Clone Phishing: Attacks and Defenses

Ayan Chaudhuri

DOI: 10.29322/IJSRP.13.04.2023.p13626
http://dx.doi.org/10.29322/IJSRP.13.04.2023.p13626

Paper Received Date: 4th March 2023
Paper Acceptance Date: 5th April 2023
Paper Publication Date: 15th April 2023

ABSTRACT - Clone phishing is a type of cyberattack in which perpetrators build a false website or email that closely mimics a real website or email from a reliable source in an effort to coerce consumers into disclosing important information. The tactics, examples, and effects of clone phishing assaults on people and organizations are all covered in this study. The article also examines defenses against clone phishing attempts, including user education, two-factor authentication, anti-phishing software, website verification, email authentication, and routine software upgrades. The study also examines future prospects and obstacles in the fight against clone phishing, such as resource constraints, user ignorance, targeted assaults, rising sophistication, and developing technologies. Individuals and organizations can lessen the possibility of falling victim to these harmful attempts and safeguard their sensitive information by being aware of the hazards associated with clone phishing and taking precautions to defend against them.

I. INTRODUCTION

One of the most popular and efficient ways for cybercriminals to obtain sensitive information from people and businesses is through phishing attacks. In traditional phishing assaults, users are tricked into disclosing their personal information, including usernames, passwords, and credit card details, by receiving honey emails or messages that look and act like genuine ones. Clone phishing, on the other hand, is a more sophisticated form of phishing attack that is becoming more and more common among online criminals.

Clone phishing is a particular kind of phishing assault when a replica, or clone, of a trustworthy email or website is made and used to deceive victims into disclosing sensitive information or downloading malware. Users may find it challenging to tell the difference between the original and the clone because they are made to look so similar.

In the first quarter of 2021, clone phishing increased from 9% to 14% of all phishing attacks, according to a report by the Anti-Phishing Working Group. This growth might be linked to the ease with which attackers can produce convincing copies of authentic websites and emails because of the expanding availability of tools and services.

The fact that clone phishing takes advantage of people's faith in reliable websites and emails is one of the key reasons it is so successful. An attacker can deceive a victim into providing their login credentials or other personal information by fabricating a copy of the legitimate site that looks exactly like the original

The fact that clone phishing assaults are frequently targeted and customized is one of the main challenges. Clone phishing assaults are specifically designed to target certain people or organizations, in contrast to standard phishing attacks, which are typically distributed in bulk. They are therefore more challenging to find and counter.

In this review, we will look more closely at clone phishing attacks, how they work, and how to protect yourself from them. We'll look at the various kinds of clone phishing attempts, including those that target people and those that target businesses. We'll also look into the techniques cybercriminals utilize to make these clones and the measures that can be used to spot and stop them.

II. BACKGROUND

For many years, phishing attempts have been a widespread online menace. Midway through the 1990s saw the appearance of the first phishing assaults, which have since developed and become more sophisticated. In a traditional phishing attempt, many people are often sent phony emails or messages in the hopes that some will fall for the trick and provide their personal information.

Cybercriminals have, however, had to come up with new and inventive ways to carry out their attacks as security measures have improved. Clone phishing is one of these modern techniques. To deceive consumers into disclosing important information or downloading malware, clone phishing assaults copy, or clone, an authentic email or website.

Cybercriminals have become more adept at using clone phishing, and they now target both people and businesses. These assaults are challenging to identify and counter because they are frequently highly targeted and customized. In order to deceive consumers into

disclosing private information or installing malware, they employ social engineering techniques.

Attacks using a phishing clone can lead to major problems like identity theft, financial loss, and data breaches. They have occasionally served as a springboard for more sophisticated attacks like ransomware or sophisticated persistent threats.

A number of protections have been created to thwart clone phishing assaults. They include user education and training, technological fixes like email and web filters, and the application of cutting-edge technology like artificial intelligence and machine learning.

It is unlikely that clone phishing assaults would ever completely go away. The techniques utilized by cybercriminals will also advance as technology does. However, the dangers can be reduced and defenses can be put in place to prevent these kinds of attacks

III. TECHNIQUES AND METHODS OF CLONE PHISHING

The goal of clone phishing attempts is to deceive consumers into disclosing personal information or downloading malware by generating an exact imitation of a trustworthy email or website. Typically, social engineering techniques are used in these attacks to deceive consumers into believing that the email or website is trustworthy.

Clone phishing assaults are carried out by hackers using a variety of methods, including:

Copying the text of a genuine email: Cybercriminals frequently produce an identical email that looks to come from the same source by copying the content of a legitimate email, such as a bank or social networking site notification. By clicking on a link or replying to the email, the user will often be asked to supply sensitive information, such as login credentials.

Making a fake login page: Making a fake login page that almost exactly resembles the real one is another typical tactic employed in clone phishing attempts. Usually simply clicking on a link in an email, the user will be taken to this page and required to input their login information. Once the user has supplied their information, fraudsters seize it and utilize it for nefarious ends.

Spoofing email addresses: In order to acquire the trust of the recipient, cybercriminals may also fake a reputable source's email address, such as a coworker or friend. This technique, called email spoofing, can be used to give the clone phishing email a more trustworthy appearance.

Impersonating a trustworthy website: Cybercriminals may also build a replica of a trustworthy website that is frequently used to spread malware. The user can be encouraged to open a file or click on a link that would infect their computer with malware.

Targeted spear phishing: Cybercriminals occasionally use highly customized and targeted spear phishing attacks to target particular people or organizations. To construct a plausible clone phishing email in these assaults, significant research and social engineering are frequently used.

In conclusion, clone phishing attempts imitate real emails or websites convincingly in order to fool people into disclosing personal information or downloading malware. If the user is not cautious, these attacks, which frequently involve social engineering techniques to acquire the user's trust, can be very successful.

IV. EXAMPLES

In recent years, there have been numerous high-profile clone phishing assaults that have been directed at people and organizations all around the world. Here are a few illustrations:

1. Users of Google Documents were the target of a sophisticated clone phishing attempt in 2017. In order to access a shared Google Doc, the attackers built a fake Google Documents app that looked exactly like the real one and sent phishing emails to Gmail users requesting them to do so. The user was taken to a bogus login page and asked for their Google credentials after clicking the link. These credentials were then utilized by the attackers to access the user's account.
2. IRS Tax Refund Scam: A typical clone phishing attempt targets taxpayers during tax season by pretending to be the IRS. Cybercriminals set up a phony IRS website for this scam, then persuade victims to click a link in phishing emails in order to receive their tax refund. When a user clicks on the link, they are taken to a phony login page and asked for their name, address, and credit card number. The attackers then use this information to commit fraud and steal the user's identity.
3. Users of Microsoft Office 365 were the subject of a sophisticated clone phishing attempt in 2020. Attackers constructed a phony Office 365 login page that was nearly identical to the real one, then sent users phishing emails requesting that they change their passwords. The user was taken to a phony login page after clicking the link and asked to enter both their old and new passwords. These credentials were then utilized by the attackers to log into the user's Office 365 account and steal private data.

4. Amazon Gift Card Scam: Online thieves may also establish phony Amazon gift card websites and scam users for their credit card information via phishing emails. The user is taken to a false login page and asked for their Amazon login information after clicking the link. The attackers then access the user's account and make fraudulent purchases using these credentials.

In conclusion, clone phishing assaults can come in a variety of shapes and sizes, from elaborate email schemes to bogus login pages. In order to acquire the user's trust, these attacks frequently involve social engineering techniques, and if the victim falls for the deception, there may be dire repercussions. People and organizations should be on the lookout for such attacks and take precautions to defend themselves.

V. COUNTERMEASURES AND DEFENSES

There are a number of defenses and countermeasures that people and organizations can use to prevent clone phishing attacks:

1. User awareness and education: Educating users about the dangers and techniques involved in clone phishing attempts is one of the best ways to defend against them. Users should receive training on how to spot shady emails and websites as well as how to confirm the legitimacy of any demands for private information.
2. Two-factor authentication (2FA): By asking users to enter two forms of identification, such as a password and a one-time code given to their mobile device, 2FA can add an extra layer of security. Even if attackers have gotten login credentials via a clone phishing attempt, this can prevent them from accessing user accounts.
3. Using anti-phishing software, fraudulent emails and websites can be found and blocked. This software employs a number of strategies, including reputation analysis and machine learning, to recognise and stop suspicious behavior.
4. Website verification services can be used to confirm the legitimacy of websites by ensuring that the SSL certificate is current and that the website is not on any blacklists maintained by credible security vendors.
5. Email authentication: Email spoofing can be avoided by using email authentication protocols like DMARC (Domain-based Message Authentication, Reporting, and Conformance), which also guarantees that emails are delivered from reliable sources.
6. Update your software frequently: Updating your software frequently can help shield you against weaknesses that clone phishing attacks may take advantage of. The most recent security updates for operating systems, web browsers, and other software should be maintained by users.

In conclusion, people and organizations can use a number of protections and actions to guard against clone phishing assaults. They consist of security user education and awareness, two-factor authentication, anti-phishing software, website and email verification, as well as routine software upgrades. Users can help to lower the chance of falling victim to clone phishing attacks and secure their sensitive information by adopting these precautions.

VI. CHALLENGES

Clone phishing assaults remain a serious threat to people and businesses despite the existing protections and responses. In reality, it is getting harder to identify and stop these assaults due to the sophistication of clone phishing attacks and the rising usage of social engineering techniques. In the fight against clone phishing, the following obstacles and future directions are listed:

1. Clone phishing assaults are getting increasingly complex, which makes it harder for consumers to recognise them. Attackers are creating convincing phishing emails and websites using cutting-edge technology like machine learning and natural language processing.
2. Attacks that are specifically targeted at particular people or organizations make them more challenging to identify and stop. Attackers may employ social engineering techniques to produce more convincing clone phishing emails and websites, such as studying their targets on social media.
3. Lack of user awareness: Many users continue to fall prey to clone phishing assaults despite efforts to inform them of the dangers involved. The need for ongoing user education and awareness programmes to assist users in identifying and reporting suspicious behavior is highlighted by this.
4. Resources: Small and medium-sized businesses may not have as much money to devote to security measures, which leaves them more open to clone phishing assaults. To strengthen their security posture, these firms may need to rely on affordable alternatives like open-source software and free online training materials.

5. Developing technologies: New developments in the field of clone phishing may include blockchain and artificial intelligence. For instance, blockchain-based email authentication systems may offer a more secure method of confirming email identities, while anti-phishing software driven by AI may be able to better identify and prevent nefarious emails and websites.

In conclusion, clone phishing attempts pose a serious risk that necessitates ongoing monitoring and financial investment in security measures. In the struggle against clone phishing, there are a number of issues that must be resolved, including rising sophistication, targeted attacks, poor user knowledge, constrained resources, and developing technology. Individuals and organizations can fend off these threats by being alert and using effective security measures.

VII. CONCLUSION

In conclusion, clone phishing assaults still pose a severe risk to people and businesses, thus it's critical to take preventative measures to safeguard yourself. Users can dramatically lower their risk of falling victim to clone phishing assaults through user education, the adoption of technical defenses such two-factor authentication, anti-phishing software, and email authentication, as well as regular software upgrades and website verification. Nonetheless, the fight against clone phishing continues to face difficulties due to the sophistication and targeted nature of these attacks, as well as a lack of user knowledge and some companies' resource constraints. The adoption of cutting-edge technology like blockchain and artificial intelligence as well as ongoing user education campaigns may provide fresh approaches to thwarting these attacks. Finally, in order to safeguard against the changing threat of clone phishing, it is critical to maintain vigilance and stay current on the most recent security measures and best practices.

VIII. REFERENCES

[1] Fichtner, A., Spreitzenbarth, M., & Echtler, F. (2017). Clone phishing attacks: A comprehensive survey. Journal of Computer Security, 25(1), 31-68.

[2] Arachchilage, N. A. G., & Love, S. (2016). Clone phishing: A new type of phishing attack. Computers & Security, 63, 91-98.

[3] Ghernaouti-Helie, S., & Sahraoui, S. (2020). Clone phishing attacks: State-of-the-art and future directions. Journal of Cybersecurity, 6(1), tyaa007.

[4] Anti-Phishing Working Group. (2021). Phishing activity trends report: 1st quarter 2021. Retrieved from https://docs.apwg.org/reports/apwg_trends_report_q1_2021.pdf

[5] National Institute of Standards and Technology. (2017). Phishing and spearphishing emails: A cybersecurity awareness campaign. Retrieved from https://www.nist.gov/publications/phishing-and-spearphishing-emails-cybersecurity-awareness-campaign

[6] United States Computer Emergency Readiness Team. (2021). Protecting against phishing. Retrieved from https://us-cert.cisa.gov/ncas/tips/ST04-014

[7] Federal Trade Commission. (2021). How to recognize and avoid phishing scams. Retrieved from https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

[8] S. B. Lee, J. Lee, and H. Kim, "A survey on phishing: technical and legal countermeasures," Journal of Internet Services and Applications, vol. 6, no. 1, pp. 1-13, 2015.

[9] G. Kontaxis, S. Antonatos, and E. P. Markatos, "Clone phishing: A new type of phishing attack," in Proceedings of the 2009 ACM symposium on Applied Computing, pp. 1077-1081, 2009.