EUROPEAN UNION AGENCY
FOR CYBERSECURITY

COUNTERING SIM-SWAPPING

Overview and good practices to reduce the impact of SIM-Swapping Attacks

December 2021

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

For contacting the authors please use resilience@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

Georgia Bafoutsou, Slawomir Bryska and Marnix Dekker (ENISA)

ACKNOWLEDGEMENTS

We would like to thank Mr. Albert Nguyen, who assisted ENISA in the preparation of this report.

We are very grateful to all the experts who took the time to complete the online survey.

We would also like to acknowledge the experts who participated in the telephone interviews and contributed to the validation of the report:

Remi Van De Calseijde (Liberty Global), Joerg Robel (Head of Corporate Security / Integrity Services Telefónica Germany), Nicolas Marcarian (Analyste Investigations Fraude et Affaires Publiques, Bouygues Telecom, France), Laura Bongiorno (Security & Fraud Manager, FastWeb, Italy), Peter Krogos (WIND Hellas), Nikos Niskopoulos (Information Security and Data Protection Officer, Vodafone Greece), Ignace Vanoverschelde (Proximus, Belgium), Frédéric Perrot, Laurent Papillon (Orange France), Wittfoth, Mark, Rosal Cosano, Jorge (European Cybercrime Centre (EC3), Europol), Fraud and Security Team of GSMA, Francesco Bernabei (AGCOM, Italy)

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN: 978-92-9204-539-5 DOI: 10.2824/252043

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Subscriber Identity Module (SIM) swapping is a legitimate procedure performed by a customer to change their SIM card when:

- the SIM card has been lost, damaged or stolen; or
- they change to a new device with another SIM card format or
- they move to another provider – number portability

Attackers abuse the providers' ability to quickly and seamlessly port a telephone number to a device containing a different subscriber identity module (SIM). As a result, the attacker takes over the account and can receive all the SMS and voice calls intended for the legitimate subscriber. Fraudsters can perform online banking frauds but also circumvent the two-factor authentication (2FA) used to secure social media and other online accounts.

In this study, we give an overview of how this attack works, list measures that providers can take to mitigate the attack and make recommendations for policy makers and authorities in the telecom sector and other sectors.

Since 2017 there have been several media reports about SIM swapping attacks, targeting people within the cryptocurrency community[1, 2] but also bank accounts [3] and social media and email accounts[4].

To avoid being vulnerable, the subscribers should restrict their personal information exposed on social media, update passwords regularly, never open messages and attachments from unknown sources, frequently check their financial statements and avoid associating their phone number with sensitive online accounts. If possible, other authentication mechanisms available should be chosen. For more information check ENISA leaflet – How to avoid Mobile SIM Swapping

Mobile Network Operators (MNOs), banks and authorities have already been collaborating to mitigate fraudulent SIM swapping. Banks can use an Application Programming Interface (API) provided by the MNOs to check whether a SIM swap has been recently performed.

- MNOs should reinforce fraudulent SIM swapping detection and blocking mechanisms, by enhancing the internal processes to provide the customer with a preferably seamless experience.
- Banking institutions should consistently apply the EU regulations such as the Directive (EU) 2015/2366 (PSD2), and take advantage of the available technical solutions provided by the telecommunications operators.
- Finally, national authorities should encourage and enhance coordination between the MNOs and the banking sector. Cooperation with Europol and national Computer Security Incident Response Teams (CSIRTs) and law enforcement agencies should also be promoted. Basic guidelines could be issued to efficiently direct operators, banks and the public.

[1] https://www.zdnet.com/article/wave-of-sim-swapping-attacks-hit-us-cryptocurrency-users/
[2] BlockFi discloses failed hack attempt after SIM swapping incident | ZDNet
[3] https://www.telegraph.co.uk/news/2019/11/30/bank-customers-lose-91-million-five-years-sim-swap-scams/
[4] https://www.nytimes.com/2019/09/05/technology/sim-swap-jack-dorsey-hack.html

1. INTRODUCTION

1.1 POLICY CONTEXT

Promoting the interests of the citizens and consumers of the European Union constitutes one of the general objectives set out in Article 3, paragraph 2 of the new EU telecom security legislation: the European Electronic Communications Code[5] (the 'EECC'):

In the context of this Directive, the national regulatory and other competent authorities as well as BEREC, the Commission and the Member States shall (…)

(d) promote the interests of the citizens of the Union (…) by maintaining the security of networks and services, by ensuring a high and common level of protection for end-users through the necessary sector-specific rules.'

The EECC contains specific security requirements for electronic communication providers, including aspects such as the confidentiality of communications. Most of the security requirements are set out in articles 40 and 41 of the EECC, though its recitals also provide guidance on these requirements. For example, recital 94 requires implementation of the state-of-the-art measures to cover aspects such as handling security incidents, compliance assessments and monitoring.

Furthermore, under the EECC, more communication services are in scope, particularly the so-called Over-The-Top (OTT) communications services, such as Gmail, WhatsApp, and Skype. The EECC aims to protect consumers, irrespective of the chosen communication tool, focusing on the functionality (electronic communication), rather than on the underlying technology or implementation choices[6].

Security of electronic communications networks and services does not only translate to minimising the risk of service deterioration or outage, but also to protecting individual customers, for example against fraud, such as SIM swapping attacks.

1.2 SIM SWAPPING ATTACKS

Similarly, to many other attacks against the confidentiality, integrity and authenticity of electronic communications of individual subscribers, in SIM swapping attacks, the attacker's objective is to gain control of the targeted subscriber's mobile account in order to perform a range of actions associated with his mobile number. This type of attack takes advantage of the ability of the MNO to transfer a mobile telephone number to a different SIM, a procedure referred to as 'number porting'. The attacker's objective is therefore to take over a mobile subscriber's account by changing the affiliation of that account from the original SIM card to a SIM card under the attacker's control.

The attacker typically begins a SIM swapping attack by gathering personal details about the targeted subscriber, for example through social engineering, phishing, malware, exploiting information from data breaches or doing research on social media. Once the attacker has obtained enough details to impersonate the targeted subscriber, he may be able to convince the MNO to port the subscriber's mobile number to a new SIM card under the attacker's control.

5 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, OJ L 321, 17.12.2018, p. 36

6 See, for example, rec. 95.

Should this initial part of the attack be successful, the genuine subscriber's SIM card will lose connection to the network. This will enable the attacker to receive all the SMS and voice traffic intended for the targeted subscriber, such as one-time passwords (OTPs) sent by text or telephone calls, for example to log into online banking.

The subscriber may discover he has become victim of a fraudulent SIM swap once he is unable to place or receive calls and SMS, or access his email or social media accounts.

Law enforcement agencies, MNOs, financial institutions and academia have been working on addressing the problem of fraudulent SIM swapping, including launching awareness campaigns.

1.3 TARGET AUDIENCE

This paper strives to provide guidance to national authorities supervising the implementation of Article 40 of the EECC. It may also be useful for experts working in the EU telecom sector.

1.4 PREPARATION OF THIS REPORT

The study presented in the report is using a three-tiered methodology consisting of:

- desktop research taking stock of relevant literature on the topic.
- online surveys disseminated to EU MNOs and national competent authorities, which was answered by 48 MNOs from 22 different countries and by 14 national competent authorities.
- 11 targeted interviews: 8 interviews with MNOs, 2 with Europol and GSMA experts and 1 with a national security authority representative.

The information derived from the first two steps of the process was used in order to prepare and further customize the subsequent step. The information collected was analysed, and consolidated in order to provide tangible results in line with the purpose of this study. The report was validated with the survey participants and the members of the European Competent Authorities for Secure Electronic Communications Group (ECASEC EG).

Figure: Methodology of the study

2. SIM SWAPPING – A LEGITIMATE CUSTOMER REQUEST

In order to provide an overview of the SIM swapping process, we begin by briefly describing its key component: the SIM or the embedded subscriber identity module (eSIM).

The SIM is an application hosted on a piece of hardware called the universal integrated circuit card (UICC), which contains a chip. The SIM contains an identity that unambiguously identifies a subscriber within an MNO's network. The term 'SIM card' is commonly used when actually referring to the UICC. Therefore, for simplicity, we will use the term 'SIM card' instead of 'UICC' throughout this report.

The eSIM is the embedded form of the SIM, meaning the eSIM does not exist physically on a device but is virtual. The eSIM is hosted on an 'embedded Universal Integrated Circuit Card' (eUICC).

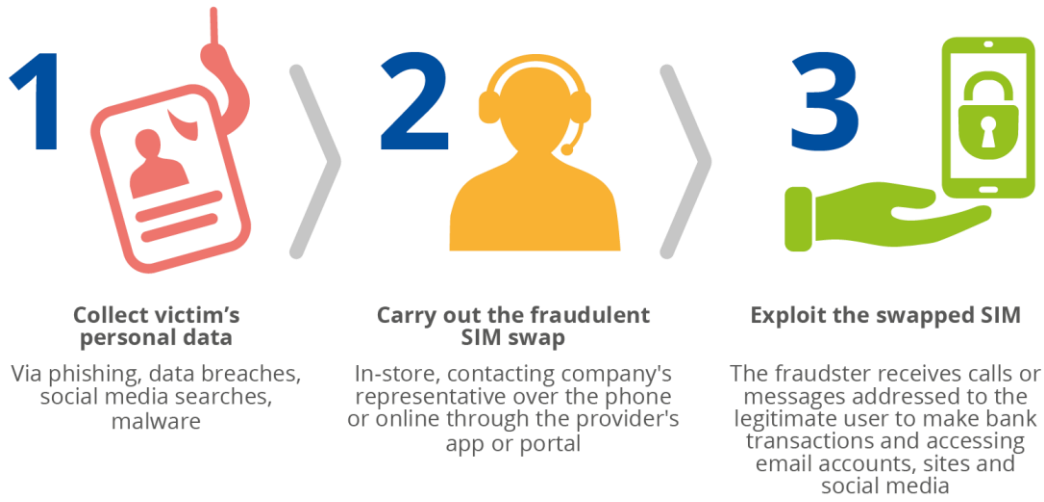
SIM swapping is a legitimate procedure performed by a subscriber to change his SIM cards, for example when:

- the SIM card has been lost, damaged or stolen; or
- the subscriber changes to a new device with another SIM card format.

In order to perform the SIM swap, MNOs commonly follow two processes:

- subscribers go to an MNO's retail store or to an automatic machine that distributes SIM cards; or
- subscribers use a remote process, such as an MNO's mobile application, self-care portal or a phone call to a customer care service.

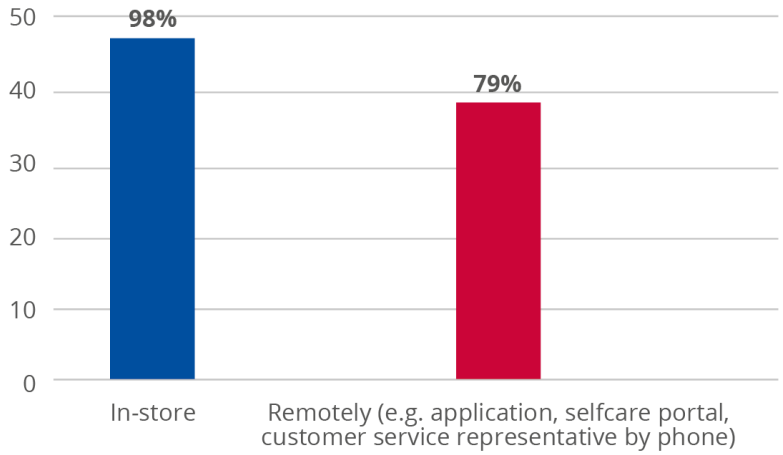
Figure 1: How a SIM Swapping attack is performed



2.1 SIM SWAP INITIATION

Almost all of the MNOs interviewed have an in-store process for the SIM swap (98% of the respondents). The majority of them also have a remote process in place (79% of the respondents):

Figure 2: SIM swapping initiation process



Whichever process is pursued, customer authentication constitutes its key component. It can be done either physically (in-store) or remotely.

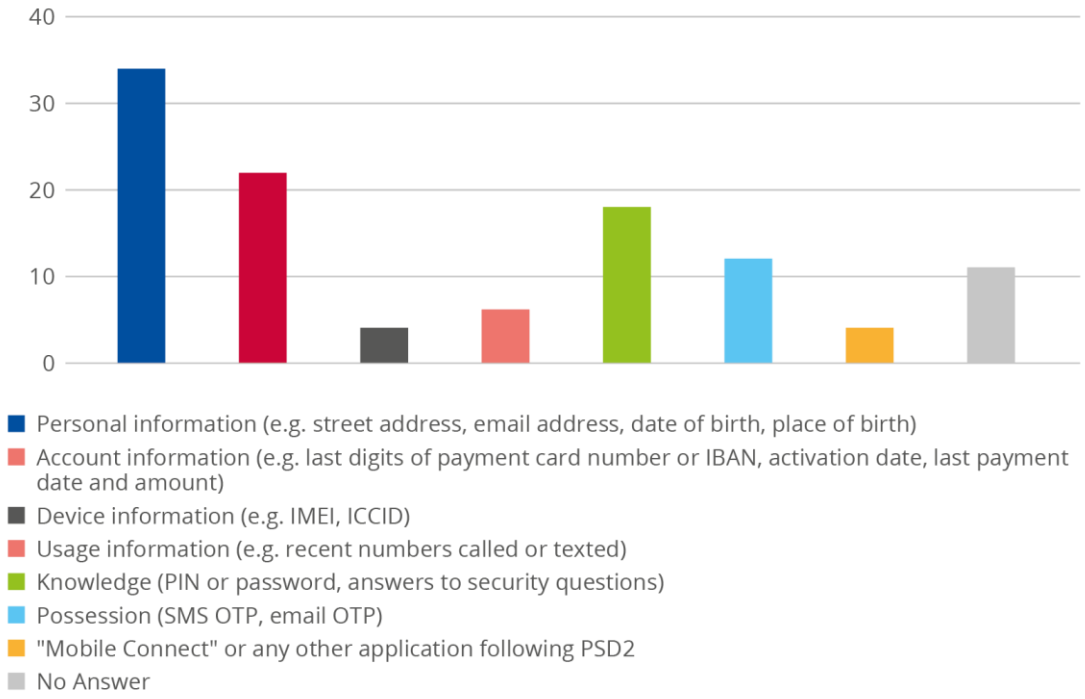
In-store subscriber authentication mostly relies on an ID check, while in case of remote authentication MNOs use several mechanisms[7], including:

- personal information (e.g. postal address, email address, date and place of birth);
- account information (e.g. last digits of payment card or international bank account number, activation date, last payment date and amount);
- device information (e.g. International Mobile Equipment Identity - IMEI, Integrated Circuit Card Identifier-ICCID);
- usage information (e.g. recently called or texted Mobile Station International Subscriber Directory Number (MSISDN));
- secret information (e.g. personal identification number (PIN) or password, answers to security questions);
- a 'possession' element (e.g. SMS OTP, email OTP);
- any application following Directive (EU) 2015/2366 (the revised payment services directive (PSD2)), such as Mobile Connect;
- biometrics; or
- call-back procedures.

Most MNOs indicated using personal information to authenticate subscribers over the phone, with the next-largest numbers using account information and secret information.

[7] Subscriber authentication method could also depend on the reason for the SIM swap. For example, number portability procedure usually has defined checks. Furthermore, a SIM swap request following a device theft may have different security controls in place than those used for a SIM swap request when needing a different SIM card formats.

Figure 3: Information used by the mobile network operators to authenticate the customers



2.2 SIM SWAP FINALISATION

The 'physical' finalisation process can be deployed in several ways:

- in-store finalisation:
    - the customer is requested to go to the MNO's retail store to receive either the physical SIM card or a quick response (QR) code to activate the eSIM;
    - alternatively, the customer may be requested to go to an automatic machine distributing SIM cards.
- postal service finalisation: either the physical SIM card or the QR code to activate the eSIM is delivered to the declared customer's postal address.

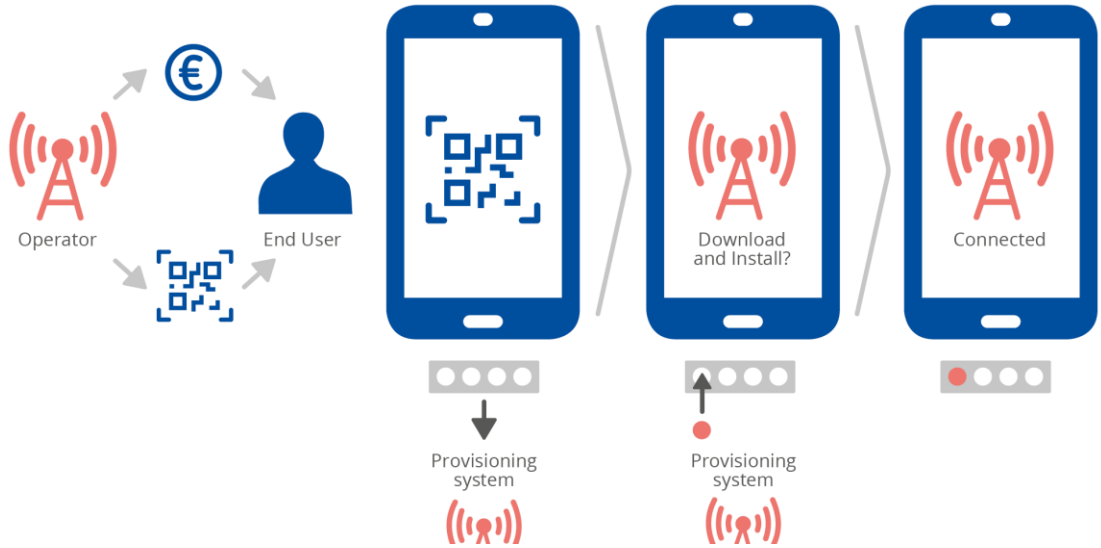
In cases of eSIMs, following a subscriber's SIM swap request via the MNO's self-care portal, the swap is usually finalised remotely by sending a QR code by email or by SMS to the customer's old device.

The subscriber scans the QR code with the new device, which supports the eSIM technology. This QR code contains the relevant information to connect to the MNO's network (e.g. subscription manager data preparation+ address – SM – DP+ address) and will download the customer's profile to the new device. The subscriber validates the activation of the eSIM on the new device.

The subscriber scans the QR code with the new device, which supports the eSIM technology. This QR code contains the relevant information to connect to the MNO's network (e.g. SM-DP+ address – Subscription Manager-Data Preparation+) and will download the customer's profile to the new device. The subscriber validates the activation of the eSIM on the new device.

Alternatively, activation of the eSIM could be requested of the provider's customer service by phone.

Figure 4: eSIM generic activation process



Source: https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf

3. SIM SWAPPING ATTACKS IN EUROPE

In order to create an overview of the attack methods and possible mitigation measures, the survey disseminated to the MNOs included questions regarding:

- statistics on SIM-swapping attacks (i.e. volumes and trends);
- processes used by the MNOs to swap customer SIMs;
- the services affected in the event of a SIM swap fraud;
- the perception of the SIM-swapping risk and some mitigations already put in place by the MNOs;
- communication with the customers and the relevant national authorities.

Numbers of fraudulent SIM swaps vary across countries and MNOs

48 MNOs from 22 countries across Europe responded to the online survey. Almost half of the MNOs surveyed (48%) did not face any SIM swapping incidents in the 12 months prior to the survey.

Figure 5: MNOs and countries represented in the online survey

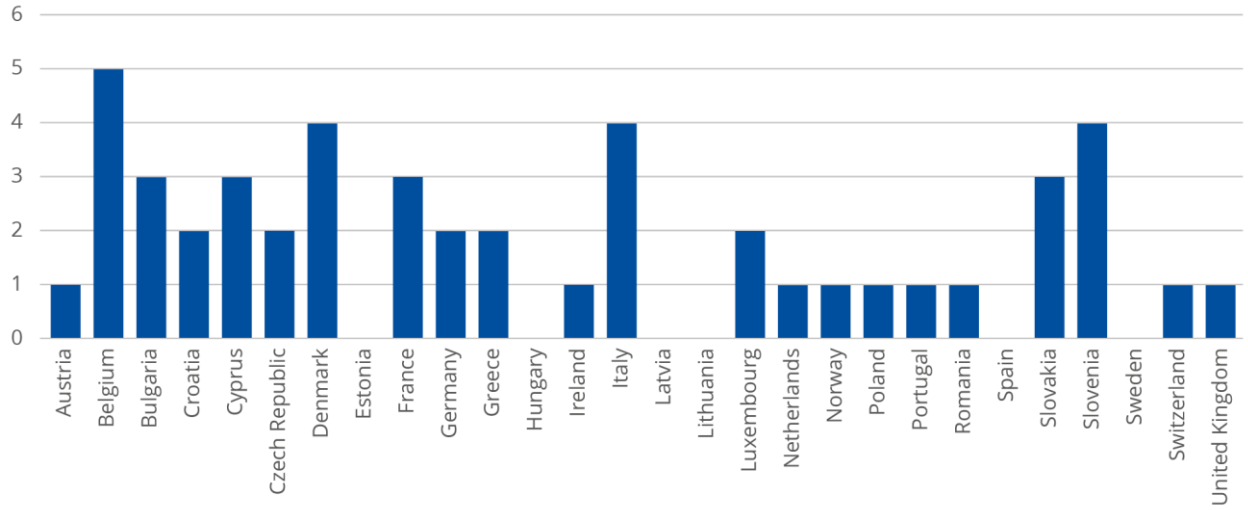
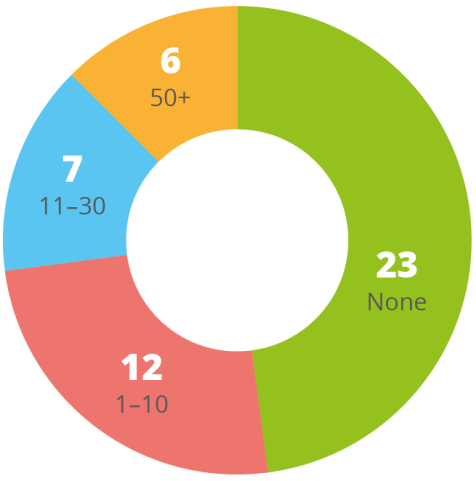
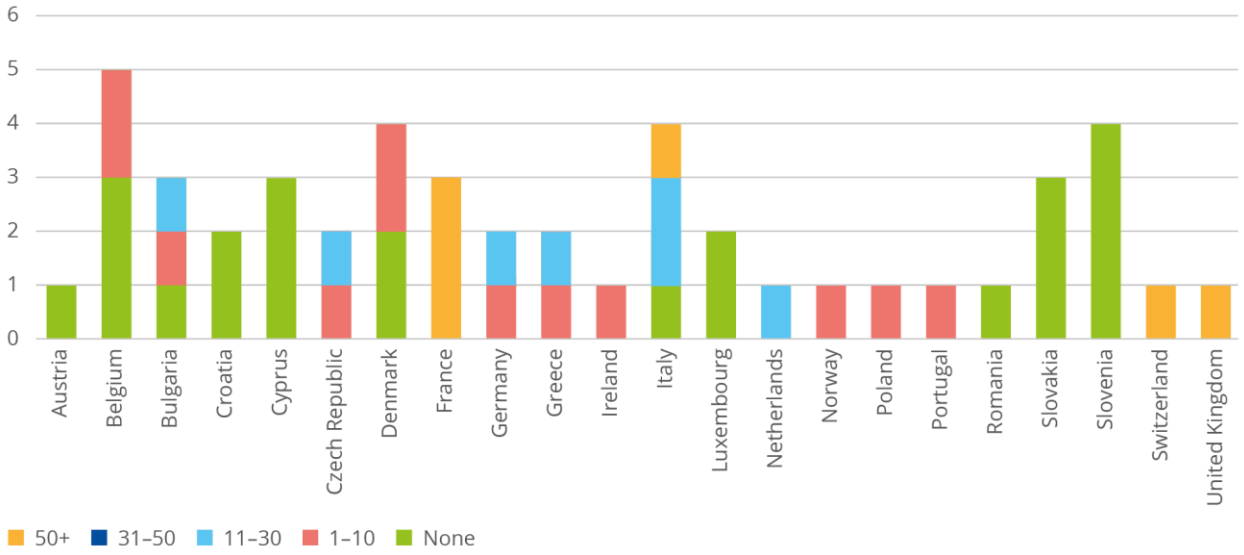


Figure 6: Number of MNOs and volume of SIM swapping incidents



Furthermore, as depicted in Figure 7, the number of SIM swapping incidents varies substantially across European countries. Based on our survey, in some countries (France, Switzerland, the United Kingdom), over 50 fraudulent SIM swapping incidents were reported per MNO, whereas in other countries MNOs have not reported SIM swapping frauds at all (Austria, Croatia, Cyprus, Luxemburg, Romania, Slovakia, Slovenia). It should be noted, however, that the number of fraudulenSIM swapping cases may be correlated to the MNO's customer base.

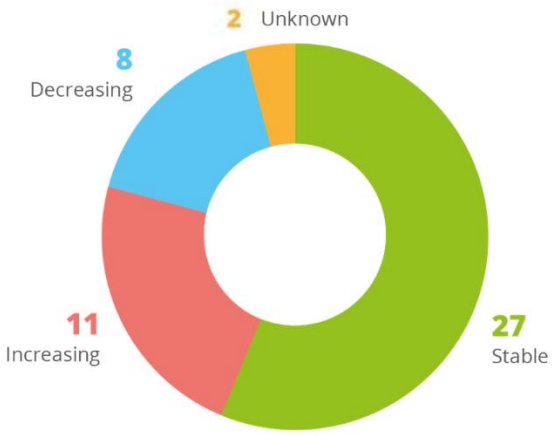
Figure 6: Distribution of the fraudulent SIM swapping incident volume per country/mobile network operator



How to read Figure 6: The vertical axis shows the number of MNOs that took part in the online survey, while the horizontal lists the countries. In Italy, for instance, four MNOs responded to the survey. Among those four, one did not face any fraudulent SIM swapping incidents (green bar), while two faced between 11 and 30 incidents (red bar) and one faced more than 50 (yellow bar).

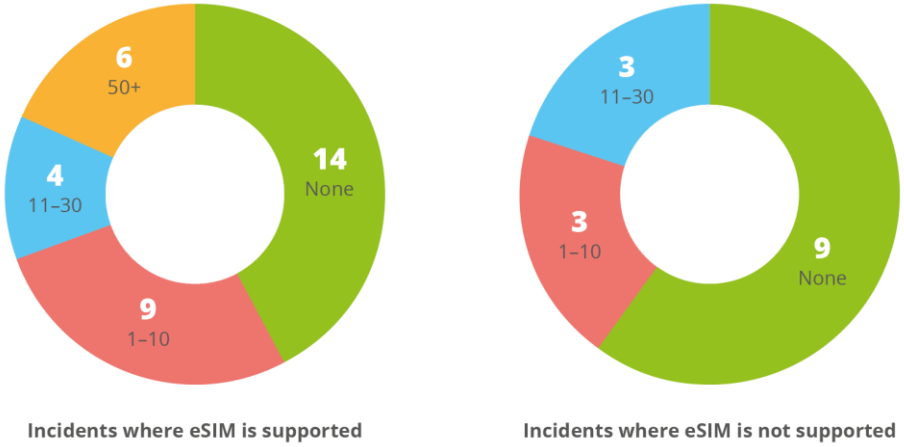
More than half of the MNOs (56 %) reported that the numbers of SIM-swapping frauds are stable, that is, not increasing or decreasing:

Figure 7: Distribution of fraudulent SIM swapping incidents trends per mobile network operator



We can note, however, a positive correlation between the use of eSIMs by MNOs and the number of reported SIM-swapping incidents. For example, six MNOs with eSIM services reported more than 50 SIM-swapping incidents during the previous year, whereas MNOs that do not have eSIMs deployed reported a limited number of fraudulent SIM-swapping cases.

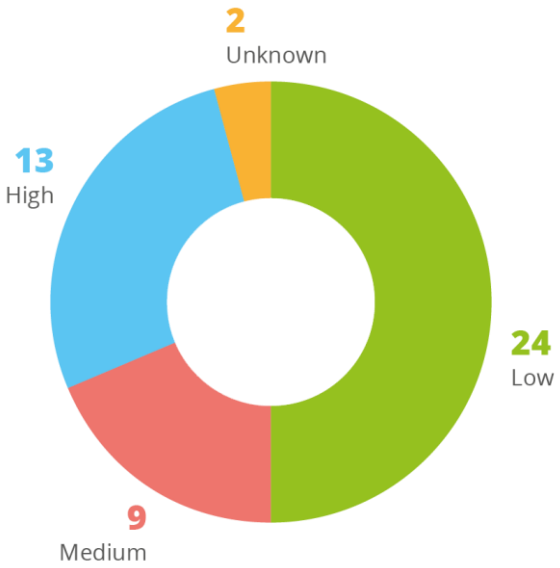
Figure 8: Correlation between eSIM use and the volume of SIM swapping frauds



As noted in the interviews, in France, before it applied strict mitigation solutions, 6–7 % of eSIM swap attempts were fraudulent. It should be stressed, however, that the growth in fraudulent eSIM swaps is not due to a lack of security of the eSIM technology, but one reason behind these figures could be that the eSIM swap processes employed by some MNOs are still relatively new.

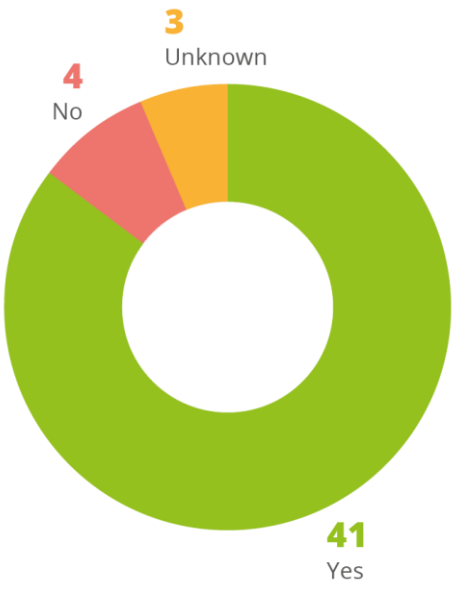
As shown in Figure 10, the majority of MNOs perceive the level of SIM-swapping fraud risk as low.

Figure 9: SIM swapping risk assessment



This could be either because most MNOs have not faced any fraudulent SIM-swapping incidents lately or because they perceive their SIM-swapping processes as strong enough to avoid such incidents.
As reported in our survey, almost all MNOs deployed risk mitigation measures to prevent SIM-swapping frauds (Figure 10).

Figure 10: Deployment of SIM swap fraud risk mitigation measures



3.1 PERFORMING THE ATTACK

3.1.1 Step 1 – accessing the subscriber's personal data

In order to perform a fraudulent SIM swap, the fraudster needs to have access to some of the subscriber's personal data. This is because specific personal details are typically requested by the MNO for authentication purposes, as part of the SIM swapping procedure.

Table 1 provides a brief description of potential methods used by attackers in order to obtain personal data, which can be used to facilitate fraudulent SIM swapping.

The estimated likelihoods provided in the table are subjective and based on the experience of the MNOs interviewed.

Table 1: Accessing the subscribers' personal data

Obtaining access to subscribers' personal data	Description	Estimated likelihood
Social Engineering on Customers (Phishing)	Customers might be contacted by fraudsters using SMS, email, social media messaging or phone calls, impersonating an MNO's or other type of service provider's employee in order to retrieve their personal information (e.g. name, date and place of birth, postal address and bank account identifier), including subscriber's credentials to the MNO's online portal	**HIGH**
Social Engineering on Mnos' Employees (Phishing)	MNOs' employees might be contacted by fraudsters using SMS, email, social media messaging or phone calls. The goal is to retrieve personal information regarding a customer (e.g. name, date and place of birth, postal address and bank account identifier)	**MEDIUM**
Bribing or Threatening Mnos' Employees	MNOs' employees might be bribed or threatened to give away personal information of the targeted customer. Furthermore, in February 2021, an employee of a telecommunications operator was charged with accepting a bribe from fraudsters who stole cryptocurrencies (*)	**LOW**
Cyberattacks on Infrastructure	Fraudsters might lead cyberattacks on MNOs' infrastructure (e.g. IT Systems, network) in order to retrieve personal data or hack subscribers' online accounts	**LOW**
Placing Fraudsters in Stores or Customer Care Centres	MNOs' employees become accomplices in fraudsters' activities. They can have easy access to customers' personal information	**LOW**

(*) https://www.justice.gov/usao-edla/pr/former-phone-company-employee-charged-rolein-sim-swap-scam-targeted-least-19-customers

3.1.2 Step 2 – Carrying out a fraudulent SIM swap

Depending on the type of SIM swap (regular SIM swap or eSIM swap), having obtained the necessary personal data and having identified the MNO's SIM swapping process(as described in section 2), the attacker:

- presents falsified identification documents in-store,
- successfully responds to the challenges (authentication questions) presented by the representative over the phone, or
- gains access to the subscriber's account on the MNO's portal, initiates an eSIM swap and then scans the QR code, which is usually displayed on that portal.

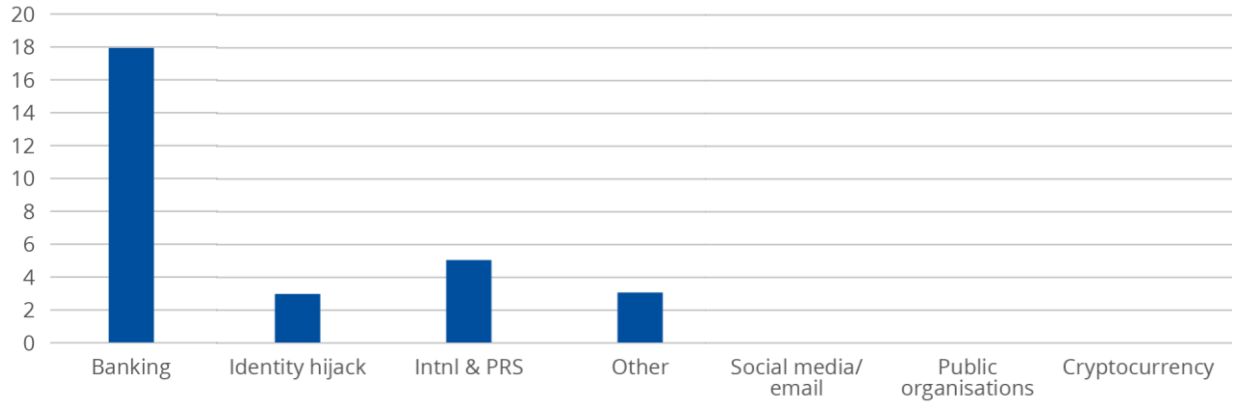
3.2 SERVICES AFFECTED

Intercepting SMSs, including OTPs for financial transactions, is one of the basic goals of the attackers. While attackers may also intercept the OTP SMS using more elaborate attack methods (such as exploiting SS7 protocol vulnerabilities), SIM swapping appears to be the easiest way of intercepting SMS to perform banking frauds, as it does not require complex or expensive technical tools.

In the banking sector, the OTP SMS has been used for more than a decade to authenticate customers when they are shopping online or transferring funds. Most banks make use of two-factor authentication because it adds a cost-efficient and consumer-friendly layer of security to the authentication process behind online banking, while complying with the strong customer authentication rules under PSD2[8].

According to the survey respondents, online banking is the service most affected by fraudulent SIM swapping. As early as April 2016, British media reported a bank account being emptied as a result of a SIM-swapping attack[9]. Less frequently, SIM swaps have also been used for taking over the victims' accounts and for placing international and premium rate service calls.

Figure 11: Customer services affected by fraudulent SIM swapping



Based on our desktop research, the compromise of two-factor authentication and subsequent access to victims' accounts can also enable a number of follow-up crimes:

- Interception of calls and messages – account takeover: the attackers receive the calls and messages intended for their victim, and can also place calls and messages in their stead, since the actual subscriber loses access to the mobile network and services.
- Making international or premium number calls: the fraudster can place calls to international or premium destinations.
- Hacking social media accounts: as some social media accounts also require a phone number to authenticate the customer, the fraudster can log into them in the victim's stead. For example, in August 2018, a number of Instagram accounts were hijacked[10]. Furthermore, in 2019, even the chief executive of Twitter had his Twitter account hijacked by hackers[11].
- Targeting the cryptocurrency community: for example, in May 2020, a cryptocurrency platform disclosed a case in which fraudsters attempted to steal funds from the platform's users [12].

[8] https://ec.europa.eu/commission/presscorner/detail/en/QANDA_19_5555
[9] https://www.theguardian.com/money/2016/apr/16/sim-swap-fraud-mobile-banking-fraudsters
[10] https://mashable.com/2018/08/13/instagram-hack-locked-out-of-account/?europe=true and https://www.wired.com/story/sim-swap-attack-defend-phone/
[11] https://www.theguardian.com/money/2020/sep/13/sim-swap-is-on-the-rise-how-can-you-stop-it-happening-to-you
[12] https://www.zdnet.com/article/blockfi-discloses-failed-hack-attempt-after-sim-swapping-incident/

4. RECOMMENDATIONS

4.1 FOR MOBILE NETWORK OPERATORS

Stricter controls for customer authentication and SIM swaps

Measures that can be applied to mitigate the attack include internal checks on aspects such as limiting staff access to customer information and the ability to perform SIM swaps; back-end system validations before executing changes; enforcement of time-based restrictions on account changes; checks, based on location of subscriber; notification of changes to customers (call-back verification); and the use of passwords and PINs by customers to access their accounts.

Performing background checks on the subscriber using a back-office team could also prove to be an effective countermeasure. Such background checks could include checking the most recently provided postal address, cross-checking the ID card presented in store with previous copies maintained under the subscriber's profile and examining the customer's recent contacts with customer representatives.

Regular and targeted training of employees

While technical controls can minimize the risk of SIM swapping, the human factor is the one that needs to be constantly managed.

According to the ENISA Threat Landscape 2020 [13], 84 % of cyberattacks rely on social engineering. As highlighted in this report, SIM swapping relies greatly on social engineering of MNOs' employees (see Table 1).

MNOs should provide regular cybersecurity awareness training for both their own and third-party employees to ensure they can recognise and appropriately deal with the SIM-swapping threat. The security awareness programme should be tailored to the audience and focused on the specific topic. For example, employees should know and understand how spear phishing and other social engineering attacks work, what they should take into account when authorising a SIM swap and the actions they should take to minimise the risk of fraud.

There should be well-documented and checked processes that are regularly communicated and followed with vigilance. Moreover, records of the training courses and those who attended should be maintained.

API between Mobile Network Operators and banks

Several initiatives have been launched across Europe for wider cooperation between the MNOs and banks. Specifically, banks can use an application programming interface (API) provided by the MNOs to check whether a SIM swap has been recently performed.

Such an API has been developed in several EU countries as a cross-MNO initiative. In Italy, for instance, the national regulatory authority, AGCOM ([14]), has been coordinating a trial in which participated representatives of the Bank of Italy, the Italian Data Protection Authority, the Ministry of Economic Development, the police (including financial police), banks, operators that offer messaging services to the banks and MNOs. The trial involves MNOs informing banks of

[13] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents
[14] https://www.agcom.it/

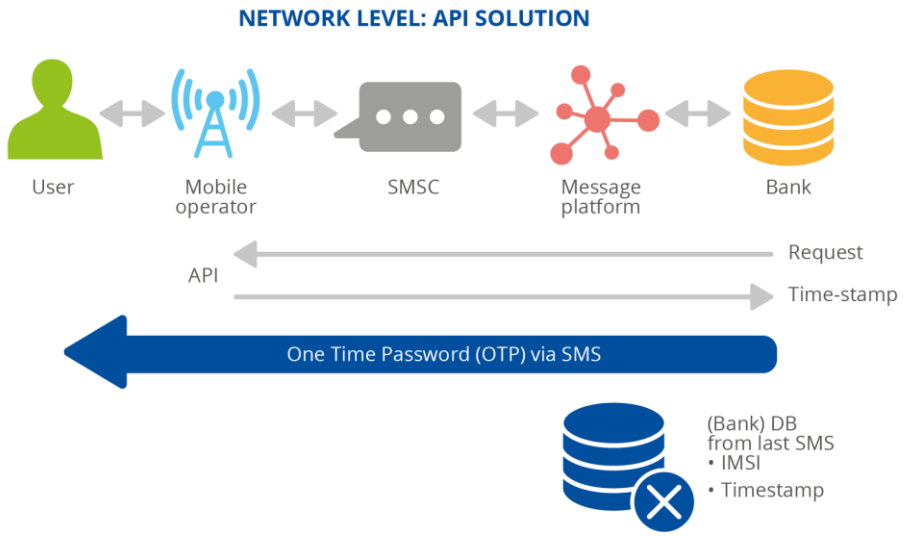
the latest SIM swap, either through the subscriber's IMSI or hashed IMSI or by sending information about the time of the latest SIM swap.

In summary, the API works as follows.

- **Step 1:** the customer initiates a fund transfer on their mobile banking application or on a computer.
- **Step 2:** the bank interrogates the customer's MNO's database through an API.
- **Step 3:** the customer's MNO checks whether a SIM swap has recently occurred on the customer's MSISDN. Alternatively, the bank sets the timing threshold (e.g. 24 hours) and the MNO responds if a SIM swap occurred in less than the timing threshold.
- **Step 4:** if no recent SIM swap has been detected on the customer's MSISDN, the customer's MNO communicates this piece of information to the bank as a response in the API.

  If a recent SIM swap has been detected on the customer's MSISDN, the information is sent from the MNO to the bank and the bank performs additional checks in order to authorize the transaction.
- **Step 5:** the bank can proceed with the fund transfer following the bank's process (e.g. sending an OTP SMS to the customer).

Figure 12: API check process for a legitimate banking transaction



Instead of using an API, two other alternatives have also been considered:

- The MNO sends to the bank the timestamp of the most recent SIM Swap through the SMPP protocol, after having received a relevant request from the bank.
- The MNO provides the customer's IMSI (or hashed IMSI), using the standard protocol – SS7/MAP (through the answer to Send request Info For SM)

In Annex A, are presented in more detail the alternatives used for communication of the sim swap information from the MNOs to the banks.

Avoid remote SIM swapping processes

According to the MNOs interviewed, regardless of the initial request (in store or remote), SIM-swapping frauds are usually avoided when a physical finalisation process is set up. Therefore, if there is no solution deployed for strong remote customer authentication, the best solution is to have a mandatory in-store SIM swap procedure, or to perform the finalisation of the process using regular post (e.g. recorded delivery). We note that these solutions also require designing specific, well-thought-out processes for authenticating the customer and verifying their postal address.

For example, interview respondents highlighted that attacks were successfully prevented with the use of alerting mechanisms in the shops' network in case of suspicious SIM swap attempts. For example, in the event of a failed attempt at a fraudulent SIM swap in a retail store, the targeted MSISDN is flagged and the neighbouring retail stores are alerted.

In countries where ID cards are still in paper format without any embedded security measures, machine-based verification of the identity documents presented is more effective in recognising counterfeit versions.

Naturally, using the postal service to deliver the new SIM card to the customer entails longer waiting periods for the conclusion of the SIM swap procedure.

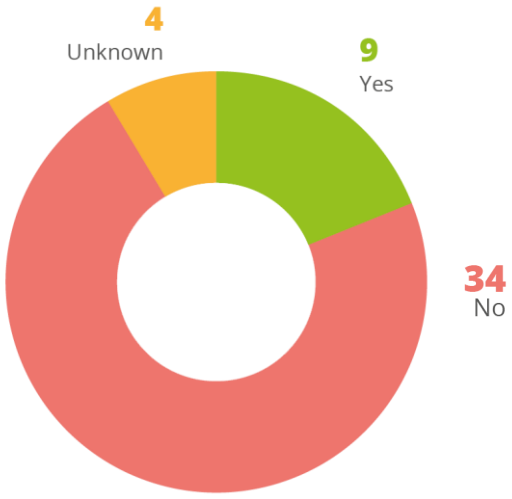
Reach out to the public

Conducting public awareness campaigns, informing subscribers about the threats, advising them on when to spot a potential incident and proposing simple mitigation solutions could contribute greatly to reducing the number of attacks and minimising their impact.

Awareness campaigns could be generic (a post on the MNO's website or social media account, a TV/radio spot) or more targeted communication could be employed (e.g. sending SMS and emails to all subscribers).

The majority of the survey respondents (i.e. 72 %)[15] noted that they had not yet communicated on this topic to their customers.

Figure 13: Subscriber communications



[15] Please note that this percentage is calculated excluding 1 MNO that did not provide a response

Restrict the provision of 'empty' SIM cards

During our research, we came across fraud cases with the attacker using an inactive SIM card and managing to perform a fraudulent SIM swap.

To address this threat, MNOs could consider not authorising SIM swaps without knowing the origin of the new SIM card. SIM cards should be provided only through the MNOs' logistics centres, while usage of existing stocks at the subscriber's disposal should be discouraged.

Additional internal controls may be implemented within the mobile network operators:

- keeping an inventory of the blank SIM cards;
- strong controls on the issuance and activation of blank SIM cards; and
- activation of the SIM cards only when the order and/or delivery is confirmed by the customer.

Artificial intelligence and behavioural analysis

Artificial intelligence (AI) may be used to perform automatic behavioural analysis of subscribers' activities. The AI engine could store several habits of each customer (e.g. connection history, IP addresses' locations) in order to have a basis for comparison at the time of a requested SIM swap.

If abnormal behaviour is detected (e.g. sudden change of the IP address location, several concurrent connections from different IP addresses), the MNO is alerted in real time in order to block the SIM-swapping process.

However, the use of AI for detecting fraudulent SIM swaps should be very carefully applied, considering the regulatory context in the light of confidentially of communications data and personal data protection. Specific guidance from the competent authorities, review mechanisms and strong controls are necessary to avoid unnecessary retention and analysis of communication and personal data.

4.2 FOR THE BANKS

API between MNOs and banks

Banks have the possibility to check whether a SIM swap has been recently performed with the use of an API provided by the MNOs. We discuss the use of such APIs in section 4.1 of this report.

Migrate from SMS two-factor authentication to app-based two-factor authentication

The latest banking frauds related to SIM swapping suggest that SMS two-factor authentication (2FA) may not provide a sufficient level of security.

App-based 2FA relies on biometric, PIN or password-based authentication of the customer, and thus does not pose a risk of the SMS OTP being intercepted. We note that such app-based 2FA is already used by many banks to authorise transactions, replacing the SMS 2FA process.

Reach out to the public

Banks, along with the MNOs, can carry out awareness campaigns towards their customers, in order to warn them about SIM-swapping attacks. For example, Alpha bank Greece has developed a web page including information on the SIM Swapping fraud. In this page, the bank explains how the fraud works, and includes advice for the clients to self-protect. On its website,

the bank also lists measures it takes to mitigate the risk of sim swapping frauds[16]. Similarly, Bank Millennium in Poland warns its customers against SIM swapping attacks[17].

We also provide more general examples of consumer outreach activities performed by banks in our upcoming report entitled 'Cybersecurity Outreach About Cybersecurity Threats by Telecom Providers'. For example, on their websites, banks already advise of some of the latest types of fraud (such as delivery and cryptocurrency scams), the steps customers can take when they feel they may become victim of one, and the channels they can use to contact the bank. Analogous information could be provided to decrease the risk of successful SIM swapping attacks.

4.3 FOR THE NATIONAL AUTHORITIES

Guidelines for secure authentication

Customer authentication is at the heart of the SIM swapping process, no matter the channel used (e.g. store, phone, chat bot, mobile application).

Competent authorities could contribute to fulfilling this objective by issuing appropriate guidelines for the MNOs. Specifically, they could recommend putting in place a set of challenges for subscribers initiating a SIM swapping process. This list of mandatory challenges could be different from one MNO to another, but the competent authority could nevertheless consider recommending a basic common set of challenges used in the SIM swapping process.

In this context, the Italian competent authority, AGCOM, carried out a public consultation on increasing security on the part of the customer as well in all cases of SIM swaps, including mobile number portability. This could also be useful in mitigating the attack in cases other than banking fraud.

The new regulation following the consultation is included in Deliberation No 86/21/CIR[18]. Mechanisms have been introduced to prevent and combat fraud attempts, including by modifying the law on mobile number portability. The user will be able to confirm to the MNO that it should continue the SIM card replacement (or portability) process, or instruct it to stop.

SIM swapping process assessment

The competent national authorities may perform ad-hoc audits to examine the existing SIM swapping processes employed by the MNOs and assess whether they are secure and actually followed by the MNOs' employees.

Providing recommendations to enhance specific processes could contribute to the mitigation of the threat.

Promoting communication and active collaboration among stakeholders

Establishing frequent communication between public authorities, MNOs and banks, sharing general information about incidents and discussing fraud prevention measures could all significantly contribute to building up risk mitigation know-how.

Furthermore, launching intuitive public awareness campaigns could contribute greatly to decreasing the threat of attacks occurring and minimising their impact.

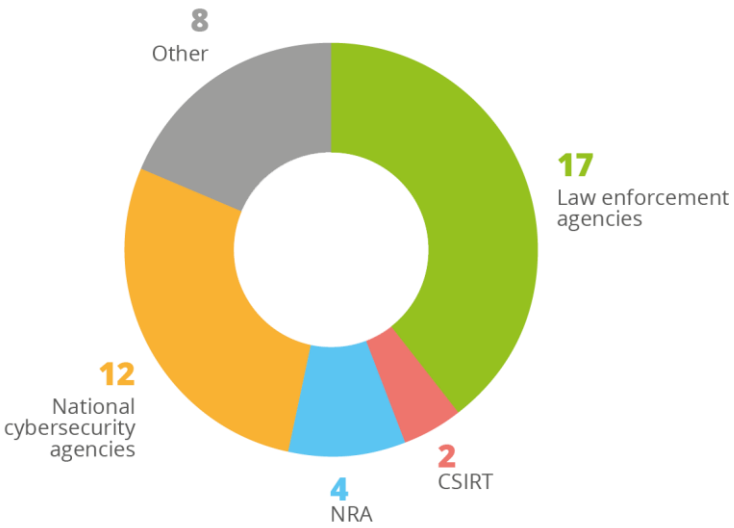
16 https://www.alpha.gr/en/retail/support-center/security/apati-sim-swapping

17 https://www.bankmillennium.pl/bankowosc-elektroniczna/bezpieczenstwo.

18 https://www.agcom.it/documentazione/documento?p_p_auth=fLw7zRht&p_p_id=101_INSTANCE_FnOw5lVOIXoE&p_p_lifecycle=0&p_p_col_id=column-1&p_p_col_count=1&_101_INSTANCE_FnOw5lVOIXoE_struts_action=%2Fasset_publisher%2Fview_content&_101_INSTANCE_FnOw5lVOIXoE_assetEntryId=23785406&_101_INSTANCE_FnOw5lVOIXoE_type=document

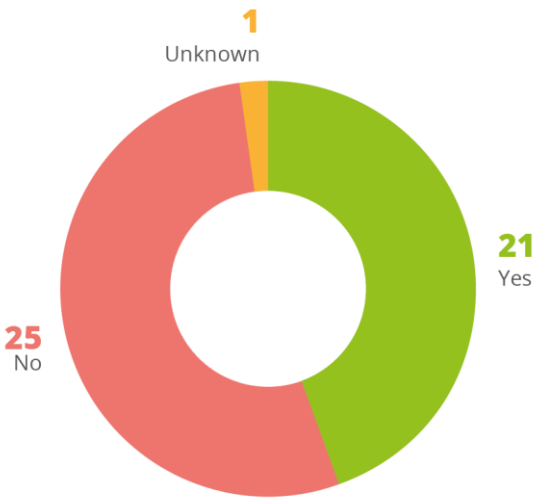
Specifically, regarding general communication with the relevant national authorities, the survey respondents said they communicated mostly with the local law enforcement agencies (40 %) followed by the national cybersecurity agency (25 %). It should be noted however, that the response provided by 5 MNOs was “I don’t know” and wasn’t considered in the respective percentages and graph.

Figure 14: Communication with the national competent authorities



However, more than half of the MNOs who responded to the online survey (53%)[19] noted that they did not share any information on specific SIM swapping incidents with their competent national authority.

Figure 15: MNOs sharing information on SIM swapping incidents with the competent National Authority



[19] Please note that this percentage is calculated excluding 1 MNO that did not provide a response

4.4 FOR THE PUBLIC

Warning Signs and recommended steps to minimize impact

The first sign of potentially falling victim to a fraudulent SIM swap is an **inexplicable and more than momentary loss** of mobile network access.

In this case, subscribers are strongly recommended to **contact their MNO** without any delay.

Also, subscribers are recommended to **check their banking transactions frequently** for any suspicious activities and, if there are any, **contact the bank and their MNO immediately.**

Finally, subscribers should act fast in case of any **unrecognized activity in their social media or email accounts**. They should **contact their MNO** and **change their account passwords**.

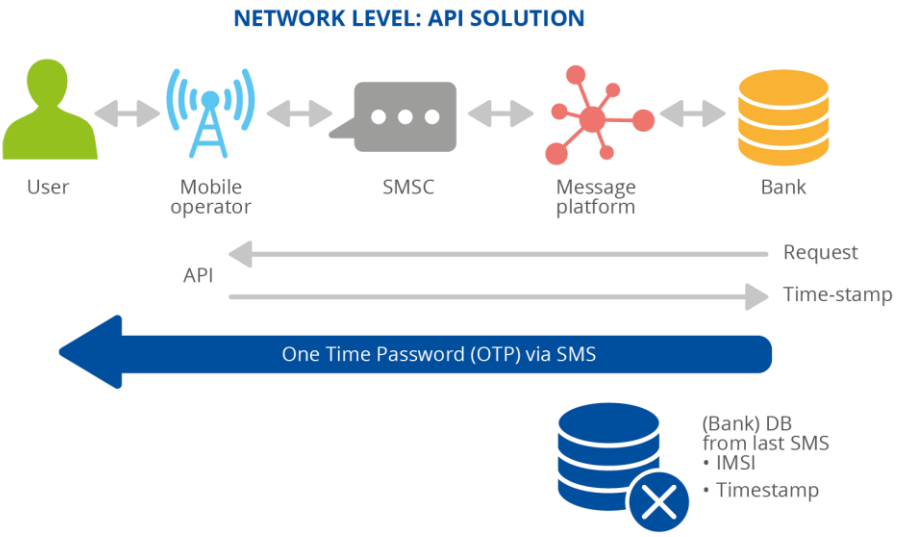
Generic self-protection advice

SIM-swapping fraud usually begins with phishing and/or social engineering against subscribers. To avoid phishing attacks subscribers should take the following precautions.

- Be cautious with the information shared on social media networks.
- Never open any suspicious internet hyperlinks or attachments received through email or messages.
- Avoid providing any personal information by email or by phone when called by someone claiming to be the MNO's representative. A real customer representative will never request personal details such as credit card details or 2FA SMS content. In some cases, MNOs can send an OTP SMS for finalising a SIM swap. This OTP password must never be communicated to anyone, even to persons who call the customers and claim to be an MNO's employee.
- Update account passwords on a regular basis.

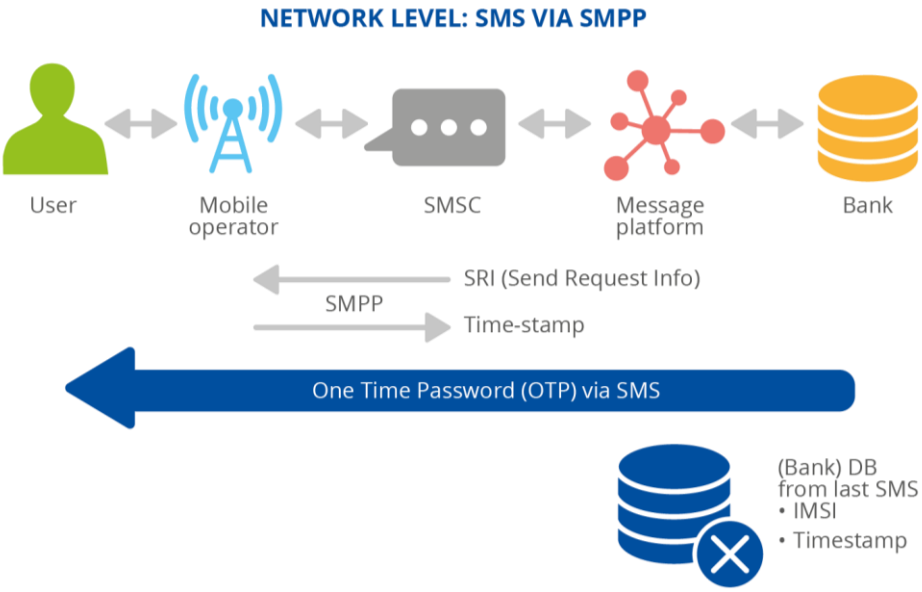
For more information check ENISA leaflet – How to avoid Mobile SIM Swapping

A ANNEX: COOPERATION BETWEEN MNOS AND BANKS

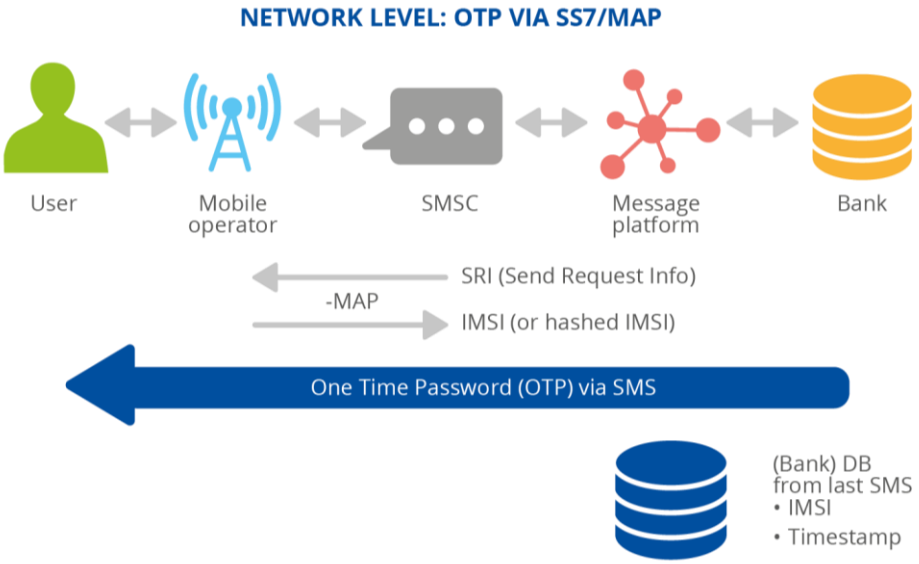
SIM Swap: API solution (timestamp or timing threshold)


Details	Advantages	Drawbacks
Timestamp: MNO provides the date and time of the latest SIM swap (if any) or Timing threshold: bank sets the timing threshold (e.g. 24 hours) and the MNO responds if a SIM swap has occurred within the timing threshold. The OTP is sent only if the SIM swap has occurred within the threshold	The bank has no need to store further personal data in a database. There is no need to maintain information on the timestamp received. All changes of IMSI are detected.	Requires software which works in real time

SIM Swap: SMS via SMPP



Details	Advantages	Drawbacks
Time-stamp provides information on how much time has passed since the last SIM swap.	Time-stamp is sent by the MNO to the banks No database for additional personal information is needed.	Operators have to develop the solution.

SIM Swap IMSI or Hashed IMSI		
		
Details	**Advantages**	**Drawbacks**
The MNO provides the customer's IMSI, using the standard protocol – SS7/MAP (through the answer to Send request Info For SM) Hashing has the same characteristics of IMSI and allows avoiding to provide personal data to the banks	No specific development by the mobile network operator: no need to develop API if just IMSI is sent. All changes of IMSI are detected.	Necessity for the bank to create a database for the IMSIs, to be able to compare the received IMSI with the last stored one. If SMS are not frequently sent – information may be not accurate enough. If SMS are too frequent, cost of service may represent an issue. In fact, comparison between IMSIs doesn't not provide the information on when the change occurred. It is required that all operations work on real time. Data protection related restrictions if not hashed IMSI sent May not work with 5G For the MNOs, need for process to communicate IMSIs to the banks Hashed IMSI requires previous development

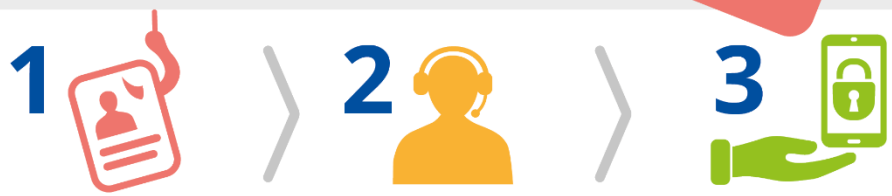
B ANNEX: HOW TO AVOID SIM SWAPPING? - LEAFLET

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

How to avoid
MOBILE SIM SWAPPING?

WHAT IS A SIM SWAPPING ATTACK?

In a SIM swapping attack, an attacker takes over your mobile phone number by asking the mobile telecom provider to link your number to a SIM card under the attacker's control.



Collect victim's personal data
Via phishing, data breaches, social media searches, malware

Carry out the fraudulent SIM swap
In-store, contacting company's representative over the phone or online through the provider's app or portal

Exploit the swapped SIM
The fraudster receives calls or messages addressed to the legitimate user to make bank transactions and accessing email accounts, sites and social media

WHAT ARE THE WARNING SIGNS?

- **Before the attack:** You receive strange phone calls asking you to share codes or SMS messages that you have received from your mobile telecom provider.
- **During the attack:** Your phone loses network connection for a longer period, and you are not able to make or receive phone calls.
- **After the attack:** You may see suspicious transactions in your banking accounts, or lose access to your social media or email accounts, or see other activity you do not recognize.

WHAT TO DO IF YOU ARE A VICTIM?

If you experience any of the above signs, ccontact your telecom provider as soon as possible.

If it confirms the SIM swap, immediately contact your bank and change the passwords to your online accounts. Furthermore, report the fraudulent activity to the police.

HOW TO PREVENT THE ATTACK?

- Avoid providing any personal information to someone pretending to be representative of the telecom provider.
- Never communicate, over the phone, the one-time passwords you receive from your mobile operator.
- Choose app-based 2-factor authentication, instead of two-factor via mobile phone or SMS.
- Be cautious with the personal information that you share on websites and social media.
- Do not open suspicious hyperlinks or attachments received through email or SMS

European Union Agency for Cybersecurity
www.enisa.europa.eu

TP-01-21-353-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-539-5
DOI: 10.2824/252043