EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CYBER THREATS OUTREACH IN TELECOM

Guidelines for national Authorities and telecom providers on outreach to users about cyber threats

MARCH 2022

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, Marnix Dekker

ACKNOWLEDGEMENTS

For the completion of this report, ENISA has worked closely with a working group of experts from national authorities, the ECASEC Expert Group (formerly known as the Article 13a Expert Group). We are grateful for their valuable input, comments and support in the process of developing of this document.

Also, in preparing this paper we conducted a survey to assess the state of play. We received survey responses from 32 providers across Europe and from 17 national competent Authorities.

Several experts from electronic communications providers were consulted through targeted interviews, provided written answers and/or peer reviewed the document:

Pedro Silva, Carla Carrinho (NOS Protugal), Vasilis Kouktzoglou, Nikos Niskopoulos (Vodafone Greece), Ivan Lescak (SWAN), Florian Pennings, Lorelien Hoet (Microsoft), Peter Gervai (Tarr Ltd HU), Frank Van Berkel, Martijn Ronteltap (T-Mobile, Netherlands), Giulia Pastorella, Magnus Falk, Heather Ceylan (Zoom), Andreas Neocleous, Loukia Pavlidou (CYTA), Stephen Hermanson (Vodafone Spain, Vodafone Germany)

Their input was vital in the development of this paper and we would like to thank them for their contribution.

LEGAL NOTICE

This publication represents the views and interpretations of ENISA, unless stated otherwise. It does not endorse a regulatory obligation of ENISA or of ENISA bodies pursuant to the Regulation (EU) No 2019/881.

ENISA has the right to alter, update or remove the publication or any of its contents. It is intended for information purposes only and it must be accessible free of charge. All references to it or its use as a whole or partially must contain ENISA as its source.

Third-party sources are quoted as appropriate. ENISA is not responsible or liable for the content of the external sources including external websites referenced in this publication.

Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

ENISA maintains its intellectual property rights in relation to this publication.

COPYRIGHT NOTICE

ISBN: 978-92-9204-538-8, DOI: 10.2824/4233

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The new EU telecom legislation, the European Electronic Communications Code[1] (the 'EECC'), requires providers of public electronic communications networks or services to notify their users when there has been a particular and significant threat to these networks or services. Warning customers[2] regarding cyber threats is also industry good practice. Here are some recent examples:

- In 2020, Google warned 40,000 customers that it had detected activity from nation-state sponsored cyber-attackers against customer accounts[3].
- In 2019, WhatsApp detected attacks targeting around 1,400 users and sent each of them a warning about this threat[4].
- In 2020, T-Mobile warned its users to be on alert, following an increase in SIM swapping attacks[5].
- In 2021, Vodafone published a warning about the Flubot malware on its website, warning customers about it and explaining what they could do if their device was infected.[6]

However, warning about cyber threats is not a straightforward activity and has to be done carefully. Warning too often about cyber threats could be counter-productive because users might start downplaying or even ignoring the warnings in the long run. Likewise, there may be limited utility in warning about a general threat when there is very little customers can or are likely to do about it. On the other hand, warning a customer about a particular and imminent yet addressable threat is more likely to generate tangible results. Specifically, it may help the customer avoid the threat turning into a security incident.

Choosing the right channel and method for contacting users is important. Very frequent and badly designed warnings could result in users finding it difficult to distinguish them from fraudulent messages. As a result, in some cases, such warnings could actually lead to increasing the likelihood of fraud. Often, cyber-attacks start with an SMS message or email containing an alarming text and a call for urgent action. For example, the so-called 'helpdesk scams' warn the user about an infected PC asking them to contact customer support and install 'cleaning' software, including links and contact information that lead them to the fraudster instead.

In this paper, we aim to give guidance to national Authorities and providers of electronic communications networks and services regarding how to strike the right balance and carry out efficient and effective outreach to users about cyber threats.

In the first part of this report, we present an overview of the state of play by analysing several examples, case studies and responses from the experts working in the sector. We note that this overview reflects the situation before the EECC came into effect.

[1] 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

[2] Art 40(3) of the EECC refers to 'users'. However, for the purposes of this report, and given that not all practices described here may fall under Art 40(3), we will use the terms 'customers', 'consumers', 'users' and 'end-users' interchangeably

[3] https://www.forbes.com/sites/daveywinder/2020/03/27/hacker-threat-google-confirms-40000-nation-state-cyber-attack-warnings-issued/ .

[4] https://www.theguardian.com/technology/2019/nov/01/whatsapp-hack-is-serious-rights-violation-say-alleged-victims .

[5] https://www.t-mobile.com/news/press/how-to-fight-account-takeover-fraud

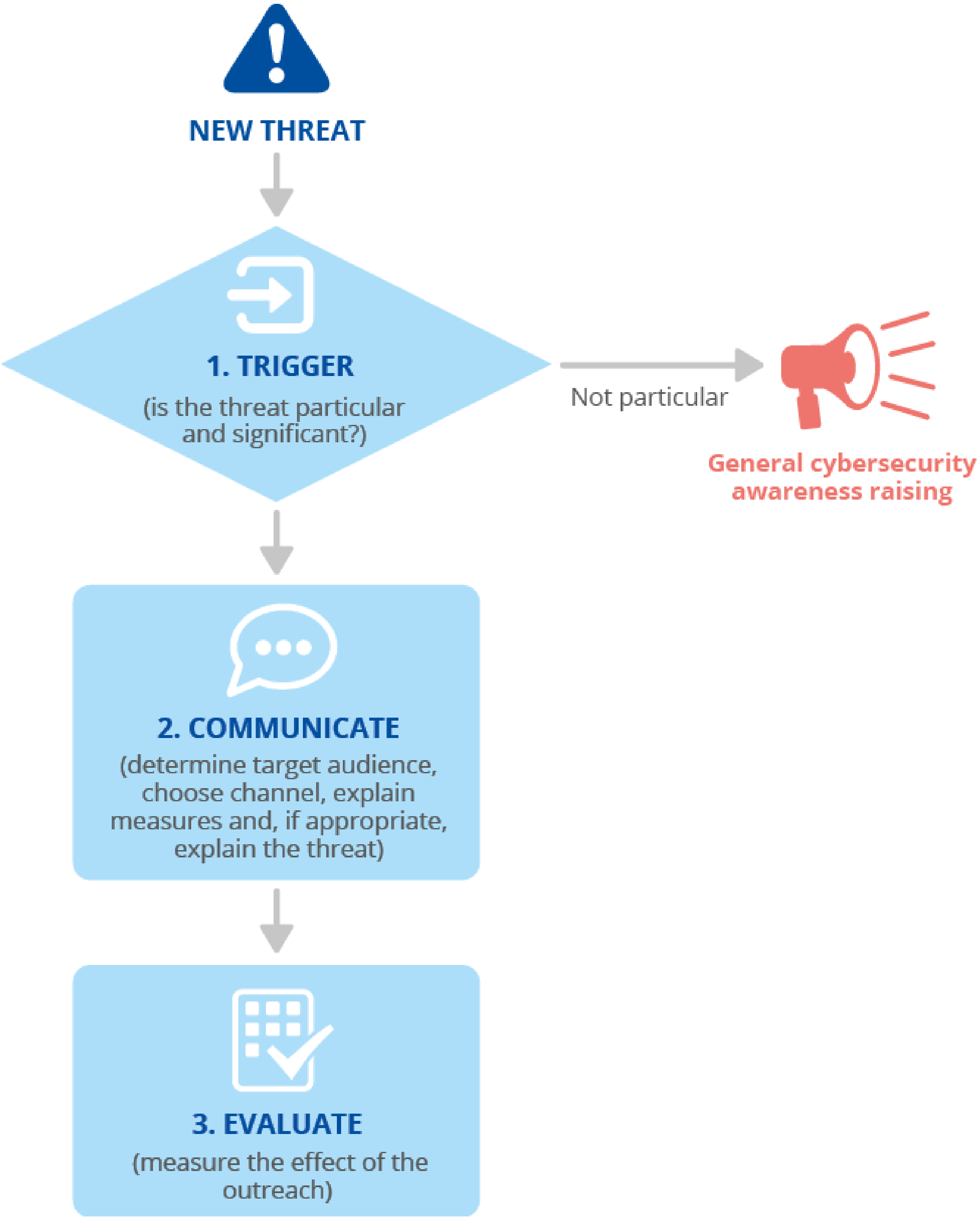
[6] https://support.vodafone.co.uk/Flubot/1656667612/What-is-the-Flubot-scam.htm

In the second part of this report, we provide a framework, a checklist, for determining whether to carry out outreach activities and how.

The checklist has three steps:

1. **Trigger:** Determine if outreach about a potential threat is needed.
2. **Communication:** Determine the right channel, and the right message.
3. **Evaluation:** Define the parameters for measuring the effectiveness of the outreach.

Figure 1: Checklist to determine whether to carry out outreach activities and how


NEW THREAT
1. TRIGGER
(is the threat particular and significant?)
Not particular
General cybersecurity awareness raising
2. COMMUNICATE
(determine target audience, choose channel, explain measures and, if appropriate, explain the threat)
3. EVALUATE
(measure the effect of the outreach)

In the Annex we fill in this checklist for a few well-known cases.

We conclude this paper with general observations:

- **Monitoring and notifying about potential threats is a new paradigm:** The EECC requires providers of electronic communications networks and services to monitor potential threats before they turn into cybersecurity incidents. In the proposal for the revised Network and Information Systems Directive[7] (the 'NIS2 proposal'), the Commission extends this approach to other sectors. While there are benefits in communicating warnings about threats before they become cybersecurity incidents, authorities and providers should collaborate to strike the right balance about which threats should be in the scope of these warnings. The proposed simple framework is sector-agnostic, and could be adjusted and reused in other policy areas, so that users are informed about cyber threats and possible preventative or mitigative measures effectively and in a timely manner.

- **Engage and collaborate with national authorities about outreach:** The national authorities we interviewed suggested that collaboration and knowledge sharing are good between electronic communications providers and authorities. Providers could engage them before reaching out to the customers. The national authorities could then also coordinate with other providers, other governmental entities, such as the national CSIRTs, and even coordinate with authorities in other sectors to address the problem.

- **Outreach does not replace other actions:** Finally, outreach to customers should be seen as a complementary measure and should not replace other actions by the authorities or the providers - specifically, applying the necessary preventive or mitigative technical measures. This is because the users receiving the communication often do not have the time and/or the know-how to deal with technical issues.

[7] Proposal for a directive of the European Parliament and of the Council of 16 December 2020 on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM(2020) 823 final, 16.12.2020.

1. INTRODUCTION

EECC, the EU's new telecom security legislation, requires providers of public electronic communications networks or services to notify their users of a particular and significant threat. Warning customers regarding cyber threats is also industry good practice.

In this paper we provide guidance on:

- Which cyber threats should trigger outreach to the customers using the networks and services?
- How to communicate about threats, which channels to use, which messages to convey?
- How to evaluate the effectiveness of the outreach?

1.1 TARGET AUDIENCE

This paper provides technical guidance to national Authorities supervising the implementation of Article 40, par. 3 of the EECC, and it may also be useful for experts working in the EU telecom sector.

1.2 POLICY CONTEXT

EECC Article 40 par. 3 requires providers of communications networks and services in the EU to notify users of particular and significant threats about the measures or remedies they can take to mitigate these threats, to protect the security of their communications. Where relevant, providers should also notify the users about the threat itself. We quote the legislative text in full:

"Member States shall ensure that in the case of a particular and significant threat of a security incident in public electronic communications networks or publicly available electronic communications services, providers of such networks or services shall inform their users potentially affected by such a threat of any possible protective measures or remedies which can be taken by the users. Where appropriate, providers shall also inform their users of the threat itself."

In the following paragraphs, we give guidance about how this step can be implemented effectively and efficiently in practice.

Note that the EU Member States are in the process of transposing the EECC into national legislation.

Note also that the European Commission recently made a proposal for a reviewed NIS Directive, the NIS2 proposal, which substitutes Article 40 of the EECC. However, current NIS2 proposal also contains the same provision about warning/notifying users of the service, which means that there would be no substantial change in this regard.

1.3 METHODOLOGY

We developed this guidance by looking into the following research questions:

- How do providers currently inform users about threats and mitigative measures and how is the effectiveness of this outreach measured?

- How do operators in other critical sectors such as banking and utilities reach out to their customers?

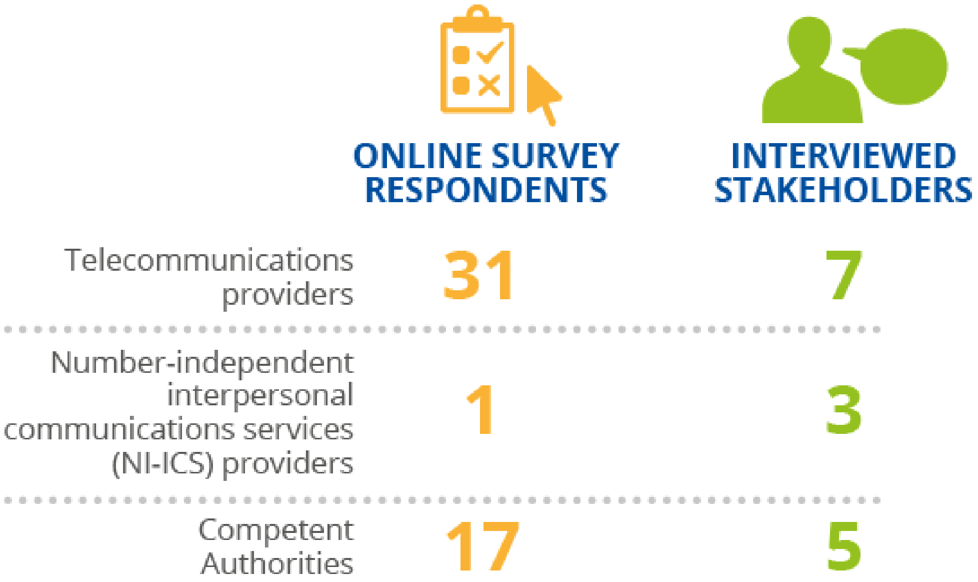
We collected information in three ways:

- **Desk research:** We have analysed publicly available sources and specialised literature on the status, practices and mechanisms in place related to consumer outreach about cybersecurity threats. The processed materials served as the basis for the online survey and the interviews.

- **Online questionnaire, targeting national authorities and telecom providers in the EU:** In total, 49 stakeholders answered the online questionnaire, from both private and public sectors at EU and national levels.

- **Interviews with stakeholders:** We held 15 expert interviews to get a better understanding of the current industry practices when it comes to reaching out to users about cybersecurity threats.

Figure 2: Overview of the research participation



	ONLINE SURVEY RESPONDENTS	INTERVIEWED STAKEHOLDERS
Telecommunications providers	31	7
Number-independent interpersonal communications services (NI-ICS) providers	1	3
Competent Authorities	17	5

2. CASE STUDIES

In this section, we provide examples of situations in which providers reach out to customers about cybersecurity threats.

Note that these case studies are indicative of the existing good practices in the industry, before transposition of the EECC into national legislation.

2.1 CASE STUDIES FROM THE TELECOM SECTOR

General awareness raising – Telenor[8]

Telenor has an awareness programme, including 10 ‘digital lessons’ introducing security awareness for typical cybersecurity threats, such as ransomware, phishing and malicious links, or fake news and false facts. The digital lessons are available for citizens and enterprises.

Videos with lifelike examples of threats – Telefónica [9]

Telefónica provides detailed descriptions of currently trending potential threats in posts on social media, which includes video explanations of threats through lifelike examples. For instance, in a video-post in May 2021, Telefónica provided information on the characteristics, consequences and preventive measures of ‘smishing’, a variant of phishing, through SMS.

Fake email examples - Deutsche Telekom [10]

On its website, Deutsche Telecom publishes information about ongoing and past incidents sorted by date, including the characteristics of the incident, the measures that have been taken to address it, and suggestions for users on how to take preventive or mitigating measures.

For example, on 19 May 2021, Deutsche Telekom published a description of fake emails allegedly sent by Deutsche Bank, Sparkasse and Amazon, which included a description of the characteristics of such messages (e.g. misspellings, strange email address), the tricks for stealing log-in data (e.g. mandatory updates, user advantages available on a link), the consequences of falling victim to those emails, as well as the mitigation steps customers could take (e.g. call customer service).

FluBot warning - Vodafone Greece [11]

Vodafone Greece maintains a webpage about the FluBot mobile phone malware, where users can find detailed information about the threat, e.g. a description of the fraud, protecting measures and a comprehensive list of steps a user can take to find out if he has been affected.

[8] https://www.telenor.com/get-free-access-to-online-security-awareness-program/
[9] https://m.facebook.com/watch/?v=292264332511439&_rdr
[10] www.telekom.de/hilfe/festnetz-internet-tv/sicherheit/sicherheitsmeldungen?samChecked=true
[11] https://support.vodafone.co.uk/Flubot/1656667612/What-is-the-Flubot-scam.htm

FluBot warning - Vodafone UK [12]

Vodafone UK provides a detailed description of current threats on Twitter, e.g. a description of the FluBot fraud. The tweet consists of three steps, which should be taken by the users to avoid the fraud.

Detailed incident communication, including severity scores and steps taken – Zoom [13]

Zoom provides descriptions of vulnerabilities and incidents in its 'Security Bulletin'. This bulletin entails not only descriptions of the incidents dating back several years, but also assigns a score to identify their severity based on the Common Vulnerability Scoring System (CVSS)[14]. Furthermore, it includes descriptions of measures that have been taken to mitigate the vulnerabilities. For example, on 26 March 2021, Zoom posted the details of a screen-sharing vulnerability with a CVSS score of 5.7 (medium severity), a detailed description of the consequences of using screen sharing (screen sharing users may be seen by other meeting participants for a brief moment), all the products affected and the steps Zoom had taken to address it.

Belgian Anti-Phishing Shield[15] - Proximus

The campaign aims at reducing active botnet participation from user devices. The customers are warned when they are about to access a malicious website following a phishing attack. The initiative does not only notify users of potential threats, but also navigates them to an awareness-raising site where they are walked through the steps for cleaning their device. The step-by-step instructions and immediate alerts make the process more user-friendly and easy-to-understand.

Countrywide awareness raising campaigns with provider participation - T-Mobile Netherlands

T-Mobile participates in countrywide awareness-raising campaigns about potential cybersecurity threats and mitigation measures, where the participating providers share their industry knowledge. These awareness-raising campaigns are funded by the Dutch Government and organised by the Dutch Ministry of Justice and Security.

Simple targeted awareness raising campaign – SSF Cybersecurity

The Swedish Internet Foundation conducted research in connection with leaked passwords and the Swedish internet security organisation (Stoldskyddsforeningen - SSF) turned the results of this survey into a nationwide awareness raising campaign with easy-to-understand messages. The most common leaked passwords were presented on eye-catching billboards and bus stop advertisements.

A variety of dedicated educational material for children, parents and teachers - Liberty Global[16][17][18][19]

[12] https://support.vodafone.co.uk/Flubot/1656667612/What-is-the-Flubot-scam.htm

[13] https://explore.zoom.us/en/trust/security/security-bulletin/

[14] https://nvd.nist.gov/vuln-metrics/cvss

[15] https://baps.ccb.belgium.be/en/belgian-anti-phishing-shield Belgian Anti Phishing Shield

[16] https://www.virginmedia.com/help/security-hub;

[17] https://www.virginmedia.ie/customer-support/support-by-products/broadband/online-security-safety/

[18] https://www.sunrise.ch/en/residential/mobile/freedom/options/surf-protect.html;

[19] https://www2.telenet.be/fr/serviceclient/signaler-un-abus-dinternet/

Via its subsidiaries, Liberty Global provides educational material on online safety dedicated to different age groups, parents and teachers. The material is provided in easy-to-understand formats, games, workbooks and readings for the ages of 4 to 16 in more than 10 languages. For example, the workbook for children from 13-16 years incorporates decision-making steps in real-life examples, such as what information we can share on the internet and with whom. This segmentation of the young generations allows parents and teachers to provide access to suitable learning materials for the children.

Interactive learning environment with hands-on tasks designed for children - Google[20]

ess interactive videos, games and materials to become 'internet awesome' and learn to use the internet safely. 'Interland' includes hands-on practice with four challenging games (namely 'Share with care', 'Don't fall for fake' and 'Secure your secrets'), and helps children learn how to act responsibly in unsafe situations. The interactivity of the platform provides a unique learning environment specifically designed for children, who may find it easier to learn new things through interactive formats.

2.2 CASE STUDIES FROM THE BANKING SECTOR

Automatic tracking, alerting and blocking of suspicious activities – Santander Bank[21]

In the finance sector, banks must send alerts to users if their system detects anything suspicious. For example, the Santander Bank in Spain uses a behavioural biometrics solution called "Trusteer", which develops a customer profile based on normal user activity. It can detect abnormal activity and continuously authenticates the user. When the solution does detect abnormal behaviour, they alert the customer and block unauthorized transactions before they cause damage.

Obligatory guidelines on source authenticity and potential precautious actions

Banks are required to include cybersecurity awareness material on their websites, as their customers must be careful with checking the authenticity of sources that are asking for account details and take precautions while using the bank's websites[22].

BNP Paribas has a dedicated subpage for awareness raising, on which the internet banking risks, the bank's security practices and client recommendations are listed [23].

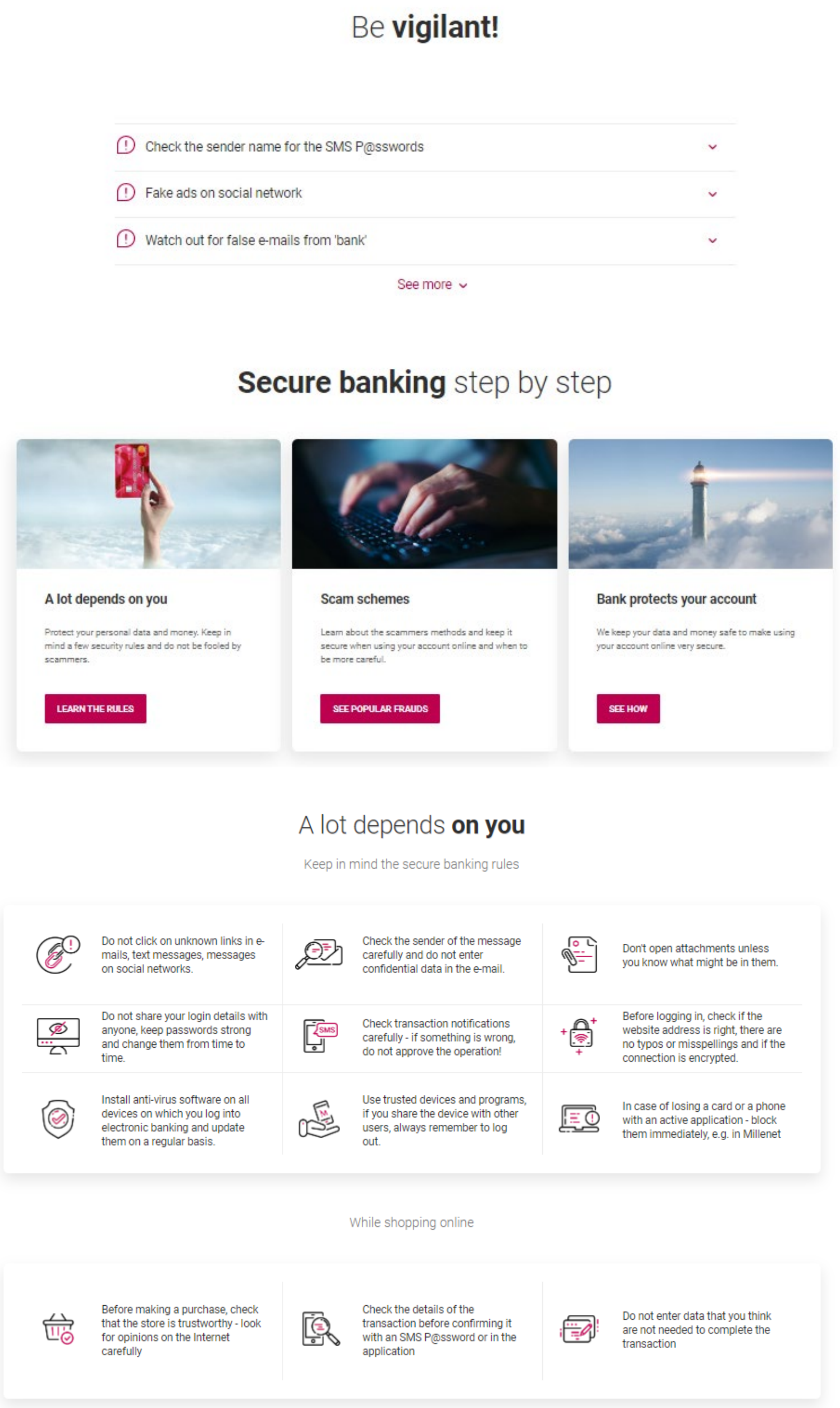
[20] https://beinternetawesome.withgoogle.com/en_us/

[21] https://www.ibm.com/blogs/client-voices/outsmart-bank-fraud-real-time-cybersecurity/

[22] https://www.byteacademy.co/blog/banking-cyber-security

[23] https://chile.bnpparibas.com/en/__trashed/

Figure 3: Bank Millennium's warnings and advice usually for social engineering



Be **vigilant!**

- Check the sender name for the SMS P@sswords
- Fake ads on social network
- Watch out for false e-mails from 'bank'

See more

Secure banking step by step

A lot depends on you

Protect your personal data and money. Keep in mind a few security rules and do not be fooled by scammers.

LEARN THE RULES

Scam schemes

Learn about the scammers methods and keep it secure when using your account online and when to be more careful.

SEE POPULAR FRAUDS

Bank protects your account

We keep your data and money safe to make using your account online very secure.

SEE HOW

A lot depends **on you**

Keep in mind the secure banking rules

- Do not click on unknown links in e-mails, text messages, messages on social networks.
- Check the sender of the message carefully and do not enter confidential data in the e-mail.
- Don't open attachments unless you know what might be in them.
- Do not share your login details with anyone, keep passwords strong and change them from time to time.
- Check transaction notifications carefully - if something is wrong, do not approve the operation!
- Before logging in, check if the website address is right, there are no typos or misspellings and if the connection is encrypted.
- Install anti-virus software on all devices on which you log into electronic banking and update them on a regular basis.
- Use trusted devices and programs, if you share the device with other users, always remember to log out.
- In case of losing a card or a phone with an active application - block them immediately, e.g. in Millenet

While shopping online

- Before making a purchase, check that the store is trustworthy - look for opinions on the Internet carefully
- Check the details of the transaction before confirming it with an SMS P@ssword or in the application
- Do not enter data that you think are not needed to complete the transaction

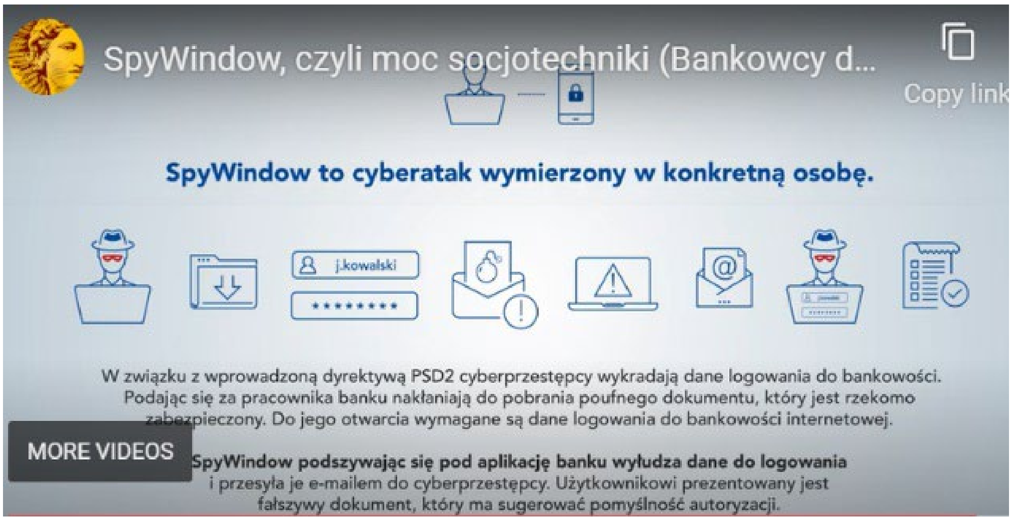
On its internet banking log-on page [24], Bank Millennium also provides information on the most common vulnerabilities, threats and mitigation measures. Apart from providing advice on good login practices, Bank Millennium's warnings and advice usually relate to social engineering tactics[25] – for example: fake authorisation SMS, fake ads on social networks and fake emails claiming to originate from Bank Millennium. In addition, Bank Millennium advises on the security measures it has in place to minimise cybersecurity risks.

Alior Bank, with its own Computer Emergency Response Team ('CERT')[26], also provides advice on its website regarding the most common threats and vulnerabilities, and how to minimise them. It also provides descriptions of, and guidelines on security measures the bank provides, such as multi-factor authorisation.

Alior's advice goes beyond its banking services. The bank provides general cyber-hygiene awareness-raising on conducting oneself online – for example, on offers that seem 'too good to be true'[27].

We note that Alior Bank has a series of short educational videos[28] in which it provides simple language information on selected threats and vulnerabilities, for example fake banking websites, SpyWindow, applications coming from unknown third parties or security of connected devices.

Figure 4: Alior Bank's SpyWindow



SpyWindow, czyli moc socjotechniki (Bankowcy d...

SpyWindow to cyberatak wymierzony w konkretną osobę.

W związku z wprowadzoną dyrektywą PSD2 cyberprzestępcy wykradają dane logowania do bankowości. Podając się za pracownika banku nakłaniają do pobrania poufnego dokumentu, który jest rzekomo zabezpieczony. Do jego otwarcia wymagane są dane logowania do bankowości internetowej.

SpyWindow podszywając się pod aplikację banku wyłudza dane do logowania i przesyła je e-mailem do cyberprzestępcy. Użytkownikowi prezentowany jest fałszywy dokument, który ma sugerować pomyślność autoryzacji.

Information on the "SIM Swapping" fraud – Alpha Bank Greece[29]

Alpha bank Greece has developed a web page including information on the SIM Swapping fraud. On 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.

[24] https://www.bankmillennium.pl/en/log-in
[25] https://www.bankmillennium.pl/en/electronic-banking/internet-banking-security
[26] https://www.aliorbank.pl/dodatkowe-informacje/bezpieczenstwo/cert-alior.html
[27] https://www.aliorbank.pl/dodatkowe-informacje/bezpieczenstwo/bezpieczenstwo-edukacja.html
[28] https://www.aliorbank.pl/dodatkowe-informacje/bezpieczenstwo/bezpieczenstwo-filmy-edukacyjne.html
[29] https://www.alpha.gr/en/retail/support-center/security/apati-sim-swapping

Cybersecurity-related advice to both B2C[30] and B2B[31] segments - National Westminster Bank (NatWest)

National Westminster Bank (NatWest) provides cybersecurity-related advice to both B2C[32] and B2B[33] segments. In the latter case, information related to preventive and mitigative measures is further divided based on the size of the business.

For example, in the B2C part of its website, NatWest advises on some of the latest types of fraud (such as delivery and cryptocurrency scams), the steps customers can take when they feel they may have become a victim of one, and the channels they can use to contact NatWest.

Specifically, NatWest, several other banks, and telecommunications companies in the United Kingdom are operating a pilot scheme offering customers one specific number they can call regardless of which bank they do business with – similar to calling the police – if they have reasons to believe they are at risk of fraud[34].

[30] https://www.natwest.com/fraud-and-security.html.

[31] https://www.natwest.com/business/security.html.

[32] https://www.natwest.com/fraud-and-security.html.

[33] https://www.natwest.com/business/security.html.

[34] https://stopscamsuk.org.uk/159 .

3. STOCK TAKING OF CURRENT PRACTICES

In this section, we look at current good practices in the industry, using data from the online survey and the in-depth interviews.

We asked industry experts detailed questions about the kind of outreach they perform now. We used the following structure for this survey:

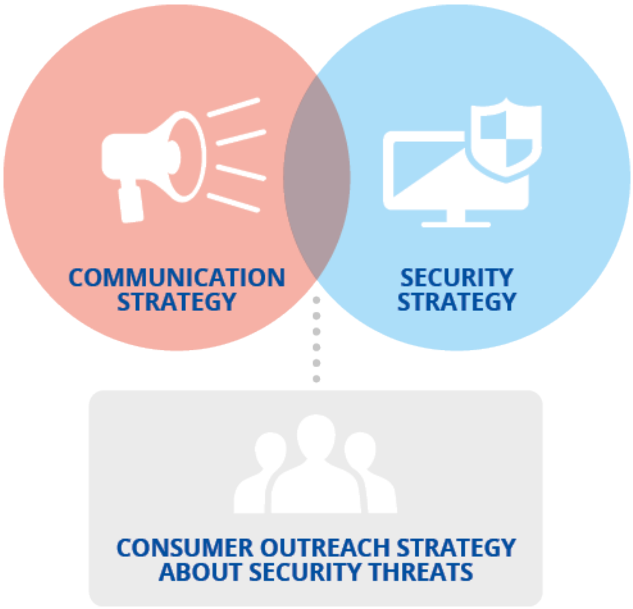
1. **General approach:** What is the general approach to user outreach?
2. **Triggers for outreach:** Which factors and circumstances trigger an outreach to customers?
3. **Content of the communication:** What information is shared with the customers?
4. **Target audience:** What is the target audience of the outreach?
5. **Communication channels and frequency:** What are the channels used for the outreach?
6. **Measuring effectiveness:** How is the effectiveness of the outreach measured?

3.1 GENERAL APPROACH

The overall strategy for user outreach needs to take into account the general cybersecurity strategy of the provider, as well as its communication strategy:

- **Provider's cybersecurity strategy** - What are the provider's high-level plans to build resilience to threats and ensure its users (natural persons and businesses) benefit from trustworthy services?
- **Provider's communication strategy** - How should the company communicate about a threat? How – in what language and style – should the message be formulated? What channels should be used in specific cases? How can the effects of this communication be measured?

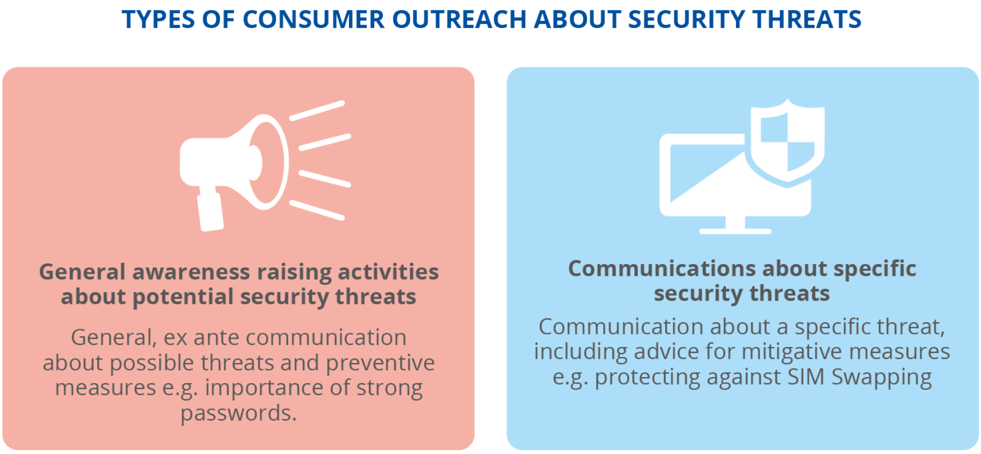
Figure 5: Connection between communication and security strategy



When reaching out to their customers, providers of electronic communications and services mix two approaches:

- Targeted communications about specific security threats
- General awareness raising activities about potential security threats

Figure 6: Two general types of user outreach about security threats



TYPES OF CONSUMER OUTREACH ABOUT SECURITY THREATS

General awareness raising activities about potential security threats

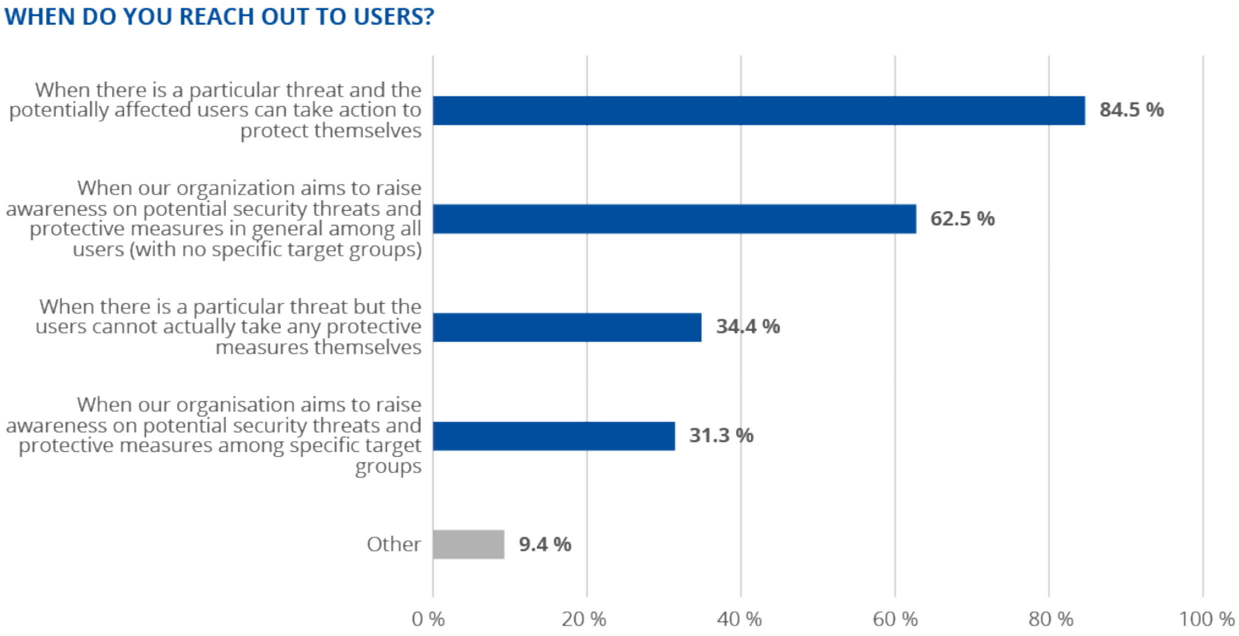
General, ex ante communication about possible threats and preventive measures e.g. importance of strong passwords.

Communications about specific security threats

Communication about a specific threat, including advice for mitigative measures e.g. protecting against SIM Swapping

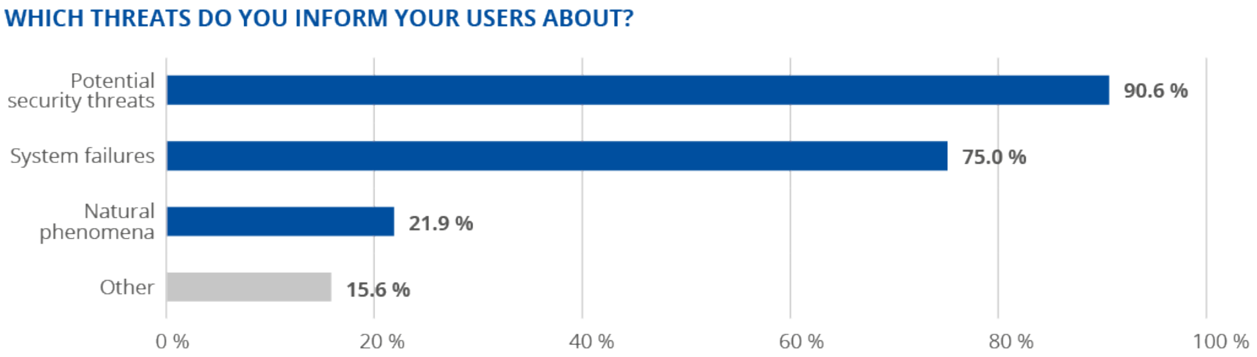
Most providers carry out user outreach only when customers can actually take preventive or mitigative measures. Based on the surveys and the interview responses, providers appear to be mindful of the risk of information overload.

Figure 7: Survey responses on when electronic communications providers reach out to users



Providers reach out about malicious actions (potential security threats) and system failures, but rarely about natural phenomena. See the diagram below.

Figure 8: Survey responses: Threats users are informed about



The main reported goal for the providers in their user outreach is to increase user awareness about cybersecurity threats. Other aspects, such as brand protection, reportedly do not play an important role.

3.3 CONTENT OF THE COMMUNICATION

The content of the outreach is often adjusted to the knowledge and competency level of the users, with focus on sending a clear message. Cybersecurity is a challenging topic and, if messages are not specific and sufficiently understandable, they are less effective.

Communication about specific threats often includes facts about the nature of the threat, potential impact, steps that have been taken by the provider so far, etc. The most frequent topics are:

- phishing e-mails,
- data breaches,
- system failures or
- denial-of-service attacks (DoS).

The majority of experts agree that besides the preventive and/or mitigative measures users may take, they should also be informed about the threats themselves. Incorporating information on examples of specific threats in the communication, supports its effectiveness. Some providers provide detailed, lifelike examples of threats.

3.4 TARGET AUDIENCE

When reaching out to users about security threats, electronic communications providers generally target those who are directly affected by the threat.

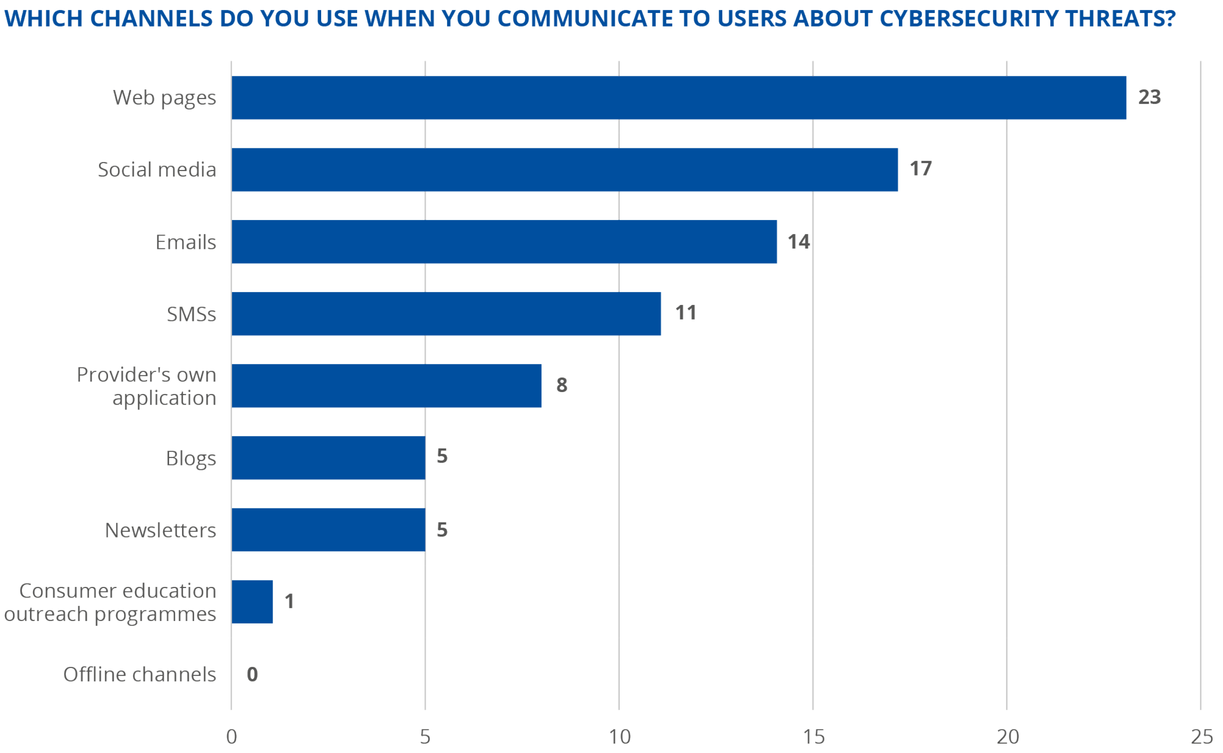
Providers do not segment their customers in groups (for example based on age, etc.). The more the communication is targeted and specific, the more likely it is to trigger action by the customer.

Communication with the business segment is different. In this segment, outreach goes to the corporate account and the procedures are integrated in standard IT processes, as part of technical support. The communication is typically more technical and more strictly monitored, for example, by ticketing systems.

3.5 COMMUNICATION CHANNELS USED

Providers use different communication channels, depending on the type of outreach. See the chart below – showing survey responses from experts working in the sector.

Figure 9: Survey responses: channels used for communication about threats



In case an action is required from the users: direct channels are the most commonly used.

Social media posts may reach a wider audience. However, if we were to take the number of ‘likes’, comments and shares as the indication of their effectiveness, it would often appear to be limited.

In general, it would appear that number-independent interpersonal communication service providers (NI-ICS or OTT providers), such as WhatsApp and Facebook generate more impact with outreach using their social media than traditional telecom providers.

Providers often also use their own website for informing customers about threats. Typically, the messages can be found on the home page to ensure that customers can easily find these warnings.

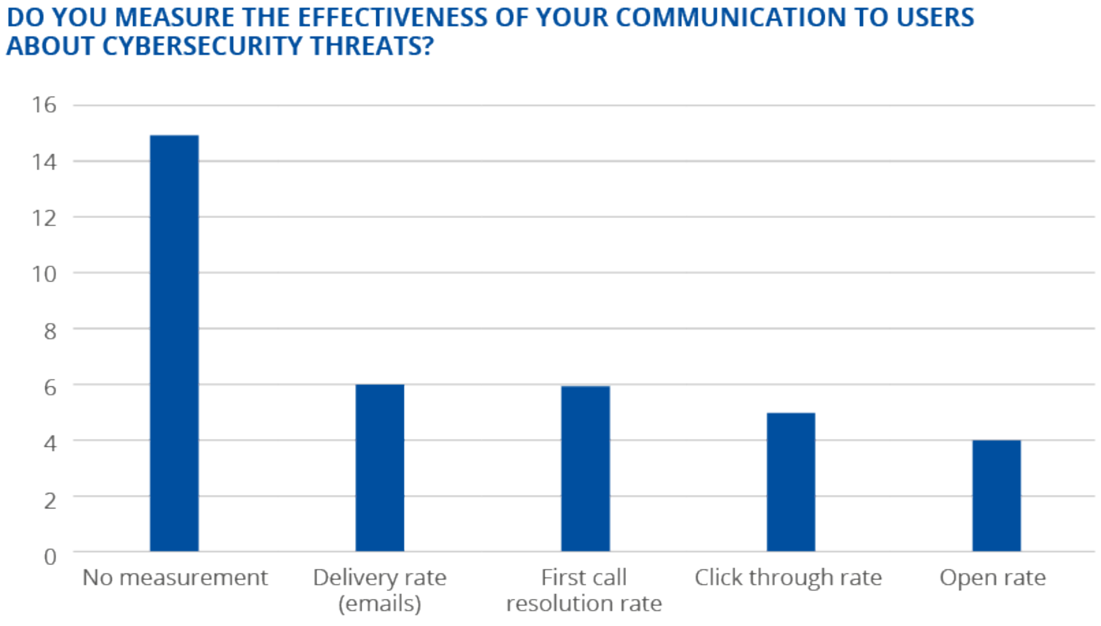
Direct communication, such as emails or SMS, appears to be more effective. Mass communication, such as press releases and social media posts, reach large groups, but are not as effective as direct communication.

Electronic communications providers detect a significant number of threats on a daily basis. Communicating every single threat would be ineffective, so in most cases providers only approach their users in high-risk cases, in order to increase the chances of grabbing their users’ attention.

3.6 MEASURING EFFECTIVENESS

Most providers do not measure the effectiveness of their outreach about threats. However, several providers plan to implement such measurements. The providers who do measure the effectiveness of their communication to users regarding security threats, mostly focus on monitoring whether the target audience has been reached properly and the requested actions have been implemented by the users.

Figure 10: Survey responses: Measurement of the effectiveness of communication to users regarding security threats



Note: Some providers selected more than one ways of measurement

The following KPIs are monitored most frequently:

- **Delivery rate of emails**: The percentage of emails that were actually delivered to recipients' inboxes, calculated by subtracting hard and soft bounces from the gross number of emails sent, then dividing that number by gross emails sent,
- **First call resolution rate**: no repeat calls or contacts are required to follow-up on the initial call, and
- **Click through rate**: the ratio of users who click on a specific link to the number of total users who view a page, email, or advertisement hosting that link.

4. OUTREACH FRAMEWORK

Following a review of the current industry practices and considering the requirements of Article 40, par. 3 of the EECC, in this section, we provide three high-level steps that can be followed by electronic communications providers for notifying threats to their users. Our framework consists of a decision point (Trigger- whether to proceed with user outreach) and two factors for consideration that will shape the outreach (Communication and Evaluation).

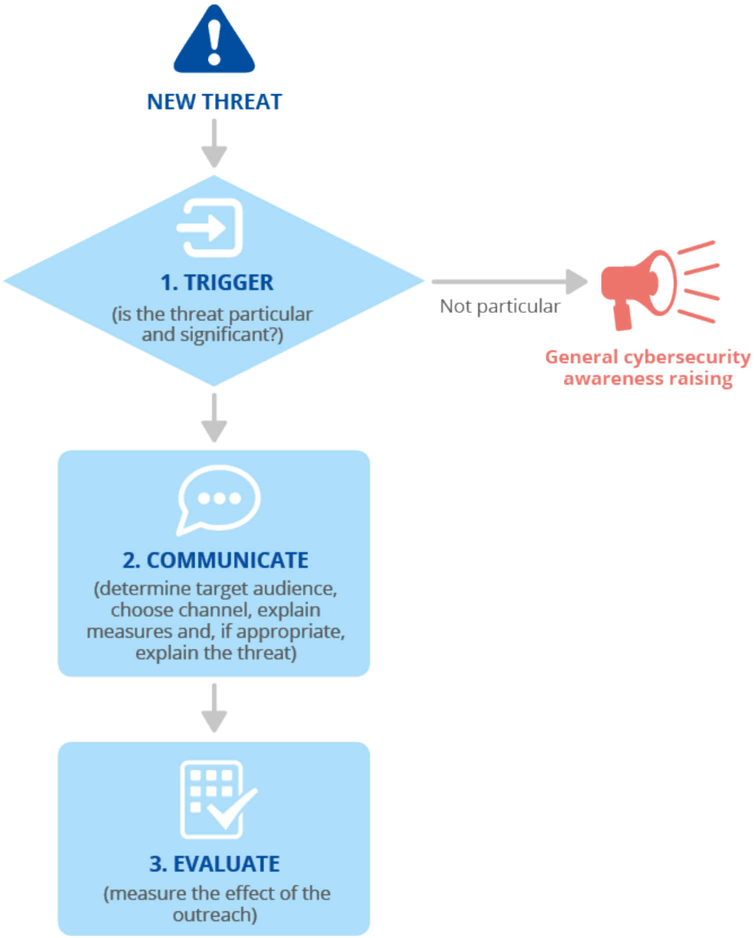
In the end of this section, the steps are included in a checklist that can be used by the provider to structure the information of a specific outreach campaign and explain the reasoning behind it on the basis of Article 40, par. 3 of the EECC.

4.1 FRAMEWORK

Article 40, par. 3 of the EECC includes several factors/circumstances having to do with communication to users about cybersecurity threats and the kind of outreach action required. It provides that if a threat is **particular** (i.e. it is not a general or common threat) or **significant** (i.e. it poses a risk to the customer), providers should **communicate possible protective measures or remedies to all users that are potentially affected** and if appropriate (i.e. if such communication does not result in increasing the overall level of risk), **inform customers of the threat** itself.

We outline these factors/circumstances and actions in the flow-chart below.

Figure 11: Framework for user outreach about cybersecurity threats


NEW THREAT
1. TRIGGER
(is the threat particular and significant?)
Not particular
General cybersecurity awareness raising
2. COMMUNICATE
(determine target audience, choose channel, explain measures and, if appropriate, explain the threat)
3. EVALUATE
(measure the effect of the outreach)

We go over the three steps in more detail and provide guiding questions.

4.2 TRIGGER

When a new threat is found, an assessment should be made on a case-by-case basis to decide if outreach is needed, and to ensure that there is added value in the outreach. It is important to strike a balance between the communication objectives and the risk of 'customer fatigue'. If providers send messages too often, customers may start to ignore them.

Questions to ask:

- Is it a particular threat? Or is it a more general and common threat?
- Is it a significant threat?
- What is the potential impact of the threat for the customers?
- What is the likelihood that the threat materializes?
- Does the security threat affect a particular component of the network, a particular service, or transmitted, stored or processed data?
- Would communication lead to unnecessary loss of trust or fatigue?
- Can users take measures to mitigate/prevent the threat?
- Is it appropriate to communicate about the threat itself? Would such communication not result in additional (potentially significant) risks?

4.3 COMMUNICATION

Communication about a specific threat should include description of the threat and well-defined instructions for threat mitigation or prevention. Simple messages with practical information are most effective in reaching the target audience. The following questions are important to answer:

- Who is targeted and affected by this threat?
- What is the best channel for reaching out to this group of customers?
- Is a specific action required from the customer? If so, direct channels could work best.
- Is it appropriate to use multiple channels and messages?
- Could a simplified explanation/message be provided for non-expert users?
- Will there be a separate message and channel for the B2B segment?
- Is it appropriate to inform the customers about the threat itself? Would such communication not result in additional (potentially significant) risks?

4.4 EVALUATION

Evaluating the outreach about threats is important, but it is not always easy to define the right parameters. The parameters should be defined on a case-by-case basis.

- What parameters and KPIs can be used to evaluate if the outreach/communication reached all the targeted users?
- What parameters and KPIs can be used to evaluate if the users took the required actions (such as a password change)?
- What parameters and KPIs can be used to evaluate the overall effectiveness of the outreach (such as a decrease in the number of infected smartphones)?

4.5 CHECKLIST

In this section, we provide a basic checklist that can help in structuring the information and explaining the reasoning behind carrying out user outreach.

Figure 12: Checklist for notifying customers about threats

CHECKLIST FOR NOTIFYING CUSTOMERS ABOUT THREATS

THREAT INFORMATION	**Short name**	Descriptive name of the threat
	Date	Date
	Description	Short description of the threat
	References	Reference to background information, media reports, etc
	Nature of the threat	Choose from: System failures, Natural phenomena, Malicious actions, human errors, third-party failures.
	Potential impact	Describe the potential impact on the network or service
1. TRIGGER	**Particular?**	Determine if the threat is particular or common/general.
	Significant risk?	Determine if there is a significant risk: Assess the likelihood and the potential impact to find the level of risk.
	Outreach or not?	Yes or no
2. COMMUNICATE	**Channel?**	Choose from: SMS, emails, social media (general or direct), company's app, company's website, other (please specify)
	Measures or remedy?	List specific measures the customer can take or, if there are none, explain what the outreach aims to achieve.
	Include threat information?	Assess whether information about the threat itself can be included in the outreach.
3. EVALUATE	**Communication received?**	Describe how to measure if the communication reached the customers.
	Did customers take action?	Describe how to measure if the customers reacted
	Other KPIs?	Describe other KPIs that can be used to assess effectiveness.

4.6 ISSUES/CHALLENGES

Warning about cyber threats, even following the framework described in the previous paragraphs is not an easy task. It has to be done carefully, taking into account several issues and challenges that could interfere with the effectiveness of the communication.

- **There is a risk of causing fatigue:** Warning too often about cyber threats could be counter-productive, because users could start downplaying or even ignoring the warnings in the long run. Likewise, there may be limited utility in warning about a general threat when there is very little the users can do or are likely to do about it. On the other hand, warning a customer about a particular and imminent yet addressable threat is more likely to generate tangible results. and prevent the threat from turning into a security incident.

- **There is a risk of increasing the likelihood of fraud:** Choosing the right channel and method for contacting the users is important. Very frequent and badly designed warnings could result in the users finding it difficult to distinguish them from fraudulent messages. As a result, in some cases, such warnings could actually increase the likelihood of fraud. Often, cyber-attacks start with an SMS message or email containing an alarming text and a call for urgent action. For example, so-called 'helpdesk scams' warn the user about an infected PC asking them to contact customer support and install 'cleaning' software, including links and contact information that lead him to the fraudster instead.

- **Outreach does not replace other actions:** Outreach to customers should be seen as a complementary measure and should not replace other actions by the authorities or the providers – specifically, applying the necessary preventative or mitigative technical measures. Obviously, the users receiving the communication often do not have the time and/or the know-how to deal with technical issues. In general, it is not a proposed to rely on communication alone as a mitigative measure.
  For example, in the case of the Flubot malware, in some country's providers started to block certain SMS messages to avoid infection, which could be much more efficient than just warning the customers about the malware.

5. CONCLUSIONS

The new EU telecom security legislation, the EECC, requires providers of public electronic communications networks or services, to notify their users in the case of a particular and significant threat to these networks or services. Warning customers in case of cyber threats is also industry good practice.

However, warning about cyber threats is not a straightforward activity and has to be done carefully. In this paper we proposed a checklist that could help providers and authorities determine whether to carry out outreach activities and how, and we outlined several issues/challenges.

In the NIS2 proposal, the Commission extends the approach of user outreach about cybersecurity threats to other critical sectors. The proposed simple framework is sector-agnostic, could be adjusted and reused in other policy areas, so that users are informed effectively and in a timely manner about cyber threats and possible preventative or mitigative measures.

Collaboration and knowledge sharing between national authorities and electronic communications providers in the case of specific and important threats is very important. It could promote coordination also with other providers and other governmental entities, such as the national CSIRTs and lead to successful threat mitigation.

For instance, AGCOM[35], the national regulatory Authority of Italy led a trial involving the Bank of Italy, the Italian Data Protection Authority, the Ministry of Economic Development, Police and Financial Police, Banks, operators that offer messaging services to the banks and MNOs. The trial involves MNOs informing banks of the latest SIM swap, either through the subscriber's IMSI, hashed IMSI, or sending time information of the latest SIM swap.

In the case of the Flubot malware, the Belgian Institute for Postal Services and Telecommunications had a discussion with the electronic communication providers on how to respond in a coordinated way. The Authority supported the electronic communication providers by creating a forum for discussing and sharing good practices, filter rules and suspicious links. They agreed on how the electronic communication providers should reach out to their users and what measures they could take (blocking URLs and outgoing traffic/calls, and asking customers to factory reset their devices).

Finally, it is important to note that outreach to customers should be seen as a complementary measure and should not replace other actions by the authorities or the providers - specifically, applying the necessary mitigation and/or preventive technical measures.

[35] https://www.agcom.it/

ANNEX: EXAMPLES

A.1 WARNING USERS ABOUT FLUBOT SCAM MESSAGES

FluBot is an Android malware that is used by cyber attackers to steal passwords, online account login information, personal details and banking information. This information is then used to make payments, take over accounts and perform identity theft. FluBot spreads via SMS messages, and infected smartphones send SMS messages to the contacts listed in the infected smartphone to try and infect other customers[36].

CHECKLIST FOR NOTIFYING CUSTOMERS ABOUT THREATS

THREAT INFORMATION	**Short name**	**Flubot phishing SMS messages in Q1 of 2021**
	Date	03 March 2021
	Description	Flubot is a malware that infects smartphones
	References	https://www.proofpoint.com/us/blog/threat-insight/flubot-android-malware-spreading-rapidly-through-europe-may-hit-us-soon
	Nature of the threat	Malicious (malware)
	Potential impact	Compromised smartphone of the user (Android) and more malicious SMS messages targeting contacts.
1. TRIGGER	**Particular?**	Yes. While SMS-ishing is not a new threat, Flubot is a new threat that is spreading fast. Threat is not common.
	Significant risk?	Yes. Likelihood is medium, impact is high, so the risk is high.
	Outreach or not?	Yes
2. COMMUNICATE	**Channel?**	SMS and webpage: the risk is high, so using direct channel is appropriate: SMS. In addition, use the website and social media
	Measures or remedy?	The outreach aims to create awareness about phishing via SMS. Also, specific actions to remove the malware are proposed
	Include threat information?	Threat information is not sensitive, there are many media reports about Flubot. Therefore, threat information can be included.
3. EVALUATE	**Communication received?**	Measure the SMS delivery rate Measure the numbers of visitors on the Flubot webpage
	Did users take action?	N/A – no specific action is required
	Other KPIs?	Number of helpdesk tickets and complaints about Flubot

A.2 WARNING CUSTOMERS ABOUT SIM SWAPPING ATTACKS

Fraudulent SIM swapping is a type of fraud in which the attacker takes over a mobile subscriber's account by changing affiliation of that account with the original SIM card to a SIM card under the attacker's control.

This type of attack takes advantage of the mobile network operator's ability to quickly and seamlessly affiliate a mobile telephone number with a different SIM. This ability, usually referred to as 'number porting', is normally used when a subscriber has lost his device, the device has

[36] For example, see the news articles at https://www.proofpoint.com/us/blog/threat-insight/flubot-android-malware-spreading-rapidly-through-europe-may-hit-us-soon

been stolen, the SIM card has been damaged or when the subscriber wishes to switch service to a new device.

An 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 by doing research on social media. Once an attacker has obtained enough details to convincingly 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.

Should this initial part of the attack be successful, the genuine subscriber's SIM card loses connection to the network. This will enable the attacker to receive all the SMS and voice traffic intended for the targeted subscriber. This, in turn, will enable him to undermine or indeed exploit SMS-based security measures, as SMS-based authentication is often used in online banking portals, as well as for social media and email accounts (e.g., one-time passwords sent via text or telephone calls).

CHECKLIST FOR NOTIFYING CUSTOMERS ABOUT THREATS

THREAT INFORMATION	**Short name**	**Sim Swapping attack**
	Date	10 December 2021
	Description	Fraudulent SIM swapping is a type of fraud in which the attacker takes over a mobile subscriber's account by changing affiliation of that account with the original SIM card to a SIM card under the attacker's control.
	References	https://www.enisa.europa.eu/publications/countering-sim-swapping
	Nature of the threat	Malicious action (Social engineering on the providers' employees or the user, cyberattacks on providers infrastructure)
	Potential impact	Takeover of the subscriber's account that enable exploiting SMS-based security measures (2FA authentication, e.g. one-time passwords sent via text or telephone calls) to perform financial transactions, or access social media and email accounts).
1. TRIGGER	**Particular?**	Yes. SIM swapping is threat that is spreading fast. It targets a specific individual's activity. Threat is not common.
	Significant risk?	Yes. Likelihood is medium, Impact is high, so the Risk is high
	Outreach or not?	Yes
2. COMMUNICATE	**Channel?**	Direct channels used: Calls and email messages to targeted subscribe Indirect channels: Posting of warnings on the company's website and social media accounts
	Measures or remedy?	Providers are requested to be cautious with their personal data and the warning signs of the attack are highlighted
	Include threat information?	Threat information is not sensitive; there are many media reports about SIM Swapping Fraud. Threat information can be included.
3. EVALUATE	**Communication received?**	Measure the numbers of visitors on the SIM Swapping webpage SMS delivery rate
	Did customers take action?	Measure the click-through rate in the webpage and the social media sites
	Other KPIs?	Evaluate how soon users realized that they have been attacked, evaluate the impact of the attack based on user's helpdesk tickets

A.3 WARNING CUSTOMERS ABOUT WHATSAPP EXPLOIT

The WhatsApp exploit enables the installation of malicious software from the NSO Group, a firm from Israel that is behind a software tool called Pegasus.

The cyber-attack exploited WhatsApp's video calling system in order to send malware to the mobile devices of a number of WhatsApp users.

NSO spyware was used to exploit a vulnerability in the app to target more than 1,400 people between approximately April 2019 and May 2019. One hundred of those targeted were human rights defenders according to WhatsApp, in countries around the world. The vulnerability, first published about in May, allowed attackers to install spyware by calling the target using WhatsApp.

CHECKLIST FOR NOTIFYING CUSTOMERS ABOUT THREATS

THREAT INFORMATION	**Short name**	**WhatsApp hack**
	Date	June 2019
	Description	More than 1,400 WhatsApp users were targeted by NSO technology in a two-week period in May 2019. The cyber-attack exploited WhatsApp's video calling system in order to send malware to the mobile devices of a number of WhatsApp users. WhatsApp worked with an academic research group to identify the victims of the attacks and the technology used against them.
	References	https://en.wikipedia.org/wiki/Pegasus_(spyware), https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones
	Nature of the threat	Malicious action (Pegasus Malware)
	Potential impact	Once Pegasus malware penetrates a smartphone, it can steal its contents — texts, photos, videos, emails — and can turn on its camera and microphone for real-time monitoring without the user ever detecting a problem.
1. TRIGGER	**Particular?**	Yes. Pegasus software was used to gain access to user's smartphones. An average person is not the target of this specific piece of software, which is built to sell to governments to target individuals and does not work on a large scale. Threat is not common.
	Significant risk?	Yes. Likelihood is medium, impact is high and so the risk is high.
	Outreach or not?	Yes
2. COMMUNICATE	**Channel?**	Privately warn the affected customers
	Measures or remedy?	No specific measures
	Include threat information?	Threat information is not sensitive; there are many media reports about Pegasus software. Threat information can be included.
3. EVALUATE	**Communication received?**	Measure the SMS delivery rate
	Did customers take action?	N/A
	Other KPIs?	Number of helpdesk tickets and complaints about WhatsApp hack

TP-09-21-454-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: 978-92-9204-538-8
DOI: 10.2824/4233