Cyber Security Best Practices

CyCord

One stop shop on all Cyber Security related matters

Table of Contents

Cyber Security awareness and knowledge sharing can be our best defense against emerging cyber threats. Let us work together to maintain high standards of Cyber and Information Security in the Country.

1. General Computer Usage:

- Use account with limited privileges on systems and avoid accessing with administrator privileges for day-to-day usage.
- Keep Operating System, Application and Anti-Virus software's updated by applying the latest service packs and patches.
- Backup all important files at regular intervals.
- Do not leave the system unattended. Use systems screen locking functionality (such as a screen saver that won't deactivate without a password) to protect against physical access, or just log out of everything so that anyone who wants access has to login again.
- Remove/uninstall unnecessary programs or services from computer.
- Restrict remote access. If file sharing is not required in your day-to-day work, disable file and print sharing.
- Securely remove files or data you no longer need to prevent unauthorized access to them. Merely deleting sensitive material is not sufficient, as it does not actually remove the data from your system.
- Scan all the files that you download whether from websites or links received from e-mails.
- Do not download unfamiliar software from the Internet.
- Restrict users' ability to install and run unwanted software applications by applying software restriction policies appropriately and disable running executables from unconventional paths.
- Supervise maintenance or rectification of faults of the system(s) by service engineers.
- Use Defender Credential/Device Guard on Windows 10 and Windows Server 2016 to enforce constrained language mode and application white-listing by leveraging advanced hardware features where supported.
- Prohibit any remote logon to the system.
- Minimize and completely deny granting administrator privileges for users of local PCs, especially for users who work with external information systems.

2. General Internet Browsing:

- Be conscious of what you are clicking on/downloading. Download software from trusted source only.
- Verify those you correspond with. It is easy for people to fake identities over the Internet.
- Do not store official information/documents on Internet Cloud (iCloud, Google Drive, Dropbox etc.) or Internet connected computers.
- Make a habit of clearing history from the browser after each logout session.
- Delete Windows "Temp" and "Temporary Internet files" regularly.
- Avoid using services that require location information. Avoid posting of photos with GPS coordinates.
- Remember search engines track your search history and build profiles on you to serve you personalized results based on your search history.
- Some pop-ups have what appears to be a close button, but will actually try to install spyware when you click on it.
- Be wary of free downloadable software. There are many sites that offer customized toolbars or other features that appeal to users, which are likely to have backdoors. Remember that things on the internet are rarely free. "Free" screensavers, games, software's etc. may generally contain Malware.
- Frequently check unusual folder locations for document (.doc, docx .xls, .xlsx and .def) file extensions (in search options, select advanced search options, make sure you checked "Search System folder", "Search hidden files and folders" and "search subfolders").
- Don't respond to emails, instant messages (IM), texts, phone calls, etc., asking you for your password.
- Be extremely careful with file sharing software. File sharing opens your computer to the risk of malicious files and attackers. Also, if you share copyrighted files, you risk serious legal consequences.

3. Malware Defense:

- Always set automatic updates for Operating System, Anti-Virus and Applications.
- Enable hidden file & system file view to find any unusual or hidden files.
- Turn off auto play (Start -> Run -> type gpedit.msc ->Computer Configurations -> Administrative Templates -> Windows Components -> Select "AutoPlay Policies" -> Double Click at "Turn off Auto play" -> Select Enabled -> Set "Turn off Auto play on:" to "All drives").
- Create the following parameter in the registry of PCs running Windows 8 (and up) and all the servers using Windows 2012, to prohibit storing unencrypted passwords in RAM (which are usually leveraged by Mimikatz).

  HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Control/SecurityProviders/WDigest/UseLogonCredential=0
- Type: %temp% in "run" and delete all entries after opening any suspicious attachments.
- Type cmd in run and type netstat –na. Checkout Foreign established connection and IP addresses. Check the IP address for its ownership.
- Type "msconfig" in "run" and check for any unusual executable running automatically.
- Check Network adapter for data/packets received and sent. If the outgoing / sent is unusually high, then it is very likely that the system is compromised.
- Type "ipconfig /displaydns" in command prompt and look out for any URLs which you have not accessed recently.
- Always be cautious while opening attachments even from the known sources. Try to use non-native applications for opening attachments. Example for word document use, WordPad to open the attachment.
- When in doubt, better to format the Internet connected computer rather than doing some "patch works".
- Prohibit any remote logon to the system (RDP, SMB, RPC) for local administrators.
- Check regularly if any unusual applications running from %appdata%, %tmp%, %temp%, %localappdata%, %programdata%.
- Isolate hosts in the same VLAN, so that one workstation would not be able to gain access to another one on network levels L2/L3, and could access shared network segments (printers, servers, etc.)

- Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources as well as addresses and block these before receiving and downloading messages.
- Disable file and printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Disable or prevent ActiveX controls in Microsoft Office Word Document from running without prompting.
- Disable Macros in Microsoft office documents (doc/docx, xls/xlsx, ppt/pptx and mdb/accdb). By default, Microsoft products come with VBS Macro disabled.
- Disable Java Scripts or similar scripting functions in Adobe Acrobat Reader for PDF files.
- Configure built in "File Protection Setting" feature in Microsoft office 2010.
- Configure built in feature for "Protected View" settings in Microsoft Office 2010 to open the Microsoft Office word documents in Protected view.
- Check for unrecognized tasks being registered in task scheduler using "**Schtasks /Query /FO LIST /V**" from command prompt.

4. USB Storage Device (Pen Drive / External Hard Disk etc.):

- Use only authorized official USB storage devices for official work.
- Records of USB storage devices should be maintained.
- Damaged/faulty Removable Information Storage media (RISM) should never be handed over to outsiders/manufacturer for repair.
- Sensitive information should be stored on removable media only when required in the cases of assigned duties.
- All media must be stored in a safe and secure environment.
- All media must be handled with care and it must be ensured that it is not kept near magnetic material or exposed to extreme heat or pollution.
- The computers should be enabled with "Show hidden file and folders" option and "Hide protected operating system files" should be disabled to view hidden malicious files in USB storage devices.
- Make sure there is no hidden file or folders present in the Media.
- Autorun/Autoplay feature should be disabled in all the computers.
- Avoid Baiting (Someone gives you a USB drive or other electronic media that is preloaded with malware in the hope you will use the device and enable them to hack your computer). Do not use any electronic storage device unless you know its origin is legitimate and safe.
- Scan all electronic media for Malware before use.

5. Password:

- Passwords must be changed at regular intervals.
- Always use different passwords for different accounts.
- Do not share passwords with anyone.
- Passwords should never be written down or stored on-line without encryption.
- Do not reveal a password in email, chat, or other electronic communication.
- Do not reveal a password on questionnaires or security forms.
- Always decline the use of the "Remember Password" feature of applications.
- All users should be aware of how to select strong passwords.
- Strong passwords contain at least thirteen alphanumeric characters (except in the case of BIOS, if the same is not possible) in combination of lower case characters, upper case characters, numbers and "Special" characters (e.g. @#$%^&*()_+|~-=\`{}[]:";<>/ etc).
- Password history should be enforced wherever possible to ensure that the users are forced to select different passwords with a user account.
- Maximum password age should be configured to enforce the period of time (90 days) that a password can be used before the system forces the user to change it.

6. Social Engineering:

- Social Engineering is an approach to gain access to information through misrepresentation. It is the conscious manipulation of people to obtain information without realizing that a security breach is occurring. It may take the form of impersonation via telephone or in person and through email.
- Some emails entice the recipient into opening an attachment that activates a virus or malicious program into recipient's computer.
- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information.
- Don't send sensitive information over the Internet before checking a websites security. Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information.
- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic.
- Take advantage of any anti-phishing features offered by your email client and web browser.
- Immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future.

7. Best Practices for Mobile Phones / Tabs:

- Do not store any classified/sensitive data (text/video/ photograph) in the device.
- Before downloading any App, same should be checked for its reputation/review. Read vendor privacy policies before downloading Apps and App permission should be reviewed closely.
- Disable installing of third party Apps from unknown sources.
- Disable background data for Apps which are not used frequently.
- Avoid use of wallet aggregator Apps, which stores/links other e-wallets and banking Apps.
- Auto start, data usage for each App and App permission should be controlled through the security features available (depends on OS and make of the phone).
- Review the default privacy settings of smart phone Apps or services and, if needed, change the settings; e.g. settings about whether or not to attach location data to images, to social network posts, etc.
- Relevant anti-virus software should be installed in the smart device and same be updated regularly.
- Turn off GPS location services when not needed.
- Disable/remove the Apps which are not needed.
- When device is idle, it should get locked and require a password/PIN or swipe pattern. Set the device to lock in relatively short time.
- Take back-up of data (contacts, personal photos, etc.) on external media.
- Do not reply or click on link on SMS or messages or photos sent by strangers.
- Be cautious with public Wi-Fi. Many Smartphone users use free Wi-Fi hotspots to access data (and keep their phone plan costs down). There are numerous threats associated with Wi-Fi hotspots. To be safe, avoid logging into accounts, especially financial accounts, when using public wireless networks.

8. Incident Prevention, Detection and Response:

Incident Prevention

- Use firewalls to create a buffer zone between the Internet and other untrusted networks used by creating firewall rules to deny traffic by white-listing only authorized protocols, ports and applications to exchange data across the boundary to reduce the exposure of systems to network based attacks.
- To limit the lateral movement as well as other attack activities, use Endpoint Security/network firewall to prevent Remote Procedure Call (RPC) and Server Message Block (SMB) communication among endpoints whenever possible.
- Adopt application whitelisting policy on all endpoint workstations to prevent malicious code or unauthorized software from gaining execution on endpoints.
- Remove unused or unpatched software from the computer, particularly remote desktop software, if any.
- Ensure that application control (to allow only approved scripts to run) prevents unapproved programs running regardless of their file extension.
- Ensure all end point systems having antivirus or a malware protection program running on it and is always up to date with latest signatures.
- To mitigate certain malware family, which executes from user directory, block execution from user profile directories (%AppData%, %LocalAppData%, %Temp%) and its subdirectories.
- To prevent malicious scripts from running on click, the notepad program can be associated (with always use this app option) with script file extensions such as .hta, .js, .jse, .vbs, .vbe, .wsf and .psl.
- Perform regular red-team/blue-team exercises on the network to re-establish the rules, configurations and policies.
- Conducting of phishing drills among users via simulation will make them more sensible to handle such attacks.

Incident Detection

- Monitor DNS activity for potential indications of tunneling and data exfiltration.

- Regularly check for configuration changes and appropriate usage of configuration for possible intrusion.
- Deploy Microsoft SysInternals Tool **'SysMon'** to monitor and log system activity to the Windows Event Log.
- Restore the system to a last-known good back up or proceed to a fresh installation.

Incident Response

- Disconnect the infected computers from LAN/Internet immediately.
- Block / Restrict connectivity to the malicious domains /IP addresses shared by various security agencies. Take the forensics image of the identified machine connecting to such domains after Isolating.
- Remove unused or unpatched software from computers, particularly remote desktop software, if any.
- Change passwords of all email and online services from another secure computer.
- Hard Disks of the infected computers may be formatted after taking backup of data.
- Operating systems and applications should be re-installed from clean software.
- Backup data should be scanned for virus before restoring it.

9. Organization Level Security Controls:

- Enforce **Multi-Factor Authentication (MFA)** to prevent phishing attacks that steal email credentials. In case MS Office 365 is being used MFA should be enabled. MFA should also be enabled for Windows logins which would be effective against brute force attacks particularly using Remote Desktop Protocol (RDP).
- Enable **network segregation** (partitioning of a network to keep critical parts of the infrastructure away from the internet and from less secure internal networks) to contain malicious activity and prevent successful propagation of the malware. This can prevent direct attacks on systems that should not be internet facing. Effective monitoring of log-ins and auditing of sensitive data can be put in place to ensure that the data is tracked.
- Install **Anti-Phishing software** that can run on the mail server and examine emails for any hyperlinks containing phishing websites/malwares. This can prevent credential loss and malicious code execution through phishing.
- Ensure **Patch management** (software running on the network is patched and up-to-date) is done on regular basis especially on servers where unpatched remote desktop software if present could lead to cyber-attacks. Else remove unused or unpatched software from computers, particularly remote desktop software. Close ports that need not be connected to the internet.
- Enforce **Password policy** in the organization to ensure that a minimum strength of password is complied with across the network. This would help in preventing brute force attacks and from attackers taking advantage of default passwords.
- Periodical **audit of IT systems** to be carried out.
- **Legacy computers** (particularly internet facing servers) **to be taken off** so as to reduce attack surface.
- **Educate staff** on phishing attacks and email compromise frauds.
- Use **Firewall Access Control Lists** to restrict direct network access to user machines so only approved devices are allowed to connect to them.
- Perform **regular backups** to allow quick restoration of impacted devices. Ensure backups are kept offline and make sure there is a recovery plan in place.

- To secure the web application, **regular Vulnerability Assessment and Penetration Testing (VAPT)** of the entire Information and Communications Technology (ICT) infrastructure from competent auditors and testers, may be carried out.
- Proper inventory of all assets should be maintained.
- All sensitive data communicated over a network within physically secured boundaries may be cryptographically secured as per user.
- The network diagram should be updated to give details of all new network devices. All critical assets be clearly identified.
- Logs of all network devices and systems should be maintained. Access to these logs should be restricted. They should be analyzed and correlated with policies regularly.
- Administrative access to configure devices should be from specific computers only (based on IP or MAC).
- Signatures to be updated for signature-based Intrusion Detection regularly after scanning and installing them on a separate and isolated machine.
- Remote management should be permitted only for firewalls of network segments communicating unclassified information.
- Router/Switch configuration should be properly documented and regular back up of Router/Switch configuration should be done.
- Unused router, switch ports should be disabled and only authorized persons should have administrative privileges to configure the routers, switches etc.
- Training programs/seminars should be conducted periodically to aware the users.

Work From Home (WFH) Environment

- Only approved users and devices by the head of the organization should be allowed.
- The organizations must ensure provision of accessing personal computer / devices of employees is done in a standardized and secure manner.
- Appropriate device configuration must be maintained and security capability must be deployed, to prevent remote access of data from

outside the organizations boundary by allowing only approved devices based on the unique parameters (MAC ID, IP etc.) of the device.

- Two factor authentications should be implemented on different communication channels (like SMS for OTP and user name and password through secure protocol over the Internet).

Video Conferencing - Securing the VC Cameras

VC cameras, which are not protected with any password or having weak password, could be exploited to eavesdrop into the ongoing video conferencing, monitor calls, read call logs, CDR's of VC, intrude/interrupt ongoing call, etc. The vulnerability could be further exploited through remote maintenance module to switch on the camera and monitor activities. To prevent such attacks:

- Set a strong password to manage the VC camera.
- Disable administration interfaces from remote access.
- Disable use of default accounts/passwords.
- Check periodically to detect any misconfigurations or missing patches.

For Secure use of commercial VC solutions for discussions between Governments and parent partner organizations:

- A separate system may be designated by the organization. Such system should not store any classified or sensitive information.
- The background for the meeting should be chosen in such a manner (like plain wall, curtains or background option of the VC application) so that no sensitive documents / surroundings are visible during VC.
- Wherever possible, an isolated Internet connection should be preferred for such VCs. Logical isolation may also be considered for VC systems so that other internal systems are not exposed to the VC network.

10. Email Security Practices:

- Do not open/reply email links (hyperlinks/web links/URLs mentioned in the body of such mails) claiming to offer anti-spyware software. The links may serve the opposite purpose and actually install the spyware it claims to be eliminating.
- Scan mail attachments before downloading/opening.
- Use two factor authentication wherever possible.
- Use different email accounts for personal and professional purposes.
- Periodically check last log-in activity for any unauthorized access.
- Change passwords of all online accounts (emails and others) from another secure computer, if any suspicious activities like email access from foreign IP addresses, etc. are noticed.

--------End--------

Disclaimer: The information provided is for awareness and knowledge enhancement purposes and without warranties of any kind.

CyCord Support Team

cycordsupport.mha@gov.in
011-20861946/48
+91-7292045198
https://cycord.gov.in