Pedagogía y Sociedad
UNIVERSIDAD DE SANCTI SPÍRITUS
José Martí Pérez
ISSN: 1608-3784
RNPS: 1903

Recibido: 13/10/2023, Aceptado: 22/12/2023, Publicado: 10/1/2024
Volumen 27│ Número 69│ Enero-Abril, 2024│

[Translated article]

A phishing process and guidelines for identifying fake websites

Proceso de phishing y pautas para la identificación de sitios web falsos

Cristian Camilo Barrantes Bernal[1]

E-mail: ccamilobarrantes@ucundinamarca.edu.co

https://orcid.org/0009-0003-1515-9313

Snattan Andrey Espitia Velásquez[1]

E-mail: saespitia@ucundinamarca.edu.co

https://orcid.org/0009-0000-8592-4998

[1]Universidad de Cundinamarca. Cundinamarca, Colombia.

How to cite this article (APA, Seventh Edition)

Barrantes Bernal, C. C. y Espitia Velásquez, S. A. (2024). Proceso de phishing y pautas para la identificación de sitios web falsos. *Pedagogía y Sociedad, 27* (69), 46-66. https://revistas.uniss.edu.cu/index.php/pedagogia-y-sociedad/article/view/1745

ABSTRACT

Introduction: Phishing is a form of cyber-attack that relies on social engineering and remains a latent threat in the digital world. In this article, a phishing process is explored in a local environment, focusing on the creation of a fake website, where the importance of training in mitigating this risk is highlighted.

Objective: To analyze the process of phishing on the Internet by cloning a website in a controlled environment and generating guidelines for the identification of fake websites.

Methods: The research is explanatory and laboratory-based.

Results: Key guidelines for identifying fake websites are provided, including: verifying the source of the communication, avoiding clicking on suspicious links, and using two-factor authentication. This was done taking into account the different parts of phishing in a local environment.

Conclusion: The importance of training, constant education and awareness of phishing and its techniques to detect it, in an ever-changing digital world, are the key tools in protecting confidential information and mitigating phishing.

Keywords: computer science; computer security; cybernetics; data protection; social engineering

RESUMEN

Introducción: El phishing es una forma de ataque cibernético que se basa en la ingeniería social, que sigue siendo una amenaza latente en el mundo digital. En este artículo, se explora un proceso de phishing en un entorno local, centrados en la creación de un sitio web falso, donde se destaca la importancia de la capacitación en la mitigación de este riesgo.

Objetivo: Analizar el proceso de phishing en internet mediante la clonación de un sitio web en un ambiente controlado y la generación de pautas para la identificación de sitios web falsos.

Métodos: La investigación es de tipo explicativa y de laboratorio.

Resultados: Se ofrecen pautas fundamentales para identificar sitios web falsos, que incluyen: verificar la fuente de la comunicación, evitar hacer clic en enlaces sospechosos y utilizar la autenticación de dos factores. Esto se realizó teniendo en cuenta las diferentes partes del phishing en un entorno local.

Conclusiones: La importancia de la capacitación, la educación constante y la toma de conciencia sobre el phishing y sus técnicas para detectarlo, en un mundo digital en constante cambio, son las herramientas clave en la protección de la información confidencial y mitigación del phishing.

Palabras clave: cibernética; informática; ingeniería social; protección de datos; seguridad informática

Introduction

The Internet is one of the main technological pillars on which contemporary society has been built, becoming synonymous with communication, which has allowed access to a wealth of knowledge at the click of a button. It is used to access banks, make purchases, download applications and this, without checking its origin; then, accept terms and conditions without reading the permissions that are negligently granted, without giving it the importance that unquestionably represent personal data. Unfortunately, its accelerated evolution is a latent problem in the field of computer security.

One of the greatest dangers on the Internet is phishing, it is presented in the form of impersonation of web pages with the purpose of stealing information to obtain some economic benefit. According to the Internet Crime Report provided by the Federal Bureau of Investigation (Internet Crime Report, 2021), phishing is one of the crimes reported with the greatest loss for victims in 2021. The use of this type of fraud has been diversifying over the years, which implies a growth in the volume of attacks and the complexity of the techniques used by cybercriminals. According to the National Cybersecurity Institute, employees are a key element in preventing this type of fraud because they are the ones who have access to and control over the company's tools, which makes them the target of cybercriminals. One of the biggest challenges when it comes to mitigating phishing has to do with the human factor, since the effectiveness of this type of fraud depends to a greater extent on user error, which is why awareness is essential for prevention.

This research aims to analyze the process of phishing on the Internet, through the cloning of a website in a controlled environment and the generation of guidelines for the identification of fake websites, in order to make Internet users aware of the security of their data.

Theoretical framework or conceptual references

Currently, computer security is a very important factor in protecting the privacy of any individual, since the information is stored in technological media, according to Baca Urbina in his book: *Introduction to computer security*, this could be defined as:

> Computer security is the discipline that, based on internal and external policies and standards of the company, is responsible for protecting the integrity and privacy of the information stored in a computer system, against any type of threat, minimizing both physical and logical risks, to which it is exposed. (2016, p. 12)

For this reason, it is important for both individuals and organizations to protect confidential information and data, as failure to do so exposes them to a variety of threats that can have significant personal and business consequences. Data has become the core of day-to-day operations, which implies an increase in the amount of sensitive information stored and processed, ranging from financial and personal data to trade secrets.

The advancement of technology increases exponentially and unfortunately computer security does not advance at the same speed, which leads systems to be in a constant state of vulnerability in one way or another. As time passes, information technologies become increasingly important in human life, which makes Internet users more susceptible to various virtual threats whose objective is the theft of confidential information. Among these threats is Phishing, defined by Belisario Mendez of the University of Buenos Aires as:

> Phishing is a type of social engineering attack that has existed for more than 20 years. It consists of deceiving the victim, through impersonation of trusted sources, so that he or she voluntarily provides sensitive information. (2014, p. i)

Despite being an old type of scam, phishing continues to be a threat that is increasing over the years. One could even say that it has improved to such an extent that it could be defined as a set of techniques used by cybercriminals, where the impersonation of a company is originated. The most recurrent means on which these types of fraudulent attacks are usually developed are email, social networks, SMS and phone calls.

Phishing attacks are by far the most common type of virtual threat, and their prevalence is due to their versatility. This type of fraud has become a widespread threat that can be combined with the use of malware or exploits that are introduced inside files that when executed infect the victim's device or execute a sequence of code to take advantage of system vulnerabilities.

One of the best known at present is ransomware, a type of malware that involves the encryption of information that prevents access to the owner of the device, in order to request a payment or ransom for the data (kidnapping of information). The use of keyloggers is also very common in phishing; this is a type of spyware that can record the keys pressed on a computer. On the other hand, there are exploits that by means of a sequence of commands can generate a reverse connection with the attackers so that they can take full control of the device through a port, which is why phishing has become a worldwide problem.

There are several recommendations to identify phishing, since the cybercriminals who apply this set of techniques follow similar patterns. In many cases the attackers send alarmist messages in order to scare the user and make them believe that they must solve a problem immediately by accessing links or attachments to the statement in question. It is also common that the body of the message contains grammatical or editorial errors since many of these attackers use translators to send the same message in several languages and thus extend the scope of their fraud. In the field of cybersecurity, if attackers want to breach a system, they must direct their efforts towards the weakest link. One of the reasons why phishing is so effective is because it exploits a human vulnerability. The use of social engineering, cloning of official pages and various techniques to make the URL as identical as possible to the spoofed page increases the complexity of detection.

According to the Internet Crime Report provided by the Federal Bureau of Investigation (Internet Crime Report, 2021) phishing implies that there is an inefficiency in its mitigation, despite the variety of techniques currently employed to eradicate the problem. It is not enough just to increase the efficiency of the techniques; there should also be training and awareness-rising for internet users, to strengthen the weakest link in the chain. According to the National Institute of Cybersecurity (INCIBE), employees are fundamental for the prevention of this type of fraud, since they are the ones used by cybercriminals to perpetrate their scams. Some of the phishing detection techniques most commonly used by organizations rely on list-based methods, heuristic methods, machine learning, text mining and natural language processing (Hernández Dominguez and Baluja García, 2021).

List-based methods consist of verifying a large number of databases where some websites are already classified as phishing. The problem with this method lies in the false positives, i.e. those pages that are classified as phishing without being so; and the false negatives that are phishing but are not classified as such. Heuristic methods use visual similarity techniques using optical character recognition. This type of detection is performed by taking the same lists mentioned above to make different comparisons and classify suspicious web pages, which is why it drags the same problems of the lists. Thanks to the advance in algorithms and creation of machine learning models, a series of classification techniques have been used to identify and classify phishing. The results of these algorithms are varied since they all use very different mathematical calculations that are more efficient according to the conditions of the problem to be solved. Among these algorithms we can have decision trees (DT), random forests (RF), naive Bayes (NB) and Bayesian networks, neural networks (NN) and deep learning (DL), finally text mining in conjunction with natural language processing, allows establishing relationships in the body of the text messages or emails, which can determine if it is a phishing attack.

For developing the methodology it is important to keep in mind the different laws and legal repercussions within the country of Colombia regarding the intervention of computer systems. On January 5, 2009, the Congress of the Republic of Colombia enacted Law 1273:

> By means of which the Penal Code is amended, a new protected legal right - called “Protection of information and data” - is created and systems that use information and communications technologies are fully preserved, among other provisions. (para.1)

Classified under Article 269A: Abusive access to a computer system, and Article 269C: Interception of computer data, which indicate the following:

> Article 269A: Abusive access to a computer system. Whoever, without authorization or outside of what has been agreed, accesses in whole or in part a computer system protected or not with a security measure, or remains within it against the will of whoever has the legitimate right to exclude it, shall incur a prison sentence of forty-eight (48) to ninety-six (96) months and a fine of 100 to 1,000 legal monthly minimum wages in force. (Law 1273, 2009).
>
> Article 269C: Interception of computer data. Whoever, without prior judicial order, intercepts computer data at its origin, destination or inside a computer system, or the electromagnetic emissions coming from a computer system that transports it, shall incur a prison sentence of thirty-six (36) to seventy-two (72) months (para. 4).

In order not to incur in crimes related to intrusion, in this laboratory all the equipment and devices used are property of the members involved in the creation of the article, therefore, there is direct authorization to access the devices.

Within the legal framework it should also be taken into account the hindering of the systems involved in the network typified in Article 269B: Illegitimate hindering of computer system or telecommunication network, of law 1273 of 2009 which states the following:

> Article 269B: Illegitimate obstruction of a computer system or telecommunications network. Whoever, without being authorized to do so, prevents or obstructs the normal operation of or access to a computer system, the computer data contained therein, or a telecommunications network, shall incur a prison sentence of forty-eight (48) to ninety-six (96) months and a fine of 100 to 1000 legal monthly minimum wages in force, provided that the conduct does not constitute a crime punishable by a higher penalty. (para. 3)

In this case, the development of the laboratory will be carried out completely in a private network to avoid inconveniences at the time of intervening communications for which one does not have permissions.

Finally, the articles in charge of the typification regarding the use of malicious software and impersonation of websites are Article 269E: Use of malicious software, and Article 269G: Impersonation of websites to capture personal data, of the law 1273 of 2009 which indicate the following:

> Article 269E: Use of malicious software. Whoever, without being authorized to do so, produces, traffics, acquires, distributes, sells, sends, introduces or removes from the national territory malicious software or other computer programs with harmful effects, shall incur a prison sentence of forty-eight (48) to ninety-six (96) months and a fine of 100 to 1,000 legal monthly minimum wages in force. (para. 6)
>
> Article 269G: Impersonation of websites to capture personal data. Whoever with an illicit purpose and without being authorized to do so, designs, develops, traffics, sells, executes, programs or sends electronic pages, links or pop-up windows, shall incur a prison sentence of forty-eight (48) to ninety-six (96) months and a fine of 100 to 1,000 legal monthly minimum wages in force, provided that the conduct does not constitute a crime punishable by a more severe penalty. (para. 8)

For this reason, the process performed within the methodology of the article cannot show code that could be considered malware, nor can the detailed laboratory procedure and steps involving the violation of the laws mentioned within this legal framework be disseminated.

Methodology

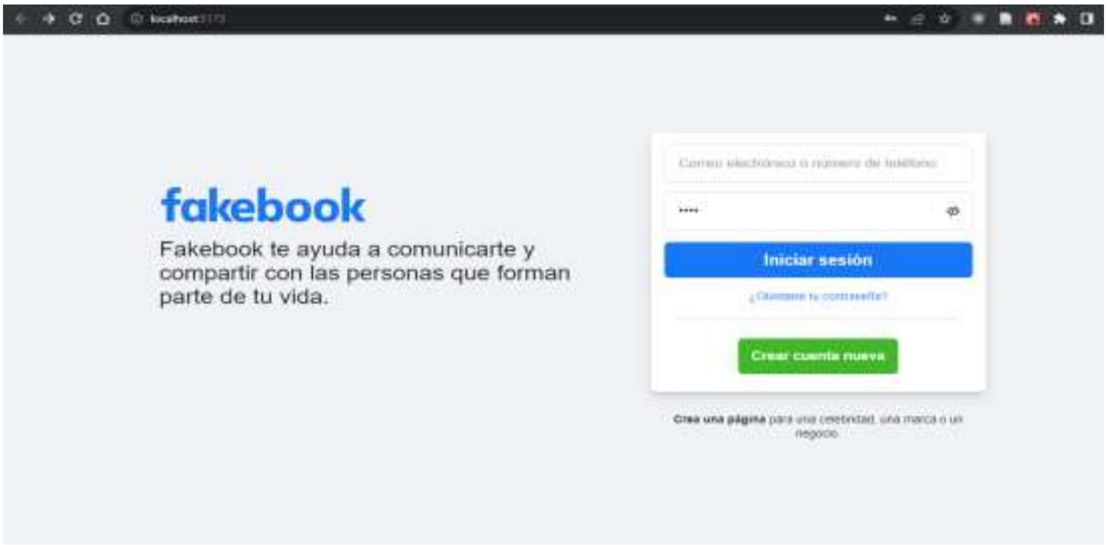
The following research is of an explanatory and laboratory type. It consists of the development of a controlled phishing environment where the position of victim and attacker was adopted, in order to show how cybercriminals obtain the credentials of the personal accounts of their victims through the impersonation of official websites, taking advantage of the disbelief and ignorance of Internet users, this being one of the most influential factors in the efficiency and profitability of this type of crime. The objective of the research was to provide the user with the necessary guidelines to identify an attack of this type as the phishing process developed in order to generate awareness in the reader.

In the process the following stages will be considered: creation of a fake website, identification of the type of attack, determining the phishing techniques for the laboratory and finally generating the deployment of the attack.

First stage:

Due to its simplicity, in this experimental case the Facebook login was used It should be noted, that not all pages require the same amount of work. The code can be created manually from scratch or generated using cloning tools; both options with their pros and cons. Cloning provides access to a template more quickly, but due to the length of the code, modification can be more difficult and complex; on the other hand, creating a template manually provides greater control but requires extensive periods of time and extensive knowledge in software development.

Figure 1: *Fake website*



fakebook

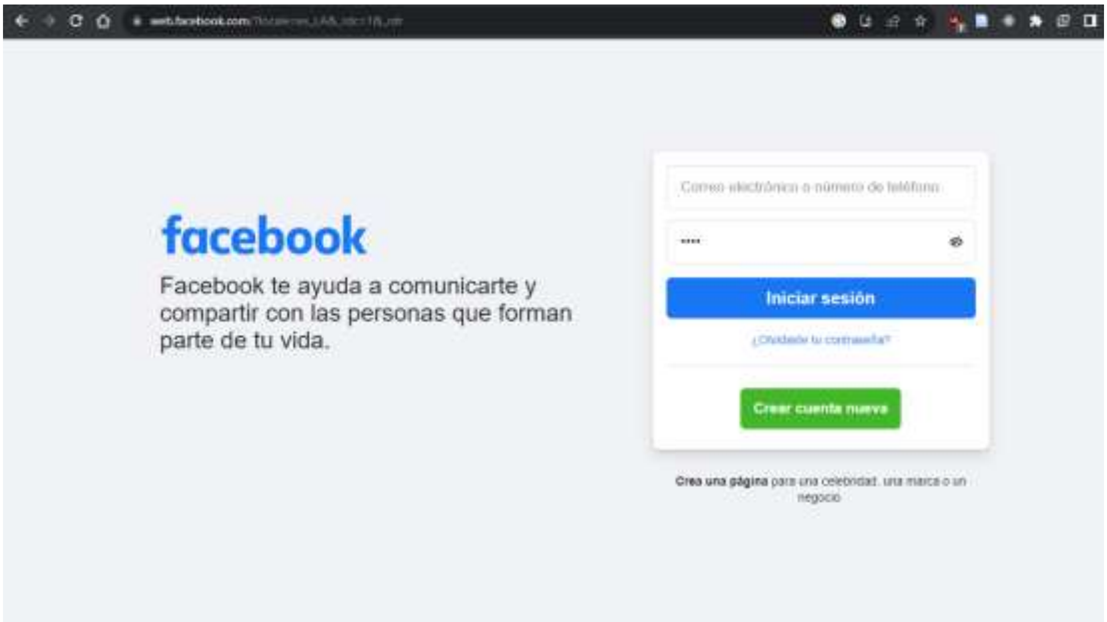
Fakebook te ayuda a comunicarte y compartir con las personas que forman parte de tu vida.

Correo electrónico o número de teléfono

••••

Crea una página para una celebridad, una marca o un negocio.

Figure 2: Original website



web.facebook.com

facebook

Facebook te ayuda a comunicarte y compartir con las personas que forman parte de tu vida.

Correo electrónico o número de teléfono

••••

Crea una página para una celebridad, una marca o un negocio

Second Stage:

In this stage the type of attack that could be launched was evaluated given that the target can be specific or generalized. Phishing is characterized as a set of versatile techniques, which can be integrated to obtain a more robust and sophisticated attack. In the case of this laboratory, a specific attack was performed taking into account the different techniques that could be more appropriate.

In a generalized attack, social engineering is often used and the bait is usually deployed through a message that can be received by email or text message; it is also common for the subject of the message to be alarmist or urgent, asking victims to click on links leading to the fake website URL.

In a specific attack, the target or victim is someone in particular, because of this it is common to use certain techniques such as man in the middle (MITM), DNS cache poisoning (DNS Spoofing), use of spyware such as keyloggers or malware of various types that allow monitoring and / or send information directly to the attacker.

Figure 3: *MITM Schematic*

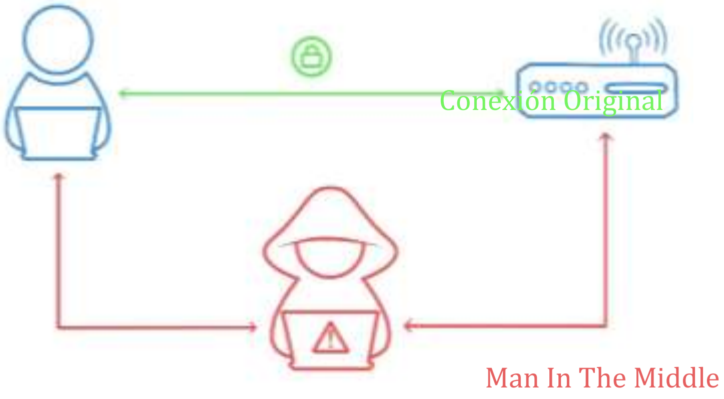


Figure 4: *DNS Spoofing Schematic*

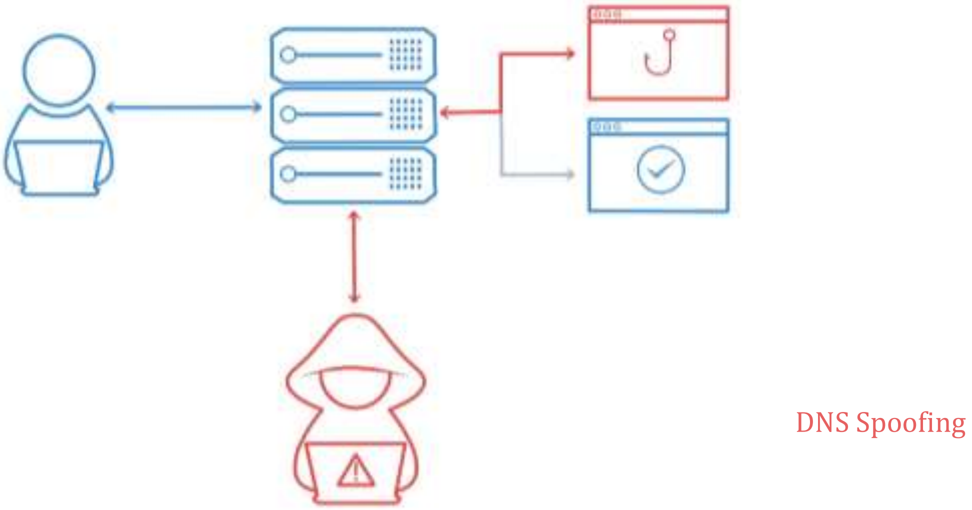
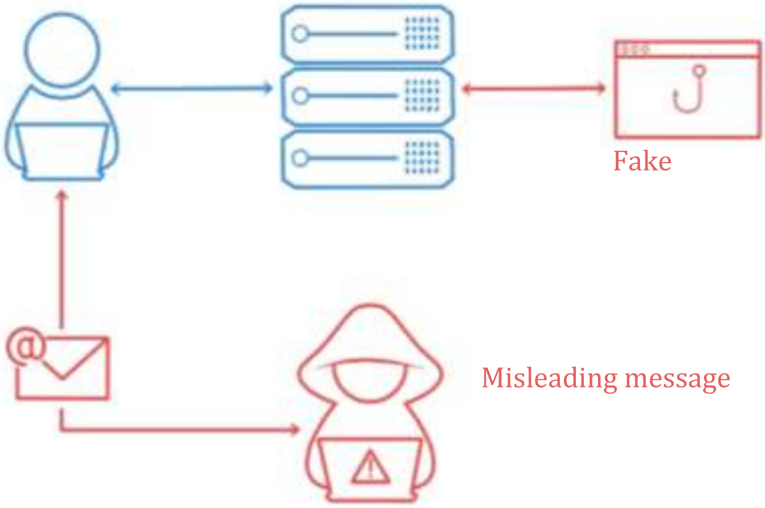


Figure 5: *Spoofing message scheme*



Third stage:

For this stage, man in the middle (MITM) and DNS cache poisoning (DNS Spoofing) techniques will be used because the type of attack defined in the previous stage was targeted or specific.

DNS Spoofing

DNS SPOOFING consists of redirecting a user who is the victim of this attack to a fake website that is not the one they want to access, but has the same domain name as the site the user wants to visit. There are two variants of this attack:

Cache poisoning: It is based on modifying the information contained in a domain server, i.e. the attacker redirects the requests made by a user to a domain, let us call it “X”, to a different domain “Y” to create a kind of smokescreen where the user provides the requests to the attacker on the real website “X” but they arrive at the fake site “Y”.

For this, attackers must be connected to the victim user's server and network where they will have access to review all the packets and requests that the user makes in a domain, thus creating a false DNS record on the server with which they will divert the IP address to a fake domain. Then the attacker sends a request to the real domain so that the victim user provides sensitive data and these records reach the fake DNS and are saved in the cache (Pastor Iglesias, 2022).

ID Spoofing: This alternative is basically making the victim user believe that the attacker's machine is a DNS server capturing the UDP (User datagram protocol) ID which “is a transaction-oriented protocol, and delivery and protection against duplicates are not guaranteed” (Pastor Iglesias, 2022, p. 8).

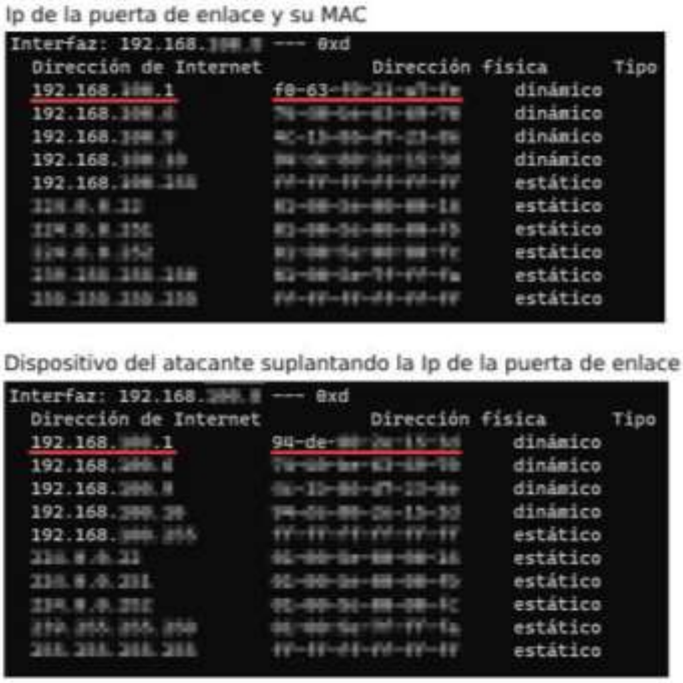
This is one of the Internet protocols that allow sending information without the need to have a receiver or wait for a response, making it one of the fastest protocols and without delays.

ID Spoofing directly connects the victim user to the fake domain and makes them believe that they are connected to the real domain they are trying to access.

Man in the middle

MITM: Refers to Man In the Middle, which refers to a cyberattack in which the attacker stands between two parties trying to communicate in order to intercept their messages or data. The main targets of these attacks are to obtain banking data or login credentials, for example, as this is how they can get the most profit. Being real-time, these attacks often go unnoticed until it is too late (Martínez Pérez, 2022).

Figure 6: *MITM*



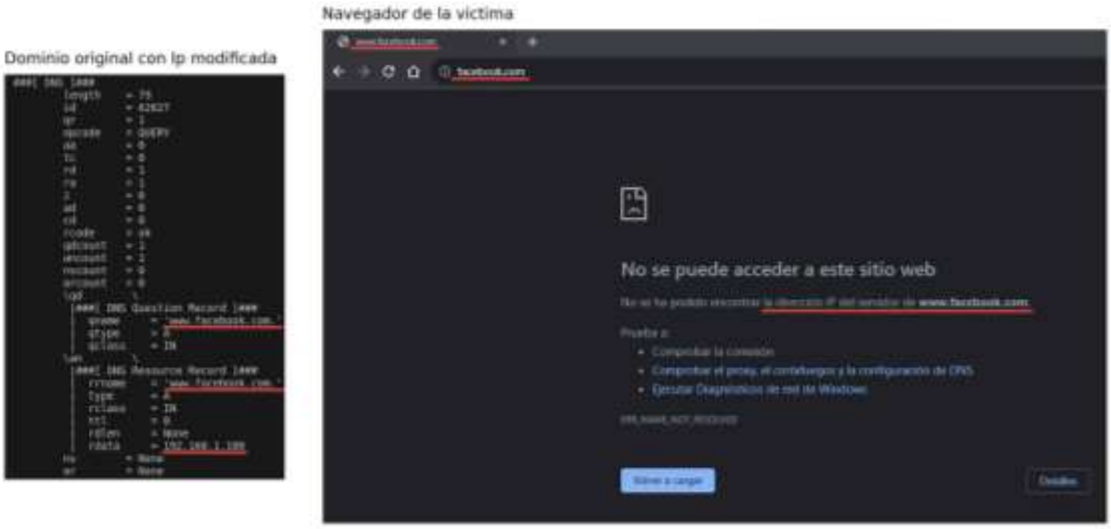
Ip de la puerta de enlace y su MAC

```
Interfaz: 192.168.[redacted] --- 0xd
  Dirección de Internet          Dirección física      Tipo
  192.168.[redacted].1           f0-63-[redacted]      dinámico
  192.168.[redacted]             [redacted]            dinámico
  192.168.[redacted]             [redacted]            dinámico
  192.168.[redacted]             [redacted]            dinámico
  192.168.[redacted]             [redacted]            estático
  [redacted]                     [redacted]            estático
  [redacted]                     [redacted]            estático
  [redacted]                     [redacted]            estático
  [redacted]                     [redacted]            estático
  [redacted]                     [redacted]            estático
```

Dispositivo del atacante suplantando la Ip de la puerta de enlace

```
Interfaz: 192.168.[redacted] --- 0xd
  Dirección de Internet          Dirección física      Tipo
  192.168.[redacted].1           94-de-[redacted]      dinámico
  192.168.[redacted]             [redacted]            dinámico
  192.168.[redacted]             [redacted]            dinámico
  192.168.[redacted]             [redacted]            dinámico
  192.168.[redacted]             [redacted]            estático
  [redacted]                     [redacted]            estático
  [redacted]                     [redacted]            estático
  [redacted]                     [redacted]            estático
  [redacted]                     [redacted]            estático
  [redacted]                     [redacted]            estático
```

Figure 7: *DNS Spoofing*



Dominio original con Ip modificada

```
###[ DNS ]###
     length    = 75
     id        = 42627
     qr        = 1
     opcode    = QUERY
     aa        = 0
     tc        = 0
     rd        = 1
     ra        = 1
     z         = 0
     ad        = 0
     cd        = 0
     rcode     = ok
     qdcount   = 1
     ancount   = 1
     nscount   = 0
     arcount   = 0
     \qd        \
      |###[ DNS Question Record ]###
      |  qname     = 'www.facebook.com.'
      |  qtype     = A
      |  qclass    = IN
     \an        \
      |###[ DNS Resource Record ]###
      |  rrname    = 'www.facebook.com.'
      |  type      = A
      |  rclass    = IN
      |  ttl       = 0
      |  rdlen     = None
      |  rdata     = 192.168.1.100
     ns        = None
     ar        = None
```

Navegador de la victima

No se puede acceder a este sitio web

No se ha podido encontrar la dirección IP del servidor de www.facebook.com.

Prueba a:

- Comprobar la conexión
- Comprobar el proxy, el cortafuegos y la configuración de DNS
- Ejecutar Diagnósticos de red de Windows

ERR_NAME_NOT_RESOLVED

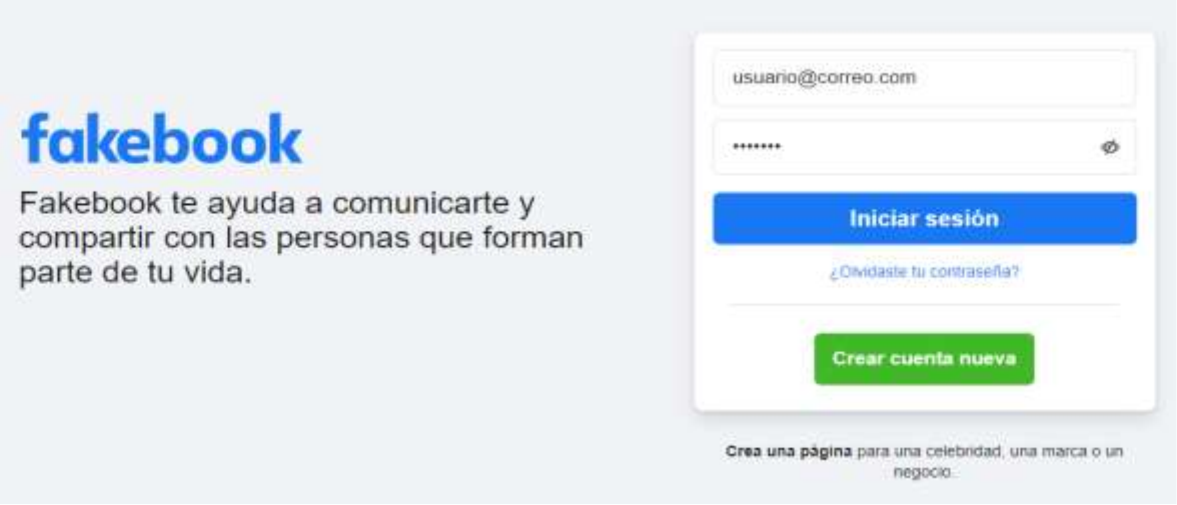
Figure 6 shows two screenshots that were taken from the console of the victim's Windows operating system. There it can be observed the change of the MAC address associated with the first IP address that corresponds to the network gateway. This indicates that the attacker's device is in the middle of the communication and supplants the IP of the gateway; that is why the MAC is different, since this corresponds to the MAC of the attacker's device.

In Figure 7, there are also two screenshots; the first one corresponds to the attacker's terminal, and the information of the packet received with the real Facebook domain and an IP modified by the attacker associated with this domain can be observed. This IP does not actually lead to any website. On the other hand, the second image shows what happens in the victim's browser; the URL is original but returns an error because the altered IP is not found on the Internet. However, if that IP was associated with a domain containing the phishing page the victim would be redirected there.

Fourth stage:

To obtain the credentials in this final stage, the backend that will be connected to the “Fakebook” login was created. An MITM and a DNS Spoofer were also implemented as part of the attack to intercept the communication in a local network and redirect the victim to the fake website, which will have the same URL as the original page. Once the information is sent to the backend, the victim will be directed to the login of the spoofed page so that for the user it will look like a typing error in his credentials.

Figure 8: *Form submission*



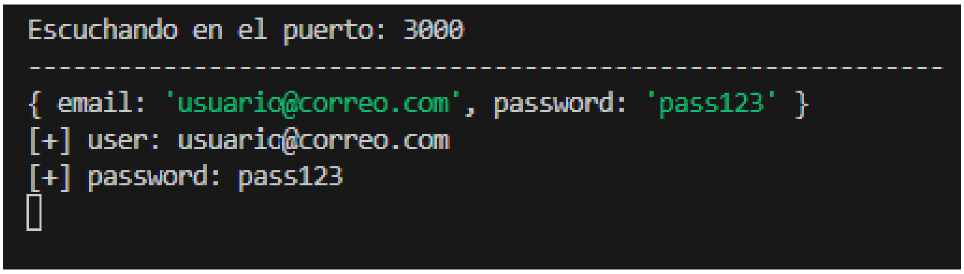
Fakebook te ayuda a comunicarte y compartir con las personas que forman parte de tu vida.

usuario@correo.com

•••••••

Crea una página para una celebridad, una marca o un negocio.

Figure 9: *Data received by the back-end*



```
Escuchando en el puerto: 3000
--------------------------------------------------------------
{ email: 'usuario@correo.com', password: 'pass123' }
[+] user: usuario@correo.com
[+] password: pass123
```

Results

In the process carried out in this paper, the attack is focused on a specific victim. In general, most attacks tend to be generalized and that is why the guidelines for identifying this type of fraud change with respect to the target of the attackers, due to the variety of means and social engineering applied to capture the victim, however, there are some processes that are used in most cases.

That said, targeted attacks are presented. These are the most difficult to identify because they act on one or a group of specific victims, usually phishing attacks that use persuasion techniques and social engineering focused on the topics of interest of the victim. They are known as spear phishing. Added to this the techniques used in fraud are more complicated to detect and require greater care. As it is possible to observe in the development of the laboratory, the URL is the same as that of the supplanted website, which makes the identification process at first sight useless. It is necessary the use of software and specialized tools that allow to identify the IP associated to the domain or to monitor the network packets to visualize a traceability. The identification of this type of attacks could be sectioned according to the different parts of phishing; the first one: the bait, the second: the hook, third: the catch.

The first one: the bait. The first thing to take into account is that there is always an initial contact of the attacker with the victim. The most recurrent means are emails, SMS or phone calls. It is important not to give private information using these means without making sure that they are reliable communication channels. In the case of SMS, it is difficult to identify their legitimacy. There are messaging services that allow sending messages customizing the sender and the message body. For attackers it is as simple as writing a credible message with a sender requesting the opening of a link to log in, change the password or simply requesting the user to access for a specific reason related to the account. The recommendations in this type of cases are the following:

- Do not access links from media other than the official ones.
- Check that the body of the message has no inconsistencies or wording problems. This will depend on how careless the attacker is, in the most generalized attacks it is common to find inconsistencies.
- Do not open or download attachments without making sure of the originality of the sender or do it directly from official sources.
- Check to whom the message is addressed, in generalized attacks the victim will be referred to without using his name, replacing it with Mr., user or you.

The second one: the hook. Once this type of messages is accessed, either because the victim overlooked the details of inconsistency or due to negligence, in the case of downloading attachments of dubious origin, it is advisable to have updated antivirus services; so that if they detect that the files are not harmless, the execution of processes that may compromise the integrity of the device information or functionality will be prevented. In addition to this, if the link performs a redirection as in the laboratory, it is recommended to enter erroneous data. Many of the phishing attacks redirect to the real page once the registration of the data is done. Its objective is to steal the credentials and not to validate if these are correct or not. Taking into account the previous information, the recommendations are the following:

- Have antivirus and operating systems updated in the devices to avoid any type of malware, in case of downloading suspicious files.
- Enter the wrong data the first time you enter the website and be aware of the behavior of the page. If it is phishing, there will be a redirect, i.e. it will seem that the page is reloaded again. If it is legitimate, you will see typical login errors. Phishing pages do not perform validations.
- Check from another device the official website of your account and compare if there are noticeable differences. This is something that is not 100%

effective; the similarity of the page will depend on the work employed by the attacker.

- Verify the URL and if the site is secure or not. Browsers represent this with a padlock before the URL. There are a variety of techniques to make the URL the same as the original, some more complex than others, but it is a detail to take into account.

The third one: the catch. In this last one it must be taken into account that the actions are no longer preventive, but reactive. It is taken for granted that the attacker already has the credentials, so the recommendations are the following:

- Have two-step verification enabled on all your accounts. In case your password and username are obtained by the attacker, the double verification will prevent access.
- If you receive notifications of verification on two of your accounts, without trying to access your account, it is likely that the attacker is trying to Access. Change the credentials and deny all access attempts that are not requested by yourself.

Conclusion

In conclusion, phishing is a widespread problem encompassing a set of methods that incorporate several disciplines related to information systems, giving it a degree of versatility that makes it difficult to detect. This article takes a group of specific techniques to demonstrate just how this type of fraud works and its shortcomings. Despite its versatility and complexity, it is not always successful, because it exploits the ignorance of users. The guidelines formulated in this article are based on the laboratory where the phishing process was carried out in a local environment, including guidelines for the most generalized attacks, since these are aimed at reaching as many users as possible, which leads to failures identified in the results section of this article.

References

Baca Urbina, G. (2016). *Introducción a la seguridad informática*. Grupo Editorial Patria. https://books.google.com.ec/books?id=IhUhDgAAQBAJ&printsec=copyright#v=onepage&q&f=false

Belisario Méndez, A. N. (2014). *Análisis de Métodos de Ataques de Phishing*. [Undergraduate Thesis, Universidad de Buenos Aires]. http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0840_BelisarioMendezAN.pdf

Hernández Dominguez, A. & Baluja García, W. (2021). Principales mecanismos para el enfrentamiento al phishing en las redes de datos. *Revista Cubana de Ciencias Informáticas, 15*(1), 413-441. http://scielo.sld.cu/pdf/rcci/v15n4s1/2227-1899-rcci-15-04-s1-413.pdf

Internet Crime Report 2021_IC3 Report.pdf. (2021). *Federal bureau of investigation.* https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Ley 1273. Normatividad sobre delitos informáticos. (2009). https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

Martínez Pérez, F. J. (2022). *Análisis de los ciberataques. El ataque Man-in-the-middle y el SSLSTRIP* [Undergraduate Thesis, Universidad Politécnica de Madrid]. https://oa.upm.es/76147/1/TFG_FRANCISCO_JAVIER_MARTINEZ_PEREZ.pdf

Pastor Iglesias, R. (2022). *Análisis actual de los Ataques Man-In-The-Middle por DNS Spoofing* [Undergraduate Thesis, Universidad Politécnica de Madrid]. https://oa.upm.es/71578/1/TFG_RAUL_PASTOR_IGLESIAS.pdf

Conflict of interest

The authors declare that they have no conflicts of interest.

Authors' contribution

C.C.B.B.: Writing and editing of the article, structuring and expression of ideas, data collection and analysis.

S.A.E.V.: Literature review. Data collection.