

¿ESTAMOS FORMANDO ADECUADAMENTE A LOS CIUDADANOS PARA EVITAR EL PHISHING Y SUS VARIANTES?

ARE WE ADEQUATELY TRAINING SOCIETY TO AVOID PHISHIN AND ITS VARIANTS?

Xicu-Xabiel García-Pañeda¹, David Melendi-Palacio¹, Víctor Corcoba-Magaña¹, Roberto García-Fernandez¹, Alejandro García-Pañeda², Dan García-Carrillo¹

¹Universidad de Oviedo, xabiel@uniovi.es

²Bosch

Received: 12/feb/2025 – Reviewing: 14/feb/2025 - Accepted: 26/may/2025 - DOI: <https://doi.org/10.52152/DNT11435>

To cite this article: GARCIA-PANEDA, Xabiel, MELENDI-PALACIO, David, CORCOBA-MAGAÑA, Víctor et al. ARE WE ADEQUATELY TRAINING SOCIETY TO AVOID PHISHIN AND ITS VARIANTS? DYNA New Technologies, January 2025, vol. 12, n. 1, [12P.] <https://doi.org/10.52152/DNT11435>

ABSTRACT:

Phishing is a technique usually based on the exploitation of both the confidence and concern of the users. An alarming message delivered by an organization of trust is the best mechanism to motivate users to act, even against their will. A frequent approach to diminish the impact of said technique is to train users and provide them with a set of recommendations. These recommendations are based on several characteristics common in phishing attacks. Our thesis is that training is currently ineffective because procedures and technology have imperfections which help fraudsters deceive users. To prove our conclusions, we present the analyses of two massive campaigns of bank-smishing attacks occurred in 2021 and 2022. The fraud was suffered by an estimate of 7,000 users and both cases have a similar anatomy. Our team has deeply analyzed these attacks to produce forensic reports for more than 30 court cases. We have studied cellular phones, phone call records, logs from bank systems and other forensic sources to analyze scammer procedures and techniques. Also, we discuss the reasons why we state that there is need of an updated approach towards phishing attacks. Users' training and awareness techniques must be redesigned and, apart from that, changes must be made in the procedures of organizations. Finally, we consider that it is necessary to improve the underlying technologies in services such as e-banking or e-shopping.

Keywords: Phishing, fraud, cybersecurity, forensic analysis, online banking, user training

RESUMEN:

El phishing es una técnica que generalmente se basa en explotar la confianza y la preocupación de los usuarios. Un mensaje alarmante emitido por una organización de confianza es el mejor mecanismo para motivar a los usuarios a actuar, incluso en contra de su voluntad. Una estrategia frecuente para minimizar el impacto de esta técnica es capacitar a los usuarios y proporcionarles un conjunto de recomendaciones. Estas recomendaciones se basan en varias características comunes de los ataques de phishing. Nuestra tesis es que la capacitación actual es ineficaz porque los procedimientos y la tecnología presentan defectos que facilitan a los estafadores engañar a los usuarios. Para respaldar nuestras conclusiones, presentamos el análisis de dos campañas masivas de ataques de smishing bancario ocurridas en 2021 y 2022. El fraude afectó a un estimado de 7000 usuarios y ambos casos presentan una estructura similar. Nuestro equipo ha analizado en profundidad estos ataques para elaborar informes forenses para más de 30 casos judiciales. Hemos estudiado teléfonos celulares, registros de llamadas telefónicas, registros de sistemas bancarios y otras fuentes forenses para analizar los procedimientos y técnicas de los estafadores. Además, discutimos las razones por las que confirmamos la necesidad de un enfoque actualizado frente a los ataques de phishing. Es necesario rediseñar las técnicas de formación y concienciación de los usuarios y, además, implementar cambios en los procedimientos de las organizaciones. Finalmente, consideramos que es necesario mejorar las tecnologías subyacentes en servicios como la banca o las compras electrónicas.


Palabras clave: Phishing, fraude, ciberseguridad, análisis forense, banca en línea, formación de usuarios

FUNDING

This research has been supported by Catedra Telecable – Universidad de Oviedo and Unión de Consumidores de Asturias.

1. - INTRODUCTION

Phishing is a family of cyberattacks in which the main scam element is social engineering. There are many different variants including smishing (using SMS), vishing (using a phone call), spear-phishing (directing the attack to a specific group of people), whaling (an attack on a high-profile target), etc. However, the background tactic is always the same: an initial message to trick the victims and a

	Are we adequately training society to avoid phishing and its variants?	
RESEARCH ARTICLE	Xabiel G Pañeda, David Melendi, Víctor Corcoba, Roberto García, Alejandro G. Pañeda, Dan García	Computers technology Others

trap simulating a real website in which the victims divulge their personal information. In most cases, phishing attacks have an economic purpose. The goal is to obtain access information to a bank account, a shop account or a credit card and use this information to purchase products or transfer money. The worldwide impact of these attacks is enormous. According to the last annual report of the Internet Crime Complaint Center, phishing was one of the top five crime types in the U.S.A. in 2023, with 298,878 victims and a loss of \$18,728,550 in that year alone [1]. Similarly, phishing remained the most commonly used attack vector among online fraud schemes in 2023 in the European Union [2]. In the particular case of Spain, there were 46,612 bank frauds only in 2023 [3].

Since the key element is the deception of the victims, different organizations and companies regularly produce training resources to educate users and warn them about these attacks. In general, these resources are usually learning pills about frequent recommendations for users. Some of these pills include examples to make comprehension easier for users. Nevertheless, several studies have evaluated the effectiveness of phishing training programs. These works indicate that while training can improve users' ability to detect phishing attacks, its actual impact remains limited [4] [5]. In fact, the findings suggest that traditional approaches, such as phishing training or simulations, might not significantly reduce users' susceptibility to phishing, especially when it comes to personalized content [6]. Currently, generative AI makes it easier to generate personalized texts for users [7].

Given the fact that bank customers have been the principal target of phishing attacks, at least since 2018 [8], we have compared the most common recommendations with the different steps of a real bank smishing attack. After the analysis of the attack, we have concluded that the methods used by fraudsters render the recommendations of these organizations ineffective. Firstly, because scammers have improved their attacks and some of the characteristics in the original phishing campaigns are no longer present. Secondly, because banks and other organizations usually fail to meet their own recommendations, creating confusion among their own users.


The rest of the paper is organized as follows. Section 2 describes the current regulatory context in Europe. Section 3 enumerates common anti-phishing recommendations provided by different types of organizations. Section 4 analyzes two real smishing bank frauds. Section 5 includes a discussion about why current recommendations to avoid phishing attacks are not useful. Finally, Sections 5 and 6 provide the main conclusions of our analysis and future works.

2. - REGULATORY FRAMEWORK

In recent years, the European Union has significantly strengthened its regulatory framework in cybersecurity to protect its citizens, institutions, and critical infrastructures against cyber threats. Among these regulations, one of the most important is the NIS2 Directive (Directive (EU) 2022/2555) [9]. Its goal is to achieve a high level of cybersecurity across the European Union. It establishes a set of requirements regarding risk management, incident management, and information sharing. This is being applied in most sectors, including the banking sector. The directive emphasizes the need to protect information systems and to raise user awareness to minimize the success of attacks such as phishing.

Additionally, the European Union adopted the Cyber Resilience Act (Regulation (EU) 2024/2847) [10] in 2024, which complements the NIS2 Directive. This law establishes a set of mandatory cybersecurity requirements for all products containing any digital element (hardware or software) that are connected directly or indirectly to other devices or networks. Its fundamental principle is "security by design and by default". This obliges manufacturers to integrate and maintain cybersecurity mechanisms throughout the entire lifecycle of their products. Furthermore, it also forces manufacturers to implement processes for vulnerability management, to provide security updates, and to transparently inform users about cybersecurity and support features for their products.

Another important regulation is the Cyber Solidarity Act (Regulation (EU) 2025/38) [11], approved in December 2024. This regulation establishes a framework for coordinated action at the European level to detect, prepare for, and respond to large-scale cyber threats. A central component of this law is the creation of a European Cybersecurity Alert System comprised of a network of national and cross-border hubs. These hubs are responsible for real-time monitoring, threat detection, and information sharing across the EU. It also introduces a Cyber Emergency Mechanism designed to respond to significant cybersecurity incidents. This mechanism includes an EU Cybersecurity Reserve composed of pre-selected and trusted private sector entities that may assist member states during a severe cyber crisis. The reserve aims to provide rapid incident response support, ensuring that critical services and infrastructure are restored quickly. Furthermore, the Cyber Solidarity Act mandates the implementation of a cybersecurity incident review mechanism. This facilitates the assessment of significant cyber incidents with the goal of analyzing the effectiveness of response strategies and extracting lessons-learned for future improvements. In the context of phishing, this law's emphasis on threat information sharing and coordinated response mechanisms is important, as these types of attacks often exploit cross-border vulnerabilities and can spread rapidly across networks.

	Are we adequately training society to avoid phishing and its variants?	
RESEARCH ARTICLE	Xabiel G Pañeda, David Melendi, Víctor Corcoba, Roberto García, Alejandro G. Pañeda, Dan García	Computers technology Others

The Digital Operational Resilience Act (DORA), formally known as Regulation (EU) 2022/2554 [12], complements the European Union's cybersecurity framework by specifically focusing on the financial sector's digital resilience. This law has been in effect since January 2025. It requires financial entities to implement a robust framework for managing risks related to information and communication technologies (ICT). This includes the identification, protection, detection, response, and recovery from incidents, including phishing attacks. Furthermore, it obliges institutions to conduct regular digital operational resilience tests to assess their preparedness. Finally, it also includes strict incident notification protocols, requiring entities to notify competent authorities of significant ICT-related incidents within specific timeframes. DORA ensures that financial institutions protect their technological infrastructure and encourages a culture of continuous improvement in cybersecurity practices.


All these recently adopted regulations recognize that cybersecurity is not merely a technological issue but also demands organizational and human efforts. Our study aligns with the European Union's strategic objectives [13] by emphasizing the necessity for an updated approach to phishing awareness that includes not only user training but also modifications in corporate practices and technological innovation.

3. - ANTI-PHISHING RECOMMENDATIONS

Several institutions and companies have been publishing anti-phishing recommendations over a long period of time, following human-centric mitigation strategies, also proposed in previous work [14]. The goal of said recommendations is to educate users to avoid these attacks. For example, figures 1 and 2 show training pills of two important Spanish banks. Moreover, figure 3 shows the checking list of the Spanish National Cybersecurity Institute (INCIBE) about how to avoid a SMiShing attack.



Fig. 1. Check list of a bank (A) training pill

	Are we adequately training society to avoid phishing and its variants?	
RESEARCH ARTICLE	Xabiel G Pañeda, David Melendi, Víctor Corcoba, Roberto García, Alejandro G. Pañeda, Dan García	Computers technology Others

Consejos para protegerse del smishing


- No proporciones información personal o bancaria en páginas web a las que has accedido desde un enlace incluido en un SMS. Por norma general, ninguna compañía u organismo público te va a solicitar información sensible a través de este canal.
- No respondas nunca a SMS que te resulten sospechosos. Elimínalos.
- Desconfía de todos aquellos mensajes alarmantes que tengan tono de urgencia, contengan faltas de ortografía o erratas y de los que no se dirigen a ti de forma personalizada.
- Instala un *antimalware* y un *antivirus* en tus dispositivos y realiza análisis periódicos.
- Mantén siempre actualizados el sistema operativo, el navegador y las aplicaciones de tus dispositivos.
- Descarga las aplicaciones exclusivamente desde los mercados o repositorios oficiales. Además, observa si la aplicación ha sido descargada por un elevado número de usuarios, tiene una valoración alta y opiniones positivas. Asimismo, comprueba que el nombre del desarrollador y el logo de la aplicación sean los oficiales.
- Recuerda que los mensajes SMS que envía no contienen enlaces. Si recibes alguno que incluya un link, aunque aparezca en el hilo de , es falso.

Fig. 2. Check list of a bank (B) training pill

After revising an important set of pills from banks and other security organizations we can summarize current recommendations in the following list:

- To check the content of messages and detect problems with language (e.g., with spelling or grammar).
- To verify the source of messages, so that users do not trust unknown senders. For example, to check names, email addresses, phone numbers, etc.
- To avoid using links received in messages.
- To check problems in URLs, including a verification of the usage of HTTPS and problems with encryption certificates (i.e., warnings provided by modern browsers).
- Not to provide personal information based on message requests, including user credentials.
- Not to trust urgent requests.
- To contact the organization for help.

Most of these security-awareness recommendations suggest the user to analyze the source of the messages, their contents or the URLs provided. Nevertheless, they are not totally unquestionable. The success of the implementation of these recommendations depends on the skills of the users and the context of the attack. However, the effectiveness of these recommendations depends on the sophistication of the attack.

	Are we adequately training society to avoid phishing and its variants?	
RESEARCH ARTICLE	Xabiel G Pañeda, David Melendi, Víctor Corcoba, Roberto García, Alejandro G. Pañeda, Dan García	Computers technology Others

¿Cómo podemos protegernos?

Por suerte para nosotros, las medidas de protección son muy fáciles de implementar y solo requieren que estemos concienciados y utilicemos un poco de sentido común. Además, las prisas nunca nos ayudarán cuando se trata de luchar contra los ciberataques basados en la **ingeniería social**, por lo que pararnos unos minutos a analizar el mensaje que acabamos de recibir siempre es buena idea. Hay algunas cosas que nos ayudarán a identificar y protegernos del *smishing*:

- ♦ **Desconfiar de remitentes desconocidos.** Si recibimos un mensaje de una persona o entidad desconocida informándonos de un premio o solicitando información, lo más prudente será ignorar y eliminar el mensaje. De igual modo, desconfiaremos si se trata de números de teléfono sospechosos.
- ♦ **Desconfiar de promociones, cupones o concursos.** Suelen utilizarse como anzuelos para obtener la atención de los usuarios y conseguir que accedan a enlaces fraudulentos o contactar con un número de teléfono de tarificación especial, por ejemplo.
- ♦ **No facilitar nunca información personal.** Una entidad de confianza jamás nos solicitará datos personales sin previo aviso, y mucho menos a través de un mensaje.
- ♦ **No hacer clic en los enlaces** bajo ningún concepto, ya que pueden llevarnos a webs fraudulentas. Es mejor contrastar la información primero y acceder a las páginas oficiales tecleando la URL en el navegador.
- ♦ **No bajar archivos adjuntos,** pueden contener *malware* con el que infectar nuestro dispositivo.
- ♦ **Proteger nuestras cuentas.** Utilizar **contraseñas robustas** y **sistemas de doble verificación** permitirá añadir una capa extra de protección.

Fig. 3 Recommendations of INCIBE to avoid a SMISHing attack

4. - ANALYSIS OF A REAL SMISHING BANK ATTACK


In this paper, we reconstruct and analyze two frauds suffered by thousands of users of two Spanish banks, based on several smishing campaigns launched in 2021 and 2022. In one of the cases the attack coincided with a bank merger operation. The anatomy of the attacks was very similar in both cases. It was based on a man in the middle operation used to change the “trusted” device for that user. This device was used by the bank to double check the operations requested by users, commonly, with a security code sent in a SMS message. Once this device was modified, fraudsters used their own terminal to validate transfer operations to a bank in a different country.

Since 2022 our team has examined cellular phones, phone call records, logs of the banks’ systems and other information sources to produce forensics reports for more than 30 court cases. The reconstruction of the attacks presented is based on the results of this investigation work.

A. Step 1: A message arrives

The cyberattack begins with the arrival of a SMS message such as that shown in Fig. 4. This message urges the user to act after an unusual access to his/her bank account. The SMS message includes a seemingly legitimate link to the bank website. This SMS is usually sent outside the bank opening hours. For example, the message shown in Fig. 4 was sent on a Saturday.

This message has several noteworthy aspects. Firstly, SMS spoofing is used and, thus, the SMS arrives with the same “sender ID” used in the actual messages of the bank. This causes the phone to place the SMS grouped together with legitimate messages. Secondly, the usage of the language (in this case Spanish) is totally accurate and, thus, there are no spelling or orthographic errors in the text. Thirdly, the message includes a link with a correct structure, according to the usual recommendations given to users (usage of HTTPS, i.e., encryption). Although the domain name in the URL is unusual, it contains the name of the bank.

	Are we adequately training society to avoid phishing and its variants?	
RESEARCH ARTICLE	Xabiel G Pañeda, David Melendi, Víctor Corcoba, Roberto García, Alejandro G. Pañeda, Dan García	Computers technology Others

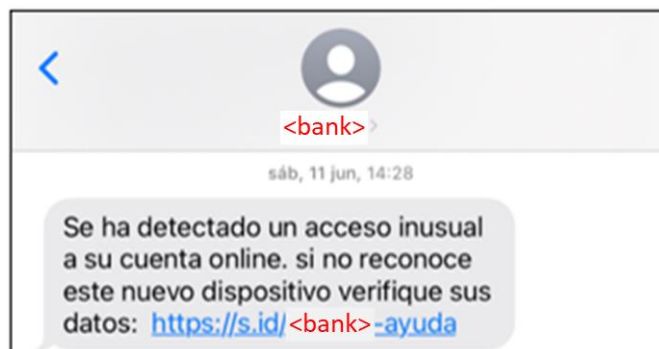


Fig. 4 Example of SMS message used in the scam (“An unusual access to your online account has been detected. If you don’t recognize this new device, verify your data: <https://s.id/<bank>-ayuda>”)


B. Step 2: The Website

The SMS urges the user to click the link to resolve the incident. Once the user clicks on the link, the browser will open a fraudulent website, which is going to be used to perform a man in the middle attack. Fig. 5 shows an example of the fake authentication webpage (left) and the genuine webpage of the bank (right). Both webpages are identical, but for the background pattern in the header section.



Fig. 5 Fake authentication webpage (left) and genuine authentication webpage (right)

Moreover, the browser does not produce any type of warning since the false webpage uses HTTPS (HTTP+TLS) and has a correct certificate installed. This means that scammers have registered a domain name including the name of the bank and have generated legitimate encryption certificates. Fig. 6 shows an example of the fake URL opened in a browser (top) and the genuine URL of the bank (bottom). The detailed information in the certificate shows that this is not a certificate of the bank, but this is something standard Internet users are unaware of. The real problem for a common user is that the warnings included in modern browsers about encryption certificates are not triggered. Everything seems perfectly normal.

	Are we adequately training society to avoid phishing and its variants?	
RESEARCH ARTICLE	Xabiel G Pañeda, David Melendi, Víctor Corcoba, Roberto García, Alejandro G. Pañeda, Dan García	Computers technology Others

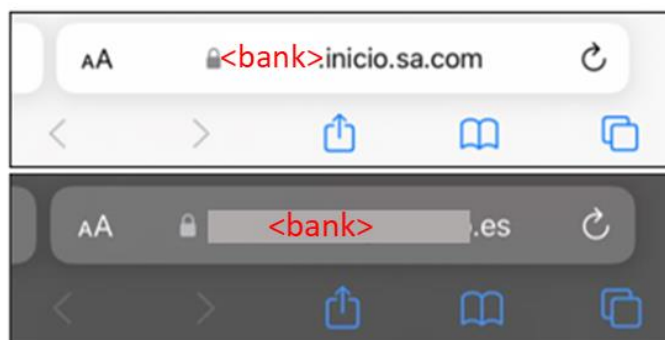


Fig. 6 URLs of fraudulent webpage (top) and genuine webpage (bottom)

C. Step 3: Gaining control

Once the user has introduced his or her credentials in the fake authentication website, scammers, operating in the middle, use them to access the real bank website or App and request a change of the trusted device for that user. This was possible at the time, because banks did not have multifactor authentication in the access to their on-line services. A secondary factor was only used to verify certain types of operations, including the change of trusted device. In this process, the bank issues a verification SMS sent to the legitimate device and including a security code. An example is shown in Fig.7.

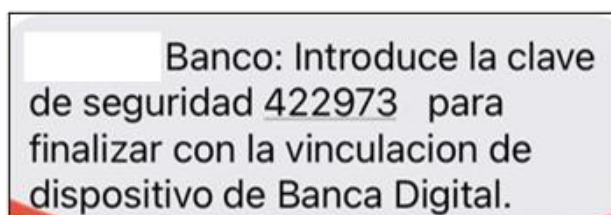


Fig. 7 Legitimate verification message sent to confirm a change in the trusted device ("The security key is 422973 to finish the connection with the e-banking device")


The code sent by the bank is requested in the fake webpage and used by the fraudsters to confirm the change of device. Users actually think that they are stopping the "unusual access" supposedly reported by the bank. Actually, once they have provided the security code, the fake webpage reports that the security problem has been finally solved and redirects the user to the website of the bank. In this process, scammers gather useful information about the device of the legitimate user thanks to the details included in HTTP headers in the communication between the browser and the forged webpage. They use these details to change the trusted device for a similar one. For instance, they always change an iPhone for an iPhone or an Android device for another Android device.

After the users have provided the verification code to scammers, the new trusted device allows them to have full control of the bank accounts of the victims. Furthermore, operations requiring validation from the user would be confirmed with information sent in push notifications delivered to that new device.

There is a slight difference between both attacks in this step. One of them works as described, and the other requires two steps and two SMS messages with codes the user has to introduce in the fake web site.

D. Step 4: The money

Once fraudsters have gained control, they begin revising the details of the bank accounts of the victim and their balance. Then, they select one of those accounts and start to perform bank transfers to accounts in foreign countries. Usually, these operations are instant credit transfers, so that the money is instantly made available on the account of the scammers. Initially, they usually try with immediate transfers of considerable amounts (e.g., 10,000 €) if there is enough balance. In case the transfer is rejected because of a lower transfer limit, they try again with lower amounts. Figure 8 shows an example of this behavior. This operation is repeated several times

	Are we adequately training society to avoid phishing and its variants?	
RESEARCH ARTICLE	Xabiel G Pañeda, David Melendi, Víctor Corcoba, Roberto García, Alejandro G. Pañeda, Dan García	Computers technology Others

until they empty the account or reach the daily withdrawal limit. In this last case, scammers wait until the following day to start again with the process until reaching the same limit again or until the account is empty. This same process is repeated with all the accounts of the user. The transfers usually go to different destination accounts. Another option was to transfer money using BIZUM operations and if the user did not have funds, scammers sometimes took out fast loans in the victim's name, before carrying out credit transfers.

YV	TRANSFERENCIA-OBTENER DATOS TI	OK	Transference undone (over limit)	13/06/2022 17:10:38.030202	9.999,00 EUR
YV	TRANSFERENCIA-OBTENER DATOS TI	OK		13/06/2022 17:10:38.892054	9.999,00 EUR
TH	TRANSFERENCIA-SIMULACIÓN INMED	MBE0128 HA SUPERADO EL IMPORTE MAXIMO PARA TRASPAS		13/06/2022 17:10:48.341942	9.999,00 EUR
XD	DIVISA-LISTADO DE DIVISAS	OK		13/06/2022 17:10:50.437578	0,00
YW	TRANSFERENCIA-OBTENER MODO DE	OK		13/06/2022 17:10:51.027962	0,00 EUR
YW	TRANSFERENCIA-OBTENER MODO DE	OK		13/06/2022 17:10:51.644378	0,00 EUR
YV	TRANSFERENCIA-OBTENER DATOS TI	OK	Transference executed	13/06/2022 17:10:57.958126	9.000,00 EUR
YV	TRANSFERENCIA-OBTENER DATOS TI	OK		13/06/2022 17:10:58.675615	9.000,00 EUR
TH	TRANSFERENCIA-SIMULACIÓN INMED	OK		13/06/2022 17:11:01.590897	9.000,00 EUR
TG	TRANSFERENCIA-EJECUCIÓN INMEDI	OK		13/06/2022 17:11:03.886113	9.000,00 EUR

Fig. 8 Bank operation logs with the operations performed

E. Step 5: The B plan

When users do not provide the code requested to verify the change of the trusted device, scammers initiate plan B. They phone the victim using a spoofed caller ID, impersonating an employee of the bank. If the client checks the phone number of the incoming call on the Internet, or has that number recorded on their phone, he or she believes that the phone call comes from the actual bank.

Scammers explain to the victim that someone has gained control of his or her accounts and that the attackers are currently ordering bank transfers. It is important to point out that scammers, using the stolen credentials of the user, had access to all the details of the accounts and the operations performed. These details were used to gain the victims' trust. Scammers warn the victim that he or she is going to receive bank transfer verification codes sent to their mobile phone and that they need those codes to stop the fraudulent money transfers. These codes may be requested using voice, but there are cases reported in which the codes are requested using the keyboard of the phone (via DTMF tones). What was actually happening is that scammers were performing bank transfers and requesting the verification codes they needed using the phone call. To support the scam, attackers use transfer concepts similar to "canceling transfer", just in case the victims were checking the operations in their accounts. That concept will make victims think that the operations are being cancelled. In fact, scammers sometimes sent apparently legitimate SMS messages stating that the operations had been cancelled. These SMS messages arrived with the same "sender ID" used in the actual messages sent by the bank and, thus, are grouped together with genuine messages. These operations will be repeated by scammers until the daily withdrawal limit is reached or until the account has been emptied. This scammer procedure is a copy of the protocol published on the bank Web site to block operations, cards and accounts. In this protocol, the client has to reveal codes received in his/her cellular phone to bank employees. Figure 9 shows information about this protocol published on the bank's website.

Bloqueo de servicio y operaciones. [redacted] podrá bloquear por motivos de seguridad tanto el servicio como determinadas operaciones cuando tenga sospechas fundadas de actividad no autorizada o fraudulenta. [redacted] le informará, telefónicamente o a través del propio servicio, del bloqueo realizado y de sus motivos procediendo al desbloqueo una vez desaparezcan dichos motivos. El Cliente podrá solicitar a [redacted] el desbloqueo telefónicamente o desde la Oficina en función de las circunstancias del bloqueo

Fig. 9 Instructions published on the bank Web page


5. - ANALYSIS AND DISCUSSION

A. The SMS message

The fact that the message received by the victim is grouped by the phone together with genuine messages sent by the bank, makes the user believe that this is a genuine message. There is no reason not to trust the message because the source looks identical.

There are no problems with the usage of the language, unlike the first phishing attacks in which texts used to be full of mistakes and grammatical errors. Thus, all the recommendations about this aspect are equally invalid, as they do not alert about the scam.

The message includes a link, and users have been frequently warned not to trust messages including links to webpages and to verify the correctness of URLs before making use of them. In fact, banks have recently informed their clients that they do not send messages

	Are we adequately training society to avoid phishing and its variants?	
RESEARCH ARTICLE	Xabiel G Pañeda, David Melendi, Víctor Corcoba, Roberto García, Alejandro G. Pañeda, Dan García	Computers technology Others

with links to web sites. However, this is not true and the usage of links in SMS and email messages has been a widespread practice for years. Some examples of genuine SMS messages sent by banks operating in Spain are shown in Fig. 10.

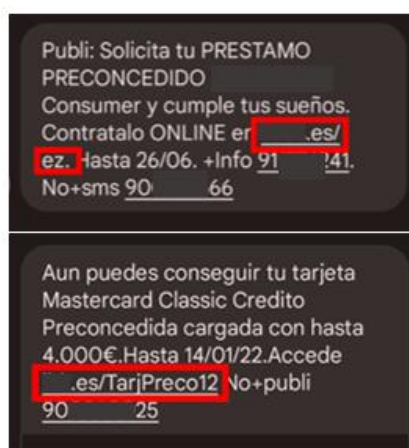


Fig. 10 Examples of genuine SMS messages sent by Spanish banks with links to websites (“Request your PREAPPROVED LOAN ... Consumer and fulfill your dreams. Contract ONLINE in ...” and “You can still get your preapproved Mastercard Classic Credit card loaded with up to 4,000€. Until 14/01/22. Access...”)


The examples shown in Fig. 10 contain links to websites. Those links are incomplete, so users do not know whether HTTPS is going to be used or not. Moreover, the messages include shortened URLs or URLs that do not coincide with the URLs users are used to when they enter their online banking services. In fact, we have also encountered a case in which a bank unknowingly provided evidence in court showing that the entity had sent the victim a SMS with a shortened URL generated with the “bitly” public service, the same day that the person suffered the fraud. So, banks send messages with links and sometimes those links are obfuscated. Moreover, although the domain name in the URL is unusual, it contains the name of the bank. Despite the fact that some banks warn their users about their legitimate domain names, we have seen cases of legitimate URLs sent in messages using domain names not in the lists provided to users. Furthermore, some banks use shortened URLs and, sometimes, generated with a public service. All this goes against the recommendations they provide. But this is also the case of all types of organizations including insurance companies, utilities, or public administrations.

In conclusion, users are used to receiving these types of messages. The fact that banks and other organizations warn users against messages with links, when they are actually making use of them, only creates confusion.

B. The webpage

Fig. 5 shows that the fake authentication webpage is identical to the genuine webpage of the bank. The webpage may be known to users due to past authentication operations. Moreover, the fact that the site uses a correct HTTPS certificate avoids triggering the default warning systems included in modern browsers. The behavior of the browser is perfectly normal, giving the user a false sense of security. Although the domain name in the URL may be an indication of fraud, it is necessary to consider that it contains the name of the bank and that organizations usually employ different domain names due to varied reasons, even pointing to the same website. Behind this situation there may be historical, marketing or organizational reasons. But it is a fact that organizations do not warn users about the legitimate domain names they will use (only one if possible). Even if this was the case, fraudsters may use homographs to deceive users. Again, there is no reason for users to be suspicious about this webpage.

It is also true that users have been warned about not giving personal details based on message requests. But it is also true that the user does not actually respond to the message with his or her credentials. The user opens a seemingly legitimate webpage and tries to access and authenticated service. It is also important to point out that this is also a frequent operation performed by banks and other organizations. We have recently received an email as part of a genuine campaign to advertise products offered by a bank. The email includes several links like the example shown in Fig. 11. It is a button shaped link. Firstly, that link does not show the URL and, thus, users cannot see the URL and check the usage of HTTPS or the authenticity of the domain name. Secondly, if the link is used, the

	Are we adequately training society to avoid phishing and its variants?	
RESEARCH ARTICLE	Xabiel G Pañeda, David Melendi, Víctor Corcoba, Roberto García, Alejandro G. Pañeda, Dan García	Computers technology Others

legitimate webpage of the campaign is opened and that same webpage has a button to open a login form in which the credentials of the user are requested. Thirdly, the email urges users to act quickly, because that promotion ends on a given date.

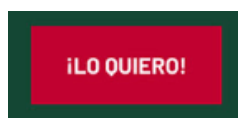


Fig. 11 Example of a link in an email sent in a campaign to advertise products of a bank, with the text “¡LO QUIERO!” (“I want it”)

It is common that organizations send messages with links to webpages and, frequently, those webpages include links to access a login form. The problem is that it is a question of time before scammers begin to mimic this practice and start to send links to a landing page instead of links to a login page. Warning users not to provide their credentials based on message requests is plainly puzzling. Again, if banks and other organizations continue to advertise their products in this way, the recommendations in this sense are not valid.

C. The urgency

Scammers typically try to make their victims panic for some reason. In the cases we have described, users are urged to act immediately because of a security problem with their bank accounts. It is necessary to understand that this type of alarm worries users independently of their background or technical skills. Users aware of this type of attack may ignore the SMS messages received, but the problem is that there is a second phase of the attack in which users receive an apparently legitimate phone call using the actual number of the bank. What is more, callers have all the details of the account and the activity of the user. Everything is very convincing.

The attacks were produced outside the bank opening hours, and users are frequently instructed to contact the bank through its official communication channels if they need some kind of support. But some users thought that this was not necessary because they received a phone call from the bank itself. Actually, a spoofed caller ID was used, but everything was carefully designed to look like something real, so it is unrealistic to ask users not to trust urgent requests. In fact, urgency is also used in the campaigns carried out by these organizations, as we have previously described. Furthermore, after a test campaign carried out in 2022, in February 2023 Spanish authorities activated the ES-Alert public alert system, which is actually based on notifications sent to mobile phones [15]. The situation will worsen as a rise in multichannel phishing attacks was already predicted in 2022 [16]. The conclusion again is that the recommendations given to users are contradictory with what organizations do.


6. - CONCLUSIONS

In this paper we have described the anatomy of two real smishing attacks performed in campaigns carried out by groups of fraudsters in Spain in 2021 and 2022. Both attacks were carefully designed to avoid anti-phishing training recommendations.

The general rule in the last few years has been that phishing scams can be stopped by educating users. Thus, recurrent anti-phishing training pills are provided to users by all types of organizations. As we have revealed, these training recommendations are not currently useful for two reasons. (1) Scammers have improved their attacks and (2) banks and other organizations continue with practices that go against their own recommendations. The result is users without the capacity to recognize scams. In fact, this continues to be true. The 2023 Payment Threats and Fraud Trends Report of the European Payments Council [17] primarily insists on user education to prevent these attacks without renewing the set of recommendations.

It is necessary to redesign how we prevent these types of frauds, by implementing new training strategies and changing corporate practices. Some suggestions follow:

- We have to redefine user recommendation pills, because they currently describe a list of symptoms only. People need to be aware of the anatomy of the attacks. It is important that they realize what is really happening on the side they cannot see nor control.
- Due to the fact that phishing techniques are constantly evolving, users need to understand that recommendations are only valid to some extent. They need to understand that the information they have received in the past may be obsolete and that they need to be constantly informed about news and changes in technology.

	Are we adequately training society to avoid phishing and its variants?	
RESEARCH ARTICLE	Xabiel G Pañeda, David Melendi, Víctor Corcoba, Roberto García, Alejandro G. Pañeda, Dan García	Computers technology Others


- Similarly, organizations must not only distribute general recommendations developed by others but also need to be proactive, in line with the European Union's strategic cybersecurity objectives [13]. This includes:
 - Tailoring their recommendations to their context and the particular characteristics of their users. Training activities must be adapted to the people's background to achieve maximum comprehension.
 - Revising and improving training activities and recommendations constantly, following a continuous improvement approach.
 - Warning users about the fact that recommendations expire.
 - Sending regular updates and reminders about recommendations and their corporate security policies.
 - Performing regular campaigns simulating attacks, to raise awareness within their users.
 - Reward users reporting phishing attacks, whenever this is possible.
 - Improving readiness of customer support staff to act when an incident is reported.
 - Fraud departments in organizations should develop simulations and analysis to anticipate their policies to the new scammer procedures.
- It is necessary to change corporate practices in certain types of organizations. Education cannot contradict the real practice if we want to do something useful.

We acknowledge that technological frauds cannot be stopped through user education alone as this demands technological solutions and strict security policies. Technology and education have to walk together. We have seen that SMS sender and phone caller ID spoofing techniques are paramount in deceiving the victims. We cannot push citizens to use dangerous services and recommend them to stay alert. Standardization organizations, telecommunication companies and governments should take responsibility for this and act to strictly control the identity of communication users. Hindering spoofing attacks would also improve the investigations aimed at discovering the fraudsters behind these attacks. Also, the procedures of banks need to be regularly revised. Hundreds of users suffering this attack, with a change of trusted device operation from an unusual location immediately followed by instant transfers close to the daily withdrawal limit should have, at least, triggered an alarm. Banks should prioritize security in their operations instead of flexibility. For instance, by enabling multi-factor authentication in the access to their on-line services, by restricting certain changes in authentication/trust components or by blocking/delaying unusual or suspicious operations. They should at least allow users to decide the experience they would like to have. The deployment of modern authentication mechanisms may also complicate these attacks since they all start by stealing user credentials. Examples are modern MFA techniques and password-less authentication. For example, Passkey is a password-less authentication mechanism developed by the World Wide Web Consortium and the FIDO Alliance [18]. This method is based on asymmetric encryption and authentication is performed locally by using biometrics or security keys.

This study provides valuable insights into the weaknesses in user training and in the recommendations typically offered to prevent phishing attacks. However, despite the fact that several proposals have been made, there are some limitations which need to be considered. Firstly, phishing techniques are constantly evolving, which means that new types of attacks may emerge that are not detectable through improved training activities and recommendations. These aspects require a continuous improvement approach. Secondly, this research has been conducted in Spain and user behavior may vary significantly in other regions with different cultural backgrounds. Lastly, many phishing attacks rely heavily on social engineering, where emotional and psychological factors can play an important role. For instance, individuals with high levels of neuroticism, who tend to experience greater anxiety, worry, and insecurity, may respond more impulsively to phishing attempts than individuals with lower levels of this personality trait. Therefore, incorporating psychological factors may be needed when assessing the effectiveness of preventive measures promoted by banks and other institutions.

7. – FUTURE WORK

The analysis of the attacks described shows the need to constantly revise security mechanisms and policies. As soon as banking systems and protocols are updated, scammers start to think about new ways to improve their attacks and overcome the new restrictions imposed. Thus, we would like to continue analyzing these attacks to keep researchers updated about changes in the mechanisms used by fraudsters, and to suggest improvements in the policies deployed at the time. Furthermore, the aim of our team is to research on technical improvements to current systems in three different fields. Firstly, in improvements during the authentication of the users and the authorization of banking transactions. Secondly, in the detection and avoidance of user spoofing in different communication

	<p>Are we adequately training society to avoid phishing and its variants?</p>	<p>Computers technology</p>
<p>RESEARCH ARTICLE</p>	<p>Xabiel G Pañeda, David Melendi, Víctor Corcoba, Roberto García, Alejandro G. Pañeda, Dan García</p>	<p>Others</p>

scenarios, such as the caller ID spoofing technique used in the attacks described. Thirly, in user and entity behavior analytics systems (UEBA) with forensic guarantees.

REFERENCES

- [1] Internet Crime Complaint Center (2023). "Internet crime report 2023". Federal Bureau of Investigation [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf
- [2] Europol (2024). "Internet Organised Crime Threat Assessment (IOCTA) 2024". Publications Office of the European Union, Luxembourg. [Online]. Available: <https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024>
- [3] Ministry of the Interior (2025). "Crime Statistic Portal". Directorate General for Coordination and Studies. [Online]. Available: <https://estadisticasdecriminalidad.ses.mir.es/publico/portalestadistico/en/>
- [4] M. H. Khan and S. T. Muntaha. "Evaluating the effectiveness of cybersecurity awareness programs in reducing phishing attacks: A qualitative study" In World J. Adv. Res. Rev., vol. 23 (2), pp. 1663-1673, 2024, DOI: 10.30574/wjarr.2024.23.2.2538.
- [5] G. Ho, A. Mirian, E. Luo et al. "Understanding the Efficacy of Phishing Training in Practice", In Proceedings of 2025 IEEE Symposium on Security and Privacy (SP), IEEE Computer Society, 2024, pp. 76-76. DOI: 10.1109/SP61157.2025.00076.
- [6] D. Hillman, Y. Harel and E. Toch. "Evaluating organizational phishing awareness training on an enterprise scale". In Comput. Secur., vol. 132, p. 103364, 2023, DOI: 10.1016/j.cose.2023.103364.
- [7] European Union Agency for Cybersecurity. "ENISA threat landscape 2024: July 2023 to June 2024". Luxembourg Publications Office, 2024. [Online]. Available: <https://data.europa.eu/doi/10.2824/0710888>
- [8] Krebs on security (2018, Nov. 2). SMS Phishing + Cardless ATM = Profit. [Online]. Available: <https://krebsonsecurity.com/2018/11/sms-phishing-cardless-atm-profit/>
- [9] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance), vol. 333. 2022. [Online]. Available: <http://data.europa.eu/eli/dir/2022/2555/oj/eng>
- [10] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance). 2024. [Online]. Available: <http://data.europa.eu/eli/reg/2024/2847/oj/eng>
- [11] Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act). 2024. [Online]. Available: <http://data.europa.eu/eli/reg/2025/38/oj/eng>
- [12] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance), vol. 333. 2022. [Online]. Available: <http://data.europa.eu/eli/reg/2022/2554/oj/eng>
- [13] "How the EU is strengthening its cybersecurity," Consilium. Accessed: Apr. 26, 2025. [Online]. Available: <https://www.consilium.europa.eu/en/policies/cybersecurity/>
- [14] B. Naqvi, K. Perova, A. Farooq, I. Makhdoom, S. Oyedeji, J. Porras, "Mitigation Strategies against the Phishing Attacks: A Systematic Literature Review", Computers & Security, vol. 132, 103387, Sept. 2023, DOI: <https://doi.org/10.1016/j.cose.2023.103387>
- [15] European Emergency Number Association. (2023, Feb. 28). Spain activates ES-Alert emergency warning system. [Online]. Available: <https://eena.org/knowledge-hub/news/spainesalert/>
- [16] J. D'Hoinne, J. Watts, K. Thielemann (2022, Apr. 1). "How to Respond to the 2022 Cyberthreat Landscape" Gartner Research [Online]. Available: <https://www.gartner.com/en/documents/4013107>
- [17] European Payments Council (2023, Nov. 7). 2023 Payment Threats and Fraud Trends Report. [Online]. Available: <https://www.europeanpaymentscouncil.eu/document-library/reports/yearly-update-payment-threats-and-fraud-trends-report-0>
- [18] FIDO Alliance. (2024, Feb. 19). Passkeys. [Online]. Available: <https://fidoalliance.org/passkeys/>