रक्षा मंत्रालय
MINISTRY OF
DEFENCE

सत्यमेव जयते

CHIEF INFORMATION SECURITY OFFICER's NEWSLETTER

FOREWORD

Due to rapid changes in Information and Communication Technologies, combined with exponential growth of the Internet, the recent past has been characterised by Cyber Security being the centre of attention, for the wrong reasons.

Prior to the present Information Age, human beings have never been forced to adopt and adapt to technology at such unprecedented rates, when technological obsolescence is now the norm rather than the exception. This has led to a significant gap in understanding of technology to the desired levels.

This newsletter is the maiden attempt towards increasing awareness of personnel in the Ministry on Cyber Security matters. This issue aims to provide some basic background in terms of terminology, useful links to advisories and guidelines.

All hyperlinks / references provided in the newsletter are for information only and does not constitute their endorsement or recommendation by the Ministry.

Your feedback and suggestions towards improving Cyber Hygiene in the Ministry may be forwarded to the MoD Cyber Cell.

V Anandarajan

Joint Secretary

Security is not a product, but a continuous process. It is as strong as the weakest link.

CHIEF INFORMATION SECURITY OFFICER's NEWSLETTER

3 BASIC RULES FOR ONLINE SAFETY

1st Rule: "If you didn't go looking for it, don't install it!" Many online threats rely on tricking the user into taking some action — whether it be clicking an email link or attachment, or installing a custom browser plugin or application. Typically, these attacks take the form of scareware pop-ups that try to frighten people into installing a security scanner; other popular scams direct you to a video but then complain that you need to install a special "codec," video player or app to view the content. Only install software or browser add-ons if you went looking for them in the first place. And before you install anything, it's a good idea to get the software directly from the source. Just as you wouldn't buy a product online without doing some basic research about its quality and performance, take a few minutes to search for and read comments and reviews left by other users of that software to make sure you're not signing up for more than you bargained. Also, avoid directly responding to email alerts that (appear to) come from Facebook, LinkedIn, Twitter, your bank or some other site that holds your personal information. Instead, visit these sites using a Web browser bookmark.

2nd Rule: **"If you installed it, update it."** Yes, keeping the operating system current with the latest patches is important, but maintaining a secure computer also requires care for the applications that run on top of the operating system. Bad guys are constantly attacking flaws in widely-installed software products, such as Java, Adobe PDF Reader, Flash and QuickTime. The vendors that make these products ship updates to fix security bugs several times a year, so it's important to update to the latest versions of these products as soon as possible. Some of these products may alert users to new updates, but these notices often come days or weeks after patches are released.

3rd Rule: **"If you no longer need it, remove it."** Many computer makers ship machines with software that most users never use even once. The average user tends to install dozens of programs and add-ons over the course of months and years. All of these items can take their toll on the performance of a computer. Many programs add themselves to the list of items that start up whenever the computer is rebooted, which can make restarting the computer more slow. The more programs installed, the more time one has to spend keeping them up-to-date with the latest security patches. For example, Java is a powerful program and Web browser plugin that most people have on their machines but seldom use (the bulky program also adds itself to the startup menu in Windows every time you update it). Meanwhile, attackers are constantly targeting systems with outdated versions of this software. If you don't need Java, uninstall it. You can reinstall it if you find it is needed for some Web site or third-party application. If you can't bring yourself to completely remove Java or if you have desktop programs that require it, consider removing it from the browser by disabling the Java add-on in whatever browser you use.

Article Source: https://krebsonsecurity.com/2011/05/krebss-3-basic-rules-for-online-safety/

HELPDESK

CISO Office: 011-23018232

Cyber Cell : 011-23794783

E-Mail ID: cybercell-mod@nic.in

रक्षा मंत्रालय
MINISTRY OF
DEFENCE

सत्यमेव जयते

CHIEF INFORMATION SECURITY OFFICER's NEWSLETTER - JULY 2018

COMMON INFORMATION SECURITY TERMS

- **INFORMATION SECURITY:** The practice of protecting both physical and digital information from destruction or unauthorized access.
- **MALWARE**: Malicious software (malware) is any software that gives partial to full control of a computer to do whatever a hacker wants. Malware can be a virus, worm, Trojan, spyware, etc.
- **INCIDENT:** Any event that is not part of the normal operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service.
- **UPDATE:** It is a software file that contains fixes for problems found by other users or the software developer. Installing an update fixes the software and prevents the problems from occurring on a computer.

FUNCTIONING OF MOD CYBER CELL

- Ministry of Defence Cyber Cell, functions under Chief Security Officer (MoD) under the overall aegis of Chief Information Security Officer (CISO) of Ministry of Defence.
- Cyber Cell monitors implementation of Cyber Security in all computers/networks of MoD within DHQ Security Zone through random checks, cyber audits and issue of periodic IT advisories.

⚠ CAUTION ⚠

- **Set PC Power ON (BIOS) password.**
- **Avoid use of USB pen drives.**
- **Keep computer firewall "ON".**
- **Use Antivirus software and keep it updated.**
- **Set default login to Standard User Account.**

GENERAL AWARENESS & GUIDELINES

Information Security Awareness for Government Employees
https://infosecawareness.in

National Cyber Security Policy, 2013
http://nciipc.gov.in/documents/National_Cyber_Security_Policy-2013.pdf

Email Policy of Government of India
http://meity.gov.in/writereaddata/files/E-mail_policy_of_Government_of_India_3.pdf

Guidelines for Use of IT Devices On Government Networks
http://meity.gov.in/content/policies-0

Desktop Computer Security Tips
http://www.cert-in.org.in/SecurityofPC/PDF/Desktop_security.pdf

Guidelines for Protection of Critical Information Infrastructure
http://nciipc.gov.in/documents/NCIIPC_Guidelines_V2.pdf

"THERE IS NO SILVER BULLET SOLUTION IN CYBER SECURITY, A LAYERED DEFENCE IS THE ONLY VIABLE DEFENCE"