Cyber Crime Information - 50

To: All members

From: cyberdost@mha.gov.in

Subject: Cyber Crime Information - 50

Respected Sir/Madam,

A new phishing modus operandi has come to the notice in which culprits utilize PDF attachments to steal the login credential of victims, as it prompts login details for opening the attachment.

Most of the times organizations like private firms, corporates or government entities share documents with user in password protected PDF. It is a concept of protecting the reliability and correctness of the information. When users receive such protected documents they are asked to open it through password.

Most of the times when a user purchases any product from e-commerce websites such as FlipKart, Amazon, Snapdeal, Myntra etc., he receives an invoice copy (PDF attachment) on his registered email address which contains product details, quantities and pricing etc.

In this new modus operandi, scammer pretend to be sales team member of well-known e-commerce organization and sends a purchase invoice/ bill to victim's email address. Once victim opens the PDF attachment it shows a login prompt, asking victims to enter his/her e-commerce login id and password to view the account summary information. A non-vigilant user might think it as a security feature designed to keep his private information safe. Once the credentials are entered, the scammers have the full access to potential victim's e-commerce account which can be misused like placing high value purchase orders, change the delivery address of already placed order, etc.

Suggestions

- Credible e-commerce organizations never ask login credentials to open any attachment.
- Always check sender's email address domain to verify the authenticity
- Always check purchasing invoice/bill at the official websites
- Do not click on any link/attachment sent by unknown sources since it may contain virus/malicious code to infect the devices.

Regards
Threat Analytical Unit (TAU)
Indian Cyber Crime Coordination Centre
CIS Division, MHA
011-23093697