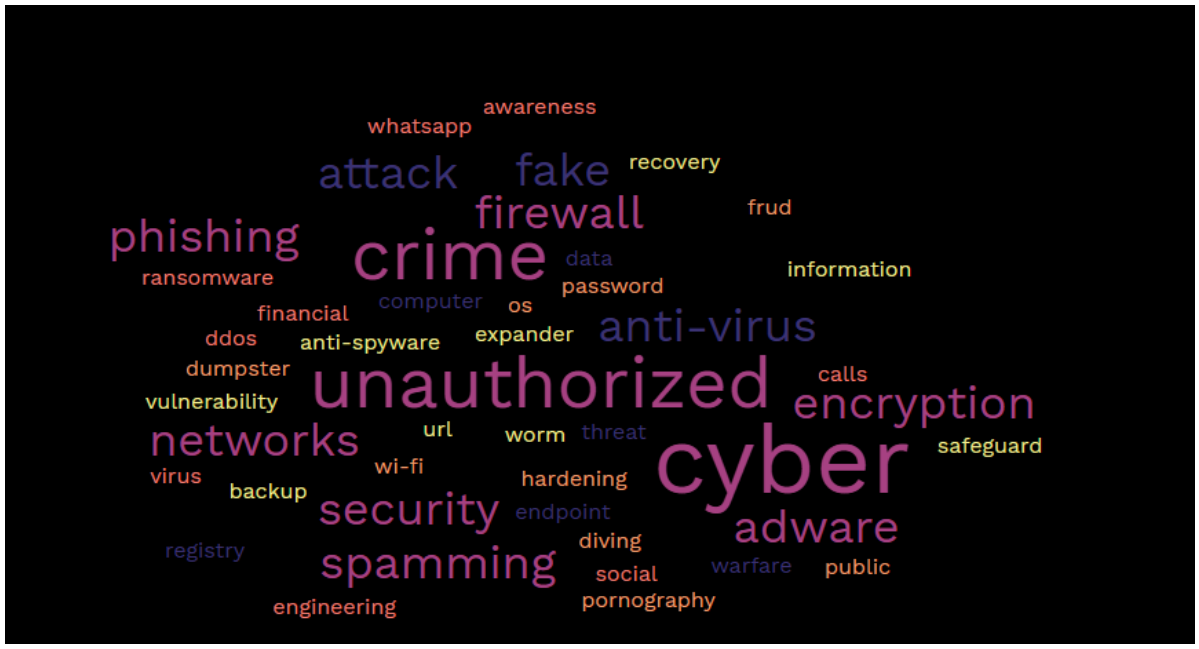


MAY 2023

# CYBER SECURITY

Cyber Security deals with securing data, devices, and networks against unauthorized use or access while assuring and maintaining information availability, and integrity. Cyber security advisories for desktop computers are notifications or warnings to inform users about potential or existing security threats and vulnerabilities that may affect their desktop computers. These advisories aim to provide users with information and recommendations on how to mitigate or address these security issues and protect their systems from potential attacks or data breaches.

Endpoint security: It involves securing every device that serves as an entry point to the network. This includes mobile devices, laptops, desktops, and servers, amongst others. Endpoint Security techniques include utilizing Antivirus and malware detection tools, restricting or allowing access only to certain users or devices, and periodically updating the software.

An effective cybersecurity strategy requires several components to work together. The combination of these components can help organizations secure their systems, infrastructure, data, and intellectual property-rights, among other essential assets.

**INDIA IS AMONG TOP 5 COUNTRIES VICTIMIZED BY CYBER CRIME**

**PROJECTED LOSSES DUE TO CYBER CRIME USD 8TN BY 2024**

**MOST IMPORTANT FACTOR IN FIGHT AGAINST CYBER CRIME IS AWARENESS AND PEOPLE'S ATTITUDE**

**40% OF ALL CYBER ATTACKS HAPPEN THROUGH MALICIOUS LINKS**

**INDIAN COUNCIL OF AGRICULTURAL RESEARCH**

ICT Unit, Krishi Bhawan,
New Delhi -110001

https://www.icar.org.in

May 2023


# Cyber Security for Desktop/ Laptop

End point security is one of the most important component of the security framework. Personal computer used without proper security measures can be being exploited for illegal activities by using the resources of such unsecure computers. It may lead to loss of personal and other sensitive data, confidential information, and theft of login credentials, like user id/passwords. Some important Security advisories for End point security are as follows:

- Enable auto-updates in Operating System and update it regularly.
- Avoid saving too much Data on Desktop and folders like Documents, Downloads.
- Keep all application Software's like MS Office, Web browser up to date by installing software updates for your application programs.
- Always install an Anti-Virus Software from a Trusted Website and make sure it automatically gets updated with latest virus signatures to prevent zero-day exploits.
- Anti-Spyware Software provides protection from spywares, make sure it automatically updates with latest definitions. So, if possible, install an anti-spyware software for security in personal computer.
- Use "Encryption" to secure your valuable Information. For encryption, password is required. Always remember the password used while encrypting it, else data would not be available thereafter.
- Strong password should be used for "Administrator" Account on computer and for other important applications like E-mail and Financial Applications.
- Remove unnecessary or unwanted programs or services from computer.
- Always keep system firmware updated with latest updates.
- Restrict remote access to computer.
- Periodically backup your computer data on external devices like CD / DVD or USB drive as the data on system may get corrupt due to Hard Disk failures or while reinstalling/formatting the system.
- Always keep recovery disk supplied by Manufacturer / Vendor of the Computer System to recover the Operating System in the event of boot failure due to system changes.
- Startup programs/services should be monitored/ controlled for optimal system performance.
- Always use screen saver with password enabled or logout from your laptop, phone, or tablet if you need to leave it unattended to safeguard against any sensitive data leakage.
- Use account with limited privileges on Desktop system and avoid accessing with administrator privileges for day-to-day usage to avoid installation of malware/ unwanted software accidentally.
- Always keep device drivers updated with patches provided by OEM as vulnerabilities in driver code can allow an attacker to gain access to the OS kernel, creating a possibility of compromising the entire OS.
- Scan external media like USB drive for Malware before use.
- Use systems screen locking functionality to protect against physical access on idle system, such as a screen saver with timeout password activated, or just log out of everything so that anyone who wants to access computer has to log in again.

# *Web Browser Security for Desktop/Laptop*

Web browsers like Internet Explorer, Firefox, and Safari are used for routine tasks like checking email, accessing e-Governance applications and browsing Internet. Web browsers must be configured securely for safe browsing.

Some safe browsing tips are as follows:

- Always keep your Web Browser updated with latest patches.
- Always have Safe Search "ON" in Search Engines like; Google, Microsoft Bing.
- Make sure to keep browser plug-ins (Flash, Java, etc.) up-to-date.
- Familiarize yourself with your browser security basics. This may include blocking third-party trackers, activating ad blockers, and automatically deleting cookies after a certain period.
- Please avoid visiting unfamiliar websites. When you come across any new sites shared by friends or strangers online, be cautious of visiting them.
- If you receive a website link that appears unusual i.e., an extra-long URL that has spelling errors or includes punctuation marks, please do not try to access this website.
- Always ensure that the website address (URL) starts with https://, not http:// especially for financial transactions online. Also ensure the validity of SSL certificate of website.
- Please disable opening of pop-up window while browsing.
- Restrict the access of unsafe plugins and extensions on your Browser.
- Verify those you correspond with. It is easy for people to fake identities over the Internet
- Only click on links from trusted sources only. Never click on a mysterious link unless you have a way to independently verify it.
- Always use URL expanders like "www.expandurl.net" to expand Shortened URLs/ Tiny URLs before clicking to avoid phishing, malware, and viruses by examining short URLs before visiting them.
- Delete Windows "Temp" and "Temporary Internet files" regularly.

# Advanced Windows Endpoint Security - Best practices

- Enable hidden file & system file view to find any unusual or hidden files. (**My Computer** -> **Tools** -> **Folder Options** -> **View** -> select enabled with "**Show hidden file and folders**" option and disable "**Hide protected operating system files**")
- Delete all the files in Temporary folder if you accidentally open any suspicious attachments. Please type: **dir % temp%** in "**Command Window**" and delete all entries.
- In case your network is running unusually slow, Type command "**netstat —na**" in "Command Window" and. Check any unusual connection and IP addresses. Check the IP address for its ownership.
- Type "**msconfig**" in "**run**" window and check for any unusual executable program entry in Boot sequence.
- Type command "**ipconfig/displaydns**" in Command prompt and look for any URLs which you have not accessed recently in the list.

# **Password – Best Practices**

Weak passwords **offer an easy pathway for cybercriminals to exploit;** and can be used to launch further attacks. If passwords are simple, short, (too) common, hackers can easily crack using widely available tools. Some best practices to avoid exploitation due to weak Passwords are as follows:

- Password must be changed at regular intervals.
- Always use different passwords for different accounts.
- Do not share passwords with anyone.
- Don't write down Passwords or store on-line without encryption.
- Do not reveal a password in email, chat, or other electronic communication.
- Strong passwords containing combination of lower case characters, upper case characters, numbers, "Special characters" (e.g. @#$%&()_+]•={[]:";<> ) should be used.
- Password should be at least 8 alphanumeric characters (except in the case of BIOS, if the same is not possible).
- Always use different passwords for different accounts.
- Password should not be composed of dictionary words, Names of family, pets, friends, colleagues, Movie / Novel / Comics. characters, Birthdays and other personal information such as address and phone numbers.

# ICT UNIT, ICAR, NEW DELHI

## CONTACT DETAILS

| | | |
|---|---|---|
|  | **Dr. Anil Rai**<br>Assistant Director General (ICT)<br>03 B, Krishi Bhawan, New Delhi -110001 | **Email**: adg.ict@icar.gov.in<br>**Tel**.: 011-23385837 |
|  | **Dr K. P. Singh**<br>Principal Scientist (ICT)<br>03 B, Krishi Bhawan, New Delhi -110001 | **Email**: kpsingh@icar.gov.in<br>**Tel**.: 011-23385835 (O) |
|  | **Dr. Himanshu**<br>Senior Scientist (ICT) & CISO, ICAR<br>513, Krishi Anusandhan Bhawan-1, Pusa,<br>New Delhi -110012 | **Email**: himanshu@icar.org.in, ciso.icar@icar.gov.in<br>**Tel**.: 011-25843369 (O) |


**Prepared By: -**

Dr Himanshu, CISO-ICAR & Sr. Scientist (ICT)
Sh N. P. Singh, CTO, ICT Unit, ICAR
Mr Adil Ansari, YP-II, ICT Unit, ICAR