International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 11 | Nov 2020 www.irjet.net p-ISSN: 2395-0072

Website Spoofing: A Detailed Study

Tushar Dutt Dave[1]

[1]Student, B.A. LL. B (Hons), 9th Semester, Manipal University Jaipur, Rajasthan, India

---

Abstract - *This paper describes the mechanism used for website spoofing, its consequences, prevention, punishment in India and how social media has become a platform to get many sitting targets without much effort. With advancements in technology and limited knowledge about cyber-crimes has resulted hackers to exploit internet easily. Obtaining personal information using spoofed websites and using that data to exploit victim economically also causes reputation damage to the sites used as basis for spoofing as customers often loses trust in those websites.*

1. INTRODUCTION

The Internet brings many opportunities, but the risks that come with such options are infinite. Some examples of these risks are cyberstalking, cyber theft, web spoofing, phishing, etc.

Web Spoofing means to deceive a user by using a fake website that looks exactly like the original website and has a similar URL (website link). With continuous development in social media and limited check on the shared content, social media has become a primary source for web spoofers to use it as a medium to attract people to their spoofed website. "Web Spoofing is the net age crime, born out of the technological advances in the internet age. "Web Spoofing" is a more modern shape of social engineering. Typically, it is a form of social engineering, characterized by using attempts to fraudulently accumulate sensitive information, such as passwords, usernames, login IDs, ATM PINs, and credit card information, by masquerading as a person, commercial enterprise in a seemingly professional electronic communique, such as an email, an instantaneous message or website. Such attacks then direct the recipient to a web page so precisely designed to appear as an impersonated agency's (often financial institution & monetary organization) personal internet site. They cleverly harvest the consumer's non-public information, regularly leaving the sufferer blind to the assault." (Neeraj Aarora, n.d.)

2. Crime associated with website spoofing

Website spoofing leads to several other crimes. It is not just limited to privacy violations. It includes identity theft, unauthorized access to passwords, theft of intellectual property, etc.

2.1 Identity Theft

Identity theft refers to obtaining personal information of someone which defines his/her identity and uses it for economic benefits, scamming, or fraud. Information collected on the spoofed website is often used for committing numerous crimes. With the continuous advancement in technology, it isn't easy to track the person as the Internet provides anonymity for online transactions.

2.1.1 How to know if your identity is used by someone else

Identity theft is not easily traceable, but these few signs can help you to know if you are a victim of identity theft:

1. Unauthorized transactions from the bank account
2. Registration emails of websites not visited by you
3. Messages or calls for feedback from any service providers which you haven't used.
4. Emails that are not sent by you.

2.2 Theft of Intellectual Property

The theft of intellectual property is defined as theft of subject matter protected by copyright, trademark, etc. Website spoofing includes copying the design of an already established website, which is a violation of copyrights.[1] Section 51 of the Copyright Act deals with copyright infringement in India.

2.3 Privacy Violation

Sometimes a spoofed website asks the victim to download attachments in which viruses/keyloggers are attached, which gives access to personal computer files to hackers. All the data on your computer, including private photos and videos, can be obtained by hackers.

2.3.1 How to prevent such viruses?

1. Never download any material from untrusted sites.
2. Install and regularly update the antivirus.
3. Perform a full malware scan using antivirus.

3. Web Spoofing Site: Hard to Detect

A web spoofing site is not a virus or malware and cannot be detected by antivirus. These websites can be accessed like a regular website without getting noticed by antivirus.

[1] Copyright Registration of Websites (https://www.copyright.gov/circs/circ66.pdf)

A web spoofing site's design can be precisely the same as the original website with minor unnoticeable changes. The website URL of a web spoofing site can also be very similar to the original but can never be the same.

Figure 1: Example of Web Spoofing Website

The above image shows a web spoofed page of Facebook. It can be seen that the design of the site is precisely similar to Facebook, and the URL is "faceb00k.com".

It becomes tough to notice such small changes, and people often become victims of such attacks.

4. Web Spoofing Not Just Limited to Obtaining Data

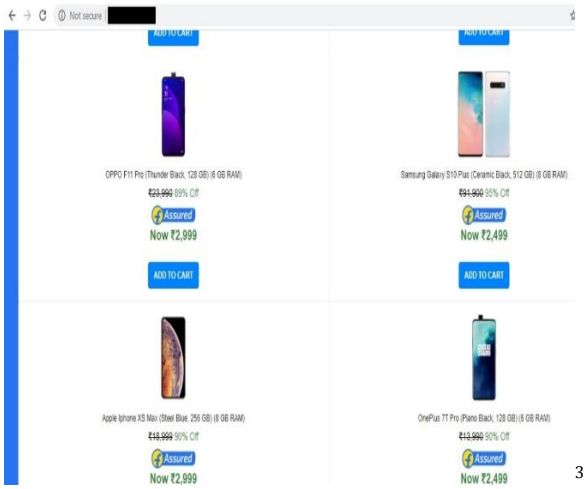
Web spoofing has become a much more severe threat than it was earlier. With easy access to payment gateways [2] web spoofers have started taking online payments instead of information.

The below demonstration will help to understand the seriousness of the problem more correctly:

(This demonstration is for education purpose only)

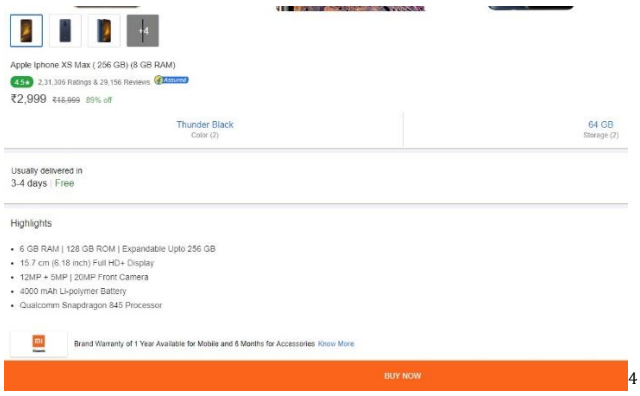
1. A website is prepared with a similar design and URL to the original website. The victim often failed to recognize the spoofed website because of the similarity in the original and spoofed website's structure.

The image below shows an online shopping spoofed site with a buy option to obtain money from the user.



[3]

*Note-The URL of the web spoofed site can never be the same as the original website. It will always have a typo or utterly different domain name.

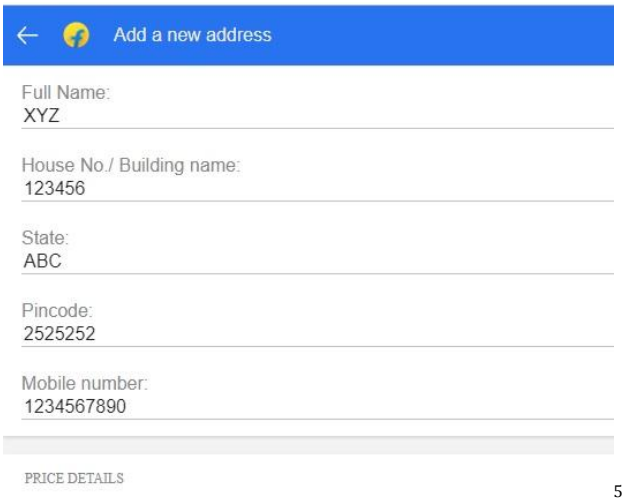


[4]

2. Collecting information about the user- This information is used afterward for different purposes, for example: Using a mobile number for promotional messages, etc.

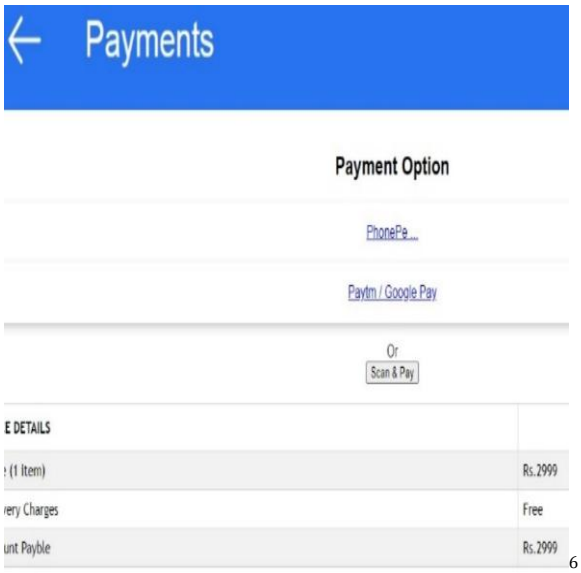
2 Payment gateways are software and servers that transmit transactions information to acquiring banks and responses from issuing banks (source: 2checkout)

[3] Web spoofing site of a shopping site.
[4] A Buy now option on a spoofed website.



[5]

3. Using a web spoofed site to take payments - By getting a payment gateway receiving online payment is made extremely easy without providing details of any kind to the user payment that can be received directly in the bank account. It is easily traceable by Police if a complaint is made in the cyber portal of India.



[6]

The above-explained mechanism is used to scam thousands of people with significantly less effort and money.

"Web spoofing is a hassle that has increased twofold within the closing year, ensuing in $1.3 billion in losses, in keeping with the 2019 Thales Access Management Index (registration required). In an excessive-profile instance of web spoofing that has left the commercial enterprise global more than a bit rattled, hackers efficaciously diverted around 500 thousand clients traveling the British Airways internet site ultimate summer to a practical-searching but a fraudulent website, without the airline having any idea it was spoofed.[7]

The spoof website online accumulated names, addresses, login information, payment info, and other information. After an overview by way of the EU's Information Commissioner's Office, British Airways faces a likely record-breaking fine for violating General Data Protection Regulation (GDPR), to the tune of £183.5 million — about 1.5 percent of the airline's annual revenue." (Stolfo, 2019)

5. How Is Social Media Helping?

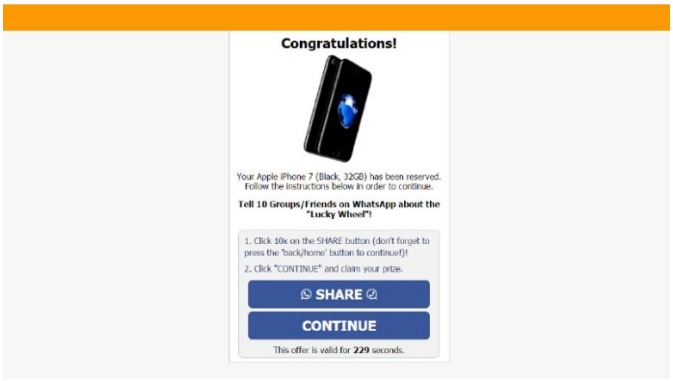
Social media provide the most extensive user base to web spoofers. With the help of social media, a quantity of traffic is directed to such web spoofing sites. These sites are promoted on social media with an exciting offer that attracts the user to the site, and if they are not careful, they become victims of a scam without even knowing that a fake website is scamming them.

[8]

Another method of getting traffic to these sites is by putting a mechanism that involves the user sharing the webpage with a few of his/her family or friends to claim the offer. This method can be far more harmful as the user share the fake website with family and friends without knowing, and the user's friends and family repeat the same. Even if the phony

[5] Web spoofing is used to collect information from the user.
[6] Taking payments from the web spoofed website.
[7] Rethinking Website Spoofing Mitigation – Dr. Salvatore Stolfo
[8] Promotion on social media of web spoofing

webpage does not have a payment method for payment, the website owner is still earning by displaying advertisements on the spoofed site. According to the government data, the cases of fraud in e-commerce have escalated by 475 percent between August 2016 and November 2019.[9]



(**Image Source** Flipkart.com)

6. Crimes originated outside India.

Section 1(2) of the IT act provides that the Act shall enlarge to India's complete and store as in any other case provided on this Act; it also applies to any offense or contravention thereunder devoted outdoor India by way of any individual.

Further, Section 75 of the IT act provides for Act to apply for offense or contravention dedicated outdoor India. -

(1) Subject to subsection (2), provisions of Act shall also apply to any offense or contravention dedicated outside India through any individual irrespective of his nationality.

(2) For sub-section (1), this Act shall observe to an offense or contravention dedicated outdoor India by using any character if the Act or conduct constituting the offense or contravention entails a computer, laptop gadget, or pc network placed in India.

7. Punishment in India for such fraudulent acts

The IT Act, 2000, is the principal Act that deals with India's legislation concerning cybercrimes. These fraudulent acts are punishable under Section 66D of the IT Act. Section 66 D says, "Punishment for cheating by personation by using computer resource. -Whoever, by means for any communication device or computer resource cheats by personating, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees."[10]

A report of such cybercrime can be filled at the cybercrime portal of India, i.e., https://cybercrime.gov.in/.

Other laws relating to web spoofing are-

1. Section 416 Cheating by Personation Indian Penal Code: " A individual is stated to "cheat by personation" if he cheats with the aid of pretending to be a few other characters, or by way of knowingly substituting one person for any other, or representing that he or another character is someone other than he or such other character truly is." (Indian Kanoon)

2. Section 51 Infringement of Copyright, Copyright Act 1957: Creating a duplicate copy of a website infringes a copyright, and the person or organization will be liable under the copyright act.

8. Consequences

The consequences of this can be dire. The data provided by the user is collected by the web spoofed site and is used to get access to other accounts as people often use similar email and passwords for different places. The data stored is further sold for various purposes. Monetary Loss of victims is common in such attacks.

The consequences of web spoofing are not limited to the victim only, but it also equally affects the organization used as the basis for spoofing. Most organizations that are attacked lost customers and suffered reputation damage as a result.[11]

[9] financialexpress.com/industry/sme/ecommerce-fraud-ecommerce-fakes-online-fraud-fake-products-amazon-flipkart-fake-products-consumer-protection-act-ecommerce-policy/1791187/

[10] https://indiankanoon.org/doc/121790054/

[11] forbes.com/sites/forbestechcouncil/2017/09/14/the-dangers-of-phishing

9. Prevention

It is nearly impossible to detect such sites if a person is not paying attention. Any message you get through email, WhatsApp, SMS that comes with a link needs to ring an alarm in mind, be it login into your Facebook account, sale offers, a message from your bank containing a link, or download movie/images. Here are a few ways that can help to keep you safe from such attacks:

1. Bookmark important sites and only access them from bookmarks.
2. Use google to access any website.
3. Don't click on suspicious offer links.
4. Always check the browser's website bar for the spelling of the website.
5. Pay close attention to sender email addresses.
6. Use 2 step verification, which requires the user to enter a code sent to you on your mobile/email and password for logging into the account.

References

1. (n.d.). Retrieved from Indian Kanoon: https://indiankanoon.org/doc/1041696/

2) Neeraj Aarora, C. L. (n.d.). Retrieved from siliconindia: https://blogs.siliconindia.com/neerajaarora/Phishing-Scams-in-India-and-Legal-Provisions-bid-vkXYC7Gm32628069.html

3) Stolfo, D. S. (2019, 07 08). Rethinking Website Spoofing Mitigation. Retrieved from Darkreading: https://www.darkreading.com/threat-intelligence/rethinking-website-spoofing-mitigation