JABS INTERNATIONAL PVT LTD

A-350, TTC Industrial Area, MIDC Mahape, Navi Mumbai - 400710, Maharashtra, India
Tel: +91-22-27784500/41412525, Email:info@jabsinternational.com
www.jabsinternational.com

210918

CYBER ALERT WHILE SENDING THE TELEGRAPHIC TRANSFER

Revolution of E-technology has opened numerous ways of communication In order to increase the productivity and efficiency level.
But as we all know every good thing has some drawback, likewise E-technology that we are using which is collectively known as E-mail, is likely to be the Topmost means of Cybercrime. Banks and corporate Sector becoming a victim of this cybercrime in a big way through phishing E-mails.

Cybercrime experts are emerging a new measures and new ways to protect against becoming a victim of this cybercrime.
But we can also take initiative and can protect ourselves through following ways while making Foreign remittance.

- We should stop using Hotmail, Gmail, Yahoo mail etc. for E-communication as Hacker can easily hack those e-mail addresses and can rob your important data which may create a big trouble. Hence to Create an E-mail in a domain name is always a safe means communication as the risk of getting hacked is very less.

- Avoid using free email ids, as they come with lesser securities. Free emails for business to be avoided

- Instead use paid business emails like Google business etc., Also use 2 level security provisions if available.

- Do not ever reply to the phishing E-mail or Suspicious E-mail, as well as please delete the spam mail and junk mail folder on daily basis.(as email contains malware/virus, which can access your data without your knowledge)

- In case if you receive an E-mail from regular supplier regarding changes in bank details, (MANY TIME HACKER USE THE DOMAIN VERY IDENTICAL TO THE REGULAR SENDER , PLS KEEP WATCH ON THE EMAIL ID)then please reconfirm the same with them only through telephonic Conversation or through Fax/WHATS APP OR SKYPE.

- Hacker also make an identical email address and inform the change of bank details, please do not trust those mails and check the mail address thoroughly and also reconfirm the payment intimation only from the payment receiver by WhatsApp or skypeand do not ever reply to the suspicious e-mail, as there might be the chances that the suppliers e-mail address has gotten hacked.

The purpose behind sharing this information with you is that, we want you to be aware of this cybercrime and to follow this practice which may triumph over en evil of Cybercrime
As we truly care and value our esteemed clients.

PS: we never ask to transfer the funds to the alternate company or to the third country, hence for any foreign

P.T.O.

JABS INTERNATIONAL PVT LTD

A-350, TTC Industrial Area, MIDC Mahape, Navi Mumbai - 400710, Maharashtra, India
Tel: +91-22-27784500/41412525, Email:info@jabsinternational.com
www.jabsinternational.com

210918

Recommendations Best Practices

- Block the malicious domain and IP address on the network Firewall and Web proxy to prevent the malicious file from accessing the external servers
- Remove unwanted applications from the affected hosts and remove unwanted Addons, Plugins and Extension from browsers
- Use a firewall to block all incoming connections from the Internet to services that should not be publicly available.
- By default, deny all incoming connections and only allow services you explicitly want to offer to the outside world
- Disable AutoPlay to prevent the automatic launching of executable files on network and removable drives, and disconnect the drives when not required. If write access is not required, enable read-only mode if the option is available
- Turn off file sharing if not needed. If file sharing is required, use ACLs and password protection to limit access
- Disable anonymous access to shared folders. Grant access only to user accounts with strong passwords to folders that must be shared
- Ensure that programs and users of the computer use the lowest level of privileges necessary to complete a ask
- When prompted for a root or UAC password, ensure that the program prompts for administration level access is a legitimate application
- Turn off and remove unnecessary services
- Configure email server to block or remove email that contains file attachments that are commonly used to spread threats, such as .vbs,.bat,.exe,.pif and .scr files
- Train employees not to open attachments unless they are expecting them
- Do not execute software that is downloaded from the Internet unless it has been scanned for viruses. Simply visiting a compromised Web site can cause infection if certain browser vulnerabilities are not patched.

SOURCE: SIMPA