Tel : 2304 3214
Fax : 2301 5686

Government of India
Ministry of Defence
Cyber Security Group-DDP
C/o Dte of Standardisation
'H' Block, PO Nirman Bhawan
New Delhi - 110011.

No. 6203/CSG/STDN/DDP

0) Oct 2014

The DG
DGQA/DGQA (L)
(As per distribution list)

CYBER SECURITY ADVISORY ON SECURITY MEASURES TO BE ADOPTED WHILE USING EMAIL SERVICES

1. Please refer Ministry of Home Affairs letter No 1/2014/CISO dated 10 Sep 2014 (copy attached).

2. Detailed advisory No 01/2014 for adopting cyber security measures while using E-mail services on internet is been forwarded herewith for necessary action please.

(Naresh Chaudhary)
Lt Col
Cyber Security Officer
Cyber Security Group – DDP
for Chairman CSG-DDP

Encl:- As Stated

745/ADG (L) Sectt
09/10/14

ADVISORY NO – 01/2014

CYBER SECURITY GROUP – DDP
SECURITY MEASURES TO BE ADOPTED WHILE USING EMAIL SERVICES

Gen

1. Security of individual PC on Internet is responsibility of the user. It is mandatory for all internet users to develop adequate knowledge on threats and mitigation while working in internet environment. Security Internet services are based on open architecture with minimal securityfeatures. They are also open to malicious attacks, hacking, virus activities and cybercrimes. Unauthorized and unregulated use of Internet can lead to compromise in security. Email is the most widely used Internet Application. Email facility is efficient and helps the users in more than one way but at the same time has major information disclosure risks which need to be guarded against from the cyber security point of view.

Aim

2. The aim of this advisory is to lay down cyber security guidelines for all Internet users whileusing Email on Internet.

Email-borne Threats

3. The widespread adoption of email through the years has been Accompanied by the development of malicious code, that is, email viruses and attacks. Email has provided hackers and crackers with an easy way to distribute harmful content to the internal network. A typical firewall alone cannot protect against such email attacks, because it simply does not analyze email and its contents.

4. Since email messages can include file attachments, hackers can sendInfected files and hope that the recipient will open them. This method makes use of social engineering to urge the end user to run the file. Other methods exist which allow a skilled and possibly malevolent cracker to **inject code through email and run custom-made applications automatically while the end user reads the email text**.

Precautions for Email usage on Internet.

5. **Connectivity.**

(a) A computer being used for Official work in the our environment shall not be connected or used to access the Internet either directly or indirectly.

(b) Stand-alone computer having no classified or official data/Info of importance, from security point of view, on hard disks can only be used to access Internet.

(c) No Info of classified nature will be passed using Internet as a media.

(d) Internet computers will be standalone machines to be used for Internet only.

(e) Under no circumstances will there be a dual facility of Internet/DDP Intranet on a single machine.

(f) Email passwords will be changed frequently and Email addresses should not reveal designation/ appointment and organization/office details.

(g) Official Email ID if so required for performance of Official duties will be on ".nic.in" domain obtained through NIC.

6. **Anti-Virus** .Use updated anti-virus software/Internet Suits.

7. ***Disable Scripting Features***

(a) Disable Scripting Features in E-mail Programs when possible.

(b) Since E-mail programs like MS Outlook frequently use the same code as web browsers to display HTML formatted messages, the vulnerabilities that affect ActiveX, Java, and JavaScript are often applicable to E-mail. Apart from disabling these features, the ability to run Visual Basic Scripting (VBS) should be removed if possible.

8. **Web Browser** Use an up to date web browser with a built in phishing filter. Web browser users should :-

(a) Disable all window pop-up functionality.
(b) Disable Java runtime support.
(c) Disable ActiveX support.
(d) Disable all multimedia and auto-play/auto-execute extensions.
(e) Prevent the storage of non-secure cookies.
(f) Ensure that any downloads cannot be automatically run from the browser, and must instead be downloaded into a directory for anti-virus inspection.

9. **Exercise Caution When Opening Attachments.** Attachments in emailare probably still the number one threat. Exercise caution when receiving email with attachments.

(a) Users should disable auto-opening or previewing of email attachments in their mail programs.

(b) Users should never open attachments from an un-trusted origin, or that appear suspicious in any way. One should especially beware of E-mail attachments with the file extensions like; exe, pif, com, bat, scr, vbs, hta. E-Mails with such attachments should be treated with great suspicion even if they come from trusted sources since E-Mail headers (like the From Address) can easily be forged.

10. **Disable "Hide File Extension" feature in OS**. By default, Windows hides the file extensions of known file types. This behavior has been used to trick users into executing malicious code. But a user may choose to disable this option in order to have file

extensions displayed by Windows. Multiple email borne viruses are known to exploit hidden file extensions.

11. Files attached to the email messages sent by some malicious programmers may appear to be harmless text (.txt), MPEG (.mpg), AVI (.avi) or other file types when in fact the file is a malicious script or an executable (.vbs or.exe, for example).

12. **Spam.** Spam is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. Most spam is commercial advertising, often for dubious products or get-rich-quick schemes. Spam costs the sender very little to send. Most of the costs are paid for by the recipient or the carriers rather than by the sender :-

(a) **Never respond to Spam.** Most spammers include a link in their mail that says "To Unsubscribe, click here". This is to entice the user to click on the link. This action will confirm to the spammers that they've got a live address. Also, if the user responds, the spammer will sell the users addresses to every other spammer and the user soon will be flooded with even more spam.

(b) **Use a spam filter.** Anti-spam software can help keep spam at manageable level.

13. **Discard Unsolicited E-Mail.** Computer worms/viruses generally propagate through E-Mail attachments. As a rule one should never open any unsolicited E-Mail. Note that no amount of security measures will work if one decides to open any arbitrary E-mail that comes along and execute its attachments.

14. **Email spoofing.** Email "spoofing" is when an email message appears to have originated from one source when it actually was sent from another source. Email spoofing is often an attempt to trick the user into making a damaging statement or releasing sensitive information (such as passwords). Spoofed email can range from harmless pranks to social engineering ploys. Examples of the later include :-

(a) Email claiming to be from a system administrator requesting users to change their passwords to a specified string and threatening to suspend their account if they do not comply.

(b) Email claiming to be from a person in authority requesting users to send them a copy of a password file or other sensitive information.

(c) Mail uses social engineering to tell the user of a contest that the user may have won or the details of a product that the user might like. The sender is trying to encourage the user to open the letter, read its contents, and interact with them in some way that is financially beneficial to the sender.

15. In case of suspicion enable the show full header option in the Email client and check the header info of the mail.

16. **Social Engineering.** Some of the social engineering techniques are asunder:-

(a) Making false claims that a file attachment contains a software patch or update.

(b) Implying or using entertaining content to entice a user into executing a malicious file.

(c) Using email delivery techniques that cause the message to appear to have come from a familiar or trusted source.

(d) Packaging malicious files in deceptively familiar ways (e.g., use of familiar but deceptive program icons or file names).

17. **Protection from Phishing Attacks**. Phishing is an example of socialengineering techniques used to fool users. Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from PayPal, eBay, YouTube or online banks are commonly used to lure the unsuspecting. Phishing is typically carried out by e-mail or instant messaging and it often directs users to enter details at a website. The e-mail would usually provide a link to a bank's web site and ask the user to click the link. It would ask him to provide certain confidential banking information like his account number, credit card number etc., failing which his account would be closed. There would be a sense of urgency and panic in the e-mail. A checklist which helps to prevent phishing is as under:-

(a) Check to see if the e-mail is indeed from the user's bank and not from just any bank. If it isn't, stop reading further and confirm the samefrom the bank by using other means like telephone.
(b) If the e-mail is not personally addressed to the user, it is most probably a fraud.
(c) Check the language and spelling of the text contained in the e-mail.If there are misspelled words or substandard language, conclude that it isnot from his bank.
(d) If the e-mail urges the user to act immediately without delay, failingwhich his account will be closed down, do not react.
(e) Users should become cautious if there is anything that even remotely feels wrong. If something feels wrong, it is most probably wrong.Confirm the same by using other means like telephone.
(f) Never click any link given inside the e-mail message. Instead, directly type the URL of the financial institution.
(g) *If the user does not know the URL of his bank's web site, take the time to call* them immediately to find out.
(h) User should never provide personal information to anybody, come what may.

18. **Cryptography**. There are many open source and paid technologies forencrypting Emails which can be used effectively to protect against majority ofthe Email threats.

(a) ***Encryption.*** Cryptographic checksums should also be used to validate the integrity of the attached files provided the sender has sent theCryptographic checksums along with the attachments. There are manyfree File Checksum utilities that compute MD5 or SHA1 cryptographichashes for files. These File Checksum utilities can generate MD5 or SHA-1 hash values for files to compare the values against a known good value. It can compare hash values to make sure that the files have not beenchanged.

(b) **Digitally Signed Email.** It is possible to use Public Key cryptography systems to digitally sign an email. This signing can be used to verify the integrity of the messages content to identifying whether themessage content has been altered during transit. A signed message canbe attributed to a specific users (or organizational) public key.

(c) **S/MIME and PGP**. There are currently two popular methods for providing digital signing. These are S/MIME and PGP (including PGP/MIME and the newer Open PGP standard). Most major Internet mailapplication vendor's ship products capable of using and understandingS/MIME, PGP/MIME, and Open PGP signed mail.

19. Avoid opening your E-Mails in un-trusted locations like Cyber Cafes etc.

20. As far as possible, avoid sharing your E-Mail Ids with un-trusted parties,vendors etc. ***it is advisable to have two Email IDs, one for sharing withenvironment and the other for use with trusted parties***.

21. Educate your family, especially children on importance of protecting yourpersonal info and Cyber Hygiene.

22. The best advice with regard to malicious files is to avoid executing them in the first place and scan them through a trusted Anti Virus/ Security Solution.

23. All concerned in the Department of Defence Production including the DPSUs, Ordnance factories and Directorates under DDP are requested to ensure dissemination and implementation of this advisory in letter and spirit.

(Naresh Chaudhary)
Lt Col
Cyber Security Officer
Cyber Security Group-DDP
Ministry of Defence (Govt of India)