रक्षा मंत्रालय
MINISTRY OF
DEFENCE

CISO NEWSLETTER

Volume 1, Issue 3

FOREWORD

In an ever evolving digital world, almost all of us use computers in our official tasks on a daily basis. It is important as users that we are aware of the security threats and vulnerabilities which can affect the computers.

The CISO newsletter is one such means of providing basic background and overview of cyber security to all users. In third edition of the newsletter, certain incidences of information compromise and identity theft are presented, which have happened/ may happen to computer users if not adhering to the cyber security guidelines.

All personnel in the Ministry are requested to go through the contents of the newsletter and forward their valuable feedback and suggestions for further improvement.

V Anandarajan
Joint Secretary

CISO NEWSLETTER

Case 1: Shri Sharma received following email:-

Beginning next week, we will be deleting all inactive email accounts in order to create space for more users. You are required to send the following information in order to continue using your email account. If we do not receive this information from you by the end of the week, your email account will be closed.

**Name (First and Last):*

**Email:*

**Password:*

**Date of birth:*

**Alternate email:*

Please contact the Support Team with any questions. Thank you for your immediate attention.

Shri Sharma was prompted to reply instantly, thinking that he might finish this small but important task in just few seconds and be at peace, but just before sending the reply, an uneasy thought crept into his mind. Somewhere he felt that this is probably not the correct method of verifying the active users.

Analysis 1. This email is a classic example of ‘phishing’ - trying to trick people into providing all personal details in one go. Don’t respond to email, Instant Messages (IM), texts, phone calls etc. asking you for your password or other private information. You should never disclose your password to anyone, even if they say they work for Government, Ministry or the service providers.

If you receive such email, mark it as spam. Option for this is given by all major email services.

Case 2: **Smt Chauhan** received an electronic greeting card (e-card) in her email from a friend. It prompted her to click on an attachment / link to see the card. Since she was curious, she clicked to see it. It was a festive season and there were several such cards she received and liked viewing them. Within one week she observed that her computer/ mobile has slowed down causing inconvenience and annoyance.

Analysis 2. Hackers/ attackers frequently adopt measures to enter your computer/ mobiles by luring their victims through new and attractive methods. Some attachments contain viruses or other malicious programs, and in general, it's risky to open unknown or unsolicited attachments. Also, in some cases just clicking on a malicious link can infect a computer, so unless you are sure a link is safe, don't click on it. Also, email addresses can be faked, so just because the email says it is from someone you know, you can't be certain of this without checking with the person. Finally, some websites and links look legitimate, but they're really hoaxes designed to steal your information. It is therefore advisable to delete such emails/ mark them as spam and not to fall into the trap by sheer curiosity.

Case 3. **Shri Pillai** is a reading enthusiast and subscribes to a number of free e-magazines. Among the questions he was asked in order to activate his subscriptions, one magazine asked for his month of birth, second asked about his place of birth while third one asked for his mother's maiden name. Shri Pillai is an aware user and knows that such information together form sensitive personal information. He, however felt that giving such information in piecemeal would be harmless.

Analysis 3. All three newsletters probably have the same parent company or are distributed through the same service. The parent company or service can combine individual pieces of seemingly-harmless information and use or sell it for identity theft. It is even possible that there is a fourth newsletter that asks for day of birth as one of the activation questions. Often questions about personal information are optional. In addition to being suspicious about situations like the one described here, never provide personal information when it is not legitimately necessary, or to people or companies you don't personally know.

CISO NEWSLETTER

Case 4. **Shri Mehta** often used to access his personal e-mail on an office computer, which was also used by other staff members. After viewing emails, he made sure that he closed the browser window before leaving the computer. It wasn't much time before he realised that someone has gained access to his email and is sending unsuitable emails to others.

Analysis 4. It is not enough to just close the browser after accessing the emails. One must log out before leaving the computer, especially on a shared computer, else next person can access the email account by simply opening the site.

Case 5. **Shri Rastogi** was using a computer in which the mouse had started to move around on its own and click on things on his desktop. Thinking it to be a mouse malfunction, he unplugged his mouse, but to no avail. It seemed that someone invisible was using the computer.

Analysis 5. Possibly someone is accessing the computer remotely through Remote Desktop or by using similar desktop sharing software, wherein he can use the computer like he would be working locally on the computer, browse through the files, view them, edit them or even delete files. Ensure that your credentials are kept private and there are no such unwanted software installed on your computer. Avoid falling prey to running unknown/ non-reputed software on anyone's suggestion.

Case 6. **Shri Rao** received an email from his bank telling him that there is a problem with his account. The email contained certain instructions and a link for him to log in to his account and fix the problem. He knew about the phishing tactics hackers usually adopt, but this email name seemed to be of bank and he did not want to loose access to his bank account anyway.

Analysis 6. Report the email as spam or phishing and delete it. Any unsolicited email or phone call asking you to click a link, enter your account information, disclose your password, financial account information, Aadhaar number, or other personal information is suspicious, even if it appears to be from a firm you are familiar with. Always contact the sender using a method you know is legitimate to verify that the message is from them.

Case 7. **Shri Shukla** has an Internet computer in his office for carrying out unclassified official work. Other staff members in the office also use the computer for routine online personal work . During routine cyber security audit, the team found the computer infected with malicious software including a keylogger. Shri Shukla took this casually, believing that there was no classified information on his computer. He, however was in for a shock when the team found a hidden text file created by the Keylogger, which, apart from others, contained sensitive information such as user activities, user names and passwords of email and banking sites.

Analysis 7. A computer, especially one being used by many people, can get infected by malware in several ways. Common causes could be use of infected pendrives, visiting unwanted sites or clicking on malicious links by some not so aware user. This, however affects other users using such an infected computer. As a protection measure, keep the OS updated, use an anti-virus software, frequently update it and run scans. Do not use 'Administrator' account of the computer for day to day functioning. Do not download/ install unnecessary software. Educate all the users, because strength of a chain is the strength of its weakest link.

It is an incorrect notion that there is no need for cyber security on a computer not handling sensitive data. Attackers are constantly looking to infiltrate into government networks and systems and such an vulnerable computers may become their entry points. Attackers study their targets over an extended period of time and put together seemingly insignificant data into considerable information over a period of time. Hence cyber security must be taken seriously for all IT assets in an organisation.

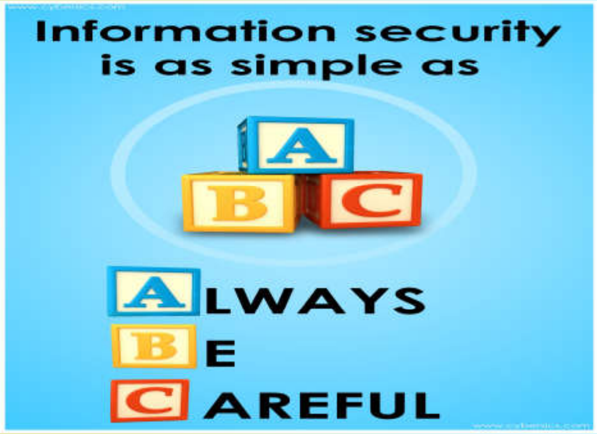
Disclaimer: The names used in case studies above are fictitious. The names have been chosen arbitrarily and do not to relate to any actual person.

CISO NEWSLETTER

GUIDELINES FOR COMPUTER USERS

DO's

- Ensure that the PC has a BIOS/ power on password
- Ensure that the anti-virus is updated with the latest anti virus definitions.
- Scan your computer for virus and other forms of malware.
- Ensure that the screen saver is enabled in official computers.
- Always logout the computer after use.
- Password protect sensitive files.



DON'Ts

- Don't let unauthorized persons use your computer.
- Don't reveal the administrator password to any unauthorized person.
- Don't install unauthorized software in office computers.
- Don't share your password with anyone.
- Don't use USB pen drives.

HELPDESK

CISO Office	:	011-23018232
Cyber Cell	:	011-23794783
E-Mail ID	:	cybercell-mod@nic.in

Designed by: Wg Cdr MR Dinesh
Cpl Abhishek Upadhyay
Case Studies: Lt Col VK Jha
Lt Cdr SM Riazuddin