MALWARE REVIEWED
- CYBER INVASION
- CYBER BUNKER
- REINFORCE
- CODEGEEK
- CRITICAL INFRASTRUCTURE SECURITY
- CYBER INVESTIGATIONS AND CYBER FORENSICS

## Security Awareness COVID-19 Tips

Not all cold and cough are symptoms of COVID-19. Get proper information from genuine sources

Not all free antivirus software protect your systems. Install genuine paid antivirus software and protect your systems

See more

### ANNOUNCEMENTS

Essay Writing Competition Results - State Level

Click here to view advisories on cyber security

Tip of day

 **WORKSHOPS 280**  
**PARTICIPANTS 19557**

 **WORKSHOPS 716**  
**PARTICIPANTS 78609**

 **WORKSHOPS 43**  
**PARTICIPANTS 10276**

### Latest Events

JAWAHARA NAVODAYA VIDYALAYA, CHAMARAJA NAGARA

**Cyber Safety: Keeping Children Safe Online**

Presented by: X ABUL DHANNA SINGH PGT MATINS

26.09.2020

### Latest News

- » Banking industry a "target of choice" for cyberattacks during Covid-19: RBI
- » Hardware Security Hackathon by IIT Kharagpur in association with DSCI & ISEA Project Phase-II
- » ISEA Virtual Presentation Conclave

### Facebook

Information Security...

Like Page

Tip of the Day 05 November 2020

### Twitter @InfoSecAwa

Pick a sentence that reminds you of password ( passphrase )

For example !Au\$pr1m123D

Always use Strong Password for mv 123 Downloads

Activate Windows Go to Settings to activate Windows.

Type here to search

3:13 PM 11/5/2020

Thank You!

# Widescreen Test Pattern (16:9)

## Aspect Ratio Test

(Should appear  
circular)

4x3

16x9

