DIRECTORATE GENERAL OF SYSTEMS& DATA MANAGEMENT
CUSTOMS, CENTRAL EXCISE & SERVICE TAX
4TH & 5TH FLOOR, HOTEL SAMRAT,
KAUTILYA MARG, CHANAKYA PURI,
NEW DELHI-110021.

To,

All Chief Commissioners of Customs/Central Excise/Service Tax
All Director Generals
All Commissioners of Customs/Central Excise/Service Tax

F.No. IV(38)/1/2013-Sys./4283 Dated: 19.09.2013

Sub: Email Account and Website Security-reg.

The Directorate General of Systems has been receiving several communications from Indian Computer Emergency Response Team (CERT-in) relation to defacement of websites maintained at the local Commissionerate level and email accounts being comprised due to reasons like weak passwords.

2. In this connection, please recall earlier communications of even number dated 06.01.2012 and 21.11.2012 (copies enclosed), wherein the need to build-in security requirements in the management of websites was emphasized along with the need to follow CERT-in guidelines on the subject (Annexure A) it is re-iterated that website security should be an integral part of website maintenance contracts and it should be ensured that the websites are hosted on Indian servers only (eg., on NIC infrastructures).

3. As regards email account security and password management, advisories have been issued from time-to-time and it is imperative that they are read and followed. (Annexure B). Commissionerates may be instructed to ensure the security of independently hosted websites under their jurisdiction and sensitize officers in respect of secure email account usage. Security guidelines for the same are annexed herewith.

Yours sincerely,

(J.M. Shanti Sundharam)

Encl:

1. Annexure A-Security of Independently Hosted Websites
2. Annexure B-Security of Email Accounts

(J. M. Shanti Sundharam)
Special Secretary & Member
Central Board of Excise & Customs
Ministry of Finance (Deptt. of Rev.)
Govt. of India, New Delhi

Website Security Instructions

All Commissionerates have to ensure that websites under their maintenance are hosted securely and follow good coding practices to ensure that the websites are not vulnerable to hacking.

1. Locating where your Website is Hosted:

Instructions from Ministry of Home Affairs require all Government websites to be hosted in India. **It may particularly be noted that websites with 'gov.in' domain have to be hosted on NIC (National Informatics Centre) web server and not on public web servers.** It has been noticed that in most cases of website defacement, the websites were actually hosted on servers located in foreign countries. If your website is hosted with some private service providers (SPs), it has to ascertained that they have not outsourced it, so that the service provider can be held accountable in the event of a breach. The location of the IP address (where the website is hosted) can be checked using sites such as www.whatismyip.com. It is re-iterated that the web hosting may be shifted onto an Indian web server, if not already done.

2. Securing your Website:

The Directorate General of Systems has received several communications from Indian Computer Emergency Response Team (CERT-In) in relation to defacement of websites maintained at the local Commissionerate level. There is an urgent need to have built-in security requirements in the management of websites maintained by local Commissionerates. The following CERT-in guidelines in the matter may be paid special attention to:

Web Server Security Guidelines

http://www.cert-in.org.in/s2cMainServlet?pageid=GUIDLNVIEW02&refcode=GuidelineCISG-2004-04

Securing IIS/ 7.0 Web Server guidelines

http://www.cert-in.org.in/s2cMainServlet?pageid=GUIDLNVIEW02&refcode=GuidesCISGu-2010-01

Guidelines for Auditing and Logging

http://www.cert-in.org.in/s2cMainServlet?pageid=GUIDLNVIEW02&refcode=GuidelineCISG-2008-01

Letter F No. IV(38)/1/2013-Systems/ dated ANNEXURE B

Security of Email Accounts

In a letter to Chairperson (CBEC), the **Director General, Computer Emergency Response Team India (CERT-In), has emphasised the need for maintaining email account security in respect of official correspondence**. The following points may be noted in this regard:

1. The password of the mail account should be more than 8 characters having a combination of alphanumeric and special character
2. The password should be updated regularly (at least once a month)
3. The user owning the mail account should not share the password with anyone
4. The contact details of the officer should be up-to-date with the System/Mail Administrator so as to receive regular updates and alerts
5. The user should keep track of his/her mail account access through 'last login' facility
6. Caution should be exercised in opening the email messages especially keeping in mind phishing, malware infected and targeted attack emails
7. The users should be sensitized regularly about latest security threats and targeted attacks
8. The computer system/desktop/laptop used to access official email account should be secure, i.e., authorised OS (operating system), Anti-virus and Firewall should installed and updated regularly
9. The official (as well as personal) email account should never be accessed from the computer systems having weak security or public systems like Cyber Café- since these are easy targets for hackers with malicious intent
10. Recent revelations have brought to light the fact that mail service providers based outside India - like Gmail, Yahoo, Microsoft, etc, are sharing data with surveillance agencies. Hence the use of Gmail, Yahoo, etc for official communication may result in sensitive and confidential information being made available to foreign agencies. Therefore **official communication (especially carrying information of national interest) should be made using only Email accounts of icegate.gov.in or nic.in domains.**