PHISHING TECHNOLOGY

Presented by:

Omar Farahan Molla

L2018-1081

University Institute of Technology

Acknowledgement

I would like to thank respected faculties of CSE for giving me such a wonderful opportunity to expand my knowledge for my own branch and giving me guidelines to present a seminar report. It helped me a lot to realize of what we study for.

Secondly, I would like to thank my parents who patiently helped me as i went through my work and helped to modify and eliminate some of the irrelevant or un-necessary stuffs.

Next, I would thank Microsoft for developing such a wonderful tool like MS Word. It helped my work a lot to remain error-free.

Last but clearly not the least, I would thank The Almighty for giving me strength to complete my report on time.

Contents

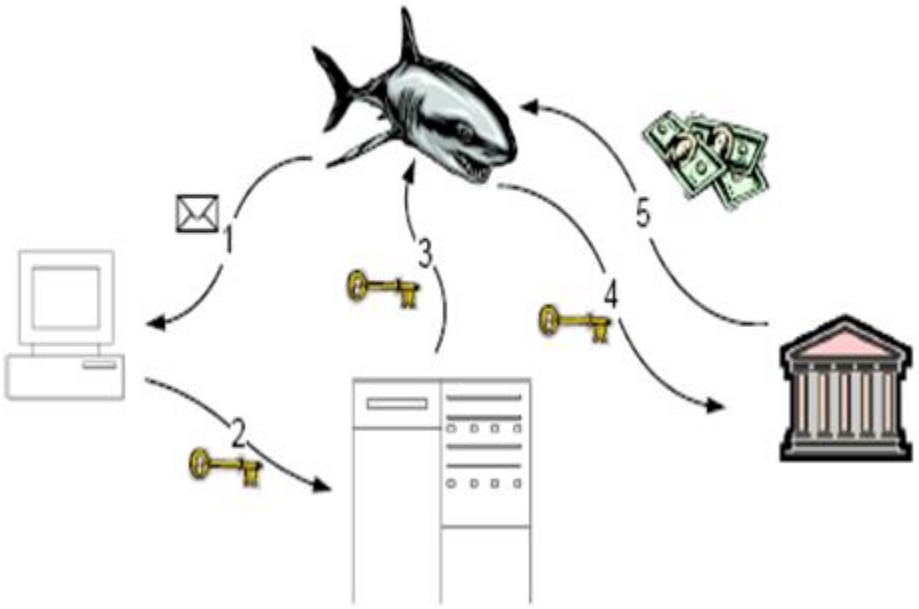
1. Introduction

In the field of computer security, Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Phishing is a fraudulent e-mail that attempts to get you to divulge personal data that can then be used for illegitimate purposes.

There are many variations on this scheme. It is possible to Phish for other information in additions to usernames and passwords such as credit card numbers, bank account numbers, social security numbers and mothers' maiden names. Phishing presents direct risks through the use of stolen credentials and indirect risk to institutions that conduct business on line through erosion of customer confidence. The damage caused by Phishing ranges from denial of access to e-mail to substantial financial loss.

This report also concerned with anti-Phishing techniques. There are several different techniques to combat Phishing, including legislation and technology created specifically to protect against Phishing. No single technology will completely stop Phishing. However, a combination of good organization and practice, proper application of current technologies and improvements in security technology has the potential to drastically reduce the prevalence of Phishing and the losses suffered from it. Anti-Phishing software and computer programs are designed to prevent the occurrence of Phishing and trespassing on confidential information. Anti-Phishing software is designed to track websites and monitor activity; any suspicious behavior can be automatically reported and even reviewed as a report after a period of time. This is also included detecting Phishing attacks, how to prevent and avoid being scammed, how to react when you suspect or reveal a Phishing attack and what you can do to help stop Phishers.

I



a. A deceptive message is sent from the Phishers to the user.
b. A user provides confidential information to a Phishing server (normally after some interaction with the server).
c. The Phishers obtains the confidential information from the server.
d. The confidential information is used to impersonate the user.
e. The Phishers obtains illicit monetary gain.

Steps c and e are of interest primarily to law enforcement personnel to identify and prosecute Phishers. The discussion of technology countermeasures will center on ways to disrupt steps a, b and d, as well as related technologies outside the information flow proper.

2. Phishing Techniques

Phishers use a wide variety of techniques, with one common thread.

2.1. Link Manipulation

Most methods of Phishing use some form of technical deception designed to make a link in an e-mail appear to belong to the spoofed organization. Misspelled URLs or the use of sub domains are common tricks used by Phishers. In the following example, http://www.yourbank.example.com/, it appears as though the URL will take you to the *example* section of the *yourbank* website; actually, this URL points to the "*yourbank*" (i.e. Phishing) section of the *example* website.

An old method of spoofing used links containing the '@' symbol, originally intended as a way to include a username and password. For example, http://www.google.com@members.tripod.com/ might deceive a casual observer into believing that it will open a page on www.google.com, whereas it actually directs the browser to a page on members.tripod.com, using a username of www.google.com: the page opens normally, regardless of the username supplied.

2.2. Filter Evasion

Phishers have used images instead of text to make it harder for anti-Phishing filters to detect text commonly used in Phishing e-mails.

2.3. Website Forgery

Once a victim visits the Phishing website the deception is not over. Some Phishing scams use JavaScript commands in order to alter the address bar. This is

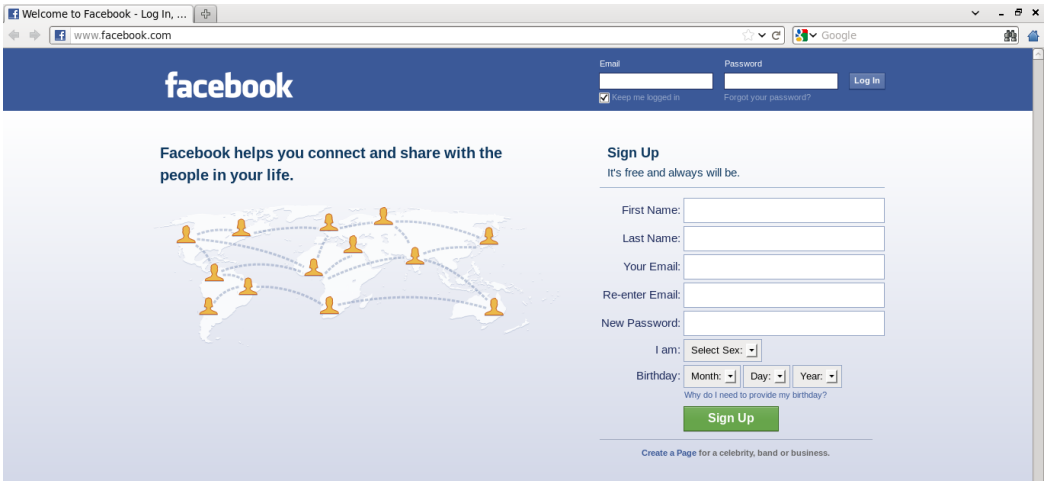
done either by placing a picture of a legitimate URL over the address bar, or by closing the original address bar and opening a new one with the legitimate URL.

2.4. Phone Phishing

Messages that claimed to be from a bank told users to dial a phone number regarding problems with their bank accounts. Once the phone number (owned by the Phishers) was dialed, prompts told users to enter their account numbers and PIN. Vishing (voice Phishing) sometimes uses fake caller-ID data to give the appearance that calls come from a trusted organization.

3. Phishing Example

3.1. Facebook Phishing



Original Facebook Login page

Fake Facebook Login page

Cybercriminals send phishing emails that include links to fake websites, such as the mobile account login page for a known mail provider, asking the victim to enter their credentials or other information into the fake site's interface. The nefarious website will often leverage a subtle change to a known URL to trick users, such as "facelook.com" (or URL in given screenshot) instead of "facebook.com".

4. Causes of Phishing

Phishing is a type of online scam where criminals impersonate legitimate organizations via email, text message, advertisement or other means in order to steal sensitive information. This is usually done by including a link that will appear to take you to the company's website to fill in your information – but the website is a clever fake and the information you provide goes straight to the crooks behind the scam.

- Misleading e-mails:
  Phishing is a cyber-attack that **uses** disguised email as a weapon. The goal is to trick the email recipient into believing that the message is something they want or need — a request from their bank, for instance, or a note from someone in their company — and to click a link or download an attachment.
- No Check of Source address:

  On the internet, the following types of address are improper source address.
  - Private Address, Unique Local IPv6 Unicast Address (ULA)
  - Unassigned Internet address
  - Special address such as 0.0.0.0, :: , documentation address and multicast address.

  In more precise terms, a normal state is one in which communication are conducted using an assigned address from ISP, an improper state is when a source address differs from assigned address from ISP.

  There are several conceivable reasons as to why a source address may be different than an assigned address. One cause could be a problem with software. It is not uncommon for software defects to result in the attachment of incorrect IP address or incorrect NAT behavior. Another cause could be spoofed IP address by malevolent software. Attackers engaging in spreading worms. DoS, or the other attacks may spoof the source address to disguise their identify or to make response difficult.

Over recent years, we have seen an increasing amount of source address spoofing associated with DoS attacks and other improper Internet communication. Smurf attacks are one of the main types of attacks that use spoofed source address. Other cases of source address spoofing have been associated with SYN flood attacks and ICMP flood attacks. Source address spoofing not only disrupts normal communication, but it also places extreme loads on ISP backbones and customer network environments due to the enormous volume of needless communication flow.

- Lack of user awareness:

  In recent years, most of our daily services have been increasingly linked to the Internet, such as online banking and online shopping, thereby making our lives more comfortable and manageable, wherever we may be and at any time of day. However, this ubiquity of service also carries a critical security threat, which can cost Internet users dearly. Therefore, improving Internet users' security awareness is a matter of high importance, especially in light of the significant growth of online services. This paper investigates the effects of security awareness and phishing knowledge on users' ability to detect phishing emails and websites. In this approach, two experiments were conducted to evaluate the effects of security awareness. The results of these experiments revealed that phishing awareness has a significant positive effect on users' ability to distinguish phishing emails and websites, thereby avoiding attacks.

- Vulnerability in applications:

  An application vulnerability is a system flaw or weakness in an application that could be exploited to compromise the security of the application. Once an attacker has found a flaw, or application vulnerability, and determined how to access it, the attacker has the potential to exploit the application vulnerability to facilitate a cyber-crime. These crimes target the confidentiality, integrity, or availability (known as the "CIA triad") of resources possessed by an application, its creators, and its users.

  Attackers typically rely on specific tools or methods to perform application vulnerability discovery and compromise. According to Gartner Security, the application layer currently contains 90% of all vulnerabilities.

It is common for software and application developers to use vulnerability scanning software to detect and remedy application vulnerabilities in code, but this method is not entirely secure and can be costly and difficult to use. Furthermore, scanning software quickly becomes outdated and inaccurate, which only poses more issues for developers to address in trying to make their applications secure.

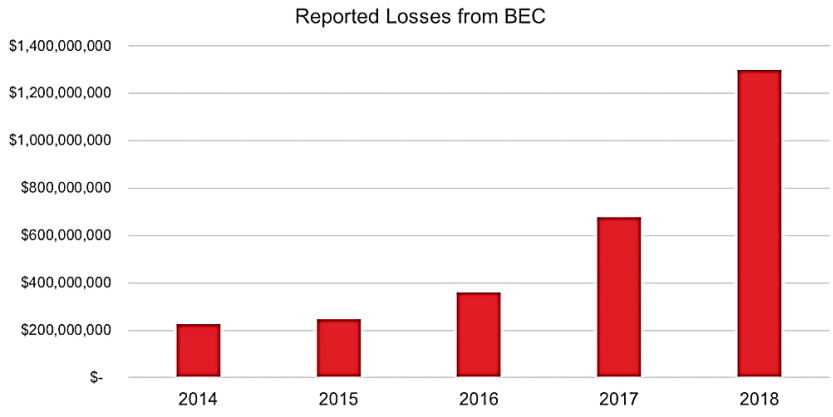
- Limited use of digital signatures

  Especially after gathering information on employees of company, an attacker (or penetration testing company) can try to use that, information to contact or trick that individual to giving the information or access they otherwise wouldn't have.

  - This initial attack can create what is known as a "pivot point" where an attacker can take the information learned and use it to cause further compromise for a company, such as taking that employees credentials to log onto the network.
  - Any amount of information gained can be used to get more information. The more information the attacker gains, the more leverage they have available to use.
  - In addition to teaching users about the different social engineering tactics, it's also useful to teach them about these underlying principles.

5. Effects of Phishing:

Business email compromise (BEC) attacks represent nearly half the total losses in 2018. The IC3 report revealed that BEC attacks cost US businesses more than $1.2 billion in 2018, doubling losses reported in 2017 and tripling that of 2016.



One of the most-costly forms of spear phishing, BEC attacks hit more than 20,000 victims in 2018. In this scam, a cybercriminal impersonates an

executive and requests an employee to execute a wire transfer, often to the tune of millions. Because of the high payoff, cybercriminals often use pretexting, a form of social engineering, to improve their chances of success. First, the cybercriminal ensures that the victim has the authority to execute the wire transfer, then they make the request. Often, they will exchange multiple emails with the victim to gain their trust.

In a recent example, St. Ambrose Catholic Parish in Brunswick, OH was scammed out of $1.75 million in a BEC attack. While the church was undergoing renovations, hackers managed to compromise internal Office 365 email accounts. Once inside, they convinced other employees that the construction company doing renovations on the church needed to change their bank account information. When the church paid the construction company two bills totaling $1.75 million, the funds went into the hacker's account. The church did not become aware of the compromise until the construction company reached out and asked why the recent bills had not been paid.

6. Anti-Phishing:

The following countermeasures to phishing include undergoing training, knowing legal concepts, implementing security control measures and building awareness through better security practices. These practices improve enterprise architecture and make it suited to resisting attacks.

- Secured Login:

  The first and foremost security step should be the use of an HTTPS site rather than an HTTP one. Whenever you login from an HTTP page, there is no guarantee that your login credentials are sent in an encrypted format onto the main page. Further, two-way authentication or certificate-based login is a must for significant logins. This is a combination of a traditional username and password along with a code sent to you on your phone.

- Implementing organization policies and procedures:
  Every firm should periodically update their policies, procedures and processes to protect its users' confidential data. That is the reason IT departments continuously put pressure on you for backups, restorations, and monthly password changes.

- Reporting:
  Reporting suspicious activity noticed in email accounts is a must for employees. They must stay alert for suspicious emails, links or attachments to maintain your security.

- Digital Signature of confident emails:
  Adding a digital layer of security makes sure that scammers are not able to alter your content. This can be done using “sending policy frameworks”. A sending policy framework is a security measure used to block forged emails. Companies using SPF policies allow mail exchangers to check if the incoming emails are from an authorized host approved by domain administrators.

- Software Updates:

  You must keep your PCs updated by installing the latest firewalls in order to prevent email spam.

- Countering Man in the Middle attacks:
  In this type of attack, phishers collect short-lived single-use passwords called user-id passwords and attack organizations. The software can detect if there are many connections from one PC to your organization’s site as this is indicative of a man in the middle attack.
  As stated at the beginning of this article, it is essential to know various types of phishing methods used by phishers and understand how to combat phishing attacks.

- Handling of spam email:
  You can configure your Anti-phishing solution to take one of several actions when faced with an email phishing attack such as permanently deleting such emails, bouncing back to the sender, storing in a dedicated folder or junk box, forwarding the email to your cybersecurity head along with relevant tags or X-headers.

7. Defend Against Phishing Attacks:

- PREVENTING A PHISHING ATTACK BEFORE IT BEGINS:

A Phisher must set up a domain to receive phishing data. Pre-emptive domain registration may reduce the availability of deceptively named domains. Additionally, proposal have been made to institute a "holding period" for new domain registration during which trademark holders could object to a new registration before it was granted. This might help with the problem of deceptively named domains, but would not address the ability of phishers to impersonate sites. As email authentication technologies become more widespread, email authentication could become a valuable preventive measure by preventing forged or misleading email return addresses. Some services attempt to search the web and identify new phishing sites before they go "live," but phishing sites may not be accessible to search spiders, and do not need to be up for long, as most of the revenues are gained in the earliest

- DETECTING A PHISHING ATTACK:

Many different technologies may be employed to detect a phishing attack, including:

- Providing a spoof reporting E-mail address that customers may send spoof emails to. This may both provide feedback to customers on whether communications are legitimate, and provide warning that an attack is underway.
- Monitoring "bounced" email messages. Many Phishers email bulk lists that include nonexistent email addresses, using return addresses belonging to the targeted institution.
- Establishing "honeypots" and monitoring for email purporting to be from the institution.

There are contractors that will perform many of these services. Knowing when an attack is underway can be valuable, in that it may permit a targeted institution to institute procedural countermeasures, initiate an investigation with law enforcement, and staff up for the attack in a timely manner.

- PREVENTING THE DELIVERY OF PHISHING MESSAGES:

Once a phishing attack is underway, the first opportunity to prevent a phishing attack is to prevent a phishing message from ever reaching a user.

- Filtering:

Email filters intended to combat spam are often effective in combating phishing as well. Signature-based anti-spam filters may be configured to identify specific known phishing messages and prevent them from reaching a user. Statistical or heuristic anti-spam filters may be partially effective against phishing, but to the extent that a phishing message resembles a legitimate message, there is a

danger of erroneously blocking legitimate email if the filter is configured to be sufficiently sensitive to identify phishing email. Phishers depend on being able to make their messages visually appear to be

from a trusted sender. One possible countermeasure is to detect unauthorized imagery in emails. There are many countermeasures that Phishers may employ against a simple image comparison, including displaying many tiled smaller images as a single larger image, and stacking up transparent images to create a composite image. This means that imagery should be fully rendered before analysis. An area of future research is how to recognize potentially modified trademarks or other registered imagery within a larger image such as a fully rendered email. A similar approach may be fruitful when applied to web sites, when a user has clicked on a link.

- Authentication:

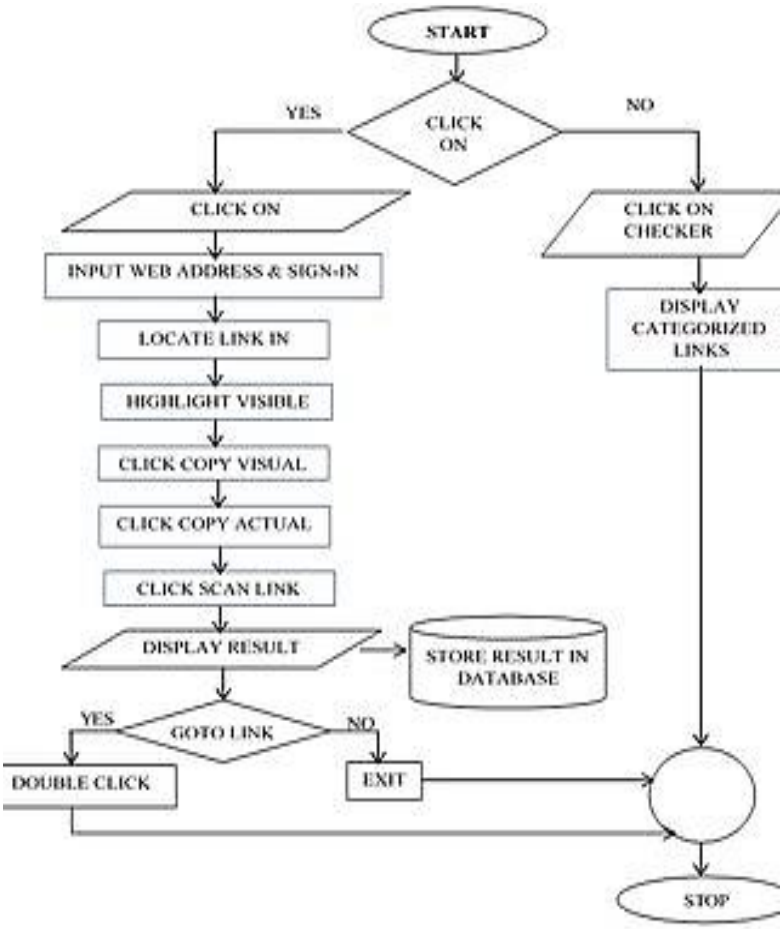
Message authentication techniques such as Sender-ID have considerable promise for anti-phishing applications. Sender-ID prevents return address forgery by checking DNS records to determine whether the IP address of a transmitting mail transfer agent is authorized to send a message from the sender's domain. Yahoo! Domain Keys provides similar authentication, using a domain-level cryptographic signature that can be verified through DNS records. Some form of lightweight message authentication may be very

valuable in the future in combating phishing. For the potential value to be realized, Sender-ID or a similar technology must become sufficiently widespread that invalid messages can be summarily deleted or otherwise treated prejudicially, and security issues surrounding the use of mail forwarders need to be resolved.

8. Anti-Phishing Software:

Anti-phishing software consists of computer programs that attempt to identify phishing content contained in websites and e-mail. It is often integrated with web browsers and email clients as a toolbar that displays the real domain name for the website the viewer is visiting, in an attempt to prevent fraudulent websites from masquerading as other legitimate web sites. Anti-phishing functionality may also be included as a built-in capability of some web browsers

Common phishing tactics take advantage of a visitor by requesting them to link out to another site, asking that the enter personal information and passwords, or redirecting them to another site completely for registration. The process usually begins by sending out a forged e-mail that looks like it was sent from the company. Some tactics include saying an account has expired and needs to be updated, or has experienced unauthorized use and needs to be verified. Many banking and financial institutions become targets for these types of scams, and they can be a considerable threat to millions of account holders and users.



Many leading web browsers and software programs have realized the impact of this trend, and have created programs that can limit the frequency of these types of scams.

Micirosoft Windows Internet Explorer 7, Firefox 2.0, Google Safe Browsing, and Earthlink ScamBlocker are just a few programs that have reduced the risks involved.

In Firefox 2.0, Phishing Protection is always turned on and checks the sites automatically for any potential risks or hazards. The list is reviewed on a regular basis, and can be configured to Firefox Security settings for maximum control. When Phishing Protection in enabled, the sites are downloaded into a list and checked for any anti-phishing services. A warning sign will appear if any suspicious activity is detected. The Netcraft toolbar makes use of a risk rating system, allowing you the option of entering a password (or not). TrustWatch makes the Internet Explorer toolbar, and can help validate a Web site and provide a site report when needed. This option also allows you to review all suspected sites and find out which ones use SSL technology. Earthlink Toolbar with ScamBlocker will verify any popup messages that you may encounter as you visit a site, and can help you find out all the details on current phishing scams.

Anti-phishing software is designed to track websites and monitor activity; any suspicious behavior can be automatically reported, and even reviewed as a report after a period of time. Anti-phishing toolbars can help protect your privacy and reduce the risk of landing at a false or insecure URL. Although some people have concerns over how valuable anti-phishing software and toolbars may be, security threats can be reduced considerably when they are managed by the browser program. Other companies that are trained in computer security are investigating other ways to report phishing issues; programs are being designed that can analyze web addresses for fraudulent behavior through new tactics, and cross-checking domain names for validity.

9. Conclusion:

No single technology will completely stop phishing. However, a combination of good organization and practice, proper application of current technologies, and improvements in security technology has the potential to drastically reduce the prevalence of phishing and the losses suffered from it. In particular:

- High-value targets should follow best practices and keep in touch with continuing evolution of them.
- Phishing attacks can be detected rapidly through a combination of customer reportage, bounce monitoring, image use monitoring, honeypots and other techniques.
- Email authentication technologies such as Sender-ID and cryptographic signing, when widely deployed, have the potential to prevent phishing emails from reaching users.
- Analysis of imagery is a promising area of future research to identify phishing emails.
- Personally identifiable information should be included in all email communications. Systems allowing the user to enter or select customized text and/or imagery are particularly promising.
- Browser security upgrades, such as distinctive display of potentially deceptive content and providing a warning when a potentially unsafe link is selected, could substantially reduce the efficacy of phishing attacks.
- Information sharing between the components involved in a phishing attack – spam filters, email clients and browsers – could improve identification of phishing messages and sites, and restrict risky behaviour with suspicious content.
- Anti-phishing toolbars are promising tools for identifying phishing sites and heightening security when a potential phishing site is detected.
- Detection of outgoing confidential information, including password hashing, is a promising area of future work, with some technical challenges.
- An OS-level trusted path for secure data entry and transmission has the potential to dramatically reduce leakage of confidential data to unauthorized parties.
- Two-factor authentication is highly effective against phishing, and is recommended in situations in which a small number of users are involved with a high-value target. Device identifier based two-factor authentication offers the potential for cost savings.
- Cross-site scripting is a major vulnerability. All user content should be filtered using a let-in filter. Browser security enhancements could decrease the likelihood of cross-site scripting attacks.

10. References:

- www.Google.com
- www.Wikipedia.com
- www.Studymafia.org
- www.Geeksforgeeks.org