---

# Phishing - The Art of fooling End Users

&

# Anti-Phishing (2-way Authentication System)

By - Rockey Killer
(skg102@gmail.com)
h4ck3r.in

---

---
Table Of Contents
---

## Introduction

Phishing is misrepresentation where the attacker uses social engineering to appear as a trusted identity. They leverage the trust to gain valuable information; usually details of accounts, or enough information to open accounts, obtain loans, or buy goods through e-commerce sites. Up to 5% of users seem to be lured into these attacks, so it can be quite profitable for scammers – many of whom send millions of scam e-mails a day.

## Phishing Techniques from Attacker's Point of View

### 1) Simple Phishing (User won't be logged in)

In this phishing attack, attacker will be creating a fake login page similar to the original login page on his server/domain. Once the phishing page is ready Attacker will convince victim to login using that fake login page and when victim will submit username/password in that fake login page that information will be sent to attacker and victim will be redirected to the original sites login page.

Now again victim will have to enter username/password to login in that site and this can make victim suspicious, and victim may identify that there was a trap.

### 2) Simple Phishing (User will be logged in )

In simple phishing attack, attacker will be creating a fake login page similar to the original login page on his server/domain. Once the phishing page is ready Attacker will convince victim to login using that fake login page and when victim will submit username/password in that fake login page that information will be sent to attacker and victim will be logged into original site. This is done by the attacker to make the attack more stealth and attackers use javascript on their phishing pages which makes the user login into the original site without asking the victim to re-enter the username and password.

Now this kind of attack is really stealth , as victim is not asked to enter the details again so this easily convinces the victim that details entered by the victim were on original site

But what if victim enters wrong information by mistake on phishing page ?

### 3) Advanced Phishing

In Advanced phishing attack, attacker will be creating a fake login page similar to the original login page on his server/domain. Once the phishing page is ready Attacker will convince victim to login using that fake login page and when victim will submit username/password in that fake login page , that information will further be verified by the server side scripting if the username/password are

accurate or wrong and in case details entered by victim are wrong then victim will be again redirected to phishing page and if the details entered by the victim are correct then that information will be sent to attacker and victim will be logged into original site.

Now even if the victim had entered the wrong information on the phishing page . Victim will be again directed on the phishing page and will be asked to enter the correct information which further convinces the victim that the login page is original.

Now what if victim has typed username/password on the phishing page but before submitting victim realizes that it's a trap then all the information entered by the victim will be lost.

4) Implementing Ajax keylogger on phishing page

---

In this Attack, Attacker uses Ajax keylogger on the phishing page. As we have discussed in the scenario above, to overcome that problem Attackers use AJAX keylogger on their phishing page which saves the keys on the server as user types them and even if the victim don't submit them but just type them still that information is trapped by the attacker and can be further misused.

5) DNS Poisioning aided Phishing

---

In this attack, attacker posions the dns of the victim and whenever victim makes a request to the dns victim is given IP address of the Attacker's server where phishing page is hosted, So even if the victim has entered the right Domain name but still victim lands up on the phishing page and the attacker is able to steal the information of the victim. Now in this kind of attack Attacker doesn't even gives a chance to the victim to be suspicious.

6) XSS aided Phishing

---

In this attack, attacker finds a vulnerable link in the original website like

www.example.com/index.php?
msg=<script>window.location="http://www.attackersphishingpage.com/login.php";</script>

now this link seems to belong to example.com however when the victim will click on this link , victim will land on the phishing page
made by the attacker.

So, these are the few ways which can be used by attackers to attack on end-users and making them victim of phishing.

## Defence from users point of view

---

### 1) Verify the URL

---

Before entering any information on the page, make sure that URL on the top of the browser is correct even if you find the look and feel of the page is quite similar to the real login page but make sure to verify that the URL on the top of the browser belongs to the right domain name.

Some times it can be tricky like there can be a phishing page of example.com on another domain like exmaple.com or something similar. So, you should closely observer the URL on the top of page.

### 2) Verify the SSL Certificate

---

Make sure to verify the SSL Certificate over the domain is there and do belongs to the right Certifying Authority.

For example login page of orkut have a ssl certificate of thawte.

You can also check the "Lock" icon There is a de facto standard among web browsers to display a "lock" icon somewhere in the window of the browser (NOT in the web page display area!) For example, Microsoft Internet Explorer displays the lock icon in the lower-right of the browser window and As another example, Mozilla's FireFox Web Browser displays the lock icon in the lower-left corner.

### 3) Inbult phishing protection in web browsers

---

Many web browser and added plug-ins today provide you with the security feature which identifies the phishing link and warns you when you visit those links. This security feature is only functional on those links which have been reported by some other user.

For example, in case of Mozilla Firefox,

Firefox 3 or later contains built-in Phishing and Malware Protection to help keep you safe online. These features will warn you when a page you visit has been reported as a Web Forgery of a legitimate site (sometimes called “phishing” pages) or as an Attack Site designed to harm your computer (otherwise known as malware).

4) Internet Security Programs

---

Many anti-viruses today have phishing protection and works in the similar way as explained above.

For example, in case of Norton,

Norton Internet Security 2010 Blocks phishing websites and authenticates trusted sites

5) Password managers can be used.

---

You can further use various password managers that are available as password manager will only work on the real websites and not on the phishing websites.

For example, in case of passpet,

Passpet have Convenient Password Management and Phishing Protection

6) Verifying the IP address of the host

---

In case you you are suspicious about a page but the URL seems to be correct then you should verify the IP address of that domain , you may be a victim of DNS poisoning.

These were the few security measures , by which you can protect yourself from becoming a victim of phishing.

# Securing login page from programmers point of view

---

## 1) Fix all your XSS vulnerabilities

---

If you are having a login authentication on your website then make sure your website is not vulnerable to XSS attacks as Attacker can use XSS Vulnerability in your website to exploit users of your website. (Can steal cookie , can redirect your users to legitimate phishing page)

## 2) Do not use pop-ups

---

Attackers most commonly use the technique of pop-ups to setup hoaxes of phishing like they whenever they redirect victim to phishing page they pop-up a message saying something "Session Expired, Log in" and they make it similar to the original website which further convinces victim to fill in the information.

So, you should remove pop-ups from your website and can inform your end-users that you don't use any pop-ups and in case they come across any pop-up in your website they should report it to Website Administrator.

## 3) Don’t be framed

---

Frames are a popular method of hiding attack content due to their uniform browser support and easy coding style, Make sure that your website can't be framed like attacker can include your web-page in a iframe and can ask easily trick victims to steal their information. You can further use frame-busters to protect your website from being framed.

## 4) Enforce local referrers

---

Local referrers should be enforced so that attacker has to host images and other content on attacker's server . This technique is commonly known as anti-leeching . If Attacker will be using images from their own server then there are few chances that they can create some differences which can help end-users to identify hoaxes.

## 5) Keep the address bar, use SSL

---

Do not lock the address bar as many websites lock the address bar so that users can not tamper data in the URL however this creates a problem for users as they are not able to bookmark login page by which they can further become the victim of phishing.

Make sure to use SSL if you are having some sensitive informations of users in your database. As this can protect your website users from sniffing and can protect your users from phishing as they can easily identify phishing page by verifying that
certificate in Address bar.

6) Fraudulent Domain Name
---

If you feel like that attackers are there who might be making hoaxes for your websites end users then make sure to take control of fraudulent domain names. Let's say you have a domain name example.com which deals in sensitive data and have many users across the globe
then there are good number of chances that attacker will book domain name like exmaple.com to attack users and to steal their username and passwords.

2 way authentication system
---

Introduction
---

2 way authentication means that before end-user enters the login information on the login page that particular login page authenticates to the end-user that it's not fake. So, let's take a scenario in which user have to enter Username and Password , So how can user identify whether he/she is accessing the right page or not. So over here we can introduce third term that is PassPhrase that is whenever user will enter the username in the login page, passphrase will be displayed to the user which is already known to the user (Most probably entered by the user at the time of registration) .

Features
---

2 way authentication should be securely developed as it will be targeted by the attackers to bypass 2 way authentication one way or other. So the passphrase chosen in 2 way authentication should be from the users side and users should be intimated that only when they see the correct passphrase then only they should enter their password.

Technology Used
---

This kind of authentication system can be built by using Ajax and any server side language and database that is compatible with AJAX. However I have used PHP/MYSQL/Javascript.

Working
---

When new user will register then we can ask the user for passphrase and will be storing that in our database along with the username and password (or say encrypted password) . Now whenever the user will login and will type username on the login page then on the backend JavaScript will request the server to provide the corresponding passphrase, if there is no passphrase corresponding username then instead we will display some random text so that automated scripts can be failed to

identify the correct username And once user will get the correct passphrase on the login page then user can type in the correct passphrase to login and can further authenticate to the website. We have to make sure that only the authenticated requests can see the passphrase and automated tools should not be able to gather the passphrase.

## Security

In this way we can develop a secure login pages in which users themselves can identify if they are on phishing page or on the original page. Of-course it is not 100% secure but can be treated as more secure as compared to traditional login pages and can highly reduce the cases of phishing if implemented in a secure way on widely used websites.

## Future

2-way authentication can be made more secure by adding up more security features. We will be looking forward to make it more secure and will be working on it as open source 2-way authentication system.

## Video Demonstration

I have tried to demonstrate some of the attacks and 2-way authentication system in this video. You can access this video at youtube in the following link

http://www.youtube.com/watch?v=mUl4Ksjp9os

## Summary

In this paper we have discussed various techniques by which attacker use phishing to attack end users. Further we have explored various way by which users can defend themselves from becoming the prey of phishing attack. Then we discusses how programmers can make their login pages secure to prevent phishing and in the end we discussed about 2 way authentication , It's working, features and future.

## References


Mozilla.com
Symantec.com
Passpet.org
OWASP.org
wikipidea.org
PHP.net
h4ck3r.in
ssl.com


## Thanks to following for their support


w4rl0ck.d0wn, chip, Atul(sir),n7nikhil6 ,h4ck3r crew,null community