Cyber Security Awareness

Communication Security Advisory for Government Officials

Presentation Contents

Cyber Security

• The internet allows an attacker to work from anywhere on the planet.

• Cyber Security is the safeguarding of computer systems and networks against data leakage, theft, or damage to their hardware, software, or electronic data, as well as disruption or misdirection of services.

Why is Cyber Awareness Important?

- **Cyber crime is a growing trend with advancement of technology**
- **Raise awareness of threats**
- **As with most crimes the police can't tackle this problem alone**
- **To encourage reporting of Cyber Crime to enforcement agencies**
- **Cyber crime is massively under reported.**

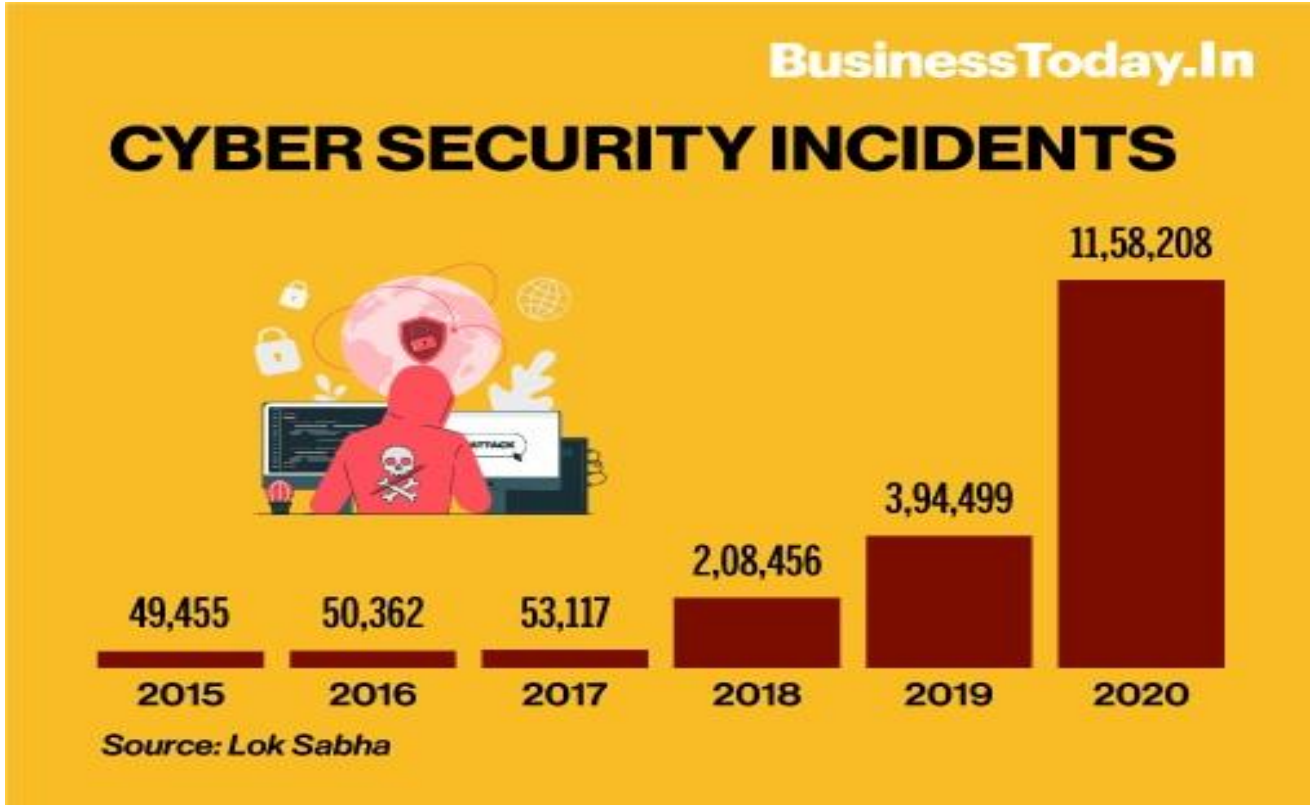
Risks caused by poor security knowledge and practice

- **Identity Theft**
- **Monetary Theft**
- **Legal Ramifications (for yourself and your organization)**
- **Departmental Action or termination as per the policies**

Causes for Concern

- On average, hackers attack every 39 seconds, 2,244 times a day.
- Since 2014, security breaches have increased by 67%.
- 68% of business leaders believe their cyber security risks are increasing.
- 25% of breaches in 2019 were motivated by espionage.
- 71% of breaches in 2019 were financially motivated.
- 4.1 billion records were exposed by data breaches in the first half of 2019.

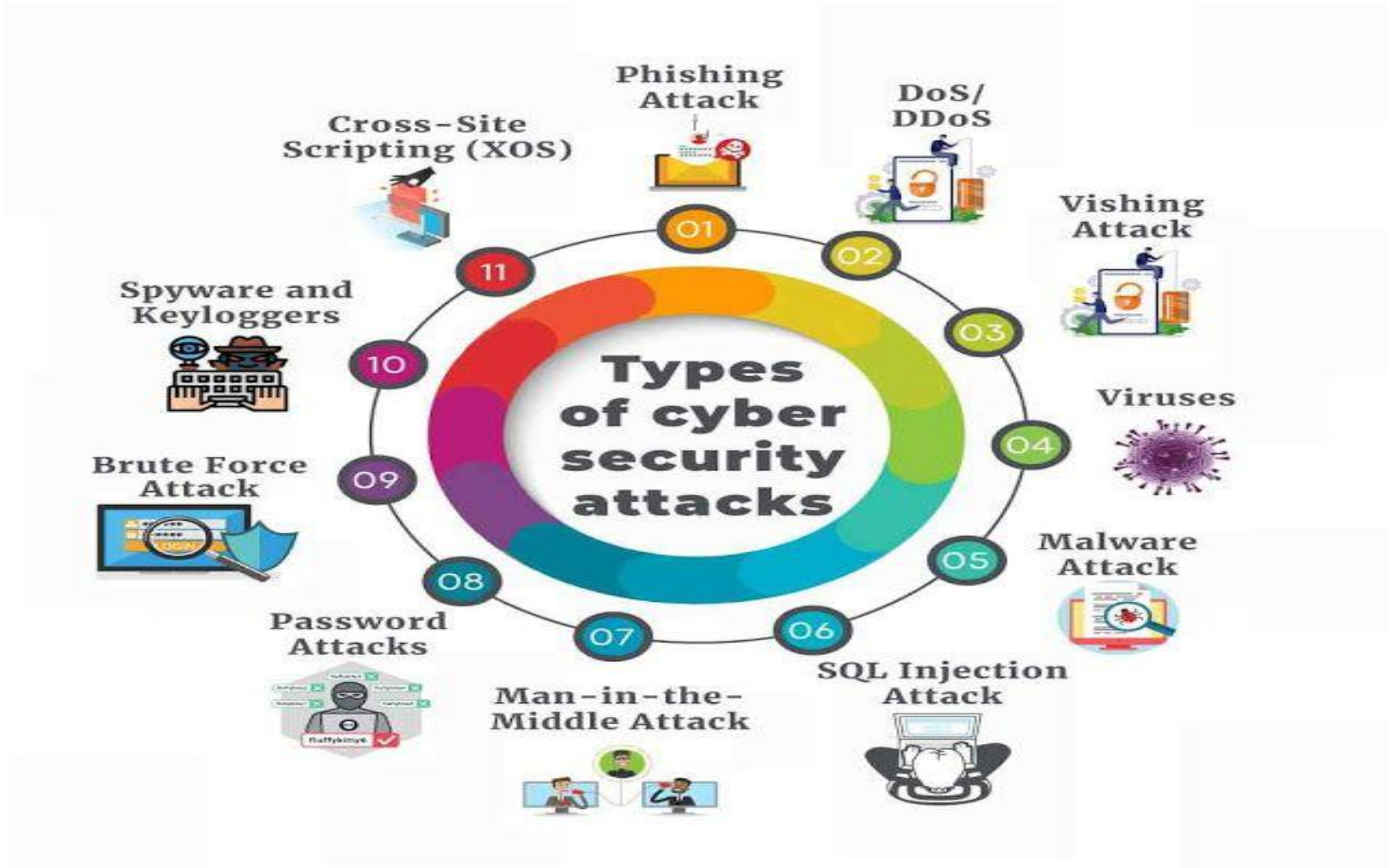
University of North Dakota:
https://onlinedegrees.und.edu/blog/types-of-cyber-attacks/



Common Causes of Cyber attacks

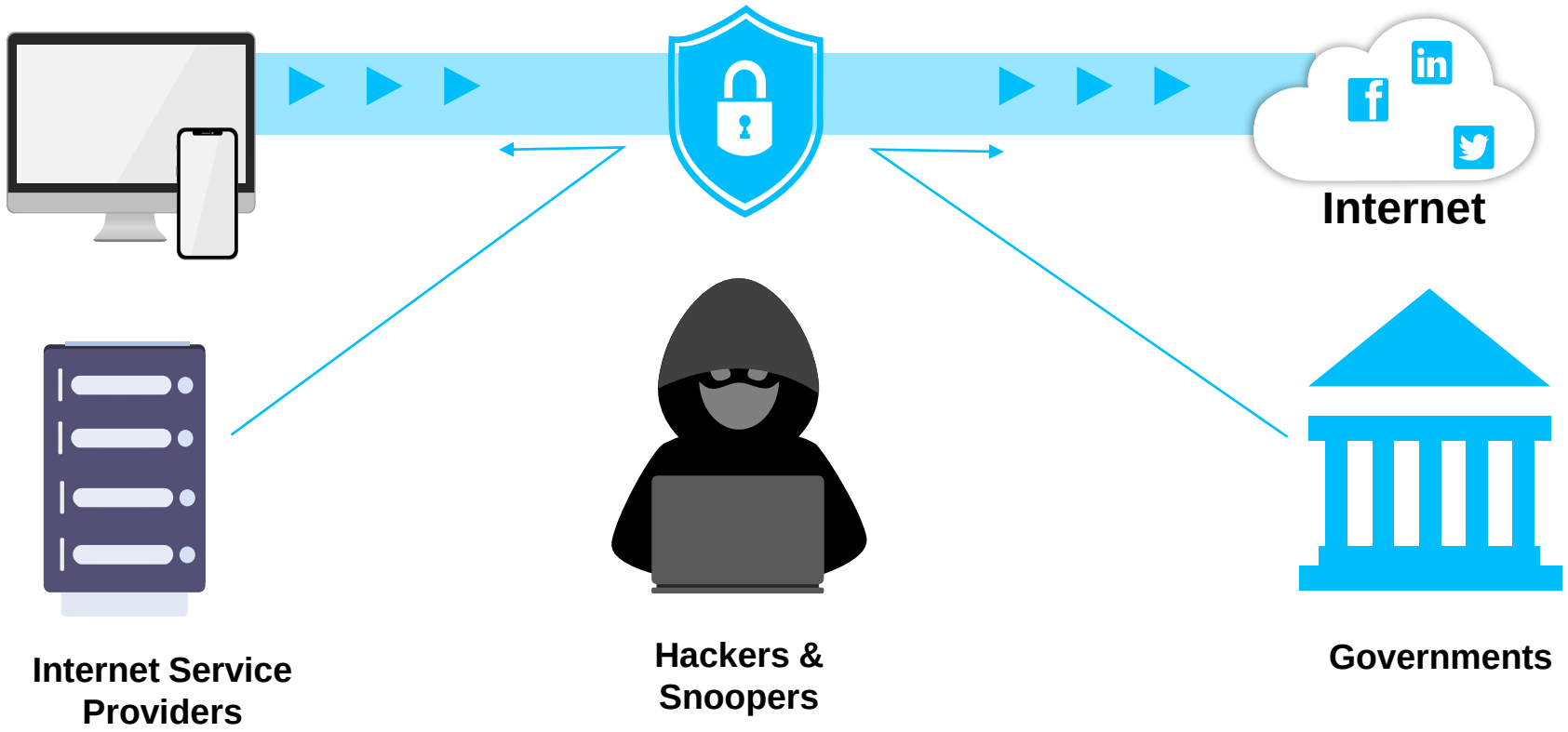
- Weak or stolen usernames and passwords
- Application vulnerabilities
- Absence of Antivirus and latest patches
- Use of Pirated Operating Systems
- System and Network Firewalls disabled
- Social engineering (tricking people into breaking security protocols)
- Poor access control (Unauthorized users have access)
- Insider threats (System Password has not set)
- Improper configuration of WIFI devices and Hotspots
- Unnecessary Ports opened on Network for Backdoor Entry

Types of Cyber Attacks



Malware

Malware is intrusive software that is designed to damage and destroy application and computer systems. Malware is a contraction for “malicious software.” Examples of common malware includes viruses, worms, Trojan viruses, spyware, adware, and ransomware.



Salient Differences

1) **Computer Virus:**
   - Needs a host file
   - Copies itself
   - Executable

2) **Network Worm:**
   - No host (self-contained)
   - Copies itself
   - Executable

3) **Trojan Horse:**
   - No host (self-contained)
   - Does not copy itself
   - Imposter Program

Phishing, Spoofing & Ransomware

- **Phishing:** a 'trustworthy entity' asks via e-mail for sensitive information such as UID, credit card numbers, login IDs or passwords. It is a kind of social engineering attack where a person steals the sensitive information of user in a fraud manner by disguising as a legitimate person.
- **Spoofing** is a kind of computer virus attack where a person steals the details of important a legitimate user and acts as another user. It is a kind of identity theft. Cyber criminals use spoofing to fool victims into giving up sensitive information or money or downloading malware
- **Ransomware** is a new type of malware that encrypts documents, pictures and other files, making them unreadable. The attacker then holds the decryption key for ransom until you agree to pay money, usually through an untraceable method such as BitCoin or other digital currency.

Do:

- Always verify the sender of a message.
- Always hover over web page links (URLs) in email messages to see where they link to – beware URL shortening services (like bit.ly) that may obscure the final web site destination.
- Be skeptical of messages with odd spelling/grammar, improper logos or that ask you to upgrade or verify your account.
- Report suspicious emails to **support@gov.in or NIC**
- Take backups of important files to avoid ransomware

Don't:

- Open an attachment from an unknown sender. Consider the source and whether or not the file was expected.
- Click on a link from an unknown sender.

Social Engineering

Social engineering manipulates people into performing actions or divulging confidential information. Similar to a confidence trick or simple fraud, the term applies to the use of deception to gain information, commit fraud, or access computer systems.

Phone Call: This is John, the System Admin. What is your password?

In Person: What ethnicity are you? Your mother's maiden name?

Email: ABC Bank has noticed a problem with your account…

I have come to repair your machine…

and have some software patches

Violation of Information Security

The classified official communication(i.e. in four categories **TOP SECRET, SECRET, CONFIDENTIAL and RESTRICTED.**) on public domain messaging platform like **WhatsApp, Telegram, messenger etc.** is a clear violation of information security instructions as provided in Manual of Departmental Security Instructions **(MoDSI)** and National information Security Policy Guidelines **(NISPG).**

According to NISPG, the Top Secret and Secret information shall be shared only in a closed network with leased line connectivity where Scientific Analysis Group - DRDO(SAG) grade encryption mechanism is deployed. However, Confidential and Restricted information can be shared on internet through networks that have deployed commercial AES 256-bit encryption.

International Threat

Information shall be harvested by private companies owning the platform as they control storage servers that are often located outside the country.

Information Tampering

Disrupt digital operations or damage information of the plans and projects yet to be formalized

Individual Information leakage

Personal information of an individual is used for adversaries or can be monetised for gains.

MHA Recommendations to maintain Cyber Security

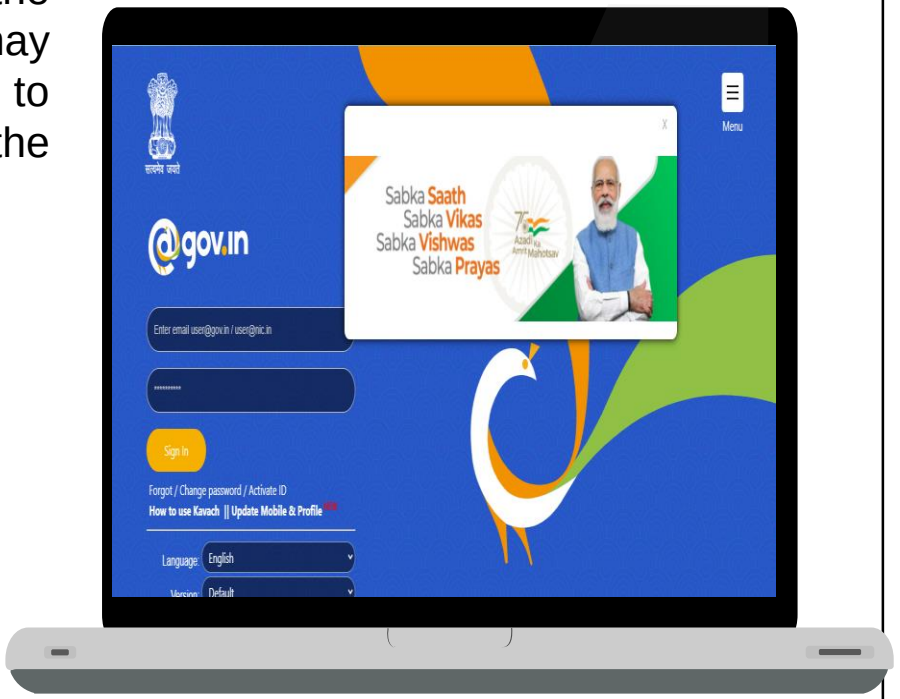
1) **Use eOffice for official communication:** The product is developed by National Informatics Centre (NIC) and aims to usher in more efficient, effective and transparent inter-government and intra-government transactions and processes. it may be advised that the Ministry/Department may deploy proper firewalls and white-listing of lP addresses. The eOffice service may be accessed through a Virtual Private Network (VPN) for enhanced security. The Top Secret & Secret information shall be shared over the e-Office system only with leased line closed network and SAG grade encryption mechanism.

Benefits of eOffice :

- Enhance transparency
- Increase accountability
- Assure data security and data integrity
- Promote innovation by releasing staff energy and time from unproductive procedures
- Transform the government work culture and ethics

MHA Recommendations to maintain Cyber Security(Cont.)

2) **Use Government Email (NIC Email) for official communication**: NIC email facility or Government instant Messaging Platforms (such as CDAC's Samvad, NIC's Sandesh, etc.) is recommended in the Ministry/Departments for the communication of Confidential and Restricted information. However, utmost care should be taken during the classification of information and before the communication of the same over internet (i.e. an information which may deserve a Top Secret & Secret classification shall not be downgraded to Confidential/Restricted for the purpose of sharing the information over the internet).

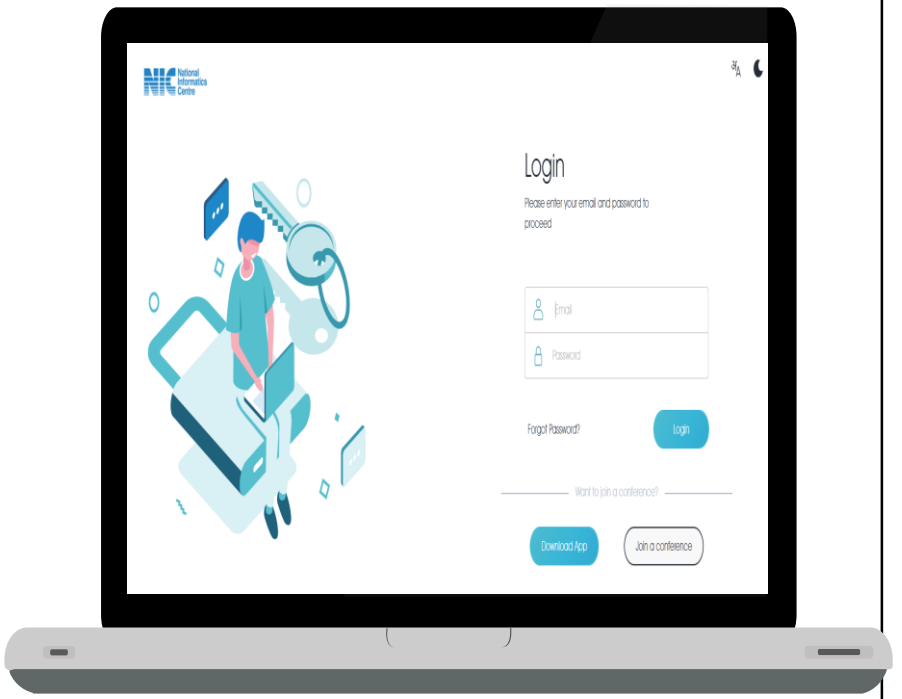


- **Features…**
  - Email platform is supported by 2-level authentication factor i.e. **KAVACH** which enables extra security.
  - The feature of **BRIEFCASE** which is used to store the personalize data similar to google drive
- **NIC never asks…**
  - … for your credentials via email or over the phone.
  - … to follow a link to clean a virus from your email mailbox, upgrade or reactivate your account.
  - … you to update or increase your email quota.

When in doubt, forward suspicious emails to **support@gov.in or NIC Division of Ministry**

MHA Recommendations to maintain Cyber Security(Cont.)

3) **Use only Government Video Conferencing solutions:** The VC platforms offered by CDAC, CDOT and NIC (BharatVC, VidyoConnect, Studio based) may be used. The meeting lD and password shall be shared only with authorized participants. To ensure better security, the 'Waiting Room' facility and prior registration of the participants may be used. However, Top Secret and Secret information shall not be shared during the VC.



Benefits of Government VC solutions :

- Due to secure network transmission which assures data security and data integrity
- Data recordings and sharing rights are confined within government organizations like CDAC, CDOT and NIC.
- It prohibits the trespassers from breaching into the system as communication happens within dedicated government network and servers.

MHA Recommendations to maintain Cyber Security(Cont.)

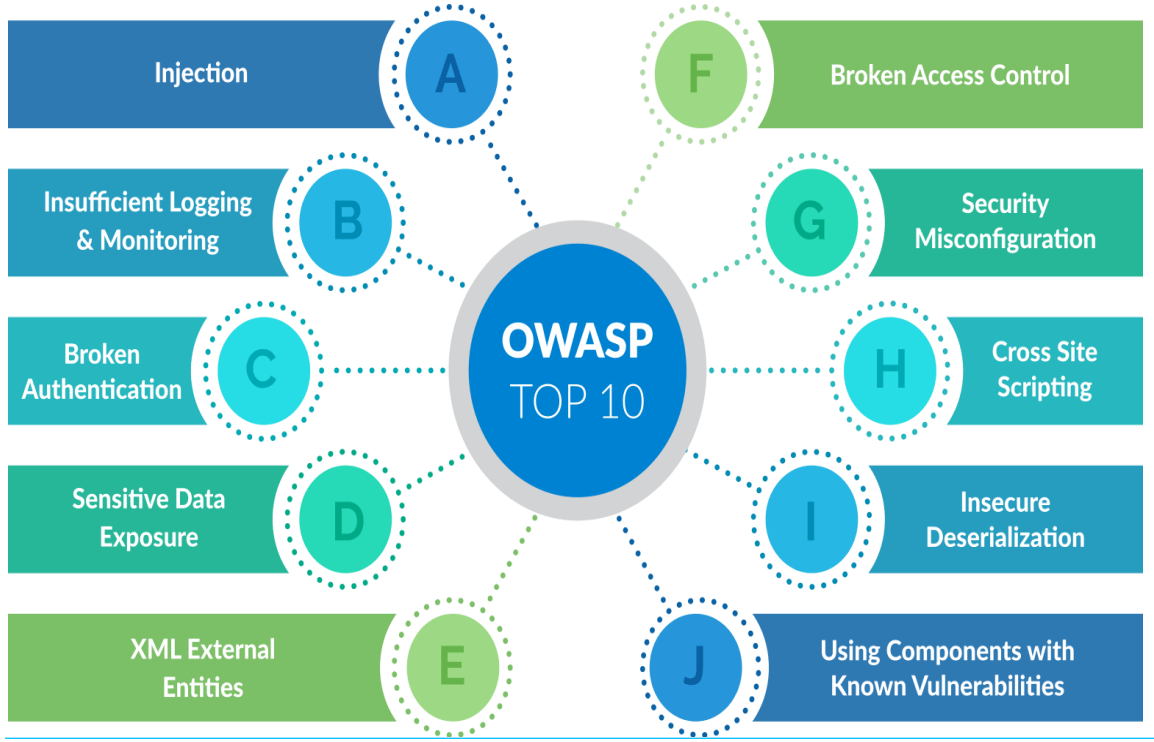
4) **Avoid Digital Assistant devices:** While discussing official information avoid usage of digital assistant devices like Amazon's Echo, Apple's HomePod, Google Home, etc. and may not be kept in office. Further, Digital Assistants (such as Alexa, Siri, etc.) should be turned off in the smart phones/watches used by the employee. Smart phones may be deposited outside the meeting room during discussion on classified issues.

Benefits of avoiding digital assistant devices:

- Decrease the chances of incident that results in unauthorized access to information.
- Increase accountability

OWASP Top 10 / Server Hardening / Incident Reporting

The **Open Web Application Security Project** (OWASP) Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.



Server hardening is **a set of disciplines and techniques which improve the security of an server**. Hardening is the changes made in configuration, access control, network settings and server environment, including applications, in order to improve the server security and overall security of an organization's IT infrastructur

- CERT-In is functional organization under **MEitY** with the objective of securing India cyber space and respond to cyber attacks.
- incident@cert-in.org.in is the email address to report any incident of cyber attack.
- For closing of Fake / clone websites and applications FIR copy is mandatory for necessary actions.

Mobile Device Security

- Keep your device software up to date – unpatched software leaves your device vulnerable to attack. Install operating system updates as well as updates to applications.
- Have anti-virus and/or anti-malware software installed, enabled and set to automatically update.
- Never leave your laptop or mobile device unattended. Thefts do happen.
- Encrypt laptops and external media that contains restricted or sensitive data.
- Make sure you backup your data frequently in case your device is ever lost or stolen.
- Ensure access to your mobile device is protected with a passcode and use built-in encryption settings to ensure that your data is safe if your device is ever lost or stolen.
- Consider using a remote tracking/wipe function if supported. For iOS devices, iCloud provides the “Find my iPhone” service for free. Android and other mobile operating systems also have similar functionality.

Cyber Security - Dos and Don’ts

Password Protection		
S.No.	**Dos**	**Don’ts**
1.	Use hard-to-guess passwords or passphrases. A password should have a minimum of 10 characters using uppercase letters, lowercase letters, numbers, and special characters. To make it easy for you to remember but hard for an attacker to guess, create an acronym. For example, pick a phrase that is meaningful to you, such as “My son's birthday is 12 December 2004.” Using that phrase as your guide, you might use Msbi12@Dec,4 for your password.	Do not use simple dictionary words, your name, username, Date of Birth, Vehicle No, Relatives, Pet names, computer terms (Admin etc.), common names (including people or city etc.), technical jargon, etc. as password. Do not use all letters or all numbers, repeating sequences and keyboard sequences, word, or number patterns (abcdefg, qazxsw, qwerty, 123456 etc).
2.	Use different passwords for different accounts. If one password gets hacked, your other accounts are not compromised.	Do not share passwords or other Sesnitive Information with others or write them down on Notepads or Sticky Note etc.
3.	Keep your passwords or passphrases confidential. You are responsible for all activities associated with your credentials.	Do not respond to phone calls or emails requesting confidential data.
4.	Change passwords on a regular basis. It helps to prevent your passwords from being compromised.	Do not use auto save for PASSWORD and other sensitive information.

Cyber Security - Dos and Don’ts

System Protection		
S.No.	**Dos**	**Don’ts**
1.	Install the NIC managed centralized antivirus for regular updates and to check malicious traffic.	Do not install and update antivirus from unauthorized sources or click on unauthorized links prompting to install antivirus or any other softwares.
2.	Enable system Antivirus, firewall and install OS patches / upgrades time to time on machines (Desktop, Laptop, mobile etc.).	Do not use EoL (End of Life) and pirated Operating System, Office Utility or any other prirated softwares. Use only genuine softwares.
3.	Always Install the softwares only receommeded by IT Department. Also, remove / delete the unnecessary softwares, folders and files from your Workstations on timely manner.	Do not install unauthorized programs on your work computer. Malicious applications often pose as legitimate software. Contact your IT support staff to verify if an application may be installed.
4.	Routinely and periodically update systems and applications for all devices.	Do not use outdated devices or unsupported software versions which increase the risk of information’s being compromised.
5.	If you are going short break, always lock your Laptop/PC. Never keep Laptop or PC unprotected. If you are going for Longer Duration Meeting etc, try to keep the Laptop on Sleep Mode to save Energy.	Do not leave laptop or other devices accessible and unattended at any time which could allow for unauthorized access. Do not leave laptop and other devices in a non-trusted environment which presents a higher risk of the device being stolen or compromised.

Cyber Security - Dos and Don’ts

Information dissemination and disposal		
S.No.	**Dos**	**Don’ts**
1.	Use of Gov.in / NIC.in emails for official communications.	Do not use personal email ids except those exempted.
2.	Use privacy settings on social media sites to restrict access to your personal information.	Do not post any private or sensitive information, such as credit card numbers, passwords, or other private information, on public sites, including social media sites, and Do not send it through email unless authorized to do so.
3.	Destroy information properly when it is no longer needed from electronic media and papers. Recycle bin should be cleaned daily.	Do not retain Information for longer than necessary.
4.	Regulate the use of USB storage devices like pen drive, smart phones, tabs etc. It has been observed that unregulated use of many such devices is one of the reasons for spread of malware in the network.	Do not create HOTSPOT on machines to avoid misuse
5.	Hard Disk should be formatted before moving Computer from different sections and responsibilities to avoid data leakage	Do not use MTNL/ AIRTEL/ VODAFONE/ JIO etc. ISP networks on official machines.

Cyber Security - Dos and Don’ts

Phishing or Smishing or Vishing Attacks		
S.No.	**Dos**	**Don’ts**
1.	Pay attention to phishing traps in email and watch for telltale signs of a scam. Always think before you click to help keep yourself and organization safe. The common actions that a malicious sender will try to get you to take are: i. Opening an attachment deemed to be highly important or urgent ii. Reply immediately (including clicking an unsubscribe option) iii. Clicking any hyperlinks in the message (including an unsubscribe option) iv. Forwarding the email message to others	Do not open mail, attachments, links (received on email, SMS and popup notifications etc.) from an unknown or untrusted source. Cyber attackers often use them to trick you into visiting malicious sites and downloading malware that can be used to steal data and damage computers/ networks. If you receive a suspicious email, the best thing to do is to delete the message and report it to NIC/ Information Security Officer (ISO)/designated security representative.
2.	Use caution if you receive an email that includes attachments or links that ask you to act. Always ensure the sender is trusted, purpose of link, URL associated with link etc.	Do not be tricked into giving away confidential information. It’s easy for an unauthorized person to call and pretend to be an employee or business partner.

Cyber Security - Dos and Don’ts

Physical information Protection		
S.No.	**Dos**	**Don’ts**
1.	Ensure that all the material shorthand notebook etc. used to prepare the final draft are treated the same way as the final draft. The unused or previously used documents should be trashed or destroyed.	Do not leave unused drafts or sensitive information lying around the office.
2.	Be aware of your surroundings when printing, copying, faxing, or discussing sensitive information. Pick up information from printers, copiers, or faxes in a timely manner.	Do not leave printouts or portable media like pen drive / CD/ DVD containing private information on your desk. Lock them in a drawer to reduce the risk of unauthorized disclosure.

News…!!!

FILES ENCRYPTED, RANSOM SOUGHT

- Hackers attacked Haldiram's servers and encrypted all its files, data and applications
- The food giant later managed to restore all data internally

US$ 7.5 lakh ransom sought

3-month delay in FIR

July 13 | Error in server reported to Haldiram's IT department. They find the servers have been hacked as part of a "ransomware attack"

July 17 | Complaint filed with Noida cyber cell

Oct 17 | FIR lodged after probe

TAKE MEASURES BEFORE IT'S TOO LATE

Graphic: Utpal Chakraborty

India ranks 3rd in cases of cyberbullying

City schools sit up as students post obscene memes on teachers online

The TOI story on Dec 19

CATEGORIES OF CYBER CRIME BY KIDS

Cyberbullying | Digital piracy | Sexting

HOW TO KEEP KIDS SAFE ON CYBER SPACE

- Use parental control software
- Place the computer in a busy area of the house
- Bookmark for safety and avoid downloads from unrecognized sources
- Set limits on late-night use; establish rules and take control
- Stay in the loop

"The problem is that a majority of such crimes has no criminal intent. They are seen as an extension of a prank. But children often don't realize the danger"
A POLICE OFFICER

RECENT DATA BREACHES

2.5 mn
Airtel: Name, DoB, phone numbers, address, Aadhaar. Up for sale for bitcoins worth $3,500

3.5 mn
MobiKwik: KYC info

20.0 mn
BigBasket: Personal information, address, PIN, IP addresses, etc for sale for $40,000

22.0 mn
Unacademy: User name, password, and email

35.0 mn
Juspay: Masked card data & card fingerprint data was for sale for $5,000 Bitcoins

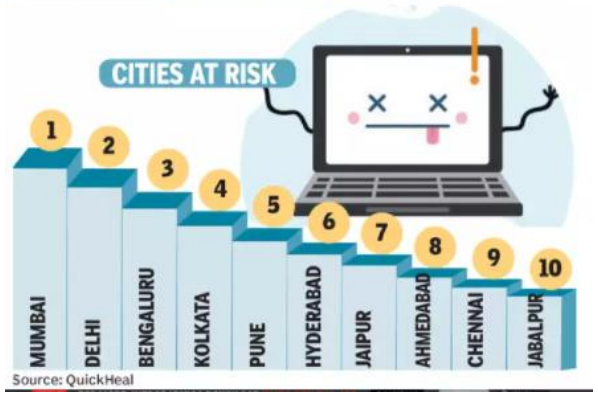
Source: News reports

CYBERCRIME TARGETS

MOST VULNERABLE STATES — Ranking

1	MAHARASHTRA	5	UTTAR PRADESH
2	DELHI	6	KARNATAKA
3	WEST BENGAL	7	RAJASTHAN
4	GUJARAT	8	TAMIL NADU
		9	MADHYA PRADESH
		10	TELANGANA
		11	HARYANA
		12	ODISHA

CITIES AT RISK



Source: QuickHeal

THANK YOU…!!!