EXPORT PROMOTION COUNCIL FOR HANDICRAFTS
"EPCH HOUSE" POCKET-6 & 7, SECTOR-C, L.S.C., VASANT KUNJ, NEW DELHI-110070
Tel: 91-11-26135256 Email: compliancecell@epch.com
Fax: 91-11-26135518, 26135519 Web: www.epch.in

EPCH ORGANIZED AN AWARENESS SEMINAR ON "HOW TO SAFEGUARD YOUR BUSINESS FROM CYBER CRIME" AT NEW DELHI ON 11TH JANUARY, 2014 (SATURDAY) AT RAJIV GANDHI HANDICRAFT BHAWAN, NEW DELHI

Export Promotion Council for Handicrafts (EPCH) organized an awareness seminar on "How To Safeguard Your Business From Cyber Crime" at Rajiv Gandhi Handicrafts Bhawan, New Delhi on 11th January, 2014 (Saturday).

Mr S S Gupta, Development Commissioner (Handicrafts) was the Chief Guest of the seminar. The seminar was also attended by Mr Lekhraj Maheswari, Chairman-EPCH, Mr R. K. Malhotra, Chairman-IEML, Mr. Prince Malik, Member-COA EPCH, Mr. Rakesh Kumar, Executive Director-EPCH and over 50 leading member exporters from Delhi, Moradabad, Firozabad and Agra. The experts present during the seminar included Mr. Shankhdhar Mishra, Dy. Commissioner of Police (Cyber Cell) in Delhi Police, Mr. Samir Datt, Expert (Cyber crime), M/s Foundation Futuristic Technologies, Dr. O. P. Wali, Professor, Indian Institute of Foreign Trade.

Mr. Rakesh Kumar, Executive Director-Export Promotion Council for Handicrafts in his inaugural address set the tone for the discussions by highlighting the need and importance of the subject matter in today's business environment wherein Cyber Technology has a significant role to play in business transactions.

The objective of the seminar was to create awareness and provide required knowledge on the cyber crime & internet security to the member exporters and new entrepreneurs as the method to safeguard ones business from cyber crime.

During the seminar Mr. Samir Datt, senior expert on CyberCrime explained the modus operandi used by cyber criminals to hack the accounts and also explained the ways and means to safeguard against such incidents. He further added that users should prevent their systems from exposure to spyware, adware, embedded programmes, browser hijackers, dialers & malwares.

Mr. Shankhdhar Mishra, DCP (Cyber Cell) in Delhi Police informed the participants about the Cyber Law of India and apprised that cyber crime is an unlawful act or activity wherein the computer is either a tool or a target or both. Cyber crimes involve criminal activities that are traditional in nature, these can be theft, defamation, fraud, forgery, and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a number of new age crimes. He informed that Cyber crimes can be categorized in two ways - one the Computer as a Target, using a computer to attack other computers. which is called. Hacking, Virus/Worm attacks, DOS attack etc. and Secondly The computer as a weapon, using a computer to commit real world crimes on actual people e.g. Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, etc. He stressed on the need for the precautionary measured briefed by the present faculty members.

Dr. O. P. Wali, Professor, Indian Institute of Foreign Trade (IIFT) informed the member exporters about the key stroke loggers, hardware, software, keylogging hardware, Firewall, auto form fillers, virtual keyboard & onscreen keyboard. He informed the participants about the following precautions to prevent from an attacker :- Install it from a compact disc or floppy disc, Use Strong Passwords, Secure your computer through Activation of firewall on the system, Use anti-virus/malware software, Block spyware attacks, Be Social-Media Savvy, Secure your Mobile Devices, Install the latest operating system updates, Protect your Data, Secure your wireless network, Protect your e-identity, Avoid being scammed, Call the right person for help etc.

Mr. Rakesh Kumar, ED-EPCH during the discussion said "that business information is a critical asset and it is important to protect from unauthorized modification, destruction and disclosure. Prevention will always be our best line of defense against cyber criminals. Like any other criminal activity, those most vulnerable tend to be the first targeted. Cyber Safety has become an important aspect in today's business environment and need to be made aware to the member exporters.

The Chief Guest Mr S S Gupta Development Commissioner (Handicrafts) in his concluding remarks expressed satisfaction over the deliberations and hoped that with the measures and safeguard available in the country against cyber crimes, the handicraft export fraternity would be able to minimize the occurrence of such happenings.

The Major Questions which were asked including the following:

Q1. Suppose, someone system have been hacked. In such case, does the changing of password for the login immediately, sufficient to prevent from any fraud that may occur in future??
Ans: In such cases, it is advisable to change the password for the login from another system because changing the password from the same system would not help as the cyber criminals manage to know the changed password again when you do it from the same system.

Q2. In the current general scenario of BYOD (Bring Your Own Device), where the same system is being used for so many of activities like personal work, professional work and sometimes fun even. So what should be done to protect ourselves from the cyber frauds when we are exposed to too many of activities from the same system?
Ans: Yes it is very much understood that a person cannot have too many of devices for different activities. But still it is suggested that there should be separate devices for at least the very important activities like generation of Purchase orders, generation of invoices etc.
It is further suggested that in case of limitation of different devices for different activities; there should be partitions made in the system so that your activities get automatically separated and you are safe.

Q3. After taking all such precautions, are there any second layer precautions that an exporter should take into care while corresponding with its buyers?
Ans: It is always advisable to encrypt all the important e-mails and messages over the internet so that even if it is hacked it remains of no use to the cyber criminals.
At the same time the following precautions should be taken to avoid becoming prey to the cyber criminals:

- Update your antivirus/antimalware detection system.
- Take the basic precautions and don't click on the links you do not know.
- Try and separate internet connected system for work and for play.
- Use your own domains and not the free e-mail ids.
- Use encryptions/digital signatures while transmitting important documents over e-mails.
- Set up standard operating procedures in the case of deviations: get on the phone.

Q4. Before we fall to the target of cyber criminals, we should know the ways of entangling a person by them. What are general kinds of financial frauds/methods?
Ans: It is always good to understand the kinds of financial cyber frauds beforehand so that if such frauds are prompted against you; you may take the necessary precautions.
These can be classified under following heads:

- **PHISING.**
- **419 SCAMS:**
    - Export Orders
    - Lottery Win.
- **E-BANKING:**
    - E-transfer of funds.
    - Change in recipient bank accounts.
    - Use of mobile phones for financial activities.

Q5. These days we generally receive missed calls (ISD) from Africa/Pakistan number. What are the dangers of calling back to such numbers?
Ans: These numbers are generally from the countries like Pakistan and Africa. In case you call back to such numbers, you start losing your internet minutes from your mobiles and also you may expose yourself to some other frauds that the criminals may have targeted you for.
It is strictly advised to not call back to the numbers from Pakistan.

Q6. What is the scope of jurisdiction for cyber-crimes, in case of lodging the case?
Ans: In case of lodging a case against cyber frauds, the appropriate jurisdiction shall be the place of first contact made on the internet.

Suppose the official is reluctant to lodge the case; you may directly approach the Court.

Q7. How long does it take to get back the money if the fraud is made in India to an Indian?
Ans: It generally takes 9 months to 1 year to get back the money in cases of frauds made in India to an Indian.

Q8. We use to receive phishy e-mails for bulk business and the same e-mail is floated to more of us. What should be done to prevent such e-mails?
Ans: This is the case of bulk mails being circulated to a huge number of people to target them falling prey to their frauds. Such e-mails are called *Spam*. In such cases, you are advised to go to the settings of the e-mail you are using and block your spam mails. This would help in preventing such e-mails to reach to your inbox.

It is also suggested to use your own domain rather than free e-mail ids. Gmail should not be used by the Indian exporters/businessmen as their official e-mail id.

Q9. Is there any helpline number for cybercrimes where a victim can get the information all about?
Ans: No, till now we do not have any helpline number for the cybercrimes. However the following two methods may be followed in such cases:

- Dial 100.
- Approach nearest Police Station.

Q10. What are the general precautions the exporters should take into care to prevent themselves from cyber-crimes?
Ans: Following precautions may be adopted:

· **Written on the internet:**
- Do not trust blindly.
- Verify them before going ahead.

· **Read all e-mails carefully:**
- Look for the changes in the e-mail ids.

· **Recipient Bank:**
- Inform all clients abroad that bank details will never change until letter is exchanged face to face.
- Payments for goods from India will never be made to an account in the third country.
- Seek verbal confirmation before release of every payment.

· **Mobile Phones:**
- Do not use all activities like social and professional from the same mobile.

· **E- Transfer:**
- Ensure that bank knows that addition of any new account for e-transfer cannot be done by mobile phone.
- Ensure that it is allowed only on the basis of written request.
- If mobile phone is suddenly switched off inform the bank to block all debits immediately.

· **Computer Systems:**
- Keep all operating systems/Antivirus/Antimalware updated.
- Sanitize system used for financial transactions.
- Use Indian service providers.

******


AWARENESS SEMINAR
ON
"HOW TO SAFEGUARD THE BUSINESS FROM CYBER CRIME"
Organized by:
Export Promotion Council for Handicrafts
New Delhi
11th January, 2014
S S GUPTA