Phishing Attacks and their preventing Methodologies

Kewal Krishan Kapoor

Syscom Corporation Ltd

Abstract- In this paper, the Phishing Attacks and their preventing methods are discussed. These Phishing Attacks are mostly used to theft or extract your personal information by various means which leads in emptying your bank accounts. In addition to this, some preventing measures should be taken in mind to get rid of these frauds.

Index Terms- Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol Secure (HTTPS), Uniform Resource Locator (URL), Secure Sockets Layer (SSL), Electronic Mail (Email), Internet Service Provider (ISP).

I. Introduction

Phishing is a technique of stealing user's personal information such as credit card or bank account numbers, user id's and asswords, and subsequently committing fraud. This technique uses the Email as a weapon

Scammers used many ways to steal your information, but most commonly through fraud emails which look very similar to real world just like

- Emails received from the bank or another institution asking you to provide the details
- Emails received from the well known companies for winning the lottery or jackpot asking you to just provide the details and, the user's greed or their necessity for money, makes their (Scammers) way easier.
- Emails received with an attachment and asking you to install or download it to increase your system performance or to win shopping points etc. These attachments mostly contain the Trojan or Viruses which scans your HARD DISK and try to find out the saved passwords, id's and other personal information and share with the Scammers without your intervention.

And once scammers have **phished** out your information, they could use it in a number of ways. Your credit card could be used for unauthorized purchases, or your bank account could be cleared out.

II. PHISHING CYCLE

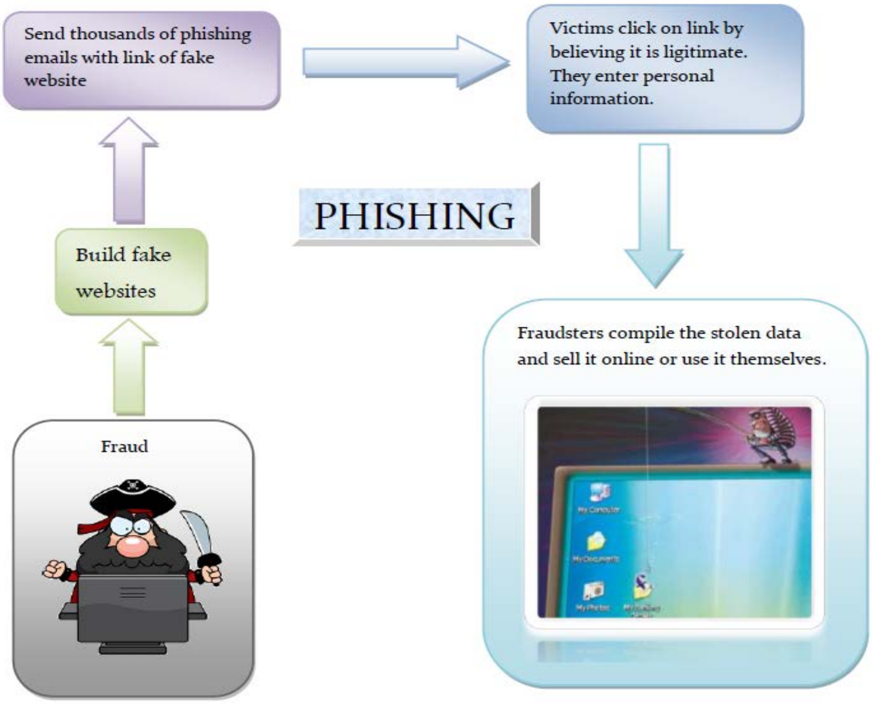

Send thousands of phishing emails with link of fake website
Victims click on link by believing it is ligitimate. They enter personal information.
PHISHING
Build fake websites
Fraudsters compile the stolen data and sell it online or use it themselves.
Fraud

Fig 1.1: Phishing Cycle

III. PHISHING ATTACKS

Following are the Phishing Attacks which generally used by the Scammers:

A. Man-in-the-middle Attacks

This is one of the most successful ways of stealing the customer information through man-in-the-middle attacks. In this case the attacker sits between customer and actual server. Then it read and stores all communications between the systems.

From this particular position as shown in Fig 1.2 the attacker can observe all the transactions.

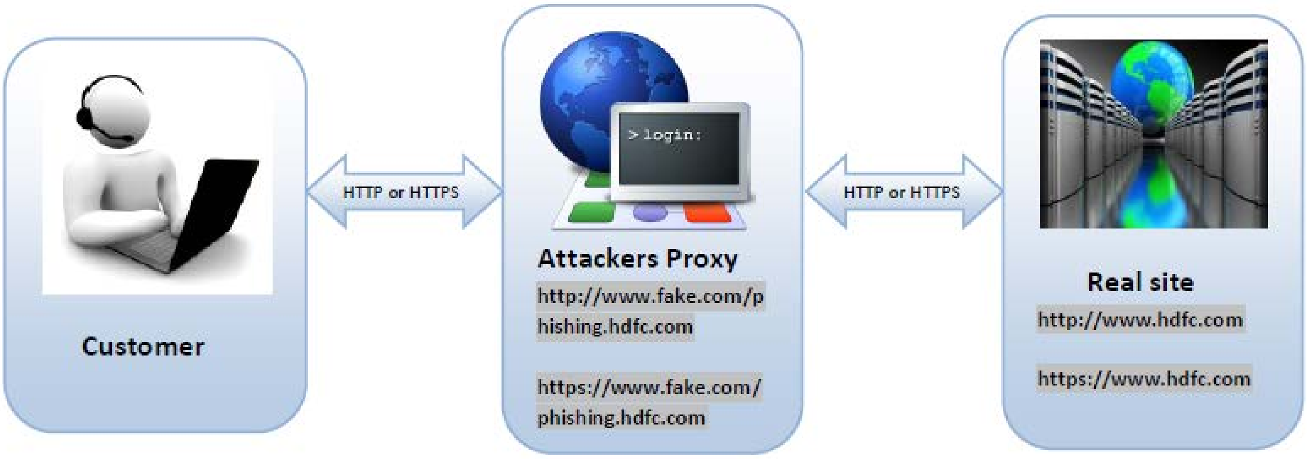


Fig 1.2: Man-in-the-middle

This attack is being successful for HTTP and HTTPS as well.

How it is conducted:

- In case of HTTP:
  - The customer connects the fraud server using the link which is received in his email.
  - Once the link is opened as web page, it looks like the real site, then the customer entered their credentials(User name and Password) to Login
  - By the same time the attacker’s server build the connection with the actual server using the same credentials and entered into it.
- In case of HTTPS:
  - Attacker creates the SSL connection between the client and their(attacker) proxy server to record all traffic in an unencrypted form
  - By the same time Attackers proxy creates their own SSL connection to the actual server
  - Once the connection is established then the attackers can use the same credentials as entered by the actual user.

B. Preset Session Attack

In this case, Phishing mail contains a Pre-defined Session ID which is used while connecting with the server. Now the attacker waits for the recipient to connect the server using the same session ID.

Once the recipient completes the authentication, the attacker is ready for raid.

The Fig 1.3 shows how the Preset Session Attack is conducted:

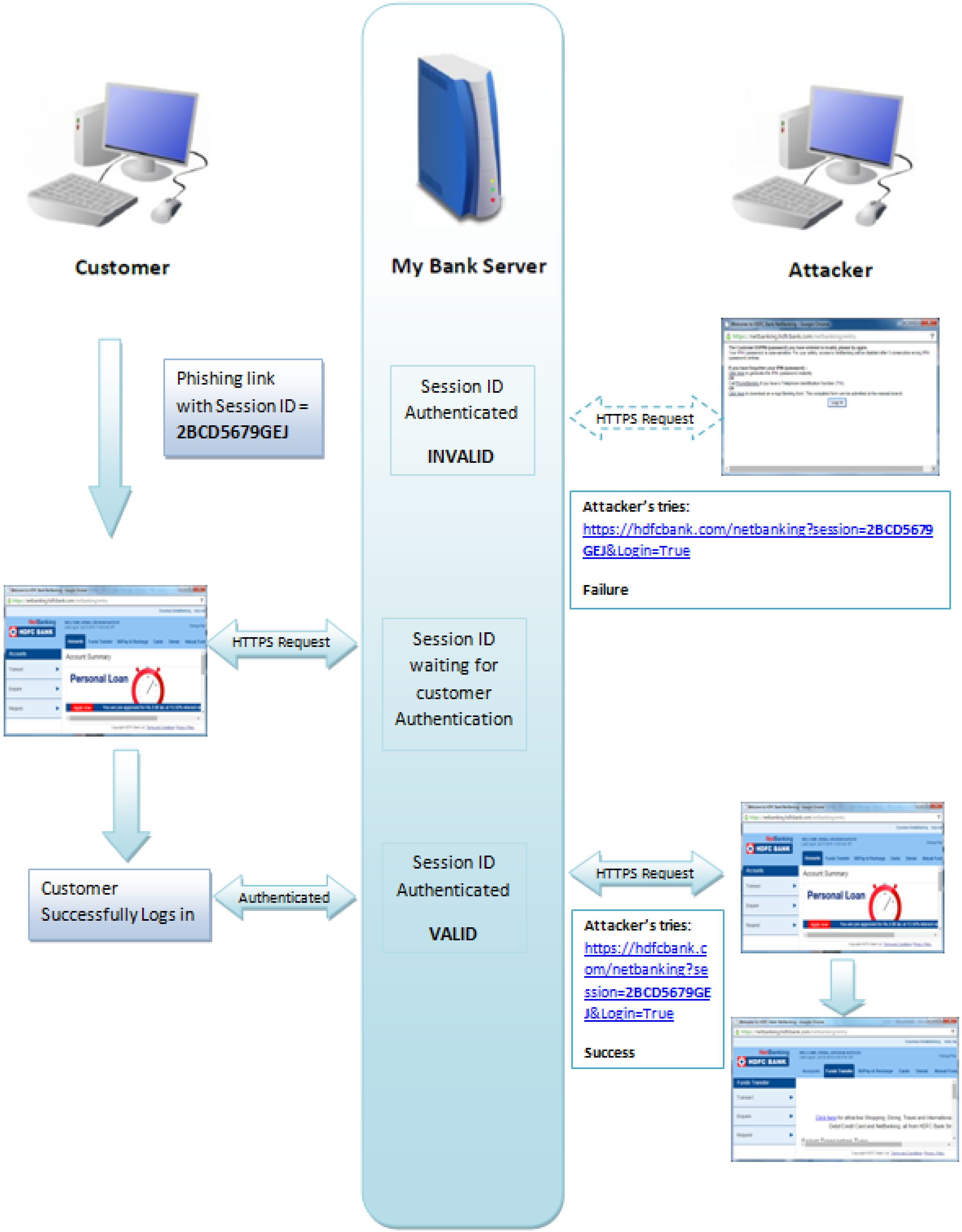

Customer
My Bank Server
Attacker
Phishing link with Session ID = 2BCD5679GEJ
Session ID Authenticated INVALID
HTTPS Request
Attacker's tries: https://hdfcbank.com/netbanking?session=2BCD5679GEJ&Login=True Failure
HTTPS Request
Session ID waiting for customer Authentication
Customer Successfully Logs in
Authenticated
Session ID Authenticated VALID
HTTPS Request
Attacker's tries: https://hdfcbank.com/netbanking?session=2BCD5679GEJ&Login=True Success
Personal Loan

Fig 1.3: Preset Session Attack

As shown in Fig 1.3, when the message recipient open the web page using the ink having session ID = 2BCD5679GEJ. At the same time the attackers tried to open the same link in every minute with the same Preset session ID and using the condition Login = true as defined in the following link:
https://hdfcbank.com/netbanking?session=2BCD5679GEJ&Login=True

Until the recipient not authenticated the link, the error message is shown at attacker's end. Once the authentication is successfully done, the attacker can access the same page and ready for Fund Transfer.

C. Trojan Attack

This attack is one of the most dangerous and favorite in the attacker's list as they just have to send the attachment or the link consisting of Trojan virus. This virus is too intelligent which do all the programmed activities by their own and provides all the details to the attacker.

How it is conducted:

i. Attacker's send the attachment or the link via email.

ii. The content of the email generally Entice the recipient either to download the attachment or follow the link to download it.

iii. When the recipient double-clicks to open the attachment, the Trojan virus got activated and starts their assigned work.

iv. It collects the information from your system by scanning it and to memorize or store the key strokes entered using the keyboard while using any web application

v. After that it sends all the data to the attacker's and also allows the attacker's to remotely control your system. Then the attackers encapsulate all the data and Game is over at the recipient end.

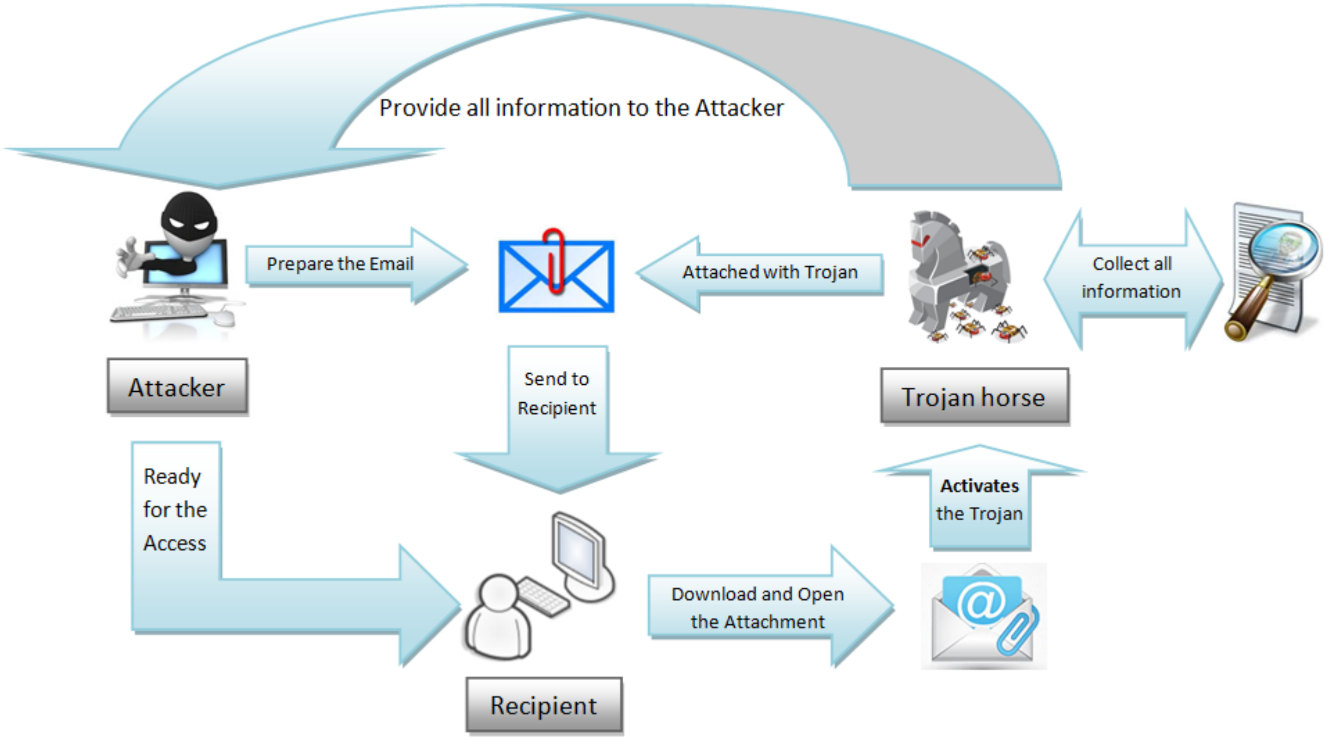


Fig 1.4: Trojan Attack

D. Graphical Substitution

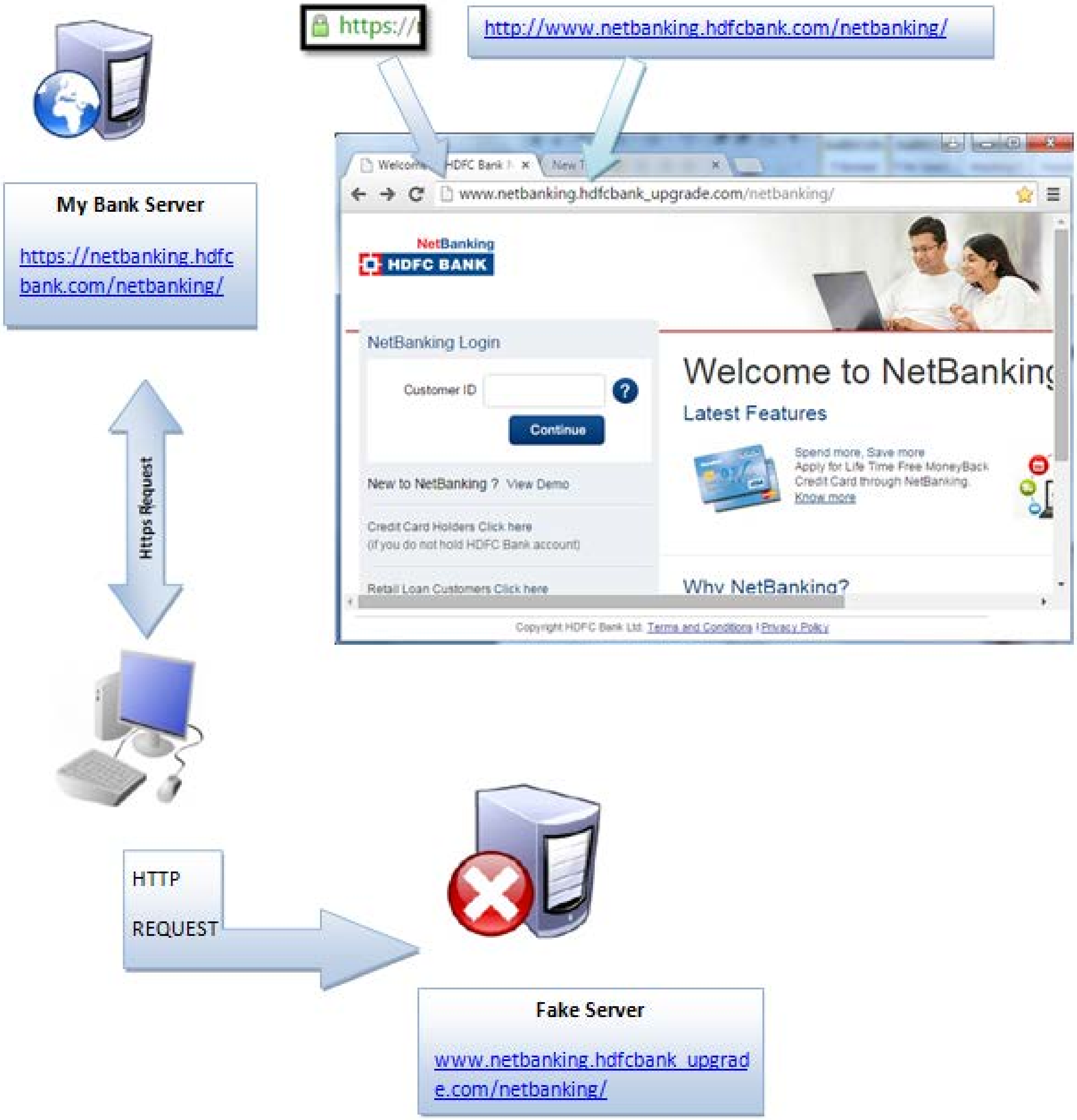
In this case, attackers replace the secure padlock and the Zone of the page source by using the images in the URL. Like for **https://** it used the image for padlock as described in Fig1.5,

How it is conducted:

i. Attacker's send the link via email.

ii. When the recipient click on the link, the expectation is the server connects with the following URL: https://www.netbanking.hdfcbank.com/netbanking

But actually the link redirects the recipient to the following fake server
www.netbanking.hdfc_upgrade.com/netbanking



New to NetBanking ? View Demo

Credit Card Holders Click here
(if you do not hold HDFC Bank account)

Retail Loan Customers Click here

Spend more, Save more
Apply for Life Time Free MoneyBack Credit Card through NetBanking.
Know more

Copyright HDFC Bank Ltd. Terms and Conditions | Privacy Policy

Fig 1.5: Graphical Substitution

iii. The attacker using their graphics techniques replaces the padlock with the image 🔒 https:// which is present in URL field and also it replaces the same with the fake address bar to hide the real information.

iv. Once the recipient fills the details like Username and Password, attackers tried the same with the real server and ready for the funds transfer.

IV. PREVENTING METHODOLOGIES

1. **Never Click on Hyperlinks within emails**

The Hyperlinks within emails can re-direct to fraud website which looks similar to real site.

If you are not 100 percent sure of the source of the email, then never click on hyperlinks within emails, whether it comes from a legitimate company or from other source. Instead of this, you can type the URL in the Internet browser address bar, or call the company on a contact number for verification and make sure it is genuine.

2. **Never download anything from an un-trusted website**

Whenever you download anything from an un-trusted website, you also receive Trojan or other viruses with that download file. When you double click on the downloaded file, the virus got activated and ready to steal your information. So to prevent from these frauds, always download from trusted websites only.

3. **Use Anti-Virus Software**

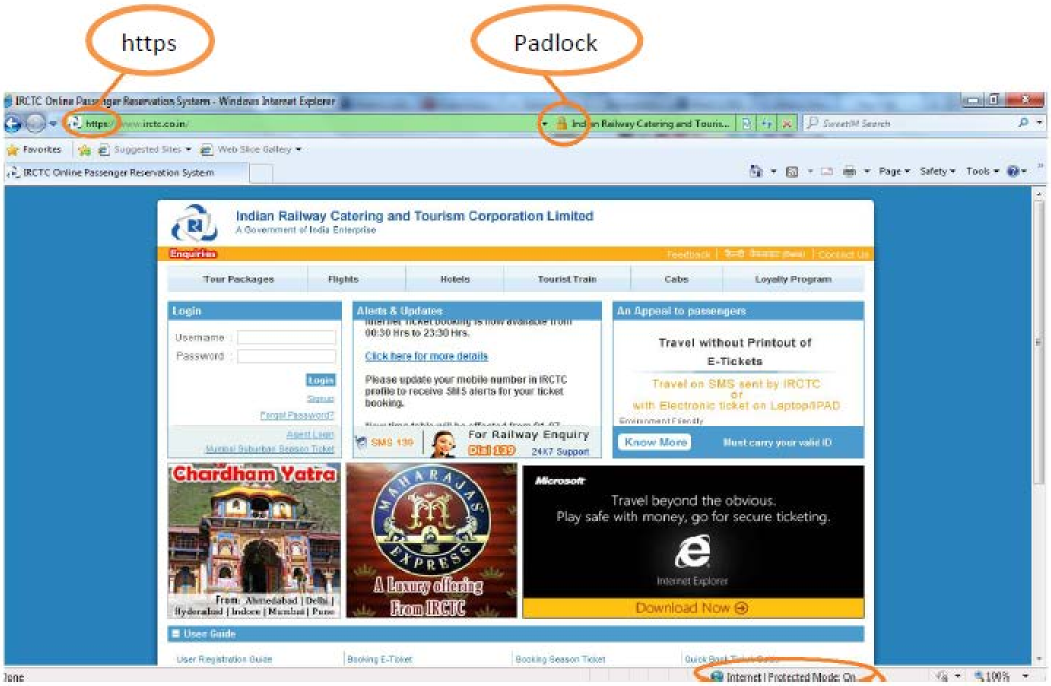
To protect against Trojan horse and other virus attacks, use anti-virus software which can detect and delete virus files before they can attack your computer. It is important to keep all anti-virus software up to date with vendor updates. These virus programs can search your computer for personally sensitive information and pass this information to attackers.

4. **Keep Software Updated (Operating Systems & Browsers)**

Many computer attackers are continually finding vulnerabilities in operating systems and Internet Browsers. Software vendors are constantly updating their software to fix these vulnerabilities and protect consumers. So always keep all the used software updated.

5. **Always look for "https" and a padlock on a site that requests personal information**

Information entered on an Internet Web Site can be intercepted by a third party. So the websites having **https** and **padlock** protects you from these kinds of activities as shown in Fig 1.6. When submitting sensitive financial and personal information on the Internet, look for the locked padlock on the Internet browser's status bar or the “https://” at the start of the URL in the address bar. The absence of these indicators shows that the web site is definitely not secure.



00:30 Hrs to 23:30 Hrs.

Please update your mobile number in IRCTC profile to receive SMS alerts for your ticket booking.

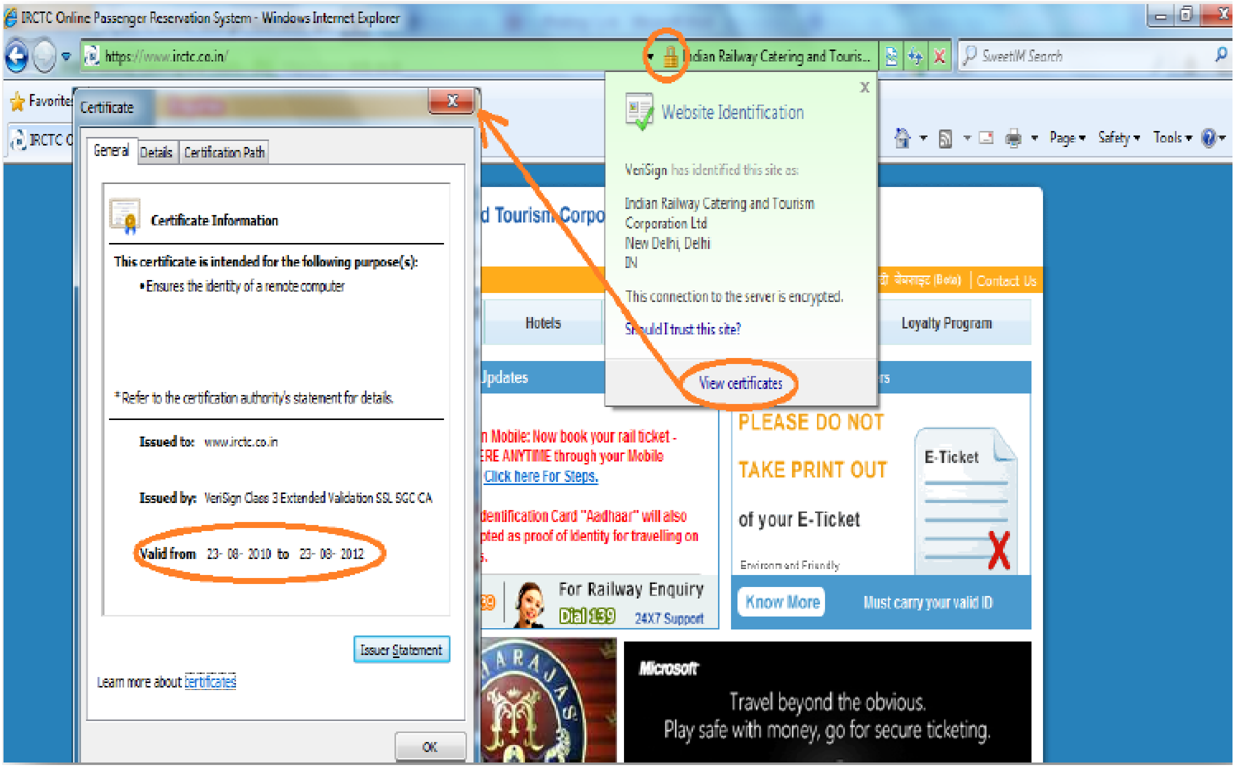
Travel without Printout of E-Tickets

Travel on SMS sent by IRCTC or with Electronic ticket on Laptop/IPAD

Travel beyond the obvious. Play safe with money, go for secure ticketing.

Fig 1.6: Padlock with HTTPS

When you click on the Padlock as shown in Fig 1.7, the pop-up related to certificate opens, then click on the **View Certificates**, after that another pop-up window opens which contains the certificate details from where you validate the web server.



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

* Refer to the certification authority's statement for details.

Issued to: www.irctc.co.in

Issued by: VeriSign Class 3 Extended Validation SSL SGC CA

Valid from 23- 08- 2010 to 23- 08- 2012

Learn more about certificates

VeriSign has identified this site as:

Indian Railway Catering and Tourism Corporation Ltd
New Delhi, Delhi
IN

This connection to the server is encrypted.

Should I trust this site?

View certificates

PLEASE DO NOT TAKE PRINT OUT of your E-Ticket

Travel beyond the obvious.
Play safe with money, go for secure ticketing.

Fig 1.7: View Certificates

6. **Keep your Computer clean from Spyware**

Spyware & Adware are files that can be installed on your computer, even if you don't want them. It monitors your Internet browsing patterns like you are searching for purchasing anything and keep an eye on your purchasing and provides the same information to companies.

For example:
If you've downloaded some music, files or documents and suddenly started getting annoying ads popping up on your screen, you could definitely be infected with Spyware and/or Adware! The website which is most popular for downloading songs (www.songspk.pk) is the best example of this.

7. **Report Phishing Emails**

You can report phishing email to reportphishing@antiphishing.org. The Anti-Phishing Working Group is a group of ISPs, security vendors, financial institutions and law enforcement agencies, uses these reports to fight phishing.
For more information check Identity Theft Help Sites below:

- http://www.consumer.gov/idtheft/
- http://www.identity-theft-help.us/
- http://www.identitytheft.org/
- http://www.usdoj.gov/criminal/fraud/idtheft.html
- http://www.ifccfbi.gov/index.asp
- http://www.fbi.gov/scams-safety/fraud

V. CONCLUSION

Now you understand the Phishing Attacks and their Preventing measures, so it is highly recommended to use the preventing methodologies in day to day life to be secure and safe from the Phishing Attacks. So the conclusion is that we cannot stop these kinds of Attacks but we can follow the safety measures to prevent from this.

ACKNOWLEDGMENT

I would like to acknowledge my co-workers for supporting and encouraging me throughout the course work.

AUTHORS

First Author – Kewal Krishan Kapoor, **Qualification /Experience:** Currently working with Syscom Corporation Ltd, a leading Telecom Company deals in SIM and SMART cards. **Email Address**: kewalkrishankapoor@yahoo.com.