Digital India
Power To Empower

Government of Maharashtra

आपले सरकार

CYBER SECURITY
AWARENESS GUIDE

An Aaple Sarkar Initiative

Devendra Fadnavis
Chief Minister
Maharashtra

Message from the Hon. Chief Minister

We are living in a world where billions of computers and devices are interconnected. This interconnection is being used for virtually every aspect of modern life and even the global economy itself has huge dependence on the same. In our Maharashtra, we are working towards building digital infrastructure, smart connected cities, digital villages and e-Governance services, in line with the vision laid down by our Hon'ble Prime Minister to transform India into a Digitally Empowered Society and Knowledge Economy.

With the growing cyber population, cyber security has become a major concern over the past couple of years and the Government has continually increased its focus in this domain. However, the Government alone cannot protect from the threats that come along and therefore need help from all citizens of the state to make smart and safe online decisions. With this thought process in mind, we have embarked on a cyber-security awareness journey.

I strongly believe that the real future of the nation lies in the hands of the children and therefore our first priority is nurturing and educating our young population of the state, on the cyber security practices. In line with the same we have prepared this brief material on cyber security awareness.

I hope this booklet would be of use to our young citizens. Wishing you all a happy and successful future.

(Devendra Fadnavis)
Chief Minister, Government
of Maharashtra

Tel. : 022-2202 5151/2202 5222, **Fax :** 022-2202 9214
E-mail : cm@maharashtra.gov.in, **Website :** www.maharashtra.gov.in

S. S. Kshatriya
Chief Secretary

Chief Secretary's Office
Hutatma Rajguru Chowk,
Madame Cama Marg,
Mantralaya, Mumbai-32.

Date : 11th August 2016

MESSAGE

The rate at which information is transmitted and consumed has increased exponentially and so has our dependence on Information and Communication Technologies (ICT). We are using computers, smartphones and internet in our daily lives for communication (e-mail), entertainment (digital audio, video etc.), transportation (car engine systems, navigation for flight), electronic shopping, online banking, medical equipments and the list goes on.

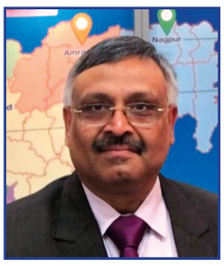
This has led to an increasing concern to ensure a secure cyber space. Over the years, the Government has been evolving its approach to keep pace with the changing nature of the cyber threat landscape. One of the key aspects for securing ourselves is enhanced awareness about these cyber threats.

Through this booklet, we intend to reach out to younger generation in schools across Maharashtra to inform them on new-age threats and also on the precautions to be taken for avoiding them.

I am sure that this exercise would be helpful in generating awareness among school children.

(S.S. Kshatriya)

Tel. (O) 022-2202 50 42 / 2202 87 62, Fax : 2202 85 94, E-mail : chiefsecretary@maharashtra.gov.in



FOREWORD

Just couple of decades ago, our understanding of the earth eco-system, in which we live, came only from the geography books wherein the description of the layers of the Earth's Atmosphere – the troposphere, the stratosphere, the mesosphere, the thermosphere and the exosphere – gave us key inputs on how life is sustained on this planet. We all now acknowledge the existence of 'Digitosphere' which invisibly cuts across all the hitherto known layers impacting almost everything from personal lives, education, health, business and trade, physical infrastructure, governance to national security. Information and communications technologies have become indispensable to the modern life. Today we critically depend on information and communications infrastructure in governing our personal lives, our societies, conducting business, running critical infrastructure and exercising our rights and freedoms as citizens.

In this era of a globally connected social, economic, political and governance sub-systems supported by a complex mosaic of electronic information systems and data infrastructure, cyber security has vaulted to the highest echelon of security concerns. Cybersecurity threats and related risks are rapidly evolving with the evolution of technology. Cloud computing, mobile computing, applications based computing, e-payment systems, mushrooming growth of sensors and increasing interconnection of smart devices (called 'Internet of Things') individually brings its own security issues. Threats get magnified as infinite supply of data becomes more integral to a wider array of personal, social, business functions. The growing use of personal handheld 'smart' devices personal handheld in various components of smart cities are in parallel increasing the security threat levels for each of us.

Every day, all around the world, thousands of IT systems are comprised. Some are attacked purely for the kudos of doing so, others for social, economic and political disruption motives perpetrated by professional cybercrime organizations, social hacktivists or even financially sponsored group for targeted attacks. While governments, businesses and professionals around the world are continuously devising strategies and developing tools to minimise the damages, it is universally being acknowledged that **the most important component of**

cybersecurity is awareness - knowing that threat exists and we need to secure our devices and data. Many of these cyber-attacks can be avoided with heightened awareness amongst citizens. A large section of the current cyber world population is our young citizen pool of students in school.

This first booklet is the stepping stone for the Cyber Security Awareness initiative undertaken by the Government of Maharashtra for its young population. The focus is on sowing seeds of healthy cyber security habits in the young minds and also exciting them to explore the possibility of joining professional cyber security workforce in future.

I express my gratitude to the following schools that helped us in shaping the content of this booklet with their valuable feedback:

- Chikitsak Samuha Shirolar High School;
- Witty International School;
- B.D. Somani International School; and
- Ryan International School

I also want to thank Hon'ble Chief Minister and the Chief Secretary, Government of Maharashtra for their guidance and constant encouragement to our team towards addressing this important aspect of cyber security. I would like to acknowledge contribution by DIT team lead by Director, IT and Head, SeMT. In this journey, we were supported by M/S Ernst & Young LLP and M/S Quick Heal as knowledge partners. I thank them for their sincere effort on this initiative.

This booklet is not intended to be an exhaustive guide to handle potential cyber threats or mitigations. This is to guide the thought process of the youngsters towards reasonable diligence on cybersecurity risks. I welcome your thoughts and feedback on this initiative to make it more useful and effective for our young citizens. Kindly share your thoughts with us on Cyber.Security@maharashtra.gov.in

15th August, 2016

Mumbai

Vijay Kumar Gautam

Principal Secretary, Information Technology

Government of Maharashtra

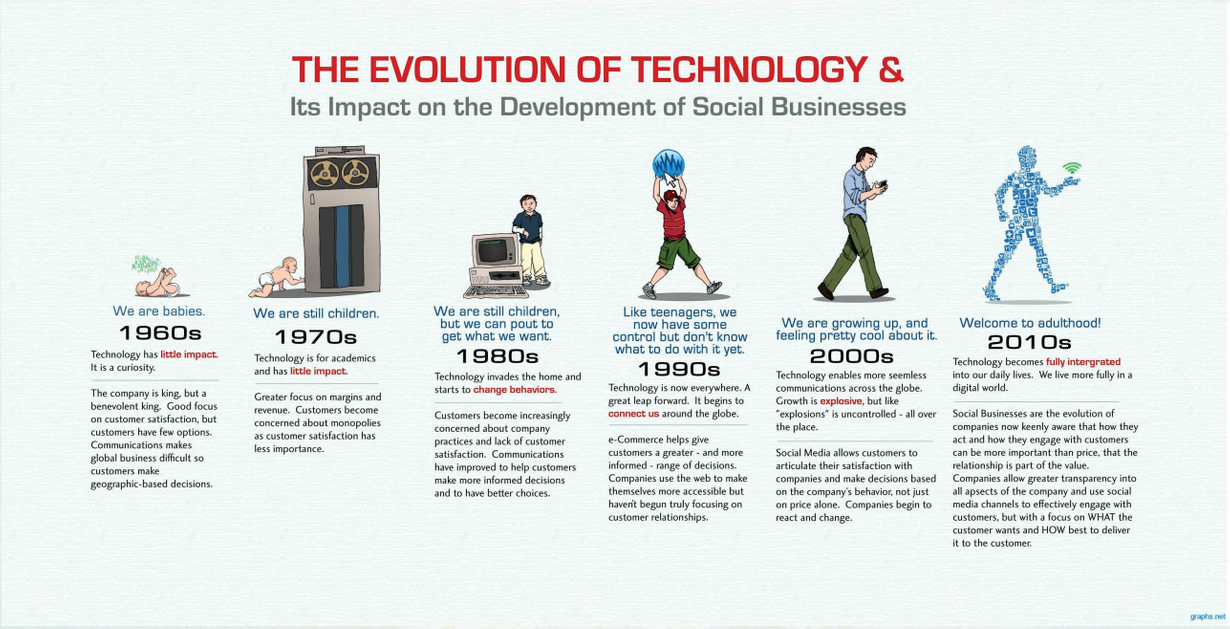
1 The Evolving Digital World…

How many of us wake up and reach out to our mobile phone the first thing?

We live in a new Digital World where computers and the internet technology today, have made it possible for everyone to easily communicate to one another, regardless of time and distance. It has become a new way of life.

But did you know that the first computer dates back to the 1930s. These were large units which occupied an entire room and had basic computing abilities.

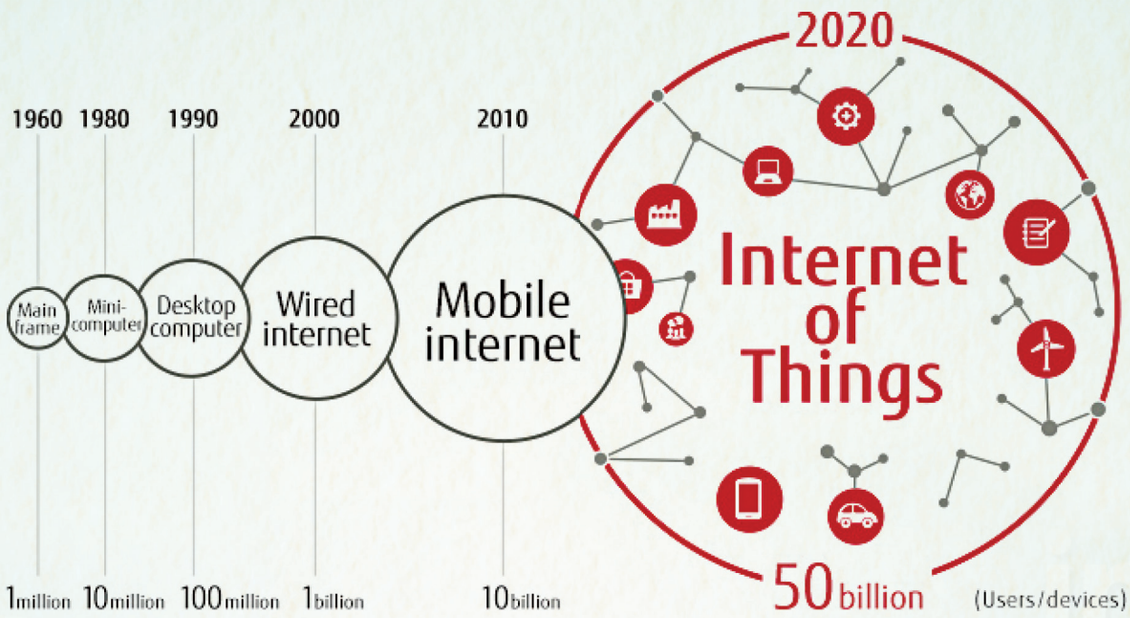
It took almost 20 years from then, to see computers being used in businesses and large organizations. Still, technology was restricted to academics and business then, and had little impact on individuals.



http://www.forbes.com/sites/sap/2012/01/10/infographic-the-evolution-of-technology-its-impact-on-the-development-of-social-businesses/

The first personal computer was developed in the 1970s. This was a revolutionary period that marked the beginning of computers literally invading our homes. Then came the home modems and internet connections.

It was in the 1990s that the World Wide Web (www) was developed and caught the fancy of all. Technology was now everywhere, and began to connect individuals across the globe. Advances in computing technology has grown exponentially since then.



Fast forward now, and we have laptops, desktops, mobile phones, and many more gadgets, some of them called as "Internet of Things (IOT) all interconnected seamlessly, and fully integrated into our daily lives.

We now live in a digital world!

2 The Emerging Cyber Threats…

Just look at some of the cyber threats below!

Apple's iOS App Store suffers first major attack

BOSTON | BY JIM FINKLE

Paris Terror Attacks Stoke Encryption Debate

Cyber-Extortionists Targeting the Financial Sector Are Demanding Bitcoin Ransoms

Ashley Madison Hackers Finally Released All the Stolen Data Online

TEEN WHO HACKED CIA DIRECTOR'S EMAIL TELLS HOW HE DID IT

APPLE TO REMOVE 256 IOS APPS USING PRIVATE API COLLECTING PERSONAL DATA

Attackers hijack CCTV cameras to launch DDoS attacks

China-Tied Hackers That Hit U.S. Said to Breach United Airlines

HOTEL CHAIN HILTON WORLDWIDE INVESTIGATING POTENTIAL POS BREACH

Rajinikanth's twitter account hacked

Telegram Explains What Happened With Its Massive Hacker Attack

Source: Digitalbeat

Posted Aug 3, 2016

PSN Down: Hacker group hits Station Network AGAIN

Express.co.uk - 04-Aug-2016

Clinton Fundraiser Being Held A

sia: hack and

publish Hillary Clinton's 'missing' emails

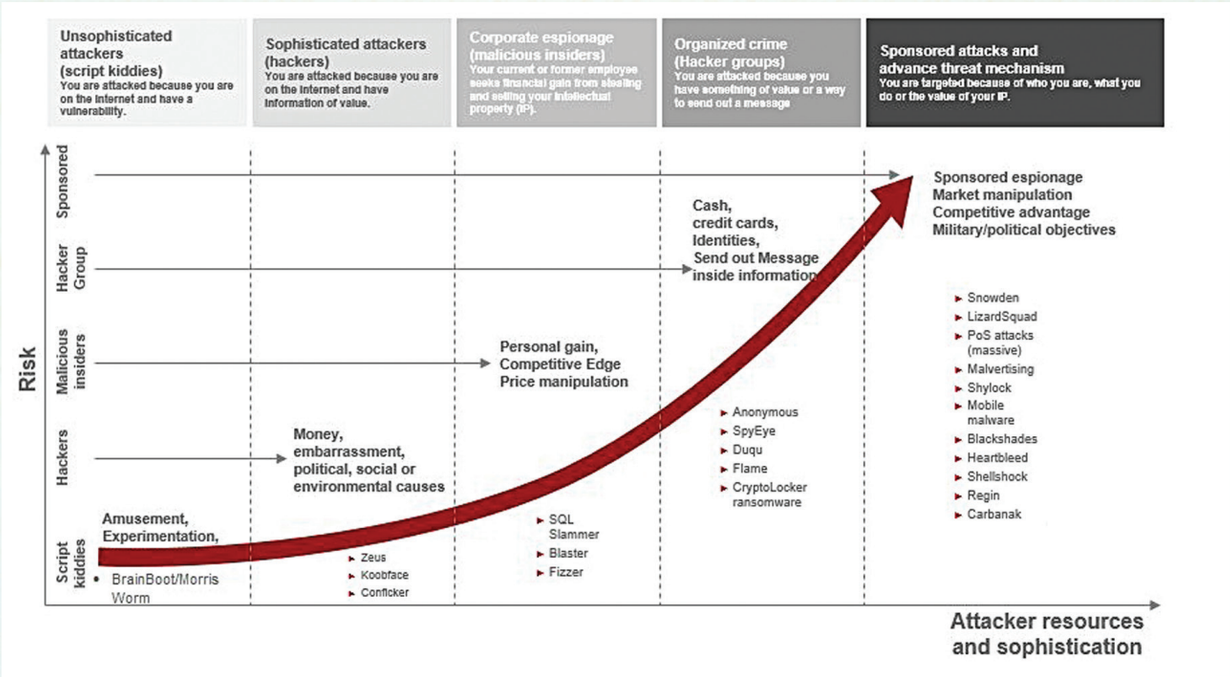
Pokemon Go servers 'HACKED by PoodleCorp' in Playstation-style DDoS attack

Advancement in computing technology has helped individuals, organizations and government in reaching outto each other. But it has its negative repercussions as well!

More and more people are also increasingly using the very same technology for their own dubious reasons, right from targeting unsuspecting individuals, to companies, banks and even the government, military and nations at large.

Like the cyber space, the cyber threats have also evolved over a period of time, since the 1980s, from simple, prankster type virus and worms, to trouble-some elements such as malware and adware, to massive worms, flash threats, and into large scale organized threats and beyond!

Cyber threats have become increasingly sophisticated over a period of time where the time from attack and spread has also narrowed down from days to seconds.



Key Statistics

144%
Increase in cyberattacks on business over a period of four years

$300 Billion-$1 Trillion
Cost of Cyberattacks a year

Nearly 6 Lakh
Facebook accounts are hacked everyday

91% of cyber-attacks are Phishing attacks

90% of large organisations reported suffering a security breach in 2014

59% see criminal syndicates as most likely source of an attack today compared to **53%** in 2014

46% of the complaints or identity theft frauds reported globally involved breaches of government documents

Most of the time, when we use the digital space, we assume that the gadgets and the technology will have enough measures to ensure that information that we share – be it about our self, our habits, family, friends, photos, pictures, financial details etc - is safe and secure and will not be misused.

But that's wrong! It is very likely that this information can fall in the wrong hands and you may be a victim to cyber threats.

The cyber threats can actually be due to very simple reasons or failures on our part. For example, if someone knows your password, he or she can simply log on as you and use your identity. You may be at risk of someone else impersonating you.

Did You Know?

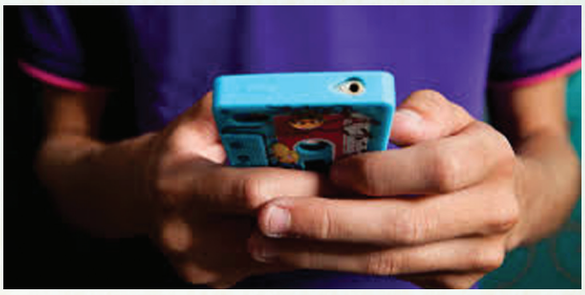
- India is the 3rd biggest source of malicious activity online
- Every 6th social media scam impacts an Indian
- India records 15 ransomware attacks per hour
- 60% of the attacks go undetected

Read on…about some common cyber threats and how you might be a victim of them.

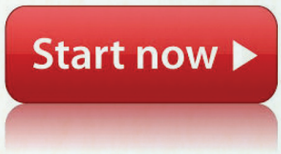
3 You can be a victim of these attacks

Malware

Vivek, like any other teenage boy loves to play online games on his phone. He usually downloads the free games available at the trusted market zones.



One day, he got an SMS "Click here to get the Latest Paid Games Online for free".



Excitedly, he clicked on the link and downloaded and installed the game. Unknowingly to him, these games had a malicious part that allowed the attacker to take control of his phone and made it unusable.

This was a "Drive-by Download" attack and due to his oversight, Vivek's phone was infected with a Malware.

New Android malware can infect your phone by simply visiting a website

Malwares can be a Virus, Worm or Trojan horse that can come to you through use of un-licensed software, unknowingly downloading free but untrusted software programs, or through the use of infected pen drives, storage cards etc.

Wondering how to be safe?

Android malware HummingBad infects 10 million phones

Security companies have noticed a sudden surge in the number of phones infected by the malware

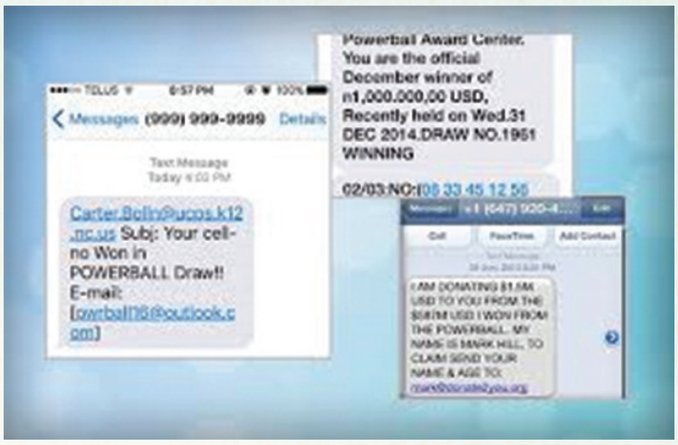
- Never click unfamiliar links or download unfamiliar content.
- Keep your computer system updated with a good anti-virus software
- Ignore any mails or invites which comes from unknown sources.
- Always scan the shared drives before using it

Phishing

Ram received an email – “Congratulations…You have won a Lottery!!!”

Now, wasn’t that tempting..!

The message said:[Dear Winner, kindly view your Lottery]



It meant that he has won the lottery.

The message said that he must immediately reply to the lottery official to claim the lottery amount.

In his excitement, Ram shared all the required personal information, including his bank account Number, IFSC Code, telephone number, and all the other details that were asked in the email. It was only later that he realized that this was a scam message which could use this personal information in an unethical way.

The fraudsters obviously attempted to make the email appear genuine and convince him!

Phishing attacks are sent via email and ask users to click on a link which redirects to a dummy site where an attacker wants victim to enter their personal data or respond to an email which will steal all your personal information. In some cases, a user has to just click on the link.

What should you do?

Follow some simple rules:

- Remember, you cannot win a lottery you have not participated in.
- Do not trust random messages or those containing obvious mistakes.
- Always check the sender’s email address. Lottery organizers will not send messages from free mail services.
- If you still think it is a real win, check all the information. Use search engines to look at the lottery, senders’ names and telephone numbers.
- If you have shared financial details, call the bank or the credit card company immediately to stop or deactivate any payments.

Spoofing

Ramesh, an employee of Government of Maharashtra, received an email claiming it to be from the Director of a Ministry. This email had a document as an attachment stating the form in the document should be filled immediately.

Ramesh, following the order, quickly opened up the attachment to fill in all the details.After some time, to his surprise, he found that many of the files in his computer were locked and encrypted!

The computer displayed a message stating that he has to pay up in order to get back his files and documents.

Upon investigation, it was found that the sender address was a spoofed one.

follow us:

hindustantimes

india | world | cities | opinion | sports | entertainment | lifestyle | tech | photos | videos

rio olympics | delhi metro's heritage line | movie reviews | Rustom Vs Mohenjo Daro | ht paath

Virus attacks 150 computers in Mantralaya

Surendra P Gangan | Updated: May 25, 2016 06:35 IST

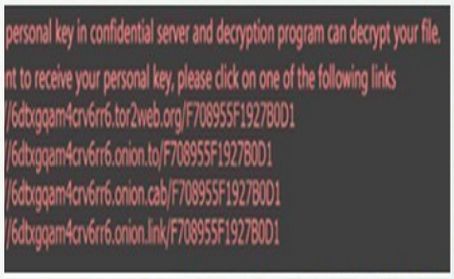
MUMBAI: Locky ransomware, a malicious software which blocks access to computers, attacked about 150 computers in Mantralaya on May 15, encrypting important files from the Public Works Department and the Revenue department.

The information technology department isolated the systems to avert further damage to the government's e-governance platform.

"The virus reportedly damaged about two lakh systems in Germany and the United States in the last two years," said an official from the IT department, adding that Locky targets the systems of multinationals with the intention of demanding money for decrypting the ransomware.

Email Spoofing is the forgery of an e-mail header so that the message appears to have originated from someone genuine whereas it is actually not.

The virus here was Ransomware which encrypted many important files on the computer and did not allow him to access it. As the name suggests, the attacker demands for a "Ransom" (money) in order to unlock and restore the files.

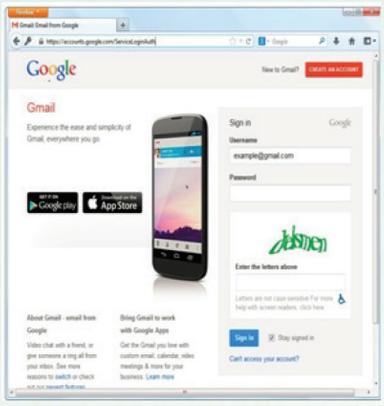


So, what should you do?

- Check the email address before you open any attachment.
- Do not open the mail if you do not recognize the sender.
- If you suspect anything suspicious, call the sender to verify the mail.
- Keep a backup of important files and documents.
- Do not proceed to pay even if you are infected. Ask an expert.
- Always keep your computer updated with a good anti-virus software.

Password Theft

Sandeep tried to login multiple times into his friend Pradeep's email account.



He used all possible combinations of letters by using Pradeep's name, date of birth, birth place. However, after few failed attempts, he was shown a CAPTCHA image to verify that he (Sandeep) is a human and is not a computer who is automatically trying innumerable attempts to crack the password.

By using a CAPTCHA image, the email provider had blocked what is called as a Brute Force Password Attack.

In fact, hackers can use many means to know your password and break into your system.

- An attacker may make use of dictionary words and combinations of standard number sequences to crack your password.
- An attacker may use a Brute-Force Method by having a computer program or script continuously try all possible combinations to gain access to an account.
- A hackermay use a program or hardware to track everything a user has typed -including their login IDs and passwords. Through such Key logger Attacks, even complex passwords can be accessed easily.

So, what should you do?

- Use long, secure passwords.
- Use different passwords for different accounts.
- Where available, use the virtual keyboard to type the passwords.

Treat your password like your toothbrush, do not share with any one

Man in the Middle Attack

Arun was trying to access his bank account online through a WiFi connection at a hotel. However, he was not aware that the connection was an "open" network and not encrypted. During this time, an attacker can eavesdrop on the conversation and communication that Arun may be doing from his computer.

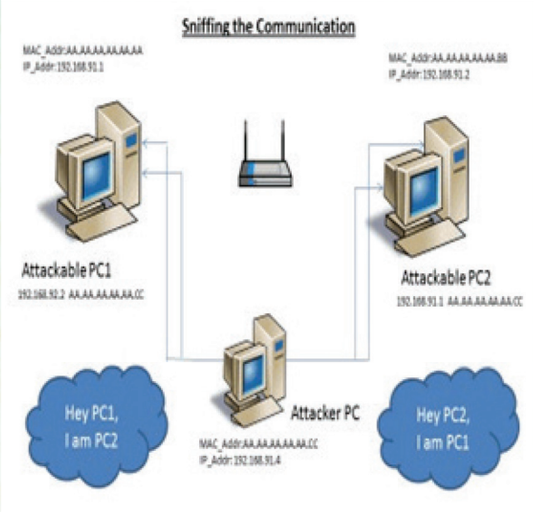
The Man in the Middle [attacker] would then receive all of the information transferred between both parties, which could include sensitive data, such as bank accounts and personal information.

Wi-Fi Hacks

Many a times you may have used free Wifi networks. You may have connected your laptop in a hotel room, or connected your mobile to a free Wi-Fi at a railway station or any other public place.

It may be possible that the Wi-Fi network is hacked and you could be sharing information that can be accessed by someone else.

Some famous attacks that have happened include the Sniffer Attack, via Side-jacking and through Public WiFi Rogue Networks.



What should you do?

- Make sure you connect to only encryptedWi-Fi points.
- If you connect to a website, and then make sure it uses only HTTPS.
- Never connect to open WiFi routers directly.

Denial of Service, Distributed Denial of Service

You are here: Home > News & Analysis>

ISPs in Maharashtra are facing DDoS attack

25 Jul 2016 , 09:34

Small and medium sized internet service providers in Maharashtra are being targeted for a Dedicated Denial of Service (DDoS) attack, affecting connectivity to people in Mumbai, Thane and Pune. A DDoS attack sends thousands of requests to a server, jamming the network and making the service unavailable to legitimate users. A server, a number of machines, are dedicatedly pinging the ISPs thousands of times in a second, denying the availability of the service to the customers.

DDoS attacks can be a co-ordinated effort from a number of users around the world, but more often networks of compromised machines are used for DDoS attacks. There are called

Recently, Internet Service Providers (ISP) in Maharashtra were target to what is known as a Distributed Denial of Service Attacks (DDOS Attack). As a result, a number of customers did not have access to internet for some time.

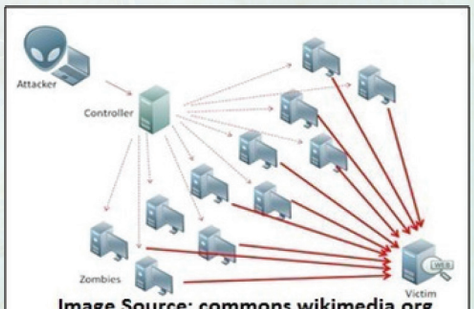


Image Source: commons.wikimedia.org

This was one the biggest DDOS attacks with the traffic of 200 GBPS being generated by the Attacker group.

A few years ago, 'Rahul', a teenage boy from Maharashtra, had been convicted (jailed) for joining a Hacktivist group for carrying a DDOS attack on a Reputed Bank. Rahul had used

his personal computer to bombard a bank's website by continuously sending access request to the Bank's web application. This in turn made the bank's web application slow and prevented other from getting access to the Login page.

Such Distributed Denial of Services (DDOS) attacks are usually conducted by use of zombies and BOTS (i.e. malware that has got downloaded on other user's computers) that is controlled remotely by an attacker. These systems belong to individuals, who are not aware that their computer is being used for the DDOS attack!

How to keep your computer safe

- Keep your system up to date with latest updates of licensed software
- Use Up-to date Anti-virus software
- Do not use Unlicensed or Pirated software
- Check your system network performance if your Internet is slow

Game Threats

A famous "augmented reality" smartphone game developed for handheld devices was released in July 2016 in a few selected countries. The game became an overnight sensation and cybercriminals started targeting it. In just a few days after the official App hit the market, people had discovered a Trojan (i.e. a malicious) version of the app available in the other markets giving way to cybercriminals to make the best out of the situation.

A famous gaming network hack was one of the largest security breach of its kind to ever hit console gamers back in the year 2011. Personal details of 77 million users were accessed with potential access to 12,000 encrypted credit card. The hack was one of the biggest security breaches in the recent history.

So, what should you do?

- Make sure you scan external drives for virus before you install any games or other software.
- Ensure authenticity of the source you are downloading games from.
- Ensure that you only buy in-game currency from trusted websites.
- Be cautious what types of links you click on social networking websites. Game notifications or invites can be a phishing technique and compromise your system.
- Protect your privacy and don't offer any confidential information to other players in the game.
- Do not give up on security settings to increase your system's speed!
- Only download games from the phone operating system vendor's application store as these have undergone security checks.
- Before installing, check the requested permissions.

4 You may be committing a crime…

You might be committing a crime if you carried out any dubious activities on the net. There are laws related to this. In India, Cyber Law is represented by Indian IT ACT 2008.

DID you know?

- Cybercrime punishments are controlled by the legislation IT Act 2008 (amendment) and associated Indian Penal Codes
- Service Providers like Internet Service Providers (ISPs), email service providers, telecom operators etc. are liable to share relevant information with the Law Enforcement Agencies (LEAs)

Here are some real life examples of threats and crimes.

Wi-Fi Hacks

A crime was recently reported crime against a student who was hacking the Wi-Fi being used by his neighbour.

To showcase his new learning on hacking to his friends, Aditya had hacked the Wi-Fi password (WEP password) of his neighbour and was able to read all his private communications. He also started using the Wireless for his personal needs like download of pirated games and software and other hacking tools to get in his neighbours computer.

"Depraved" Wi-Fi hacker gets 1 year in prison

Punishment: Imprisonment up to 3 years with fine up to five lakh rupees

Cyber Defamation

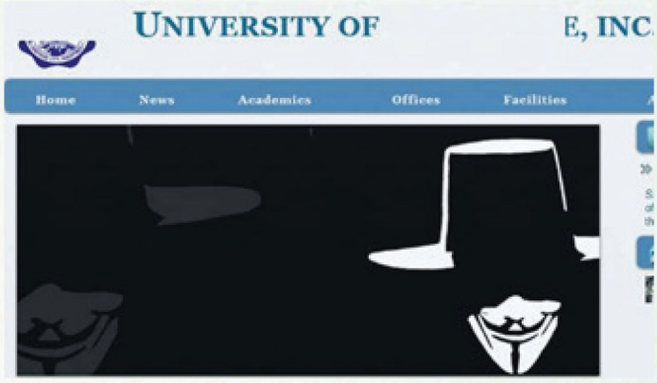
A teenaged student was arrested by the Thane police in India following a girl's complaint about tarnishing her image in the social networking site Orkut. The alleged culprit had allegedly created a fake account in the name of the girl with her mobile number posted on the profile. The profile had been sketched in such a way that it drew lewd comments from many who visited her profile. The Thane Cyber Cell tracked down the alleged culprit from the false e-mail id that he had created to open up the account

Punishment: Imprisonment up to 2-3 years with fine up to ten lakh rupees As per the IT Act:

Any person who sends, by means of a computer resource or a communication device,-

- any information that is grossly offensive or has menacing character; or
- any information which he knows to be false, but for the purpose of causing defamation
- any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages

Web Defacement



Two individuals were arrested in 2002 for allegedly defacing the website of the Mumbai Cyber Crime Cell. They had allegedly used password cracking software to crack the FTP password for the police website. They then replaced the homepage of the website with pornographic content.

Punishment: As per the IT Act: Whoever knowingly or intentionally, destroys or alter any computer source code, shall be punishable with imprisonment up to three years, or with fine which may extend up to 2 lakh Rs, or with both.

Spreading Virus and Malware

In 2006, a US citizen was convicted for conspiracy to intentionally cause damage to protected computers and commit computer fraud. Between 2004 and 2005, he created and operated a malicious software to constantly scan for and infect new computers. It damaged hundreds of US Department of Defence computers in USA, Germany and Italy. The software compromised computer systems at a Seattle hospital, including patient systems, and damaged more than 1,000 computers in a California school district.

Punishment: Imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Identity Theft

A leading Indian Airlines was duped of Rs.17 crore caused by an online ticket booking fraud, caused by credit card bookings. According to the officers working on this case, these credit card details were obtained by the thieves from various places like shopping mall, restaurant and petrol-pump employees who swipe these cards.

Punishment: Section 66C and 66D lays down a punishment of up to three years of imprisonment and/or fine up to one lakh rupees.

Cyber Pornography

A student of a leading school in Delhi recorded a pornographic clip of approximately 2.30 minutes by his mobile and circulated amongst his friends. The students were expelled from the school and two big arrests were also made in the same conjunction.

Another incident revolving around cyber pornography include the another school in Delhi. In the first case of this kind, the Delhi Police Cyber Crime Cell registered a case under section 67 of the IT act, 2000. A student created a website at the URL www.amazing-gents.8m.net. On this site, lucid, explicit, sexual details were given about various girls and teachers of the school. Girls and teachers were also classified on the basis of their physical attributes and perceived sexual preferences. The police picked up the concerned student and kept him at a juvenile home. It was almost after one week that the juvenile board granted bail to the 16- year-old student.

Punishment: Section 67 and 67A of the IT Act lays down a punishment for publishing, storing or transmitting obscene material in electronic form (Imprisonment from 2 – 10 years with fine up to 10 lakhs)

5 How to Stay Safe Online…

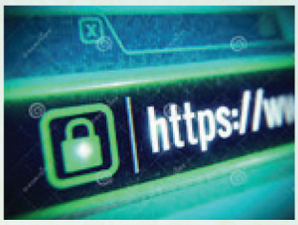
1) Being Safe on Social Media

- Make a unique password for every social media site.
- Be selective about who is accepted as a friend or follower. Identity thieves can easily create fake profiles in order to lure you.
- Do not click on links that may appear to be unusual or suspicious, even if they are sent by friends.
- Check the privacy settings and set it to the most secure setting available. Many of the applications have this in their Settings or Privacy menu.
- Do not post information that would let public know about your whereabouts such as going on vacation, leaving the house, being home alone.
- Do not post anything online that would cause problems if made public. Think!
- Remember that employers, school and university administrators and others often check Facebook, Twitter and other sites for information posted online.
- Do not post any security sensitive information.
- Always bear in mind that status updates, photos and videos posted on social networks are permanent. Even if you remove the information later, or delete your profile, there is always the possibility that someone would have printed or saved or transmitted those texts, photos, and videos elsewhere when you posted them.

2) Being safe on e-Commerce and Financial websites

- Perform research before purchasing from any new website by searching user reviews of that site.
- Do not follow shortened links such ashttp://goo.gl/cVjl4F- they may be deceptive and land on a malicious website.

- Make sure that the website being used is an encrypted website. Look for a padlock symbol!
- Check your bank statement to make sure that nothing is incorrect. Report any suspicious activity to the bank.



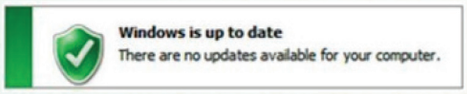
3) Maintaining a Secure system

Install anti-virus software and ensure it is up-to-date

Antivirus software programs can detect, prevent and clean computer and mobile phone viruses. Just installing an antivirus solution is not sufficient; you have to ensure that it is up-to-date to combat the latest version of malwares.

Keep your Operating System up to date

Install Operating System patches as soon as they are released, as thereafter a security hole may become public knowledge. Attackers can use this knowledge to start exploiting unpatched systems before people update.



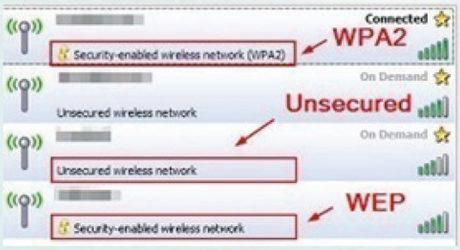
Encrypt Your Hard Drive

A lost or stolen mobile phone or computer can put sensitive data in the wrong hands. Use encryption software to encrypt and protect your hard drive.

Encryption program helps diminish the risk of unauthorized data access. It also makes data inaccessible when the encrypted computers is decommissioned or reprocessed.

Use of Firewall

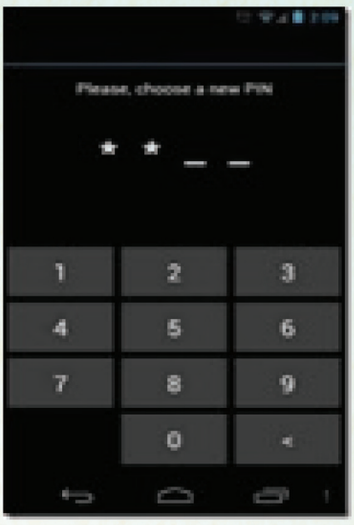
Firewalls are access control software and can validate the network traffic coming in or going out of the System. Always enable the firewall or any other application that can be used as its replacement; some Anti-virus have Firewall functionality.



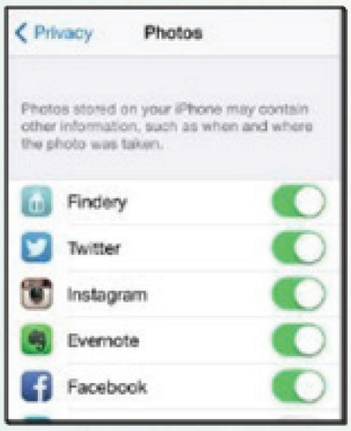
Use of Public or Open network

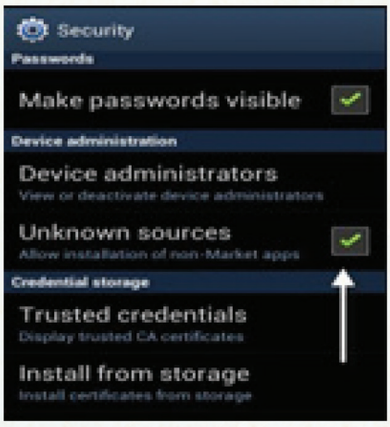
Always use secure communication mechanism (WPA or WPA2 authentication Wifi) for any communications. If required, use open network for only browsing purpose and do not share any sensitive information.

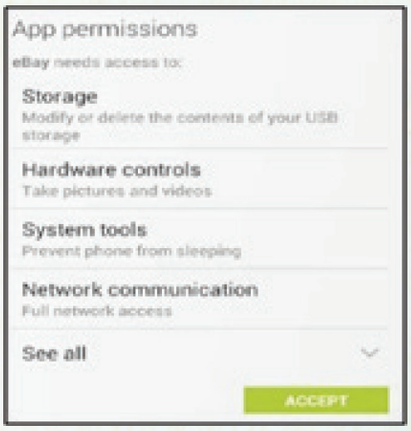
Maintaining a Secure Smartphone



- Use a Strong Password or PIN: Protect your mobile device using the inbuilt mechanisms like Passwords, PIN, Pattern or Fingerprint to prevent unauthorized access.
- Install and download applications only from the mobile operating system vendor's application market store as they have undergone the security check.
- Enable the restriction on installing applications.
- Before installing, check the requested permission and ensure it is allowed only the required minimum permissions.







6 Where to go if there is a threat

The Indian Cyber Space is evolving at a rapid pace. This evolution has definitely fuelled the growth of the Indian economy, but at the same time the growing number of cyber-attacks on our computers and networks has become a serious national security threat India is facing today.

To combat these threats, the Government has set up various programs, projects and initiatives at various levels. Some of these are mentioned in brief below. It is recommended that you go to the respective websites.

Indian Computer Emergency Response Team (Cert-In)

CERT-In is an acronym for 'Indian Computer Emergency Response Team'. CERT-In is the National Incident Response Centre for major computer security incidents in the Indian Cyber community. Reference: http://www.cert-in.org.in/

- CERT-In operates a 24 x 7 Incident Response Help desk and coordinates responses to Security Incidents and related major events. It also enlightens about the security awareness and best practices for various systems and networks by publishing advisories, guidelines and other technical documents regularly.

MEITY (Ministry of Electronics and Information Technology)

National Cyber Security Policy is a policy framework by Ministry of Electronics and Information Technology (MeitY). It aims at protecting the public and private infrastructure from cyber-attacks.

The policy also intends to safeguard "information, such as personal information (of web users), financial and banking information and sovereign data". Reference: http://deity.gov.in/andhttps://isea-pmu.in/home/

NCIIPC (National Critical Information Infrastructure Protection Centre)

NCIIPC is driven by its mission "To take all necessary measures to facilitate protection of Critical Information Infrastructure, from unauthorized access, modification, use, disclosure, disruption, incapacitation or destruction, through coherent coordination, synergy and raising information security awareness among all stakeholders".

Government of Maharashtra

Government of Maharashtra conducts regular training programs, workshops and leadership summits on various aspects of e-Governance, including Cyber Security, for its officers and employees, which are also often attended by other stakeholders in the field like consultants, media personnel, software programmers working with the State Government, etc.

The **Cyber Crime Investigation Cell** of Mumbai Police deals with the offence related to the computer, computer network, computer resource and Internet. It provides a detailed platform for a vast range of topics such as list of cyber-crimes, cyber laws and their amendments as well as general online safety tips.

For any more information on Cyber Security or to register any complaint related to cybercrime on Cyber please contact:

Cyber Security Team, Directorate of Information Technology (Mantralaya)

E-mail id: **cyber.security@maharashtra.gov.in**

CYBER CRIME INVESTIGATION CELL

Web-site: http://cybercellmumbai.gov.in/

E-mail id: cybercell.mumbai@mahapolice.gov.in

7 Daily Cyber Security Hygiene

- Keep your Operating System and all your software up-to-date.
- Keep your computer system updated with a good anti-virus software
- Keep a backup of important files and documents.
- Never click unfamiliar links or download unfamiliar content.
- Ignore any mails or invites which comes from unknown sources.
- Always scan shared drives before using them for games or any software
- Use common sense and stay attentive when navigating gaming forums and don't click anything suspicious.
- Use strong passwords and change them frequently.
- Use different passwords for different accounts.
- Where available, use the virtual keyboard to type the passwords.
- Remember, you cannot win a lottery you have not participated in.
- Do not trust random messages or those containing obvious mistakes.
- Always check the sender's email address.
- If you have shared financial details, call the bank or the credit card company immediately to stop or deactivate any payments.

- Do not proceed to pay even if you are infected. Ask an expert.
- Do not disclose un-necessary information to anyone including the admin
- Make sure you connect to only encrypted Wi-Fi points.
- If you connect to a website, and then make sure it uses only HTTPS.
- Ensure authenticity of the source you are downloading games from.
- Ensure that you only buy in-game currency from trusted websites.
- Be cautious what types of links you click on social networking websites.
- Do not offer any confidential information to other players in the game.
- Do not give up on security settings to increase your system's speed!
- Be careful of the platforms where you store your credit card information for in-game payments.

8 How about a Career as a Cyber Security Professional...

So, would you like to take up this challenging field of Cyber Security as a Profession?

As a security professional, you may work on any or all of the below areas -

- Work jointly with government agencies including defence forces, other institutions on cyber security for implementation of counter measures
- Work on policies and frameworks, on cyber security and cyber crimes
- Keep a vigil on the developments in the IT sector of potential adversaries.
- Create awareness and sensitize common citizens about the dangers of cyber terrorism.

Security as a profession has a lot of challenges, especially due to lack of awareness, the casual attitude to cyber security at individual as well as institutional level, lack of qualified manpower to implement the counter measures. In addition, Cyber-attacks have come not only from terrorists but also from neighbouring countries inimical to our National interests.

Ethical Hacker

Ethical hacking and ethical hacker are terms used to describe hacking performed by a company or individual to help identify potential threats on a computer or network.

An ethical hacker attempts to bypass system security and search for any weak points that could be exploited by malicious hackers. This information is then used by the organization to improve the system security, in an effort to minimize or eliminate any potential attacks.Individuals interested in becoming an ethical hacker can work towards a Certified Ethical Hacker (CEH) certificate.

Cyber Forensics Expert

Cyber forensics, also called computer forensics, is the process of extracting information and data from computers to serve as digital evidence - for civil purposes or, in many cases, to prove and legally prosecute cyber-crime. Cyber forensic professionals are specialists with proven expertise in this area and they must continually educate themselves on the new techniques.

A few Cyber Forensics certifications that can be looked at - CCFP (Certified Cyber Forensics Professional Certification), GIAC Certified Forensic Examiner (GCFE) and GIAC Certified Forensic Analyst (GCFA), ACIS Certified Forensic Computer Examiner (CFCE) etc.

Other Certifications: Various certifications for in-depth understanding of cyber security can be studied for such as CISA (Certified Information Systems Auditor), CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager), ISO 27001 etc.

Career Opportunities

Cyber security is also fast becoming a major growth area for Indian industry!

According to industry body NASSCOM, it would be a major revenue and job creator for the country going forward. By 2020, it has projected that the cyber security sector will create huge number of job opportunities.

9 Aaple Sarkar Initiative

Aaple Sarkar is a single, one-stop web-portal launched by the Government of Maharashtra for citizens to interact with the government.

You can access it at https://aaplesarkar.maharashtra.gov.in/en/

The Aaple Sarkar web portal is a single credible face of the Government for various interactions, such as delivery of services to citizens, right to information, citizen participation in initiatives and programs of the government, raising complaints or grievances. Since its launch, it has more than 34 lakh applications as of date of this publication.

If a student required a birth certificate, he or she can visit the Aaple Sarkar web portal and submit an online application for the same. Or if you require your examination mark-sheet, you can submit a request for it online!

Or, if you wanted to provide some suggestions or ideas on any new initiative which the government can take up, you can simply do it from the Aaple Sarkar portal.

The various sections in the Aaple Sarkar portal are:

1. Right to Service (RTS) – "Your Service : Our Guarantee"

Under the RTS portal, citizens can apply online to a host of services made available by various departments. The government official is bound to deliver these services to you within a stipulated period of time as per law.

2. Grievance Redressal – "Your complaint : Our responsibility"

If a citizen has any complaints or grievance about any function of the government, the citizen can submit a grievance through the site.

3. Right to Information (RTI) – "Your right : Right to Information"

The portal provides facility to file an RTI, make the requisite fee payment and track the application. It is the duty of the government to process your RTI application.

4. MyGov – Citizen Collaboration – "Your suggestion : Our policy"

The goal of the project is to make Citizen Engagement an integral part of governance policy, scheme, project planning and implementation. As a citizen, you can participate and present your views on any topics online through Public Consultation, Discussion Groups, Blogs and newsletters, and knowledge repository.

Going Forward

The Government of Maharashtra has an ambitious vision to make the state digitally connected.

Under the **Bharat Net** program, the Government of Maharashtra has planned high speed connectivity to all the 28000 odd Gram Panchayats in the State and the urban areas of the State. This is expected to be operationalized by the December 2018.

Under the **Digital Villages** program, the government is soon providing WI-FI hot spots, and other smart technology interventions. Recently, e-Education and Telemedicine initiatives were rolled out in few villages.

In the **Smart cities,** the Government plans to create a strong network backbone which will be capable of providing robust, secure and scalable connectivity. On this backbone, interventions like city surveillance, smart parking, smart traffic management, smart waste management, Public Wi-fi, smart transport will provide a unique experience to the citizens.

Citizen Service Centres are also planned to be increased across the state to have at least one such centre per gram panchayat.

Along with this connectivity and infrastructure, the State intends to incorporate various software applications and services into Aaple Sarkar and make it a single face of the Government. Additional functions such as Digital Locker (so that a citizen can securely store his or her certificates online), Mobile Integration (to access the service seamlessly through mobile devices), Aadhaar Enabled (Direct Benefit Transfer) etc. are planned to be implemented.

The Smart and Connected world that we are inhabiting in the 21st century puts greater responsibility on us of ensuring a safe and secure cyber-space for us and our future generations. This will be critical in taking the nation forward to achieve the mission laid down by our Hon. Prime Minister.

Under the Aaple Sarkar programme, Government of Maharashtra is also undertaking many awareness campaigns to reach out to various sectors and citizens.This awareness guide is one such mechanism and addresses the topic of “Cyber Security” while using the information highway.

Glossary of Terms

Term	Description
Adware	A software package that automatically displays advertisements, whether or not it does so with the user's consent; such programs display advertisements as an alternative to shareware registration fees or downloads advertising material to a computer after the software is installed on it or while the application is being used.
Alert Situation	A technology widely used to prevent, detect and remove many categories of malware, including computer viruses, worms, Trojans, malicious browser plug-ins, adware and spyware
Antivirus Software	The Application software deployed at multiple points in an IT architecture designed to detect and potentially eliminate virus code before damage is done and repair or quarantine files that have already been infected.
Asset	Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation
Attack	An actual occurrence of an adverse event
Authenticity	Undisputed authorship
Availability	Ensuring timely and reliable access to and use of information
Biometrics	A security technique that verifies an individual's identity by analysing a unique physical attribute, such as a handprint
Brute Force Attack	Repeatedly trying all possible combinations of passwords or encryption keys until the correct one is found
Cipher	An algorithm to perform encryption
Cryptography	The art of designing, analysing and attacking cryptographic schemes
Cyber Crime	Criminal activities carried out by means of computers or the Internet.
Cyber Law	Cyber law or Internet law is a term that encapsulates the legal issues related to use of the Internet. It is less a distinct field of law than intellectual property or contract law, as it is a domain covering many areas of law and regulation.
Cyber Defamation	Cyber defamation is not a specific criminal offense, misdemeanour or tort, but rather defamation or slander conducted via digital media, usually through the Internet.
Cyber Forensics	Computer forensics (sometimes known as computer forensic science) is a branch of digital forensic science pertaining to legal evidence found in computers and digital storage media.
Cyber Pornography	Cyber pornography is the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials, especially materials depicting children engaged in sexual acts with adults. Cyber pornography is a criminal offense, classified as causing harm to persons.
Cyber Terrorism	Cyberterrorism is the act of Internet terrorism in terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses.
Cyber Bullying	The use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature.
Cyber Stalking	The repeated use of electronic communications to harass or frighten someone, for example by sending threatening emails.
Data Leakage	Siphoning out or leaking information by dumping computer files or stealing computer reports
Data Privacy	Data privacy is the confidentiality of personal information that includes personal data and credentials stored on computer systems.
Data Diddling	The unauthorized changing of data before or during their input to a computer system. Examples are forging or counterfeiting documents and ex- changing valid computer tapes or cards with prepared replacements.
Decryption	A technique used to recover the original plaintext from the cipher text so that it is intelligible to the reader The decryption is a reverse process of the encryption.
Denial-of-service attack (DOS)	An assault on a service from a single source that floods it with so many requests that it slows down and is either stopped completely or operates at a significantly reduced rate
Dictionary Attack	A technique when an attacker uses a Dictionary in an attempt to crack the password. Therefore it is recommended to not use passwords with simple words that are part of the Dictionary.
Digital certificate	A piece of information, a digitized form of signature that is generated using the sender's private key or applying a one-way hash function.
Drive by Download	Drive by Download is one of the mechanisms used by the attackers for spreading the bad malware that may infect the system or a mobile phone.

Term	Description
Digital forensics	The process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable in any legal proceedings
Digital signature	A piece of information, a digitized form of signature, that provides sender authenticity, message integrity and non-repudiation. A digital signature is generated using the sender's private key or applying a one-way hash function.
Encryption	The process of taking an unencrypted message (plaintext), applying a mathematical function to it (encryption algorithm with a key) and producing an encrypted message (cipher text)
Email Spoofing	It is the forgery of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source. Distributors of spam often use spoofing in an attempt to get recipients to open, and possibly even respond to, their solicitations.
Email Bombing	An email bomb is a form of net abuse consisting of sending huge volumes of email to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted in a denial-of-service attack.
Ethical Hacking	An ethical hacker is a computer and networking expert who systematically attempts to penetrate a computer system or network on behalf of its owners for the purpose of finding security vulnerabilities that a malicious hacker could potentially exploit.
Firewall	A firewall is a network security system, either hardware- or software-based, that controls incoming and outgoing network traffic based on a set of rules.
Forensic Examination	The process of collecting, assessing, classifying and documenting digital evidence to assist in the identification of an offender and the method of compromise
Gaming Threats	Threats arising with the intent of making money – either by stealing and selling data, or convincing the user to hand over their bank details using the games downloaded online.
Intellectual Property Crimes	Criminal IP offences are also known as "IP crime" or "counterfeiting" and "piracy". Counterfeiting can be defined as the manufacture, importation, distribution and sale of products which falsely carry the trade mark of a genuine brand without permission and for gain or loss to another.
Key Logger Attack	A computer program that records every keystroke made by a computer user, especially in order to gain fraudulent access to passwords and other confidential information. Such an attack is a Key logger attack.
Malware	Short for malicious software. Designed to infiltrate damage or obtain information from a computer system without the owner's consent. Malware is commonly taken to include computer viruses, worms, Trojan horses, spyware and adware. Spyware is generally used for marketing purposes and, as such, is not malicious, although it is generally unwanted. Spyware can, however, be used to gather information for identity theft or other clearly illicit purposes.
Man-in-Middle Attack	It is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.
Password	A protected, generally computer-encrypted string of characters that authenticate a computer user to the computer system
Password Attack	Password attacks are the classic way to gain access to a computer system to find out the password and log in.
Phishing	This is a type of electronic mail (e-mail) attack that attempts to convince a user that the originator is genuine, but with the intention of obtaining information for use in social engineering Phishing" attacks are sent via email and ask users to click on a link which redirects to a dummy site where an attacker wants victim to enter their personal data or respond to an email which will steal all your personal information. In some cases, a user has to just click on the link.
Privacy	Freedom from unauthorized intrusion or disclosure of information about an individual
Spoofing	Faking the sending address of a transmission in order to gain illegal entry into a secure system
Ransomware	Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid. Ransomware spreads through e-mail attachments, infected programs and compromised websites.
Salami Attack	A salami attack is when small attacks add up to one major attack that can go undetected due to the nature of this type of cyber-crime. It also known as salami slicing.
Spyware	Software whose purpose is to monitor a computer user's actions (e.g., web sites visited) and report these actions to a third party, without the informed consent of that machine's owner or legitimate user A particularly malicious form of spyware is software that monitors keystrokes to obtain passwords or otherwise gathers sensitive information such as credit card numbers, which it then transmits to a malicious third party. The term has also come to refer more broadly to software that subverts the computer's operation for the benefit of a third party.

Term	Description
System Hardening	A process to eliminate as many security risks as possible by removing all nonessential software programs, protocols, services and utilities from the system
Trojan Attacks	A Trojan attack is a type of malware attack that is often disguised as legitimate software. Trojans can be employed by cyber-thieves and hackers trying to gain access to users' systems.
Wi-Fi Hacking	Wi-Fi hacking are the classic way to gain access to a wireless device is to find out the password and log in.
Web Defacement	Website defacement is an attack on a website that changes the visual appearance of the site or a webpage. These are typically the work of system crackers, who break into a web server and replace the hosted website with one of their own.
Virus	A program with the ability to reproduce by modifying other programs to include a copy of itself. A virus may contain destructive code that can move into multiple programs, data files or devices on a system and spread through multiple systems in a network.
Vulnerability	A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events

References

- http://www.business-standard.com/article/current-affairs/targeted-cyber-attacks-on-indian-businesses-increase-report-116050200754_1.html
- https://threatpost.com/hotel-chain-hilton-worldwide-investigating-potential-pos-breach/114830/
- http://www.reuters.com/article/us-target-breach-settlement-idUSKBN0TL20Y20151203
- http://researchcenter.paloaltonetworks.com/2015/08/banking-trojan-
- https://threatpost.com/cisco-warning-of-vulnerabilities-in-routers-data-center-platforms/115609/
- http://www.bloomberg.com/news/articles/2015-09-09/bitcoin-ddos-ransom-demands-raise-dd4bc-profile
- http://news.softpedia.com/news/backdoor-in-cisco-s-webvpn-service-allowed-hackers-to-steal-corporate-passwords-494161.shtml
- https://threatpost.com/apple-to-remove-256-ios-apps-using-private-apis-collecting-personal-data/115098/
- http://economictimes.indiatimes.com/news/defence/how-indian-financial-outfits-have-been-facing-numerous-cyber-attacks-from-pakistan/articleshow/48737054.cms
- http://krebsonsecurity.com/2015/11/paris-terror-attacks-stoke-encryption-debate/
- http://thehackernews.com/2015/08/ashley-madison-accounts-leaked-online.html
- https://www.wired.com/2015/10/hacker-who-broke-into-cia-director-john-brennan-email-tells-how-he-did-it/
- http://www.reuters.com/article/us-apple-china-malware-idUSKCN0RK0ZB20150920
- http://indiaforensic.com/compcrime.htm
- https://dict.mizoram.gov.in
- http://www.ndtv.com/topic/fake-facebook-profile
- https://nagpurgraminpolice.gov.in/cyber-cell.php
- http://searchenginemarketingpeople.com/blog/strange-new-digital-world/
- http://www.forbes.com/sites/sap/2012/01/10/infographic-the-evolution-of-technology-its-impact-on-the-development-of-social-businesses/
- http://www.huffingtonpost.in/entry/instagram-photos_b_5051847
- http://scam-detector.com/telephone-scams/facebook-powerball-text
- https://www.dreamstime.com/stock-illustration-https-secure-connection-sign-browser-address-concept-d-render-icon-image58133694
- http://tech.firstpost.com/news-analysis/isps-in-maharashtra-are-facing-ddos-attack-326607.html
- Information Week, Bloomberg
- Publically available information & EY cyber security report
- Gartner

Knowledge Partner

Quick Heal Technologies Limited, www.quickheal.com

In Association with Directorate of IT,
Government of Maharashtra

Contact Us: **Directorate of Information Technology,**
7th Floor, Mantralaya, Mumbai - 400 032. Phone: 022-22044586 • Fax: 022-22024177