"The project has received funding from the European Union's Internal Security Fund – Police under the grant agreement No 815347"

Deliverable D5.3

Best practices on the use of digital media for raising awareness among the public of customers and fostering cooperation with authorities

Due date of deliverable: 30/06/2020

Actual submission date: 05/11/2020

Project Details

Project acronym	SHERPA
Project full title	Shared and coHerent European Railway Protection Approach
Grant Agreement no.	815347
Call ID and Topic	ISFP-2017-AG-PROTECT, Topic ISFP-2017-AG-PROTECT Protection
Project Timeframe	01/11/2018 – 31/10/2020
Duration	24 months
Coordinator	UIC – Marie-Hélène Bonneau (bonneau@uic.org)

The content of this document represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains. The use of the content provided is at the sole risk of the user.

Document details

Title	Best practices on the use of digital media for raising awareness among the public of customers and fostering cooperation with authorities
Work Package	WP5
Date of the document	05/11/2020
Version of the document	3
Responsible Partner	DB AG
Reviewing Partner	all
Status of the document	Final
Dissemination level	CO Confidential, only for members of the consortium (including the Commission Services)

Document history

Revision	Date	Description
V0	29/06/2020	First draft structure prepared by UIC and DBAG
V1	18/09/2020	First version with contributions from all partners
V2	05/10/2020	Second version after the working meeting held on 25/09
V3	05/11/2020	Final version

Consortium – List of partners

Partner No	Short name	Name	Country
1	UIC	UNION INTERNATIONALE DES CHEMINS DE FER	France
2	DB	DEUTSCHE BAHN AG	Germany
3	FS SPA	FERROVIE DELLO STATO ITALIANE SPA	Italy
4	PKP S.A.	POLSKIE KOLEJE PANSTWOWE SPOLKA AKCYJNA	Poland
5	SNCB	SOCIÉTÉ NATIONALE DES CHEMINS DE FER BELGES	Belgium
6	SNCF	SNCF	France

EXECUTIVE SUMMARY

This deliverable aims to provide a comprehensive overview on how railway companies and authorities responsible for security in railway surroundings have used digital media to raise awareness of both personnel and passengers.

Best practices of the consortium partners as well as other stakeholders will be presented regarding using mobile applications.

The deliverable also aims at giving an overview on the potential benefits as well as the negative implications associated with the use of digital media. In addition, it gives recommendations on what should be considered when using digital media for crisis communication.

Table of contents

INTRODUCTION

1. PROJECT OBJECTIVES

Terrorist attacks carried out in recent years show an alarming increase of indiscriminate violent actions carried out against civilians gathering in public spaces. Even though railway transport represents a critical infrastructure for all European countries, stations and trains can be essentially regarded as soft targets due to their inherently open system nature. Several initiatives aiming at increasing their protection from terrorist attacks were undertaken in the past years at various levels. Nevertheless, the knowledge about the phenomenon itself and possible countermeasures is still quite fragmented and presents many gaps.

The SHERPA project aims at improving the overall protection level for stations and trains in Europe against terrorist attacks by implementing multiple synergistic actions towards the relevant stakeholders, such as: providing and sharing an up-to-date, high-value knowledge base on threats and countermeasures (both technical and procedural); defining a coherent approach for risk assessment, risk management, crisis and disaster recovery management; strengthening co-operation among stakeholders through high-level international trainings and other practical tools; outlining needs and requirements for industry and research to focus on improving the ways in which railways cope with both present and future threats.

Five among the most relevant key-players in the European railway sector (DB, FS, PKP, SNCB, SNCF) take part as partners in the SHERPA project proposal: their joint participation brings the highest levels of credibility, representativeness and authoritativeness. Furthermore, the consortium itself is led by UIC, whose aggregative nature, together with its solid expertise and experience in participating and leading European projects, will facilitate synergies among the co-applicants and between them and police, first responders and other relevant stakeholders represented in the Advisory Board such as CER, COLPOFER, The French Ministry of Transport, RAILPOL, NS and SBB.

2. PURPOSE OF THE DOCUMENT

SHERPA project aims at improving the overall protection level for stations and trains in Europe against terrorist attacks.

This document on best practices aims at fostering integrated approaches on raising awareness on security issues and crisis communication both from and to the railway using public. It also provides examples of mobile applications used by railway companies to enhance internal security communication and reporting on security incidents as well as to improve the provision of security and security information to customers.

Apart from that, the document aims to provide a comprehensive overview on how railway-related communication and social media campaigns targeting an increased security awareness for both personnel and passengers. It aims also at giving an overview on implications – both positive and negative – that the use of digital and social media might have. The document, in addition, gives recommendations on what needs to be considered when using digital and social media for security awareness.

The document is organised in 3 main parts:

- Part A on “Context and challenges”,
- Part B on “Best practices on the use of digital media for raising awareness among the public of customers”,
- Part C on “Recommendations for crisis communication”.

PART A: CONTEXT AND CHALLENGES

1. SECURITY AWARENESS

Security Awareness in facts refers to developing an understanding for security issues. To raise awareness of any given issue is to make someone conscious of something, in this case security[1]. The idea of security awareness is to provide individuals with the tools and know-how to appropriately behave if a security incident is to occur. It also incorporates the idea of the general public becoming actors in their own security, e.g. by reporting suspicious activity. "Awareness is a matter of attitude" - this statement is gladly and often spread. There are many possibilities to influence the attitude of a person or to sharpen it with regard to possible dangers or critical situations.

2. CRISIS COMMUNICATION WITH THE PUBLIC FOR TERRORIST INCIDENTS

Effective crisis communication can be defined as “the provision of effective and efficient messages to relevant audiences during the course of a crisis process[2]”. The main aims of crisis communication are usually recognised as explaining an event and its effects (what has happened, what is expected to happen), whilst providing information to mitigate harm[3]. The aim of information-seeking is to provide relief from the sense of anxiety and distress that anticipating and experiencing a disaster can cause[4]. Indeed, providing timely information can reduce anxiety and contribute to global risk

[1] Chalmers, David (1997). The Conscious Mind: In Search of a Fundamental Theory. *Oxford: Oxford University Press*. pp. 225. ISBN 978-0195105537.

[2] Freberg, K., Saling, K., Vidoloff, K. G., & Eosco, G. (2013). Using value modelling to evaluate social media messages: The case of Hurricane Irene. *Public Relations Review*, 39(3), 185–192. doi:10.1016/j.pubrev.2013.02.010

[3] Ryan, B. (2012). Information seeking in a flood. *Disaster Prevention and Management: An International Journal*, 22(3), 229 – 242.

[4] Seeger M.W., Sellnow T., & Ulmer R.R. (2003): Communication and Organizational Crisis. Westport, CT: Praeger.

reduction[5]. People also expect to receive information written in a language that is jargon-free and easy to understand[6]. Information on the evolving situation and actions advised by official sources allows people to take appropriate action. These options instil a sense of control reducing feelings of uncertainty due to the disaster[7]. Information needs change during the course of a crisis. Initial information needs after a disaster are mainly to understand what happened and to check on family and friends. Shortly after, instead, questions concerning overall survival in the short-term (food, water, shelter and medical assistance) emerge. Finally, people want to know what relief and recovery services are available and what they are entitled to (BBC Action Media, n.d.).

While general crisis communication best practices are mostly applicable to terrorist incidents, they should be considered as a special type of crisis. Indeed, terrorist actions are perpetrated in such a way as to generate massive media attention, thus amplify the impact of their attack, create a desired shock effect and spread their political message worldwide[8]. Being aware of this goal, choosing a counter communication strategy is a challenge. Security authorities are faced with the question of how to communicate on security issues without offering terrorists a broad stage and further public attention.

Another communication challenge regarding terrorist threats is that an objective assessment of terrorist risks by the authorities does not automatically generate public acceptance of the risk assessment. As such, security communication cannot be limited to objective criteria alone. It must also take into account the security perception of individual citizens and the general public perception of terrorist threats.

2.1. Terrorism communication as the main responsibility of the State

As fighting terrorism falls under the responsibility of the State, communication about terrorism is guided by the authorities. However, security communication strategies vary in European Member States. The UK, for example, is a pioneer in broad-based campaigns on the topics of "combating terrorism" and "vigilance against the unusual". In contrast to this, there is relatively little official communication in Germany, Belgium and Italy. In France, communication on terrorism evolved after the attacks in 2015 with the implementation of a public awareness platform[9]. In Poland

[5] Bossu, R., Roussel, F., Fallou, L., Landès, M., Steed, R., Mazet-Roux, G., Dupont, A., Frobert, L., & Petersen, L. (2018). LastQuake: From rapid information to global seismic risk reduction. *International Journal of Disaster Risk Reduction* 28, 32-42. doi: 10.1016/j.ijdrr.2018.02.024.

[6] Kaufman, S., Qing, C., Levenson, N., & Hanson, M. (2012). Transportation During and After Hurricane Sandy. *Rudin Center for Transportation NYU Wagner Graduate School of Public Service*, (November), 1–36.

[7] BBC World Service Trust (2008): Left in the dark: The unmet need for information in humanitarian responses, Policy Briefing #2. Available at: http://downloads.bbc.co.uk/worldservice/trust/pdf/humanitarian_response_briefing.pdf (Accessed 30 March 2017).

[8] Tenscher & Viehrig, „Public Communication in international relations“, 2010, p. 107ff

[9] French Vigipirate platform accessible at https://vigipirate.gouv.fr/

communication about terrorism is also very low-profile. Generally, the authorities, including the relevant services, communicate in this regard.

This means, whichever communication approach is used by authorities will influence and be incorporated into the communication strategy of the railway company.

Of course, as mentioned in Deliverable 3.1, it is important that the responsible authorities work in cooperation with European railway companies to take a systemic approach to security and security communication. The form of cooperation with regard to communication about threats might vary, depending on the legal and organizational embedding of railway companies. E.g., it can be steered by dedicated working groups between the security department of the railway company and ministries responsible for interior or public transport.

2.2. Railway companies' communication policies

Beyond the issue of how the authorities have chosen to address the issue of security and terrorism awareness communication, individual railway companies have different views on what is the best approach to dealing with security awareness. Any communication to public concerning terrorism threats or counter-terrorism measures remain challenging for rail companies whose main business is to provide competitive and undisturbed transport services. While raising security awareness among railway staff, railway customers and station visitors is recognised as an essential ingredient to ensure a good level of security, several other aspects must be considered: marketing, internal policies and previous experience with security incidents.

The marketing perspective poses the question of how to ensure high passenger rates and takes into account the feeling of security of passengers and customers, which forms part and parcel of the public transport product offered to users (Deliverable 3.1).

Previous experience with security issues and terrorist attacks changes the perspective of authorities and citizens. Some companies and countries in Europe have had to face terrible terrorist attacks involving public or railway transport.

As far as communication on security is concerned, there are two different contradictory approaches. Some railway companies and their responsible authorities believe that communicating with customers about security can be reassuring, while other companies and authorities believe that it must be approached very restrictively in order to avoid the risk of creating anxiety and false suspicion. It leads to contrary approaches in the European railway landscape. The differences can be seen in the way awareness campaigns are steered and how they are set up.

PART B: BEST PRACTICES

1. RESULT OF THE WORKSHOP

On January 23rd, 2020, the fifth SHERPA workshop on “Raising Security Awareness & the use of Digital Media” was held in Berlin at the DB co.lab. Around 25 participants from ten countries (Austria, Belgium, France, Germany, Netherlands, Italy, Poland, Sweden, Switzerland and UK) attended this workshop, which was organised in a very interactive manner.

During the morning session, many UIC members shared examples from their own security awareness campaigns.

FS presented its public security and anti-aggression campaign “be aware make a difference”, in which children ask potential aggressors not to touch or attack their parents. This campaign was very well received by both the public and the employees.

Focusing on staff security awareness, NS shared their “Bewust & Alert” films, which educate staff members on how to respond to left luggage.

Regarding the general public’s security awareness, PKP S.A presented their “aware = safe” films. PKP S.A also presented the “be aware / vade-mecum” campaign, which was launched to raise awareness of abandoned luggage after a fine was imposed on owners of such luggage.

SNCB showed their “quelque chose de suspect?” posters, which apply a humoristic approach when inciting citizens to report suspicious behaviours and items. They also showed posters from their Securail campaign.

The British Transport Police, together with Arriva, discussed both their “see it, say it, sorted” posters & train station announcements (for high risk trains, a user will hear the slogan every 5 minutes), which touch on the British culture by using the word “sorted”, aka taken care of, as well as their “61016” texting service for users to report crime or incidents on trains and at stations.

ARRIVA (as UITP member) presented an employee awareness campaign to deal with suspicious items and suspicious behaviour of employees and customers. In this context, it is planned to issue printed information that is to be translated into several languages. The topic of terrorist threats based on insider knowledge was also addressed.

The first afternoon session focused on the French *Vigipirate* security plan. A representative from the French Ministry of transport explained the Vigipirate plan and its implementation in France. While the plan itself has been around since before the 2015 terrorist attacks in France, those incidents reinforced the need to create a security culture among citizens. As one of the critical infrastructures cited in the Vigipirate plan, SNCF has had to implement various security measures. Thus, SNCF shared various security raising campaigns they have implemented for their staff, including two videos on the importance of always closing security doors and always reporting left luggage.

In the afternoon, the focus shifted more clearly to digital media. The development and implementation of DB's mobile application on situations and security operations was presented. This is an app intended for DB employees and relevant security actors (such as the German Federal Police) and is not available for the general public. The main advantage of the app over previous systems is its rapidity in informing the relevant people of a crisis.

Next, the UIC Security Division presented on how to better use social media for crisis communication and shared examples from UIC members using social media to effectively communicate with the general public during a crisis. The TACT (Training, Awareness and Communication Tools) Toolbox, which gathers many best practices from the members, was also presented. It's available on the UIC security private workspace. The workshop successfully helped UIC members and project partners share best practice when it comes to security awareness for both staff and users.

HEY VOLEUR DE VÉLO, TU ES OÙ ?
QUELQUE CHOSE DE SUSPECT ?
QUELQUE CHOSE DE SUSPECT ?

2. COMMUNICATION CAMPAIGNS FOR SECURITY AWARENESS

2.1. Introduction

Security Awareness has been moving increasingly in the focus of the Corporate security over the last years. It has become common sense that the level of security in a company cannot be improved without an increase in security awareness of the individual employee. The achievement of a positive and active support by all employees is seen as essential company and security task.

A proven means of sensitizing employees to security in the company is the implementation of awareness campaigns. The goal of such a campaign is ambitious, since the aim is not to achieve just a short-term effect, but rather a long-term change in employee behaviour. The core content of such a campaign is usually the set of rules in the security policy of the company or the guidelines provided by the responsible authorities, both formulating concrete behavioural requirements and instructions.

Besides the awareness raising among employees, the raising of security awareness among customers is more challenging. It must reflect the security communication strategy of the responsible authorities and balance it with the companies' communications strategy. In most of the cases such campaigns for customers are designed in cooperation with or under the supervision of the authorities.

Whatever the direction of the campaigns, they are usually designed for a longer period of up to several years and can be divided into different aims:

- **Attention raising:** The aim is to gain attention and encourage active participation.
- **Imparting knowledge and changing attitudes:** The campaign is designed to provide the knowledge necessary for understanding security measures and aims to change attitudes (and thus individual behaviour). It is the most important and at the same time most challenging part of the campaign.
- **Reinforcement:** a lasting change in attitude and behaviour is sought. Awareness measures are recommended which firmly anchor the topic in the consciousness and keep it awake.

2.2. Examples of Best Practices

2.2.1. SNCB (Belgium)

Security is a key issue for SNCB and is defined in the context of its public service missions and in the strategic security plan of its Corporate Security Service.

Security awareness within SNCB is not limited to the risks of a terrorist attack, but revolves around other security themes for which the risk of occurrence, the impact on the feeling of security and prevention possibilities are the most important, namely: securing your workspace, intrusions, thefts, vandalism, assaults.

2.2.1.1. General public awareness

2.2.1.1.1. Campaigns

Terrorism

Regarding the terrorist threat, a campaign was broadcast between 2016 and 2018 to raise awareness among travellers and employees about the detection and reporting of non-attended luggage.

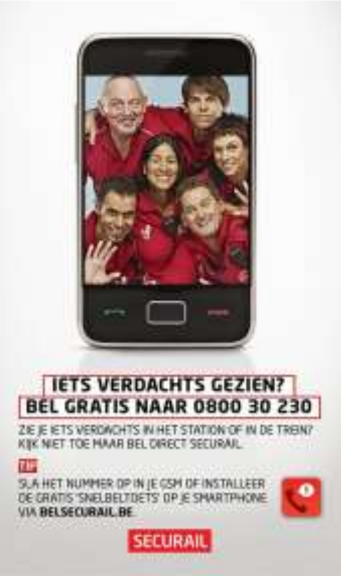
Suspicious behaviour and security

SNCB launched an awareness campaign in 2010 to encourage anyone using the railways to report any suspicious behaviour. The subject was treated in a humorous manner in order to grab the public's attention while minimizing the potential feeling of insecurity. This campaign also included the dissemination of the free emergency number of SNCB and was followed by a second one to highlight this number again, but also the Security service Securail. These campaigns were broadcast in stations as well as on social networks.

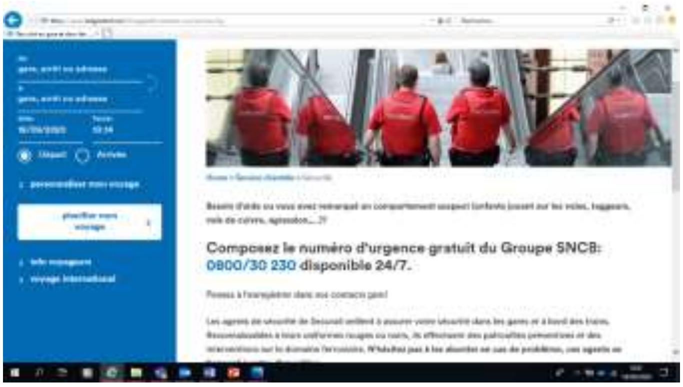
QUELQUE CHOSE
DE SUSPECT?
B

QUELQUE CHOSE
DE SUSPECT?
B

QUELQUE CHOSE
DE SUSPECT?
B


IETS VERDACHTS GEZIEN?
BEL GRATIS NAAR 0800 30 230
ZIE JE IETS VERDACHTS IN HET STATION OF IN DE TREIN?
KIJK NIET TOE MAAR BEL DIRECT SECURAIL.
TIP
SLA HET NUMMER OP IN JE GSM OF INSTALLEER
DE GRATIS 'SNELBELTDETS' OP JE SMARTPHONE
VIA BELSECURAIL.BE
SECURAIL

SOS
SECURAIL
0800 30 230
7/7 - 24/24 - Numéro gratuit



Besoin d'aide ou vous avez remarqué un comportement suspect (enfants jouant sur les voies, tagueurs, vols de cuivre, agression,...)?

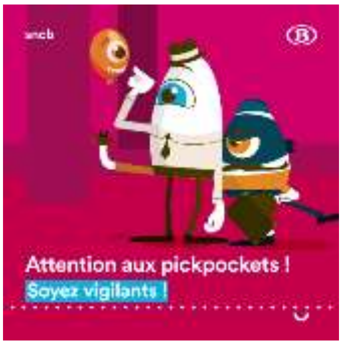
Composez le numéro d'urgence gratuit du Groupe SNCB: 0800/30 230 disponible 24/7.

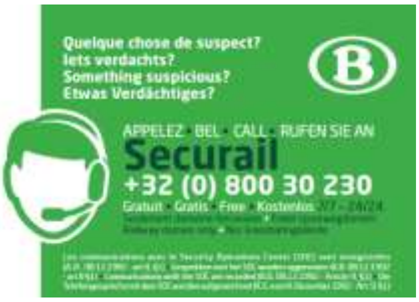
Pensez à l'enregistrer dans vos contacts gsm!

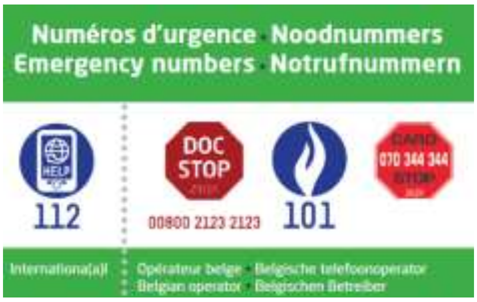
Les agents de sécurité de Securail veillent à assurer votre sécurité dans les gares et à bord des trains. Reconnaissables à leurs uniformes rouges ou noirs, ils effectuent des patrouilles préventives et des interventions sur le domaine ferroviaire. N'hésitez pas à les aborder en cas de problème, ces agents se

Pickpocketing

Each year, campaigns to increase customer vigilance regarding pickpocketing are organized. In the form of video and audio messages, but also in the form of role-plays in trains and stations in order to maximize the impact of awareness-raising. The campaigns are disseminated on social networks and information cards (bank card format) are distributed to people exhibiting risky behaviour.

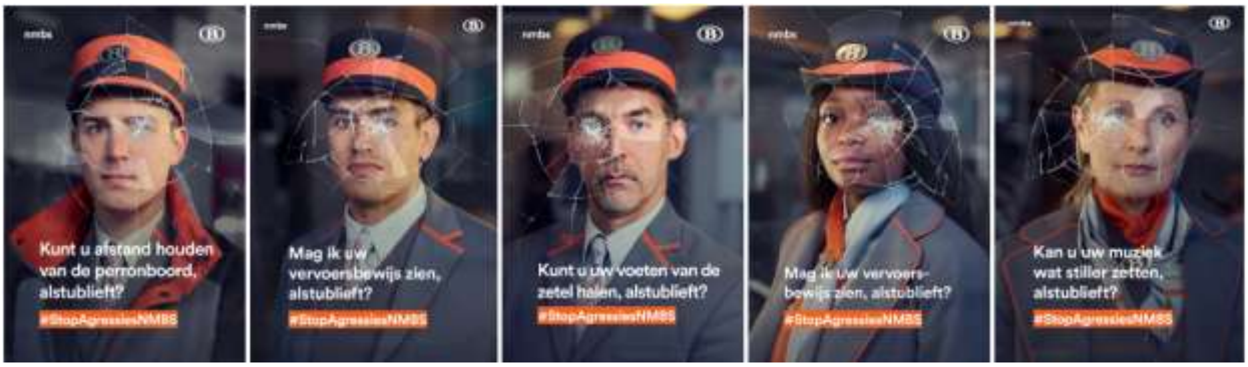



Quelque chose de suspect?
Iets verdachts?
Something suspicious?
Etwas Verdächtiges?
APPELEZ · BEL · CALL · RUFEN SIE AN
Securail
+32 (0) 800 30 230
Gratuit · Gratis · Free · Kostenlos 7/7 - 24/24


Numéros d'urgence Noodnummers
Emergency numbers Notrufnummern
112
DOC STOP
00800 2123 2123
101
CARD STOP
070 344 344
International(e)
Opérateur belge · Belgische telefoonoperator
Belgian operator · Belgischen Betreiber

Assault

At the end of 2018, the SNCB launched a campaign aimed at combating attacks against SNCB staff: #STOPAGRESSIONSNCB. The visuals were broadcast on digital screens allowing interaction with the public and on social networks. In the meantime, trade unions organised an action to ask passengers to put post-it notes with the campaign title on the windows of the trains.


Kunt u afstand houden van de perronboord, alstublieft?
#StopAgressiesNMBS
Mag ik uw vervoersbewijs zien, alstublieft?
#StopAgressiesNMBS
Kunt u uw voeten van de zetel halen, alstublieft?
#StopAgressiesNMBS
Mag ik uw vervoersbewijs zien, alstublieft?
#StopAgressiesNMBS
Kan u uw muziek wat stiller zetten, alstublieft?
#StopAgressiesNMBS

Videos

Two videos featuring a Securail security agent in his daily tasks were broadcasted on YouTube in 2011 and 2015 in order to raise public awareness about SNCB's security missions. These video clips have respectively received more than 60,000 and 23,000 views. https://www.youtube.com/watch?v=mZV_XDw_AQo,
https://www.youtube.com/watch?v=DQ2VzvweXbQ

During the spring 2020, one public TV Channel realised a show filmed on a train crossing the country. This show conveyed the image of safe public transportation and highlighted the work of Securail officers during the COVID-19 era.
https://www.een.be/tussen-eupen-en-oostende

Educational tool

SNCB has developed an educational tool to raise awareness among children aged 8 to 14 about the appropriate and safe use of railways. It can be delivered by a CSS employee or the teachers themselves and is accompanied by videos, a quiz and games to play in the classroom. This tool presents SNCB and the security service, various security themes and the consequences they entail. It also encourages auditors to be attentive to safety rules and to report any suspicious behaviour via the free emergency number mentioned above.

2.2.1.2. SNCB's staff awareness

Security Awareness is integrated in the security strategy and therefore plays an important role towards customers, but also and above all towards SNCB staff, the company's first line of defense. It can both increase the feeling of security and help to develop a culture of security within the company. Security awareness dedicated to members of staff built as part of a strategy focused on Security Awareness, can significantly increase the level of security of an organization by being aware of the risks, and being able to act in a preventive and reactive way based on these risks.

The actions taken about Security Awareness won't be the same nor be approached with the same method nor will necessarily concern the same categories of staff for all topics. Nevertheless, the goal pursued remains the same: to enable each employee to understand the importance of security within SNCB, to be aware of what is expected of them in this context and to behave adequately according to the theme. It is therefore a matter of building and maintaining a protection-oriented behavior, workers being considered Security Aware when they:

- know why it is important to work in a secure environment;
- know what it looks like in their company;
- are involved in securing the company;
- know how to recognize security related incidents; and
- know how to act to secure their company.

Trainings

In this context, operational training systematically includes a security awareness section and the procedures to be followed in the event of a crisis. In addition, some of the field staff most likely to be confronted with suspicious behavior and a terrorist tactic (security staff and station managers) have received additional training specifically aimed at developing their security culture and protection, as well as in-depth knowledge of event management in the face of a threat.

2.2.1.2.1. Campaigns

Terrorism

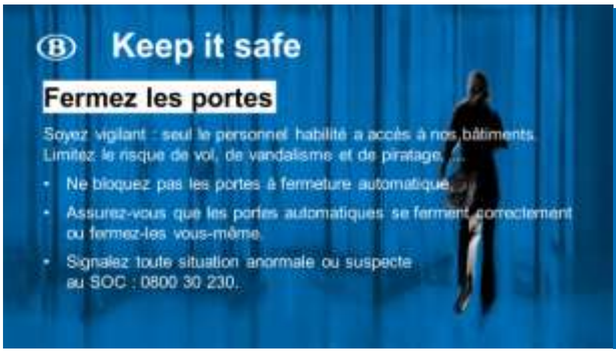
Communications based on advice from the Belgian Federal Crisis Center were also disseminated with regards to terrorist attacks.

Aware & Secure
Voici quelques réflexes à adopter et conseils formulés par le centre de crise:
1. Au Quotidien
2. Si vous vous trouvez sur le lieu d'une explosion
3. Si vous vous trouvez sur le lieu d'une attaque à main armée
4. Si vous vous trouvez sur le lieu d'une attaque CBRN
112

Security awareness

SNCB has developed a visual campaign aimed at raising awareness among all staff members (both operational and managerial) of protection-oriented behaviour. This campaign, called "Keep it safe", was broadcasted in June and September 2019 on the company's intranet. This campaign was developed in the form of texts explaining the risks and providing advice on the following points:

- Securing access;
- Lost / stolen badges;
- Welcoming visitors;
- Clean desk;
- Confidentiality;
- Business trips.

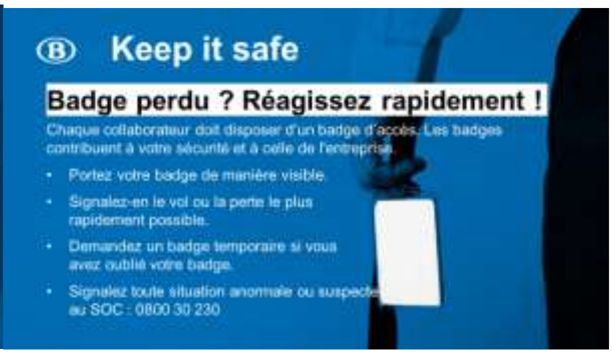


Keep it safe

Fermez les portes

Soyez vigilant : seul le personnel habilité a accès à nos bâtiments. Limitez le risque de vol, de vandalisme et de piratage, …

- Ne bloquez pas les portes à fermeture automatique.
- Assurez-vous que les portes automatiques se ferment correctement ou fermez-les vous-même.
- Signalez toute situation anormale ou suspecte au SOC : 0800 30 230.

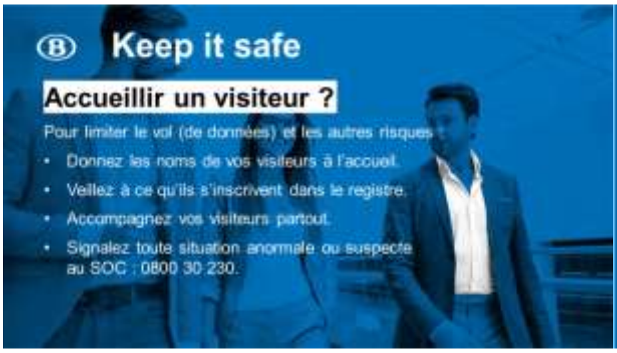


Keep it safe

Badge perdu ? Réagissez rapidement !

Chaque collaborateur doit disposer d'un badge d'accès. Les badges contribuent à votre sécurité et à celle de l'entreprise.

- Portez votre badge de manière visible.
- Signalez-en le vol ou la perte le plus rapidement possible.
- Demandez un badge temporaire si vous avez oublié votre badge.
- Signalez toute situation anormale ou suspecte au SOC : 0800 30 230

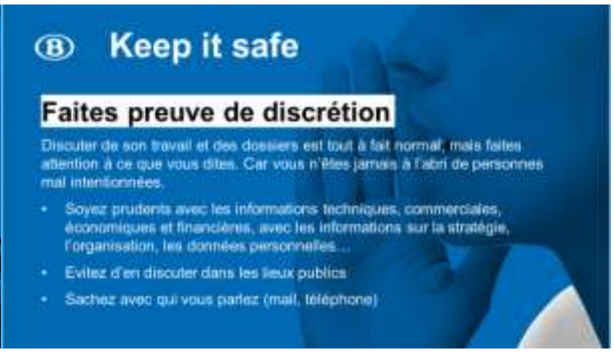


Keep it safe

Accueillir un visiteur ?

Pour limiter le vol (de données) et les autres risques

- Donnez les noms de vos visiteurs à l'accueil.
- Veillez à ce qu'ils s'inscrivent dans le registre.
- Accompagnez vos visiteurs partout.
- Signalez toute situation anormale ou suspecte au SOC : 0800 30 230.



Keep it safe

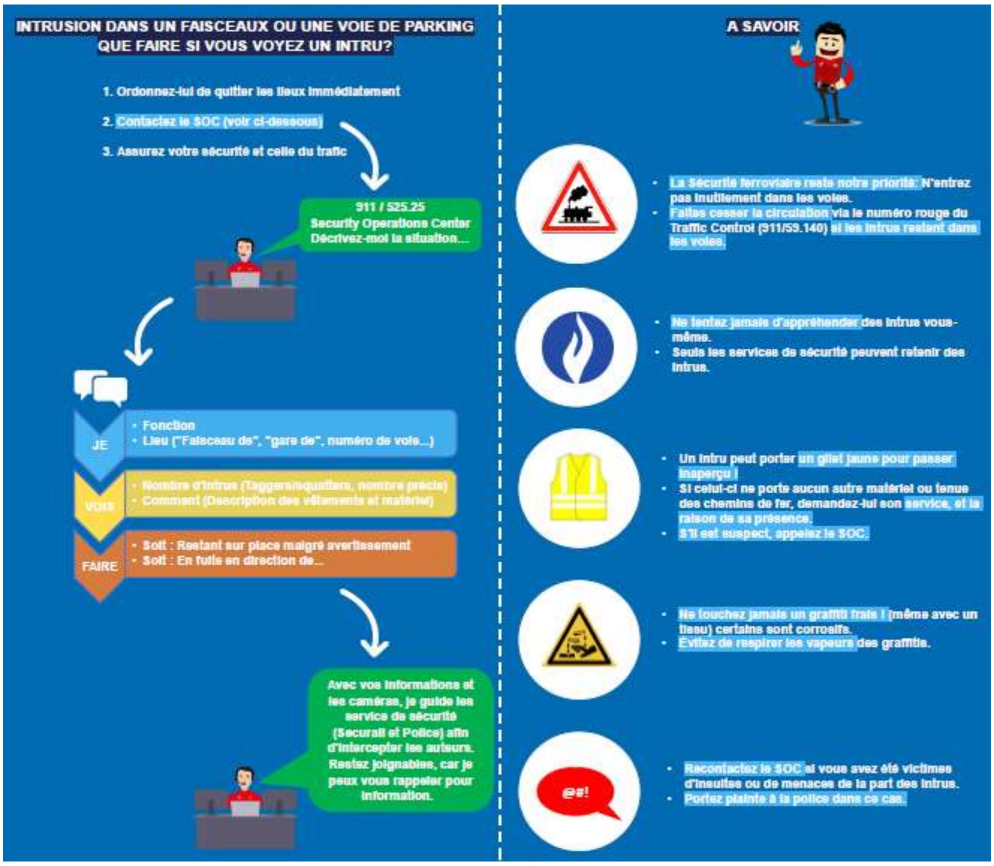
Faites preuve de discrétion

Discuter de son travail et des dossiers est tout à fait normal, mais faites attention à ce que vous dites. Car vous n'êtes jamais à l'abri de personnes mal intentionnées.

- Soyez prudents avec les informations techniques, commerciales, économiques et financières, avec les informations sur la stratégie, l'organisation, les données personnelles…
- Evitez d'en discuter dans les lieux publics
- Sachez avec qui vous parlez (mail, téléphone)

Local initiatives have also been put in place for very specific incidents, such as thefts in administrative buildings.

Other projects are under development but have not yet been released, particularly in terms of securing sensitive sites in the event of a terrorist attack, as well as concerning intrusions.



INTRUSION DANS UN FAISCEAUX OU UNE VOIE DE PARKING
QUE FAIRE SI VOUS VOYEZ UN INTRU?

1. Ordonnez-lui de quitter les lieux immédiatement
2. Contactez le SOC (voir ci-dessous)
3. Assurez votre sécurité et celle du trafic

911 / 525.25
Security Operations Center
Décrivez-moi la situation…

JE
- Fonction
- Lieu ("Faisceau de", "gare de", numéro de voie…)

VOIS
- Nombre d'intrus (Taggers/squatters, nombre précis)
- Comment (Description des vêtements et matériel)

FAIRE
- Soit : Restant sur place malgré avertissement
- Soit : En fuite en direction de…

Avec vos informations et les caméras, je guide les service de sécurité (Securail et Police) afin d'intercepter les auteurs. Restez joignables, car je peux vous rappeler pour information.

A SAVOIR

- La sécurité ferroviaire reste notre priorité: N'entrez pas inutilement dans les voies.
- Faites cesser la circulation via le numéro rouge du Traffic Control (911/59.140) si les intrus restent dans les voies.

- Ne tentez jamais d'appréhender des intrus vous-même.
- Seuls les services de sécurité peuvent retenir des intrus.

- Un intru peut porter un gilet jaune pour passer inaperçu !
- Si celui-ci ne porte aucun autre matériel ou tenue des chemins de fer, demandez-lui son service, et la raison de sa présence.
- S'il est suspect, appelez le SOC.

- Ne touchez jamais un graffiti frais ! (même avec un tissu) certains sont corrosifs.
- Evitez de respirer les vapeurs des graffitis.

- Recontactez le SOC si vous avez été victimes d'insultes ou de menaces de la part des intrus.
- Portez plainte à la police dans ce cas.

2.2.2. SNCF Corporate Security (France)

2.2.2.1. The principles of the SNCF corporate security plan

The SNCF corporate security plan is designed to protect persons using railway facilities from the threat of terrorism and uses a managerial approach. This may include the SNCF staff, their service providers, the stores operating within train stations, or, of course, the customers that use the trains and come to their stations. The plan also aims to preserve the cultural heritage as well as the goods transported. To achieve this objective, it relies on government or zonal plans that implement France's strategy against terrorism. With the higher level, more diffuse and potentially multifaceted threat that is terrorism, the protection of people on railway infrastructures is mainly the responsibility of all transport operators and SNCF personnel. Therefore, the purpose of the SNCF corporate security plan is to strengthen the basis for the protection of the rail system.

The aim is to instill a security culture, so that staff spontaneously adopt the right behavior and apply the necessary procedures

The plan is made up of capacity sheets describing in particular:

- Protection measures for SNCF facilities, which depend on and are adapted to the vulnerability of the site. For example, protection devices against ram-vehicles, evacuation procedures, handling of bomb threats or unattended items, unauthorized entrance to (?) buildings and facilities.
- The expected knowledge staff need in order to react in the best possible way in case of an attack. For example, knowing how to evacuate a station or give instructions to passengers on board of a train.
- The behavior that everyone (staff and public) must adopt in the event of an attack to avoid being exposed to the threat and to facilitate the intervention of law enforcement and rescue services.

In addition to these behavioural prescriptions, The SNCF corporate security plan is intended to be the main method for managers to monitor security within their perimeter. To achieve this aim, the SNCF Corporate Security Plan details various tools that can be used by the management team, such as:

- Vulnerability analyses to be carried out in the most sensitive entities
- Action plans to be carried out
- Managerial kits for managers
- The description of the steering and control of actions by the departments.

2.2.2.2. Implementation of the SNCF corporate security plan

The first step in implementing the SNCF corporate security plan is to convince operational managers of the importance of promoting a security culture by demonstrating what is at stake. It is also important that they are provided with simple tools to enable a security culture with their staff. Indeed, the SNCF Corporate Security Plan was designed in such a way as to be educational and easily implementable. While the SNCF Security Directorate manages the implementation process, it is up to the business activities to apply the tools and create a security culture with staff, depending on to the evolution of the threat, the adaptations of the governmental plan, the application of procedures and the level of awareness of what is at stake.

2.2.2.3. Awareness-raising tools

Managers must be able to easily discuss with their staff the various issues related to the adoption of good security behaviors. The training of managers and security correspondents is a priority to ensure that all of them master the expectations of full implementation of the Corporate Security Plan, using the tools and exercises at their disposal.

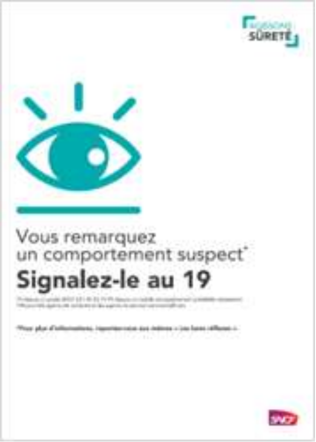
Numerous awareness-raising tools have been created for managers in different formats depending on the sensitivities of the very heterogeneous SNCF population. They form the managerial kit, which aims to help the manager talk about security in order to guide staff in knowing, applying and mastering the right security behaviors and procedures.

The managerial kit includes, among other things:

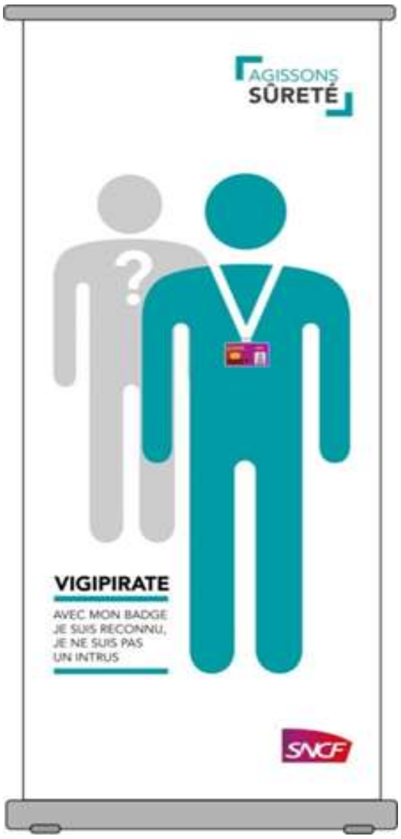
- A graphic identity created specifically for the managerial approach of the SNCF Corporate Security Plan, which can be found on all communication media related to the SNCF Corporate Security Plan.

AGISSONS
SÛRETÉ

- Security memos created for each SNCF business line, including all the behaviors to adopt and procedures to apply.
- Videos and animatics of a few seconds on security behaviors and procedures.
- A poster with one and only one clear message (calling the 19 to alert)
- A "serious game", which is a pedagogical group animation. The objective is to solve a series of puzzles on security themes.



- A kakemono to explain that it is necessary to wear a visible badge not to be considered an intruder.
- A nudge representing a padlock that is half placed on a secured door and the other half on its frame. The padlock is complete when the door is closed.
- An animation with cards (actions, quiz, information, debate...) that will allow managers to animate security by following an instruction manual. These cards include the language elements to be used during awareness raising.



2.2.3. DB AG (Germany)

Behavior in case of terrorism:

The police authorities in Germany responsible for combatting terrorist threats have published an informational leaflet that deals with the unpredictability of life-threatening situations. As it is understood that there are no generally applicable rules of conduct for extreme situations such as terrorist attacks, acts of aggression or armed attacks, the information sheet provides essential information to be well prepared and able to act safely in an emergency.

Regarding the basic recommendation "Escape. Hide. Alert." there are behavioral tips that are directed at individuals not only in the rail sector. The tips point out ways of protecting oneself and helping others. Pictograms are used to illustrate the tips.

Schutz bei Terror und Amok

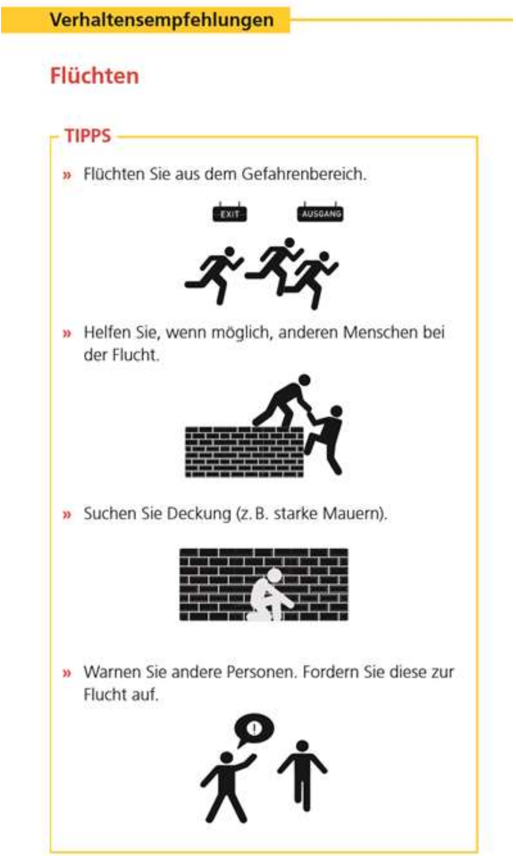
Flüchten. Verstecken. Alarmieren.

Verhaltenstipps für die Bevölkerung

Wir wollen, dass Sie sicher leben.

Ihre Polizei

Kompetent. Kostenlos. Neutral.



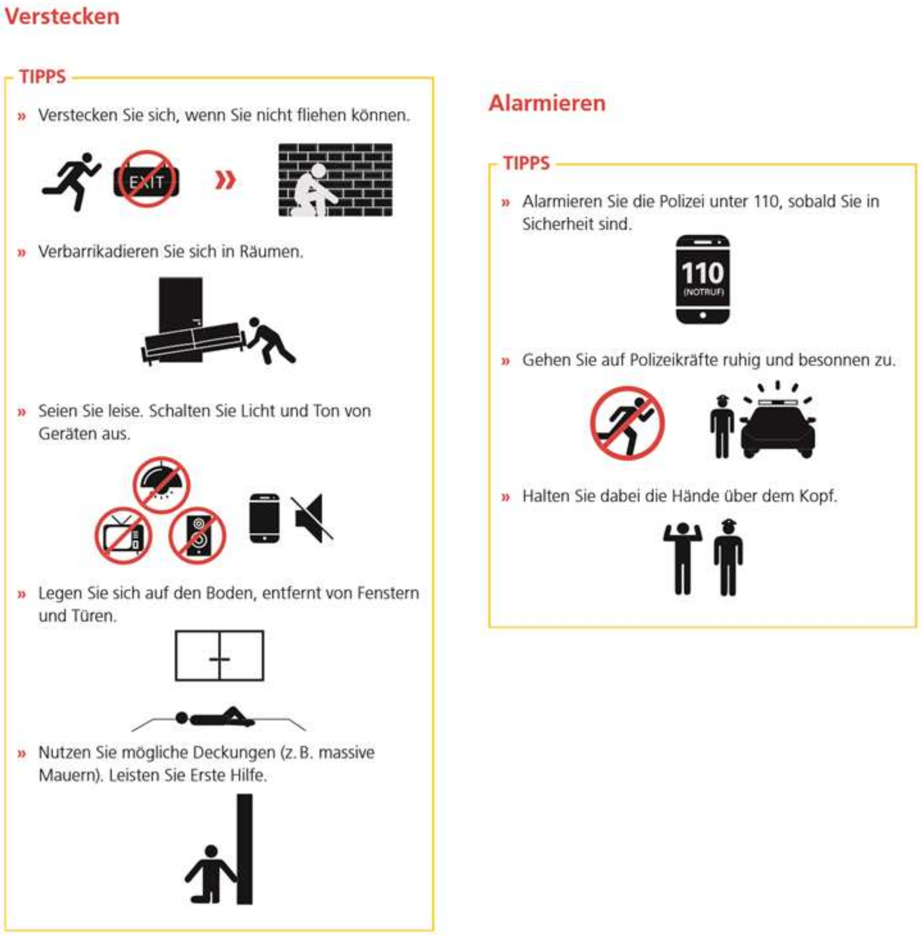
Verhaltensempfehlungen

Flüchten

TIPPS

- » Flüchten Sie aus dem Gefahrenbereich.
- » Helfen Sie, wenn möglich, anderen Menschen bei der Flucht.
- » Suchen Sie Deckung (z. B. starke Mauern).
- » Warnen Sie andere Personen. Fordern Sie diese zur Flucht auf.

EXIT
AUSGANG



Verstecken

TIPPS

» Verstecken Sie sich, wenn Sie nicht fliehen können.

» Verbarrikadieren Sie sich in Räumen.

» Seien Sie leise. Schalten Sie Licht und Ton von Geräten aus.

» Legen Sie sich auf den Boden, entfernt von Fenstern und Türen.

» Nutzen Sie mögliche Deckungen (z. B. massive Mauern). Leisten Sie Erste Hilfe.

Alarmieren

TIPPS

» Alarmieren Sie die Polizei unter 110, sobald Sie in Sicherheit sind.

» Gehen Sie auf Polizeikräfte ruhig und besonnen zu.

» Halten Sie dabei die Hände über dem Kopf.

The basic recommendations given contain the following:

- **Escape**: Escape from the danger zone. Warn people present, e.g. by means of loudspeaker announcements and other existing alarms. Identify locations and events as accurately as possible. Open all escape routes. Show others these escape routes. Make sure that everyone moves as far away from the danger zone as possible in a calm and coordinated manner.
- **Hide**: Help people to hide if escape is not possible. Open suitable rooms or parts of buildings that are made of solid masonry, do not have floor-to-ceiling windows and are lockable. Show people the way to these rooms. Barricade yourself together in suitable rooms. Show possibilities of covering, e.g. strong walls or columns. Ask everyone to remain calm. Mute all equipment immediately, but make sure that you can maintain contact with the police, i.e. do not switch off the equipment/put in flight mode. Do not send information (pictures, videos, text messages) via social media (e.g. Twitter, Facebook) directly or to friends and family. This information will lead to a flood of information on the part of the authorities and may eventually be received by the assassins, thus revealing the hiding place. Lie down on the floor, away from windows and doors. Give first aid.
- **Alert**: Alert the police - as soon as you are safe. Dial the emergency number 110. Give your name, location and function. Explain the situation. Describe as precisely as possible the location and appearance of the possible perpetrators or how the crime is developing. Stay on the phone and follow the instructions of the police.
- **Help the police.** "Walk slowly towards the arriving police forces.” "Keep your hands above your head.” "Follow the instructions of the police.” "Describe the events only in your own perception

and do not distribute any unconfirmed information.” "Be sensitive and reserved when publishing pictures on the internet.” “Do not pass on rumors via social media.”

Federal Police and DB Corporate Security:

The Federal Police performs police tasks in the area of the railway installations of the federal railways, for example in the railway stations. They are responsible for averting threats to public security there. In detail, the Federal Police has its main areas of operation in the preventions of threats and prosecution of offenders in the stations and on the railway tracks.

In addition to the proven security cooperation with the police forces of the federal states in Germany, a successful partnership for security has been established between the Federal Police and DB Corporate Security since 2000. A special area of cooperation relates to prevention work and raising security awareness. In this field, a permanent working group regularly takes initiatives on critical topics. An example for the output of the working group is a campaign to enhance civil courage in critical situations.

Enhancing civil courage:

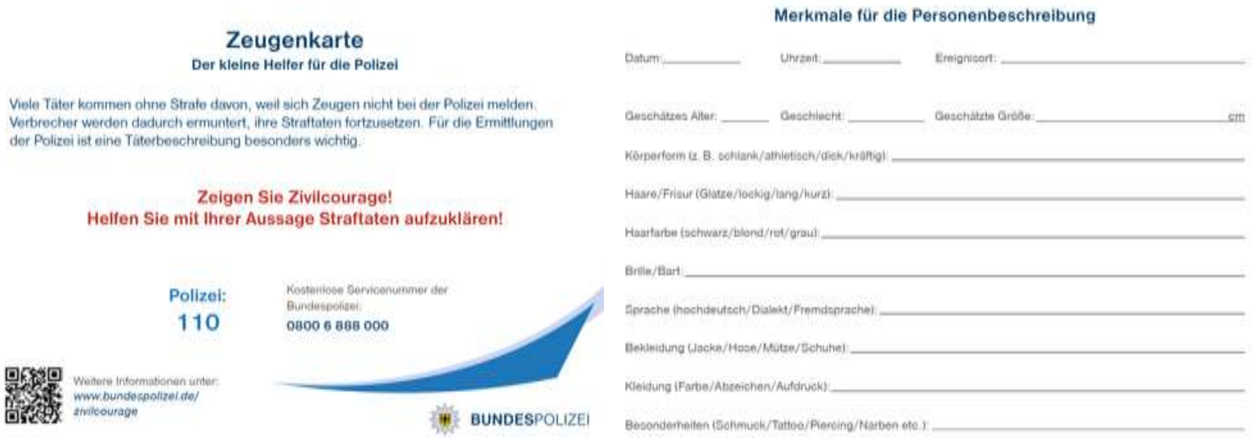
Civil courage concerns everyone! Under this motto, a short film was created in 2018 by the cooperation of DB and the Federal Police, which calls for more moral courage.
As a general message, the video provides rules for behavior in critical situations and is intended to show that everyone, regardless of age, sex, height or physique, can provide help without putting oneself in danger.

DB
Handeln Sie gefahrlos
Fordern Sie Mithilfe
Sehen Sie genau hin
Holen Sie Hilfe
Versorgen Sie Opfer
Helfen Sie als Zeuge mit
www.bundespolizei.de/zivilcourage

1. Help without putting yourself in danger:
It is not about "playing the hero" - even a cautious reaction can help! Do not look away, be attentive, talk directly to other (possible) helpers or say loudly that you are organizing help. This can already help the victim to get away.

2. Actively and directly ask others to help: Get help from other people. Talk to the man in the red jacket who is just coming out of the store or contact the train personnel. Ask for help. It is difficult to avoid such a direct approach.

3.Observe closely and memorize perpetrator characteristics: What did the perpetrator look like? What clothes did he wear? Where did he go? The police are dependent on support. Often it is small details that help to ensure that the perpetrator can be held responsible. Use the "Witness Card":



Zeugenkarte

Der kleine Helfer für die Polizei

Viele Täter kommen ohne Strafe davon, weil sich Zeugen nicht bei der Polizei melden. Verbrecher werden dadurch ermuntert, ihre Straftaten fortzusetzen. Für die Ermittlungen der Polizei ist eine Täterbeschreibung besonders wichtig.

Zeigen Sie Zivilcourage!
Helfen Sie mit Ihrer Aussage Straftaten aufzuklären!

Polizei:
110

Kostenlose Servicenummer der Bundespolizei:
0800 6 888 000

Weitere Informationen unter:
www.bundespolizei.de/zivilcourage

BUNDESPOLIZEI

Merkmale für die Personenbeschreibung

Datum: ________ Uhrzeit: ________ Ereignisort: ________

Geschätzes Alter: ________ Geschlecht: ________ Geschätzte Größe: ________ cm

Körperform (z. B. schlank/athletisch/dick/kräftig): ________

Haare/Frisur (Glatze/lockig/lang/kurz): ________

Haarfarbe (schwarz/blond/rot/grau): ________

Brille/Bart: ________

Sprache (hochdeutsch/Dialekt/Fremdsprache): ________

Bekleidung (Jacke/Hose/Mütze/Schuhe): ________

Kleidung (Farbe/Abzeichen/Aufdruck): ________

Besonderheiten (Schmuck/Tattoo/Piercing/Narben etc.): ________

4. Organize help under emergency call 110: anyone can dial the toll-free emergency call number 110. You don't have a cell phone, or the phone battery is empty? Then ask another person to call the police immediately. It is important to describe the situation briefly and concisely: Where is the event? Who is calling? What happened? How many people are were affected?

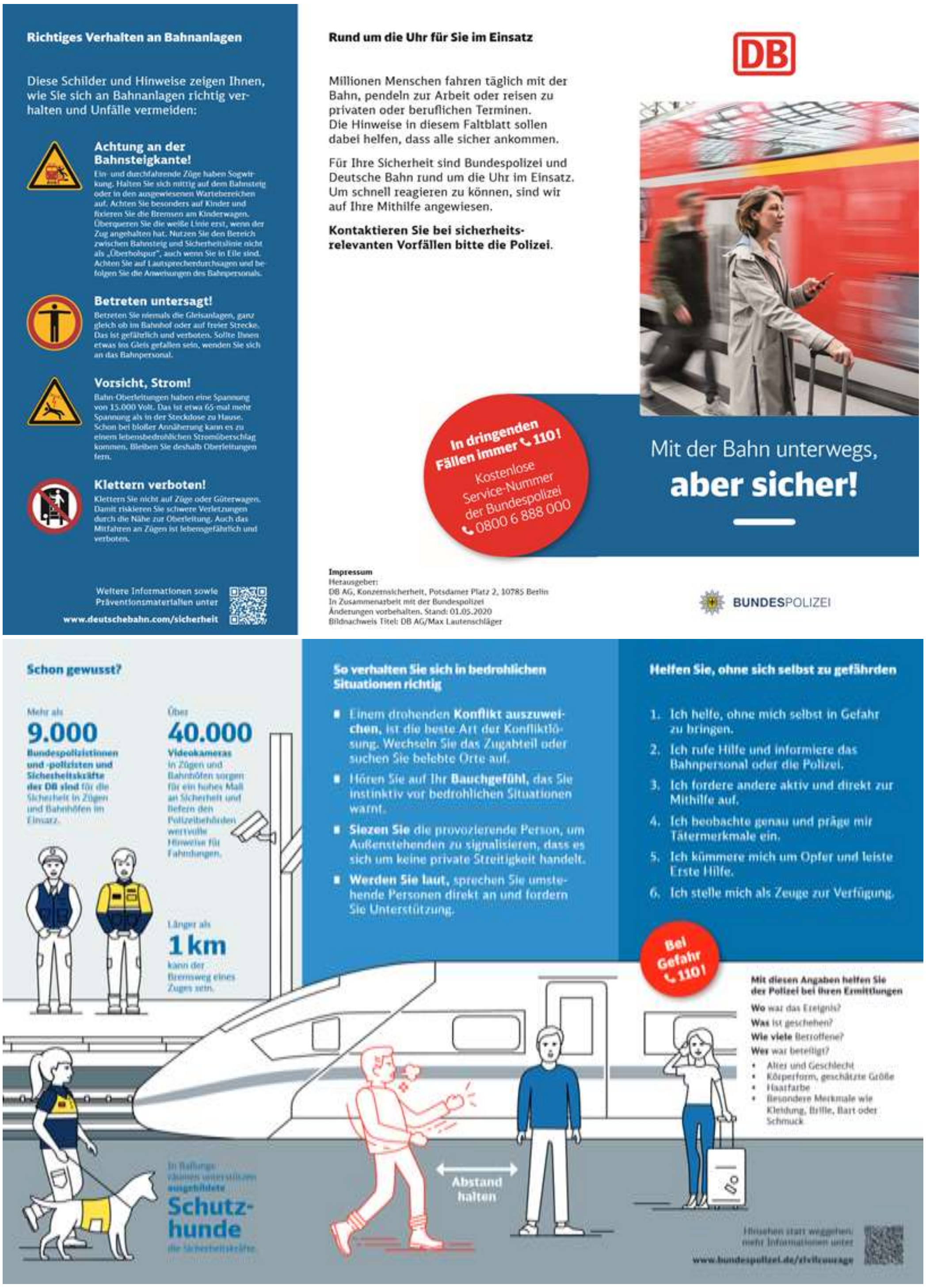
5. Take care of victims: First aid can be vital! Therefore, take care of injured persons immediately. Get an overview of how you can provide help. Also ask other people for support.

6. Make yourself available as a witness: with your statement on what happened, you contribute to the comprehensive clarification of the crime.

In line with the video, the Federal Police offers training for different age groups on the subject of civil courage. In these courses, federal police officers give tips on how to behave prudently as a witness and helper in critical situations without putting oneself in danger.

Raising Security Awareness:

Together with the Federal Police, DB's partner for threats on rail premises, DB Corporate Security has for years been raising awareness among customers and employees about common criminal offences such as pickpocketing and about moral courage. The focus of a new initiative is on safe behavior in trains and stations, with facts and background knowledge, without being too didactic.



Richtiges Verhalten an Bahnanlagen

Diese Schilder und Hinweise zeigen Ihnen, wie Sie sich an Bahnanlagen richtig verhalten und Unfälle vermeiden:

Achtung an der Bahnsteigkante!
Ein- und durchfahrende Züge haben Sogwirkung. Halten Sie sich mittig auf dem Bahnsteig oder in den ausgewiesenen Wartebereichen auf. Achten Sie besonders auf Kinder und fixieren Sie die Bremsen am Kinderwagen. Überqueren Sie die weiße Linie erst, wenn der Zug angehalten hat. Nutzen Sie den Bereich zwischen Bahnsteig und Sicherheitslinie nicht als „Überholspur", auch wenn Sie in Eile sind. Achten Sie auf Lautsprecherdurchsagen und befolgen Sie die Anweisungen des Bahnpersonals.

Betreten untersagt!
Betreten Sie niemals die Gleisanlagen, ganz gleich ob im Bahnhof oder auf freier Strecke. Das ist gefährlich und verboten. Sollte Ihnen etwas ins Gleis gefallen sein, wenden Sie sich an das Bahnpersonal.

Vorsicht, Strom!
Bahn-Oberleitungen haben eine Spannung von 15.000 Volt. Das ist etwa 65-mal mehr Spannung als in der Steckdose zu Hause. Schon bei bloßer Annäherung kann es zu einem lebensbedrohlichen Stromüberschlag kommen. Bleiben Sie deshalb Oberleitungen fern.

Klettern verboten!
Klettern Sie nicht auf Züge oder Güterwagen. Damit riskieren Sie schwere Verletzungen durch die Nähe zur Oberleitung. Auch das Mitfahren an Zügen ist lebensgefährlich und verboten.

Weitere Informationen sowie Präventionsmaterialien unter
www.deutschebahn.com/sicherheit

Rund um die Uhr für Sie im Einsatz

Millionen Menschen fahren täglich mit der Bahn, pendeln zur Arbeit oder reisen zu privaten oder beruflichen Terminen. Die Hinweise in diesem Faltblatt sollen dabei helfen, dass alle sicher ankommen.

Für Ihre Sicherheit sind Bundespolizei und Deutsche Bahn rund um die Uhr im Einsatz. Um schnell reagieren zu können, sind wir auf Ihre Mithilfe angewiesen.

Kontaktieren Sie bei sicherheitsrelevanten Vorfällen bitte die Polizei.

In dringenden Fällen immer ☎ 110!
Kostenlose Service-Nummer der Bundespolizei ☎ 0800 6 888 000

Impressum
Herausgeber:
DB AG, Konzernsicherheit, Potsdamer Platz 2, 10785 Berlin
In Zusammenarbeit mit der Bundespolizei
Änderungen vorbehalten. Stand: 01.05.2020
Bildnachweis Titel: DB AG/Max Lautenschläger

DB

Mit der Bahn unterwegs,
aber sicher!

BUNDESPOLIZEI

Schon gewusst?

Mehr als
9.000
Bundespolizistinnen und -polizisten und Sicherheitskräfte der DB sind für die Sicherheit in Zügen und Bahnhöfen im Einsatz.

Über
40.000
Videokameras in Zügen und Bahnhöfen sorgen für ein hohes Maß an Sicherheit und liefern den Polizeibehörden wertvolle Hinweise für Fahndungen.

Länger als
1 km
kann der Bremsweg eines Zuges sein.

In Ballungsräumen unterstützen **ausgebildete**
Schutzhunde
die Sicherheitskräfte.

So verhalten Sie sich in bedrohlichen Situationen richtig

- Einem drohenden **Konflikt auszuweichen,** ist die beste Art der Konfliktlösung. Wechseln Sie das Zugabteil oder suchen Sie belebte Orte auf.
- Hören Sie auf Ihr **Bauchgefühl,** das Sie instinktiv vor bedrohlichen Situationen warnt.
- **Siezen Sie** die provozierende Person, um Außenstehenden zu signalisieren, dass es sich um keine private Streitigkeit handelt.
- **Werden Sie laut,** sprechen Sie umstehende Personen direkt an und fordern Sie Unterstützung.

Helfen Sie, ohne sich selbst zu gefährden

1. Ich helfe, ohne mich selbst in Gefahr zu bringen.
2. Ich rufe Hilfe und informiere das Bahnpersonal oder die Polizei.
3. Ich fordere andere aktiv und direkt zur Mithilfe auf.
4. Ich beobachte genau und präge mir Tätermerkmale ein.
5. Ich kümmere mich um Opfer und leiste Erste Hilfe.
6. Ich stelle mich als Zeuge zur Verfügung.

Bei Gefahr ☎ 110!

Mit diesen Angaben helfen Sie der Polizei bei ihren Ermittlungen

Wo war das Ereignis?
Was ist geschehen?
Wie viele Betroffene?
Wer war beteiligt?

- Alter und Geschlecht
- Körperform, geschätzte Größe
- Haarfarbe
- Besondere Merkmale wie Kleidung, Brille, Bart oder Schmuck

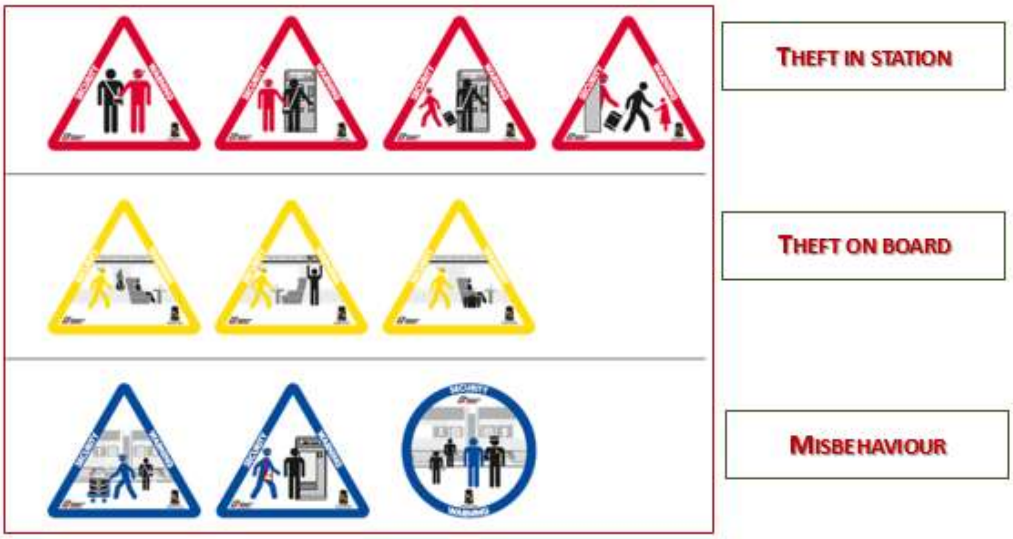
Hinsehen statt wegsehen: mehr Informationen unter
www.bundespolizei.de/zivilcourage

In close cooperation with the German Federal Police, the department of Corporate Security of DB developed a flyer, focusing on current security and safety topics. A preventive approach is taken and intends to raise awareness without scaring people. In addition to displaying the flyers in information and sales outlets and distribution via the prevention teams, further poster motifs are planned.

2.2.4. FS Italiane (Italy)

FS Italiane security policy is aimed at both maintaining staff/customer confidence and protecting the effectiveness of railway operations. Security is a central factor and a crucial element for the FS Group activities and calls for an overall cooperation both internally (among all Group Departments) as well as externally with the support of public authorities.
In order to actively improve the railway security level and promote security and feeling of security among staff and passengers, the FS Group has designed and implemented different security awareness campaigns. These projects are strictly related to the need to effectively tackle the phenomena that affect the Italian railway environment/ infrastructure (third party violence, and antisocial behaviors). In this regard, the FS Group has launched different communication campaigns:

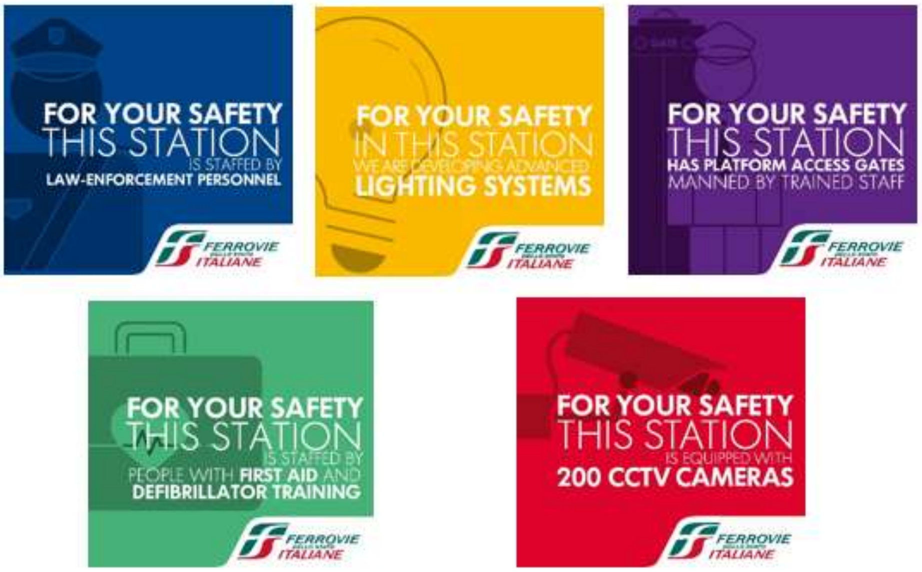
- The **"Be aware and make a difference"** campaign, which consists of posters identifying specific risk scenarios that may possibly occur to travelers in crowded and open environments, such as: pickpockets, frauds, scammers, etc. The awareness and the effective adoption of informed and preventive behaviors can effectively help travelers to avoid becoming victims of illicit acts. This campaign complemented the already implemented information initiatives consisting of brochures, advertisements and announcements.



- **The "Anti-aggression Campaign".** The aim of the "Anti-aggression Campaign" is to reduce the number of assaults against railway personnel, both in stations as well as on-board, engaging passengers through dedicated visual messages. The aim is to invite them not to ignore illicit phenomena, and inform the Railway Police, either personally or through the use of proper emergency numbers. For the campaign implementation, we asked FS staff to authorize the use of their children's images, whom, like the famous call "I want you", invited the potential aggressors to "don't touch my mother/father". We received up to 270 nominations by children aged 3/7 years old.

MIA MADRE CONTROLLA I BIGLIETTI TU DEVI CONTROLLARE DA SOLO.
MIA MAMMA DICE CHE NON DEVO RISPONDERLE MALE E MICA PUÒ VALERE SOLO PER ME.
NOSTRA MADRE DICE CHE NON DOBBIAMO RISPONDERLE MALE E MICA PUÒ VALERE SOLO PER NOI
SE SAI COME DIFENDERTI DAI BULLI DILLO A MIO PAPÀ.
IL PERSONALE FS SUBISCE SPESSO AGGRESSIONI VERBALI E FISICHE. NON RESTARE INDIFFERENTE, IN CASO DI BISOGNO, CHIEDI AIUTO.
FERROVIE ITALIANE

In addition to the abovementioned projects, the FS Security Department implemented a series of initiatives with the purpose of constantly monitoring and strengthening the feeling of security among passengers and staff. In this regard, the FS Corporate Security Department has recently launched **a campaign with the aim of raising the feeling of security** in stations, informing passengers on all the security instruments and activities available in the railway environment.


FOR YOUR SAFETY THIS STATION IS STAFFED BY LAW-ENFORCEMENT PERSONNEL
FOR YOUR SAFETY IN THIS STATION WE ARE DEVELOPING ADVANCED LIGHTING SYSTEMS
FOR YOUR SAFETY THIS STATION HAS PLATFORM ACCESS GATES MANNED BY TRAINED STAFF
FOR YOUR SAFETY THIS STATION IS STAFFED BY PEOPLE WITH FIRST AID AND DEFIBRILLATOR TRAINING
FOR YOUR SAFETY THIS STATION IS EQUIPPED WITH 200 CCTV CAMERAS
FERROVIE DELLO STATO ITALIANE

FS also monitors the so called “feeling of security”, and among its main goals, it is worth mentioning the following ones:

- informing the public of transport users properly (applying the most appropriate means and best practices in the use of media tools) with regard to potential security issues in station and on board trains, in order to raise awareness and foster a fair and ethical model of shared responsibility and cooperation in the field of security in public spaces;

- carrying out periodical surveys;
- implementing CCTV video surveillance to further increase security standards for our customers;
- social media campaign to spread news and updated information related to railway security measures;
- security messages on billboards, both on board and in stations;

As far as the railway personnel is concerned the awareness raising process is also ensured through the implementation of specific and targeted extensive **training programs** aimed at providing the railway staff with all the knowledge, instruments and capabilities necessary to deal with emerging threats.

The challenge of protecting transit and passenger rail from the evolving nature of the terrorist threat requires providing staff with a set of practical identification and management tools and measures through an ongoing awareness and training process.

2.2.5. PKP Group (Poland)

The railway security system within PKP Group concentrates mainly on improving an overall security level across major railway transport domains. It is based on several security pillars where close cooperation with national authorities and raising awareness among employees and rail service customers play a particular role.

Since terrorism poses the highest level of threat, the close cooperation embraces an engagement of relevant law enforcement agencies, which are primarily responsible for preventing and combating terrorism. Having said that, in the area of public awareness PKP S.A. focuses mainly on common offences such as pickpocketing or lost luggage rather than targeted awareness campaigns related to terrorism (which remains within the key competences of relevant national authorities as mentioned above). PKP intends to show rail users that an increased vigilance can prevent many risks without creating unnecessary fear or lacking sense of security that the overuse of the term “terrorism” may otherwise cause. However, this does not preclude to run terrorism related awareness campaigns by PKP Group among its employees via internal communication channels.

2.2.5.1 Awareness campaign

Aware = Safe Campaign

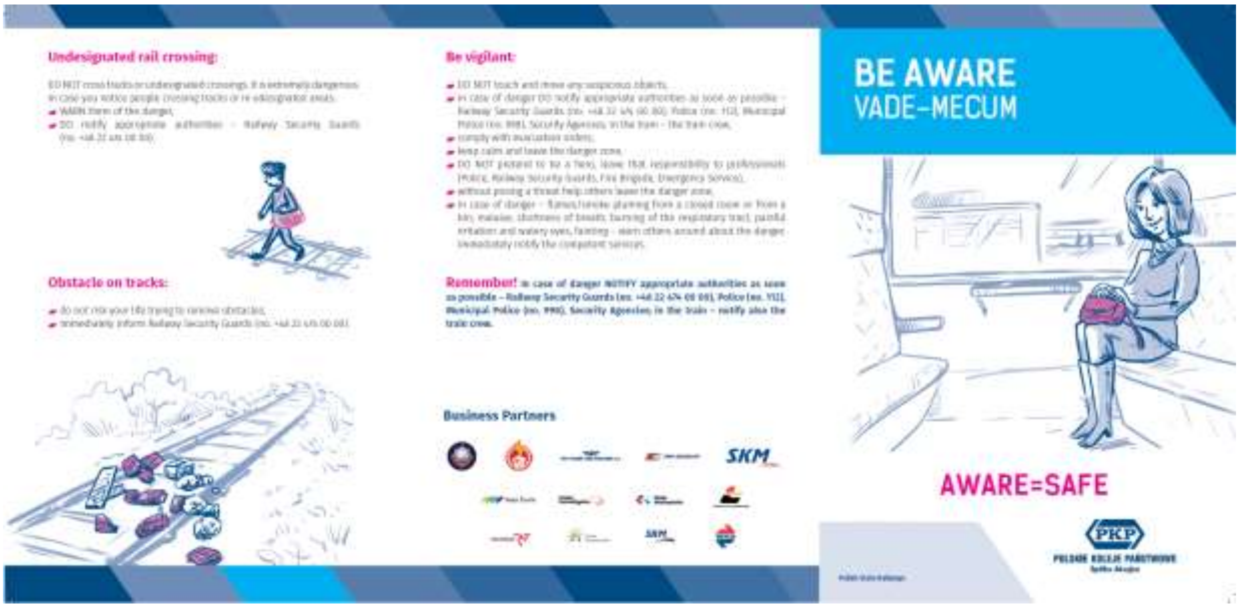
The campaign called Aware = Safe is an example of excellent cooperation between major stakeholders responsible for ensuring safety and security in railway premises. Thanks to the involvement of the national authorities, the targeted communication carries important security messages that can be associated with some terrorism threats, while avoiding naming or referring to them directly. The aim of the campaign is to raise awareness among the largest possible group of railway users in the following areas:

- Hidden explosive devices;
- Rules of conduct in an emergency situation;
- Theft;

- Undesignated rail crossing;
- Obstacle on tracks; and
- A general objective – be vigilant.

The campaign is targeting both railway customers and personnel.

The major advantage of the campaign is its wide coverage due to good cooperation and the involvement of a broad spectrum of partners including railway companies (PKP S.A, PKP PLK S.A, PKP Intercity S.A. and more), police and military police. Each partner carries out the awareness campaign through its own communication channels and using the same materials, so that passengers do not have to remember many different tips, rules or even the individual emergency numbers.



Undesignated rail crossing:

DO NOT cross tracks in undesignated crossings. It is extremely dangerous.
In case you notice people crossing tracks in undesignated areas:
- WARN them of the danger,
- DO notify appropriate authorities – Railway Security Guards (no. +48 22 474 00 00).

Obstacle on tracks:

- do not risk your life trying to remove obstacles,
- immediately inform Railway Security Guards (no. +48 22 474 00 00).

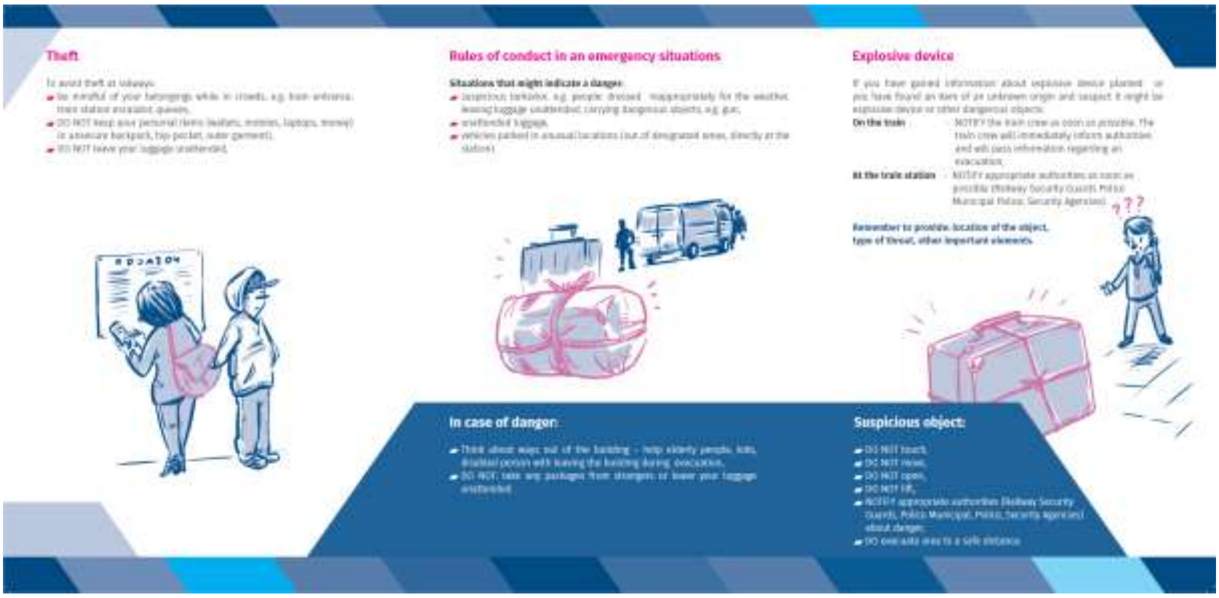
Be vigilant:

- DO NOT touch and move any suspicious objects,
- in case of danger DO notify appropriate authorities as soon as possible – Railway Security Guards (no. +48 22 474 00 00), Police (no. 112), Municipal Police (no. 986), Security Agencies; in the train – the train crew,
- comply with evacuation orders,
- keep calm and leave the danger zone,
- DO NOT pretend to be a hero, leave that responsibility to professionals (Police, Railway Security Guards, Fire Brigade, Emergency Service),
- without posing a threat help others leave the danger zone,
- in case of danger – flames/smoke pluming from a closed room or from a bin, malaise, shortness of breath, burning of the respiratory tract, painful irritation and watery eyes, fainting – warn others around about the danger, immediately notify the competent services.

Remember! In case of danger NOTIFY appropriate authorities as soon as possible – Railway Security Guards (no. +48 22 474 00 00), Police (no. 112), Municipal Police (no. 986), Security Agencies; in the train – notify also the train crew.

Business Partners

Fig. 1. Leaflet for Aware=Safe awareness campaign. Part 1. (Source : PKP S.A.).



Theft

To avoid theft at railways:
- be mindful of your belongings while in crowds, e.g. train entrance, train station escalator, queues,
- DO NOT keep your personal items (wallets, mobiles, laptops, money) in unsecure backpack, hip-pocket, outer garment),
- DO NOT leave your luggage unattended.

Rules of conduct in an emergency situations

Situations that might indicate a danger:
- suspicious behavior, e.g. people dressed inappropriately for the weather, leaving luggage unattended, carrying dangerous objects, e.g. gun,
- unattended luggage,
- vehicles parked in unusual locations (out of designated areas, directly at the station).

Explosive device

If you have gained information about explosive device planted or you have found an item of an unknown origin and suspect it might be explosive device or other dangerous objects:

On the train – NOTIFY the train crew as soon as possible. The train crew will immediately inform authorities and will pass information regarding an evacuation;

At the train station – NOTIFY appropriate authorities as soon as possible (Railway Security Guards, Police, Municipal Police, Security Agencies).

Remember to provide location of the object, type of threat, other important elements.

In case of danger:
- Think about ways out of the building – help elderly people, kids, disabled person with leaving the building during evacuation,
- DO NOT take any packages from strangers or leave your luggage unattended.

Suspicious object:
- DO NOT touch,
- DO NOT move,
- DO NOT open,
- DO NOT lift,
- NOTIFY appropriate authorities (Railway Security Guards, Police, Municipal Police, Security Agencies) about danger,
- DO evacuate area to a safe distance.

Fig. 2. Leaflet for Aware=Safe awareness campaign. Part 2. (Source : PKP S.A.).

The communication channels used in the campaign include:

- **Leaflets** – distributed to staff, passengers in trains and at the railway stations, including customer service areas.
- **Posters –** displayed at the railway stations and in the premises of companies/stakeholders.
- **Short videos** – displayed on board of the trains, at the stations and at the company/stakeholder's premises (e.g. HQs)
- **Floor graphics –** located in the most crowded areas at the railway stations.

The campaign is made in both Polish and English languages.

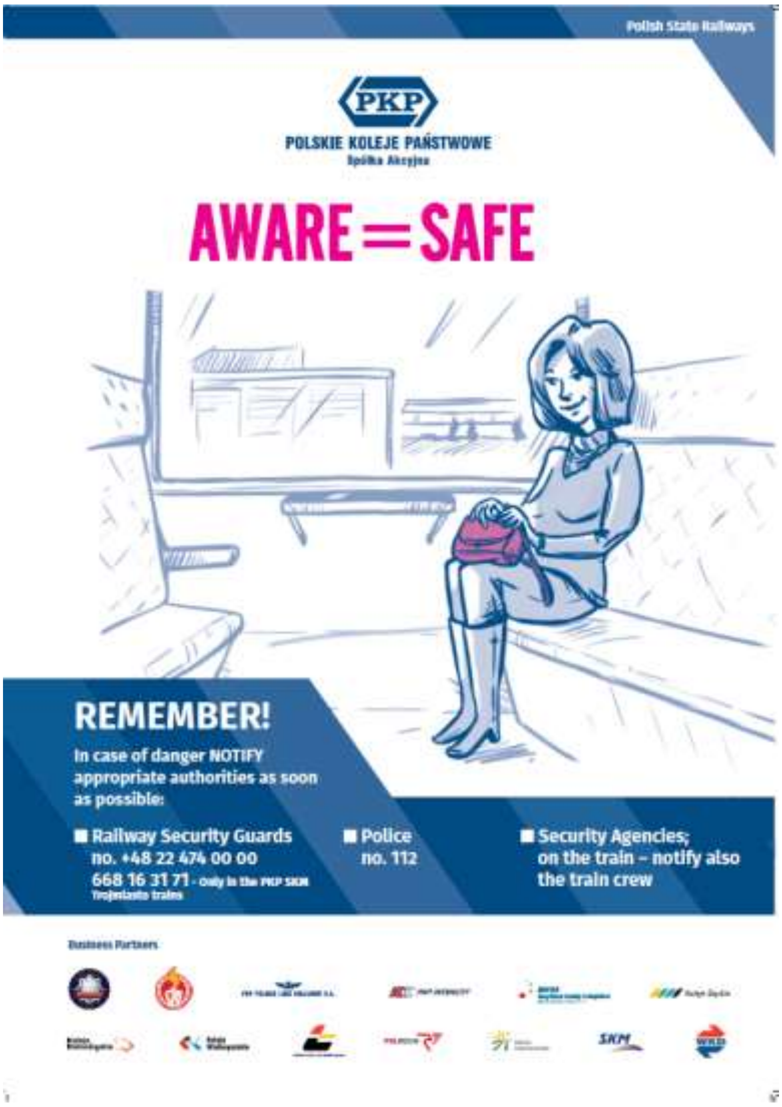

Polish State Railways
PKP
POLSKIE KOLEJE PAŃSTWOWE
Spółka Akcyjna
AWARE = SAFE
REMEMBER!
In case of danger NOTIFY appropriate authorities as soon as possible:
■ Railway Security Guards no. +48 22 474 00 00
668 16 31 71 - Only in the PKP SKM Trójmiasto trains
■ Police no. 112
■ Security Agencies; on the train – notify also the train crew
Business Partners
SKM

Fig. 3. Poster for Aware=Safe awareness campaign. (Source: PKP S.A.).

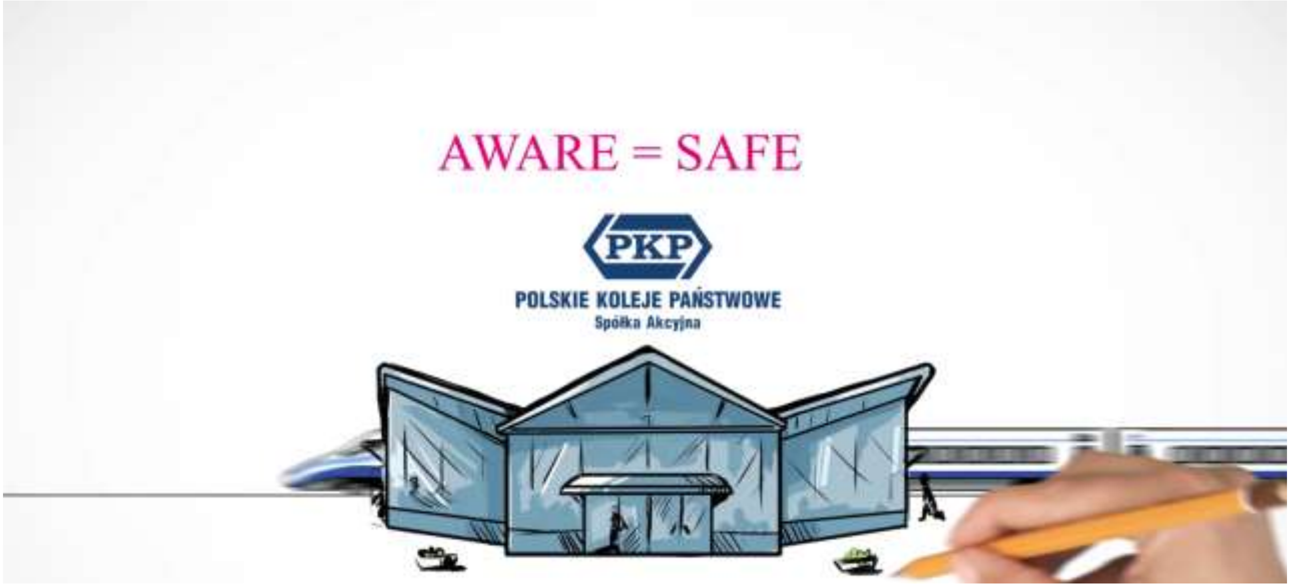


Fig. 4. Short movie for Aware=Safe awareness campaign. (Source: PKP S.A.).

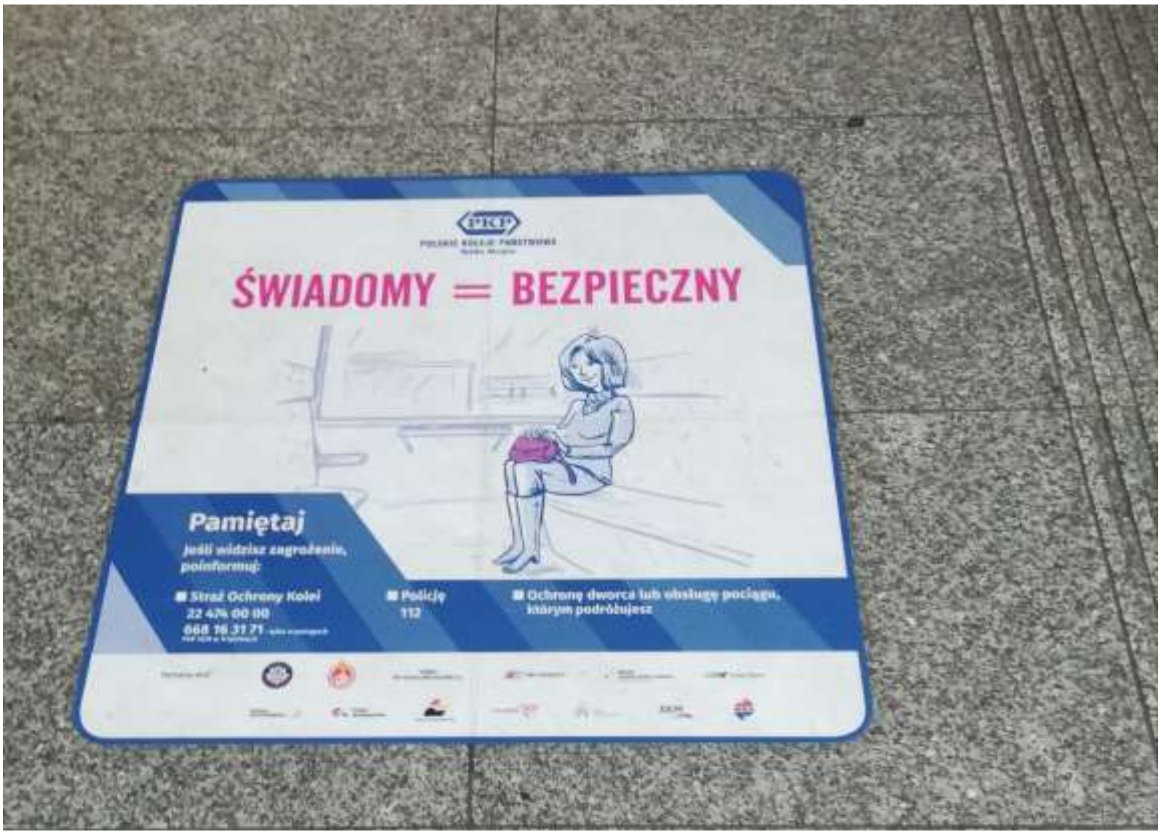

PKP
POLSKIE KOLEJE PAŃSTWOWE
ŚWIADOMY = BEZPIECZNY
Pamiętaj
Jeśli widzisz zagrożenie, poinformuj:
Straż Ochrony Kolei 22 474 00 00 668 16 31 71
Policję 112
Ochronę dworca lub obsługę pociągu, którym podróżujesz

Fig. 5. Floor graphics for Aware=Safe awareness campaign. (Source: PKP S.A.).

3. EMERGENCY NUMBERS (VOICE AND TEXT) FOR PUBLIC REPORTING

3.1. Introduction

Enlisting passengers and staff in alerting security staff any suspicious object or behaviour may be done by implementing a special emergency number, which operated by dedicated security staff, would allow for rapid reaction in emergency situations – e.g. unattended luggage, suspicious behaviour, first aid needed.

However, in accordance with the strategies of the responsible security authorities, European railway companies take different approaches to marketing and communications; however, they share the same goal of making it easier to raise the alert. Only some of the railway companies have introduced to customers a special emergency number they can call in case of a security problem (which is most often not terrorism related) The use of these special telephone numbers however is limited to national borders, and hence do not provide a suitable solution for international trains travelling across the EU.

3.2. Examples

3.2.1. SNCB emergency Number: 080030230 (Belgium)

SNCB has a free emergency number accessible to travellers in real time 24/7 for all incidents related to security: 080030230. This number is used to reach the SOC (Security Operation Centre), which dispatch the Securail teams, but also transmits security information to other competent services (police, ambulance, etc.).

Quelque chose de suspect ?
Sentiment d'insécurité ?
Témoin d'un méfait ?
Malade/malaise en gare ou dans le train ?
QUELQUE CHOSE DE SUSPECT ?
0800 30 230
0800 30 230
Numéro d'urgence gratuit

This number is displayed in stations and on platforms and is associated with the "something suspicious?" Campaign. This service isn't yet available by SMS but it is under development. The SOC will soon be equipped with a new console that will allow communication with the WhatsApp application.

3.2.2. SNCF alert number: 3117-7 (France)

Since 2010, the alert number 3117-7 has been used to respond to customer expectations regarding security. It is operational in real time, 24/7. Since 2015, the service has been available by SMS.

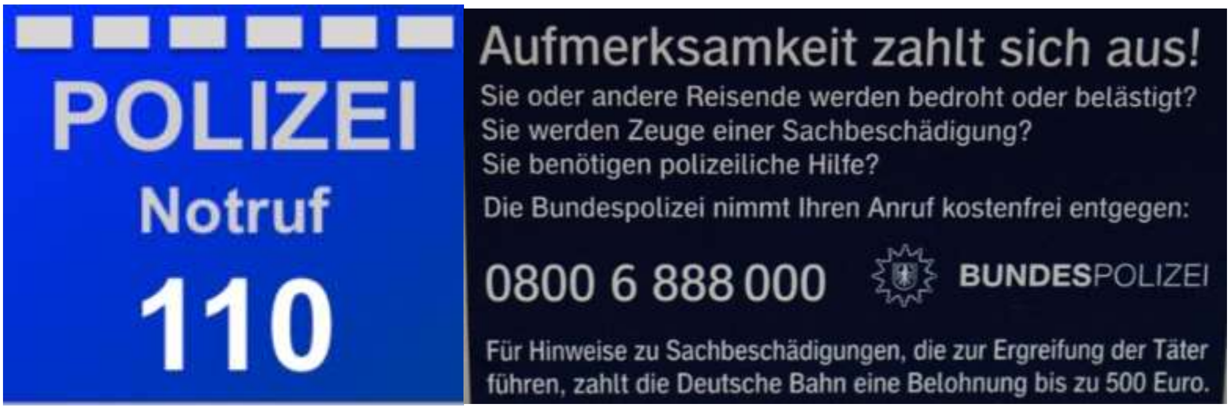
The 3117-7 alert number allow the user to report, testify or alert when they encounter incivilities or risk situations. When a customer is a victim or witness of a situation that appears to be a risk to themselves or other passengers, they can inform the call management centre by phone or by text message.

24h/24 - 7j/7
ALERTE SNCF
TÉL. 3117*
SMS 31177**

The call management centre identifies the caller, takes into account the nature of the call, and locates the origin of the call. Operators take all calls and text messages 24/7 and contact the most appropriate department to assist and rescue customers. Usually through rail operators' control rooms, the operators relay information to the emergency services (police, fire brigade, paramedics, mine clearance experts) providing the location of the customer and their knowledge of train circulation.

3.2.3. DBAG (Germany)

In case of observations which could be of interest for the police in the field of railways, customers are asked to use the service number of the Federal Police (0800 6 888 000). In urgent cases, however, advice is given to dial the emergency number 110. Only by that a direct routing to the closet police forces is possible.



POLIZEI
Notruf
110

Aufmerksamkeit zahlt sich aus!

Sie oder andere Reisende werden bedroht oder belästigt?
Sie werden Zeuge einer Sachbeschädigung?
Sie benötigen polizeiliche Hilfe?

Die Bundespolizei nimmt Ihren Anruf kostenfrei entgegen:

0800 6 888 000 BUNDESPOLIZEI

Für Hinweise zu Sachbeschädigungen, die zur Ergreifung der Täter führen, zahlt die Deutsche Bahn eine Belohnung bis zu 500 Euro.

An alert number for text messages is not establish yet. This is due to the fact that telecommunication providers are not obliged to pass on messages right away. As there is a potential danger in alerts not being forwarded to the authorities in time, such service is not offered yet.

3.2.4. FS (Italy)

Generally speaking, the Italian railway system does not have a dedicated emergency number, in use for passengers and citizens. In case of emergency, passengers and citizens can call the national emergency numbers and ask for the intervention of the railway police, responsible for the railway crimes' prevention and repression.

On the other hand, for the railway staff there is a dedicated GSM-R number, which allows rail operators to automatically contact the closest railway police control room.

3.2.5. PKP emergency number: 22 474 00 00 (Poland)

There is a dedicated emergency number (+48 22 474 00 00), which every passenger can call and report any dangerous incident or obtain necessary security-related information. This number is supported by Railway Security Guard (SOK). PKP does not use text message services for customers.

4. MOBILE APPLICATIONS FOR SECURITY AWARENESS AND CRISIS COMMUNICATION

4.1. Introduction

A wide range of emergency preparedness and disaster response smartphone applications are currently available on various app stores, with a 2014 search finding 683 results[10]. The prevalence of such apps is due to their success in efficiently spreading and collecting information before, during and after disasters[10] [11] [12]. Disaster apps enable efficient warnings[13], directly reach citizens in a given area (if the GPS is enabled)[10], and some even provide users with information about how to act prior, during and after a disaster[14].

One challenge of creating a mobile app for security awareness is to overcome the barrier of "opt-in", or downloading, the app. Thus, apps need to take into account attractivity to users. Apps must also take into account legal issues as for instance, when using users' localization to efficiently allocate security information, institutions are collecting sensitive and personal data. Therefore, the EU's General Data Protection Regulation (GDPR) has a big role to play in designing such apps, as should privacy by design[15].

[10] D. J. Bachmann, N. K. Jamison, A. Martin, J. Delgado, & N. E. Kman, (2015). Emergency preparedness and disaster response: there's an app for that. *Prehospital and Disaster Medicine, vol 30(5), 2015, pp. 486–490*. doi.org/10.1017/S1049023X15005099

[11] C. Aydin, C. Tarhan, A.S. Ozgur, & V. Tecim. (2016). Improving disaster resilience using mobile based disaster management system. *Procedia Technology, vol 22, 2016, pp. 382–390.* doi.org/10.1016/j.protcy.2016.01.027

[12] S. Tagliacozzo & M. Magni, (2016). Communicating with communities (CwC) during post-disaster reconstruction: an initial analysis. *Natural Hazards*. doi.org/10.1007/s11069-016-2550-3

[13] J. Douvinet. (2018). Alerter la population face aux crues rapides en France : compréhension et évaluation d'un processus en mutation. *Université d'Avignon*

[14] L. Fallou, L. Petersen, R. Bossu, F. Roussel. (2016). Efficiently allocating safety tips after an earthquake – lessons learned from the smartphone application LastQuake. *Proceedings of the 16th ISCRAM Conference – València, Spain May 2019*

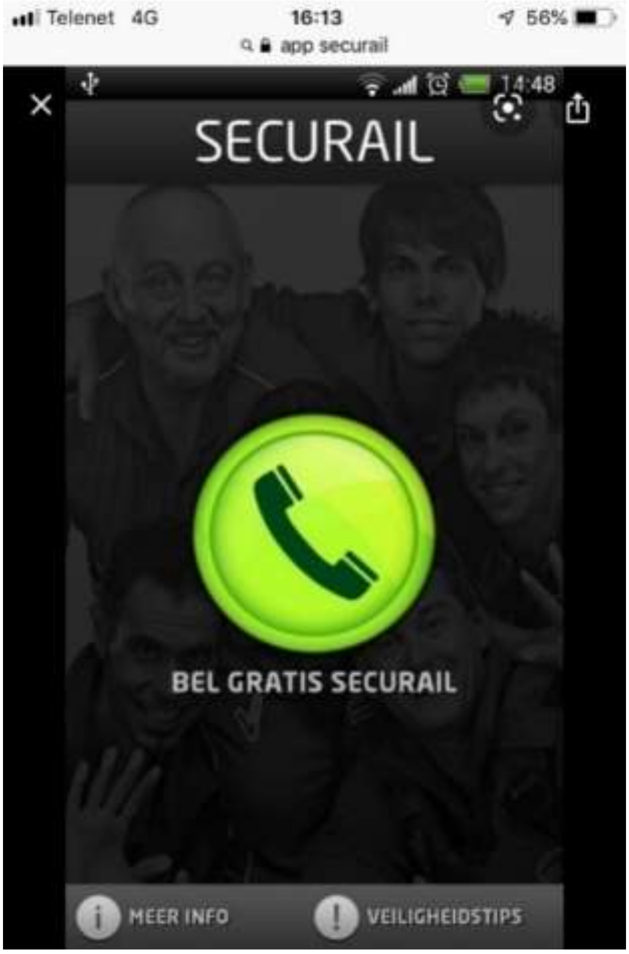
[15] L. Jasmontaite & D. Dimitrova. (2017). Online disaster management: applicability of the European Data Protection Framework and its key principles. *Journal of Contingencies and Crisis Management*

4.2. Examples of mobile applications for the public

4.2.1. SNCB (Belgium)

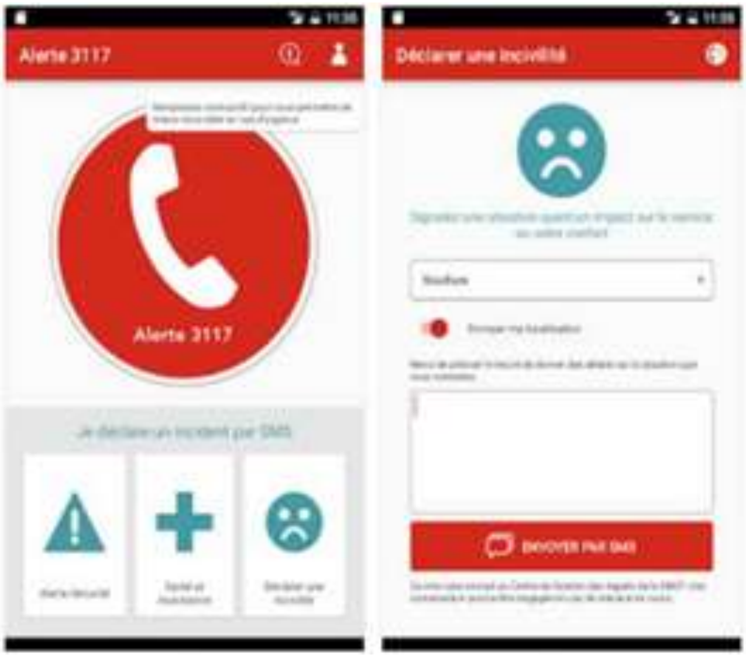
When SNCB launched its campaign to highlight the Securail service and encourage the public to memorize the free emergency number, it also developed a shortcut to be installed on the smartphone in order to facilitate access to this number.

This shortcut no longer exists; however, a new application is currently under development that will include, in addition to the number, various features such as reporting suspicious behaviour or offenses, access to preventive advice, etc. In addition, it is also planned to make this emergency number quickly available when using the "Dis Google" and "Siri" assistants.



4.2.2. SNCF 3117-7 application for on-board passenger assistance (France)

Since 2016, the 3117-7 smart phone application has been operational and available throughout France. Its users are the passengers of the railway network. The application, SMS and alert number's purpose is to discreetly collect testimonials, reports, alerts, incivilities or risk situations.



The 3117-7 app and the 3117-7 alert number allow the user to report, testify or alert when they encounter incivilities or risk situations. When a customer is a victim or witness of a situation that appears to be a risk to themselves or other passengers, they can inform the call management Centre via the mobile application, by phone or by text message.
The call management centre identifies the caller, takes into account the nature of the call, and locates the origin of the call. Operators take all calls and text messages 24/7 and contact the most appropriate department to assist and rescue customers. Usually through rail operators' control rooms, the operators relay information to the emergency services (police, fire brigade, paramedics, mine clearance experts) providing the location of the customer and their knowledge of train circulation.

The 3117-7 application has features that allow it to be used without a telephone network. It exists in several languages automatically detected. A "call button" allows to be connected directly to the call management centre. It has a SMS channel for discreet reports and declarations. It geo-locates calls. It is a simple and easy to use application.

The 3117-7 app and alert number strengthen the role of rail operators in surveillance and assistance throughout the national territory. They help by linking the competent services in a more qualified and rapid manner and identifying incidents and threats encountered throughout the network. The system is deployed on TGV, TER, Intercités, RATP and Transilien.

4.3. Examples of mobile Applications for staff

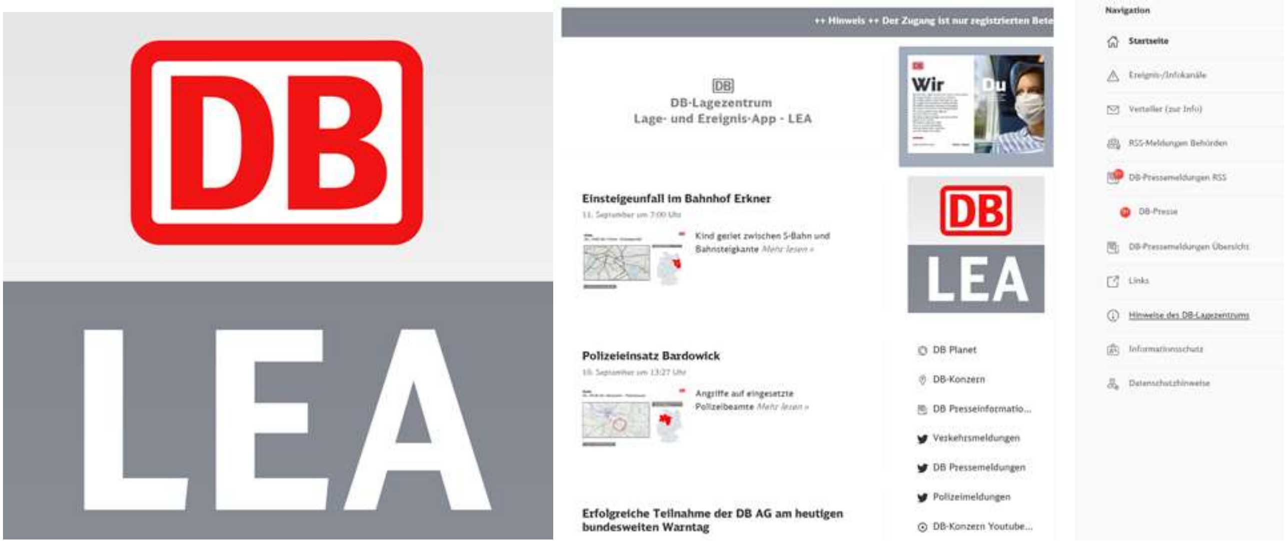
4.3.1. SNCB (Belgium)

All Securail agents will be very soon equipped with smartphones including certain applications such as Child focus (organ dealing with missing children), 112, etc.

4.3.2. DB AG (Germany)

LEA – situation and incident app

Informing employees of the crisis management team and relevant corporate security staff about a relevant situation/incident has over the years been conducted by SMS and e-mail. This did require a constant administration of lists of recipients for each incident category. Reports had to be individually formatted. The handling of the manual information administration was time consuming and error prone. With the introduction of the situation and incident application LEA at DB Corporate Security, information about security-relevant situations can be precisely directed to the relevant rail personnel and board members with ease.



++ Hinweis ++ Der Zugang ist nur registrierten Bete

DB-Lagezentrum
Lage- und Ereignis-App - LEA

Einsteigeunfall im Bahnhof Erkner

Kind geriet zwischen S-Bahn und Bahnsteigkante *Mehr lesen »*

Polizeieinsatz Bardowick

Angriffe auf eingesetzte Polizeibeamte *Mehr lesen »*

Erfolgreiche Teilnahme der DB AG am heutigen bundesweiten Warntag

Internal operating information is recorded in the situation and incidents reports and automatically channeled to the appropriate recipients. Push notifications via smartphone are sent with optional additional e-mail notification according to the communication channel selection by the recipients.

The information distribution list is reserved for a specific group of employees with security-relevant tasks in crisis management. Access to the App is restricted and only possible after individual authorization. As recipients of information, employees are obligated to use the confidential information that has come to their knowledge only for internal purposes and within the scope of their work and not to otherwise exploit, use or pass it on to third parties without prior written consent.

4.3.3. FS Italiane (Italy)

FS Railway Undertaking (Trenitalia S.p.A) is strongly focused on the design and implementation of innovative solutions aimed at increasing both the real and perceived feeling of security on board. The main purpose of the “Board Support” project is implementing an innovative app dedicated to police forces allowing Law Enforcement Agents to automatically register their presence on board, enabling them to receive alerts in case of an emergency.

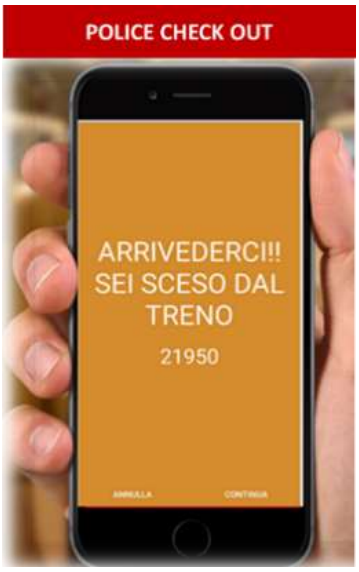
The Board Support app is available on Android and IOS stores since the 1st of April 2019. It is free to download and to proceed with the login on the app it is necessary to register on a dedicated website and insert personal credentials (username and password). For law enforcement agents accessing from a computer located inside their offices, the registration is allowed directly from the website.

The use of the app is allowed for travel on regional trains, offering the following features:

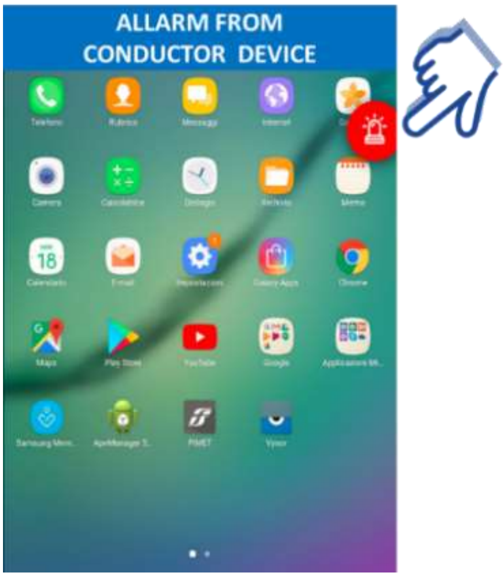
- Law enforcement can check in on board through the app, which will notify the train manager of their presence. Login can be automatic (in the case of train with Wi-Fi connection) or manual, ensured by choosing the train number and both departure and arrival stations.
- In case of an emergency, the train manager can activate the alarm button through his work device, Police on board will be immediately notified on their smartphones, ensuring a prompt intervention on board.

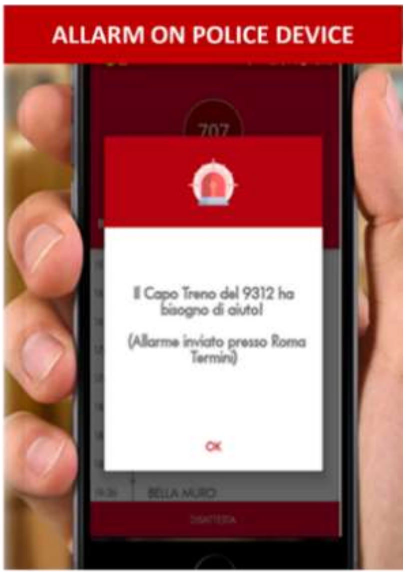
- At the end of their journey, police can check out through the app, which will notify the Train Manager. The check-out is automatic both in the case of WIFI connection on board and in the case of manual check in (depending on the arrival station of choice).

The software solution is compliant to the General Data Regulation n.2016/679 in terms of personal data processing and privacy. During the registration process, no personal data are required in order to obtain app credentials.


POLICE CHECK OUT

ARRIVEDERCI!!
SEI SCESO DAL
TRENO
21950


ALLARM FROM
CONDUCTOR DEVICE


ALLARM ON POLICE DEVICE

Il Capo Treno del 9312 ha bisogno di aiuto!

(Allarme inviato presso Roma Termini)

4.3.4. PKP (Poland)

There is a specific application called “Komunikator PLK” (for internal use only) to inform dedicated personnel about any safety and security incidents. This application is provided by the National Infrastructure Manager (PKP Polskie Linie Kolejowe S.A.). All interested parties can report on all incidents spotted or threats observed along the railway lines, where in the case where provided information is considered important, it is passed on to all relevant and authorized employees working in the rail infrastructure environment.

Fig. . Internal security-related communication tool (Komunikator PLK). (Source: PKP S.A.).

In addition, both rail employees and the public can report to the National Security Threat Map (provided by the national police) about any incidents spotted. This is very important and helpful national tool because of the wide range of incidents can be reported there, as well as due to the fact that often (especially in urban centres) , rail facilities are functionally connected to all kind of public spaces (e.g. shopping malls, transport hubs etc) where similar threats/incidents may occur. An additional advantage of this solution is the fact that every single map’s user can familiarized with previously reported incidents.

Moreover, both relevant authorities as well as the rail companies gain insight into users' reports thus can take appropriate preventive or corrective actions. The application does not require any login or personal information and is of course free of charge which all constitute another advantage.

5. SOCIAL MEDIA FOR SECURITY AWARENESS AND CRISIS COMMUNICATION

5.1. Introduction

Large scale security incidents such as the Mumbai terrorist attacks in November 2008 marked a turning point in the use of social media (e.g. Facebook, Twitter, YouTube) for sharing security information[16] (Potts, 2014). Since then, social media use as a crisis communication and security awareness raising channel has only been on the rise[17]. It has become a tool to warn others of critical areas and unsecure situations, to send alert messages or give eye-witness reports. It is a tool used both by individuals, professional security providers and local and national authorities.

Social media could be used by railway undertakings to both push and pull for both security awareness and crisis communication. The engagement of social media enables a fast dissemination of information into the public sphere (pushing) and back to the responders (pulling).

When pushing information via these platforms, one simply passively disseminates the information and employs social media as a one-way communication channel. Social media is also able to amplify one-way communication. For example, during the 2013 Westgate Mall Terror Attack in Kenya, authorities shared each other's messages on Twitter (commonly referred to as retweeting), thus reaching a greater audience and ensuring more people were able to obtain the relevant information[18]. However social media generally encourages interaction and dialogue between users, creating information space that is essentially decentralized and devoid of hierarchy[19]. As such, it might be expected that railway undertakings use social media platforms to interact with the public directly. Despite this, a recent study by Petersen et al. (2017) found that there was a relatively low expectation from the general public for critical infrastructure operators to respond to queries on social media during a crisis incident[20].

[16] Potts, L. (2014). Social media in disaster response: how experience architects can build for participation. *New York: Routledge, Taylor & Francis Group*.

[17] Reuter, C., & Kaufhold, M.-A. (2018). Fifteen Years of Social Media in Emergencies: A Retrospective Review and Future Directions for Crisis Informatics. *Journal of Contingencies and Crisis Management* (JCCM), 26(1), 1-17. doi:10.1111/1468-5973.12196

[18] Simon T., Goldberg A., & Adini B. (2015). Socializing in emergencies—A review of the use of social media in emergency situations. *International Journal of Information Management*, 35(5), 609–619.

[19] Giroux, J., Roth, F., & Herzog, M. (2013). Using ICS & Social Media in Disasters: Opportunities & Risks for Government. *Center for Security Studies/ETH Zurich*. P. 5. http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?id=166079&lng=en.

[20] Petersen, L., Fallou, L., Reilly, P., & Serafinelli, E. (2017). European Expectations of Disaster Information provided by Critical Infrastructure Operators: Lessons from Portugal, France, Norway and Sweden. *International Journal of Information Systems for Crisis Response and Management (IJISCRAM), 9(4), 23-48.* doi:10.4018/IJISCRAM.2017100102

When it comes to pulling information, monitoring social media can increase situational awareness by providing unprecedented access to eyewitness accounts of crises and be used to support decision-making. The meta-data of the social media information (e.g. geolocation) may also be useful[21] [22]. While one common concern for using social media data in emergency response is misinformation or the spread of rumours, a study of the Boston Marathon Bombings and the use of Twitter concluded that getting timely information to responders outweighs these negatives[23]. Further, it is important to keep in mind that the accuracy of social media data should be viewed in the same context as offline information, meaning that both have the capacity to be true or false[24].

Although many advantages and disadvantages of social media for crisis communication and raising security awareness are shared between platforms, differences exist and they should not be viewed as a homogenous mass when it comes to crisis communication[25]. For example, Twitter tends to focus on the now whereas Facebook tends to focus on the longer term.

While social media has been highly studied as a communication and security awareness channel for authorities, less research has examined the crucial role of infrastructure operators and how they can use social media to create a security culture. A study investigating Twitter data corresponding to 26 crises between 2012 and 2013 found that while on average 7% of tweets contained information related to infrastructure and utilities, these tweets were among the most retweeted during such incidents[26]. Further, the same Petersen et al. (2017) study demonstrated that the general public have high expectations for information to be pushed via social media by operators in a crisis context[20]. Therefore, social media is an important tool for railway operators to increase security awareness and combat the threat of terrorism.

To be most effective, social media as a security awareness and crisis communication channel should be used at each stage of the disaster management cycle: before, during and after. Before a potential incident occurs, communication should focus on preparedness and raising the general level of

[21] Yates D. & Paquette S. (2011): Emergency knowledge management and social media technologies: A case study of the 2010 Haitian earthquake, *International Journal of Information Management*, 31(1): 6–13.

[22] Pohl D., Bouchachia A., & Hellwagner H. (2016): Online indexing and clustering of social media data for emergency management, *Neurocomputing*, 172, 168–179.

[23] Cassa C. A., Chunara R., Mandl K., & Brownstein J. S. (2013): Twitter as a Sentinel in Emergency Situations: Lessons from the Boston Marathon Explosions. *PLoS Currents*, 1–12.

[24] Tapia A. H., & Moore K. (2014): Good enough is good enough: Overcoming Disaster Response Organizations Slow Social Media Data Adoption. *Computer Supported Cooperative Work: CSCW: An International Journal*, 23(4–6): 483–512.

[25] Eriksson & Olsson. (2016). Facebook and Twitter in Crisis Communication: A Comparative Study of Crisis Communication Professionals and Citizens. *Journal of contingencies and crisis management*. doi: 10.1111/1468-5973.12116

[26] Olteanu, A., Vieweg, S., & Castillo, C. (2015). What to Expect When the Unexpected Happens: Social Media Communications Across Crises. *CSCW '15, March 14 - 18 2015, Vancouver, BC, Canada, ACM 978-1-4503-2922-4/15/03.* doi: 10.1145/2675133.2675242

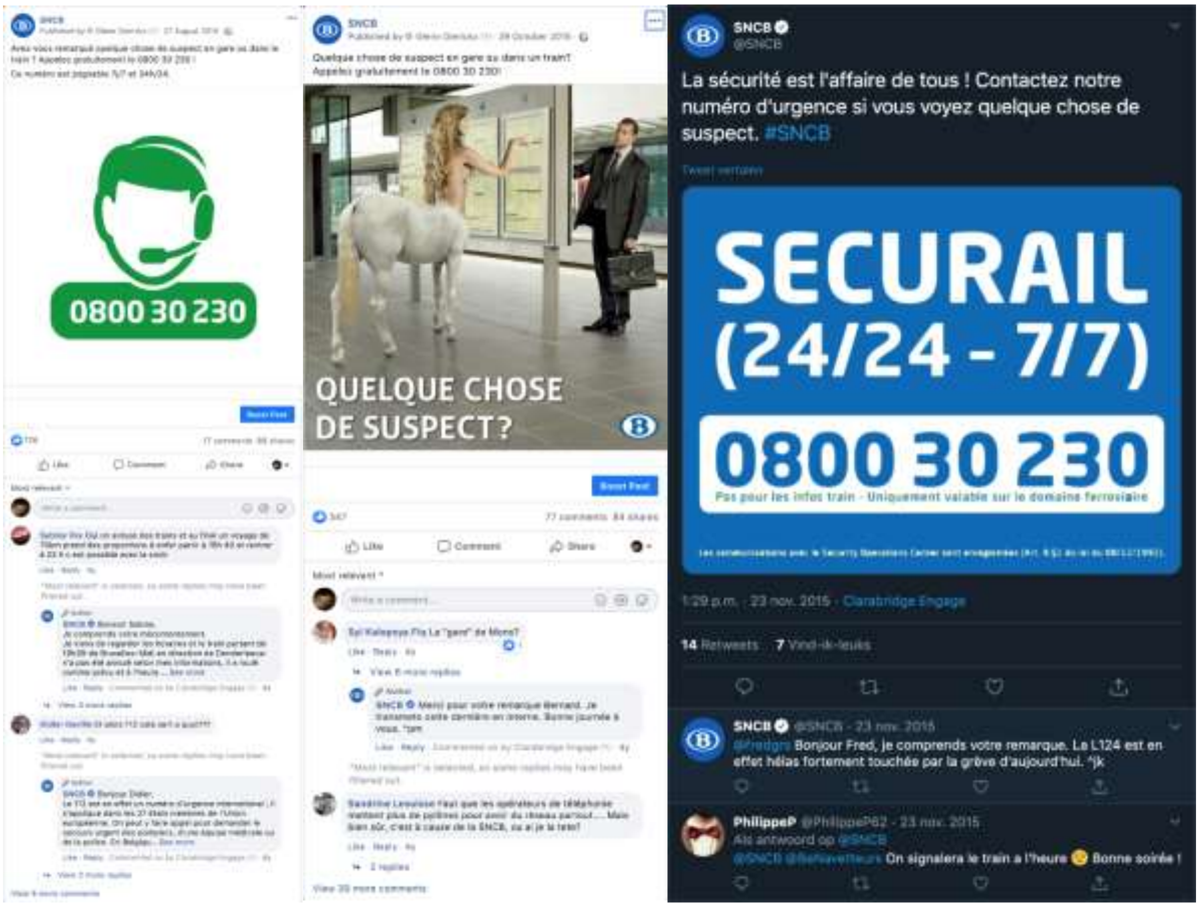
security awareness. During an event, it is important to acknowledge an event is happening and to continuously update on the event. Updates should also include the sharing of the fact that there has been no new information since the last update. Post crisis, learning from past should be used to improve the railway undertaker's communication strategies.

5.2. Examples of social media utilisation in the rail environment

5.2.1. SNCB (Belgium)

A social media communication strategy has been established by SNCB. A team of 13 community managers is dedicated to keeping the SNCB pages alive 7 days a week 16 hours a day. These networks disseminate information in real time both on traffic, commercial offers, etc. and security information. They also allow direct and transparent exchanges with the public: the average response time is 10 minutes.

Facebook and Twitter are the most used channels, but SNCB is also present on Instagram and LinkedIn.



SNCB

Avez-vous remarqué quelque chose de suspect en gare ou dans le train ? Appelez gratuitement le 0800 30 230 !
Ce numéro est joignable 7/7 et 24h/24.

SNCB

Quelque chose de suspect en gare ou dans un train?
Appelez gratuitement le 0800 30 230!

SNCB @SNCB

La sécurité est l'affaire de tous ! Contactez notre numéro d'urgence si vous voyez quelque chose de suspect. #SNCB

1:29 p.m. · 23 nov. 2015 · Clarabridge Engage

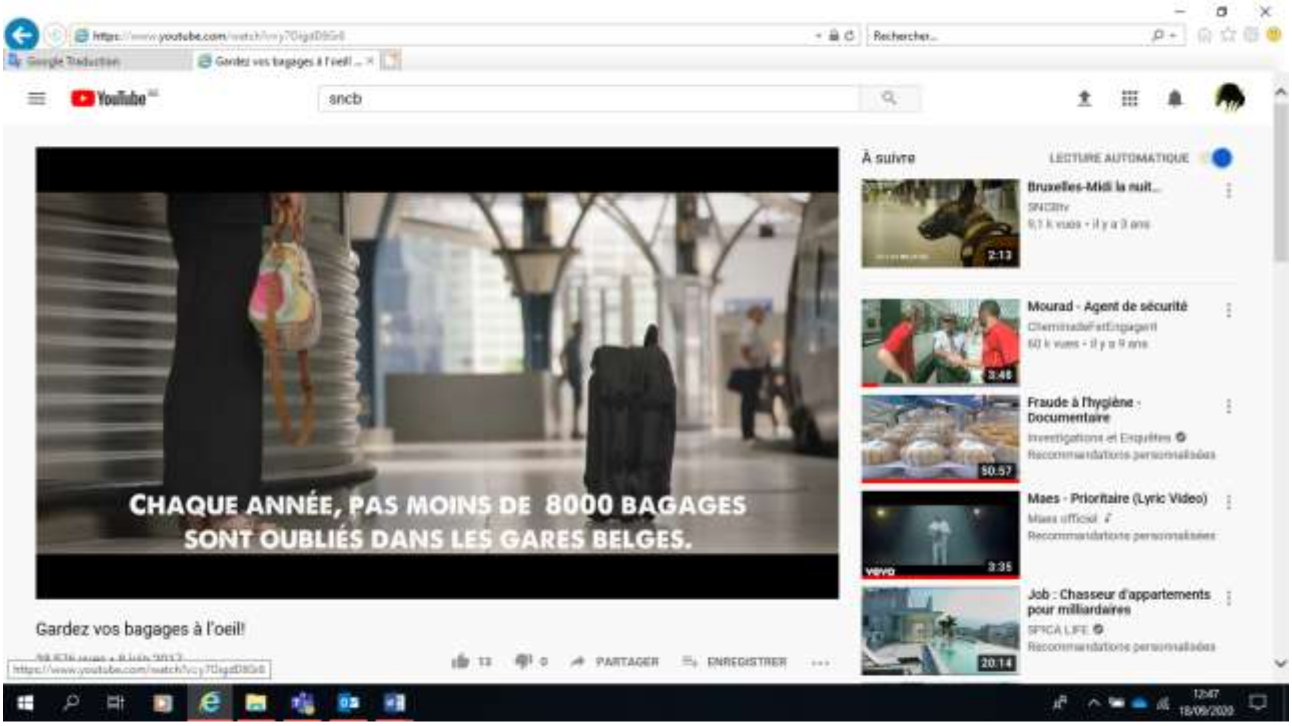
14 Retweets 7 Vind-ik-leuks

SNCB @SNCB · 23 nov. 2015
Bonjour Fred, je comprends votre remarque. La L124 est en effet hélas fortement touchée par la grève d'aujourd'hui. ^jk

PhilippeP @PhilippeP62 · 23 nov. 2015
Als antwoord op @SNCB
@SNCB On signalera le train a l'heure 😉 Bonne soirée !

0800 30 230
QUELQUE CHOSE DE SUSPECT?
SECURAIL (24/24 - 7/7)
0800 30 230
Pas pour les infos train - Uniquement valable sur le domaine ferroviaire
Like
Comment
Share
Write a comment...

There is an SNCB YouTube channel: SNCB tv, in which security-related content can be broadcasted, such as a video clip aimed at raising public awareness about unattended luggage or a video presenting the work of a Securail agent.



CHAQUE ANNÉE, PAS MOINS DE 8000 BAGAGES SONT OUBLIÉS DANS LES GARES BELGES.

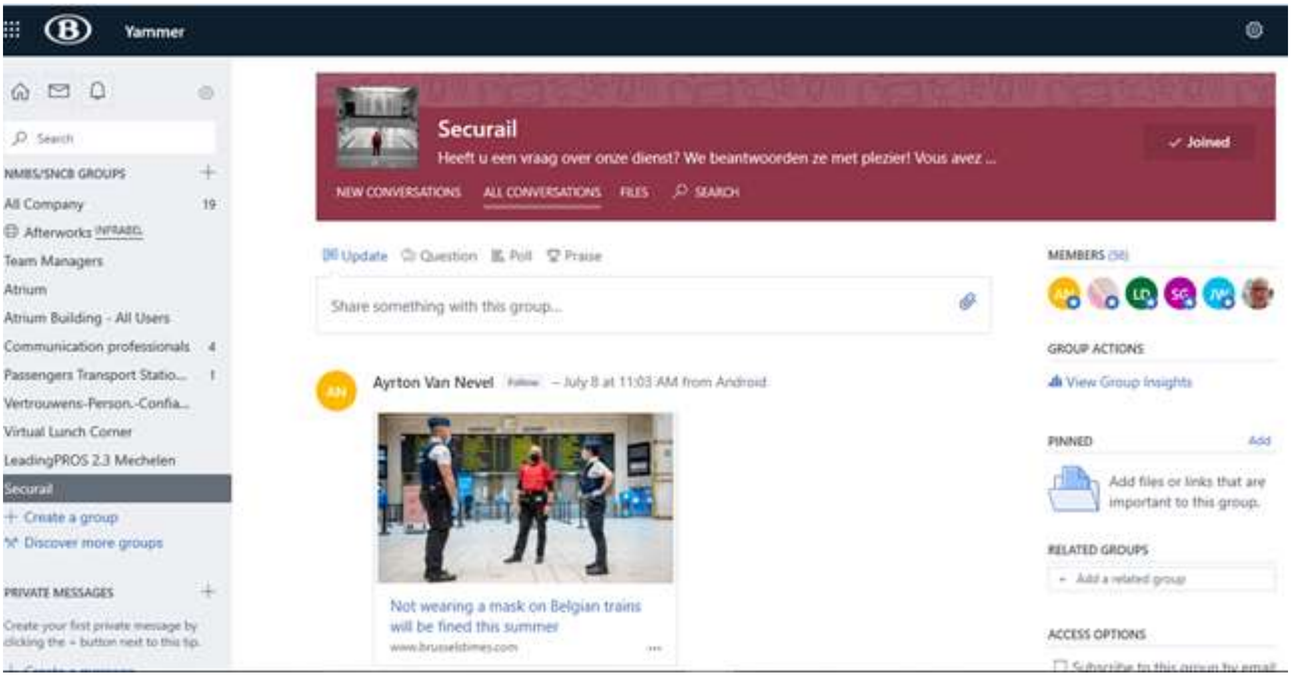
Gardez vos bagages à l'oeil!

sncb
À suivre
LECTURE AUTOMATIQUE
Bruxelles-Midi la nuit...
Mourad - Agent de sécurité
Fraude à l'hygiène - Documentaire
Maes - Prioritaire (Lyric Video)
Job : Chasseur d'appartements pour milliardaires
PARTAGER
ENREGISTRER
Rechercher...

These networks have more than 170,000 followers and 800 mentions per day and involve real time interactions when a security incident is reported. A standard response message including the toll-free emergency number is then posted.

Messages concerning danger or suspicious behaviours on social networks are filtered by community managers and communicated in real time to the Security Operations Centre, which takes the most appropriate measures.

SNCB also has an internal corporate social network: Yammer. This network works similarly to Facebook and allows all employees to share information they consider useful and to interact with each other's posts. The messages can of course be security related.



Create your first private message by clicking the + button next to this tip.

Securail

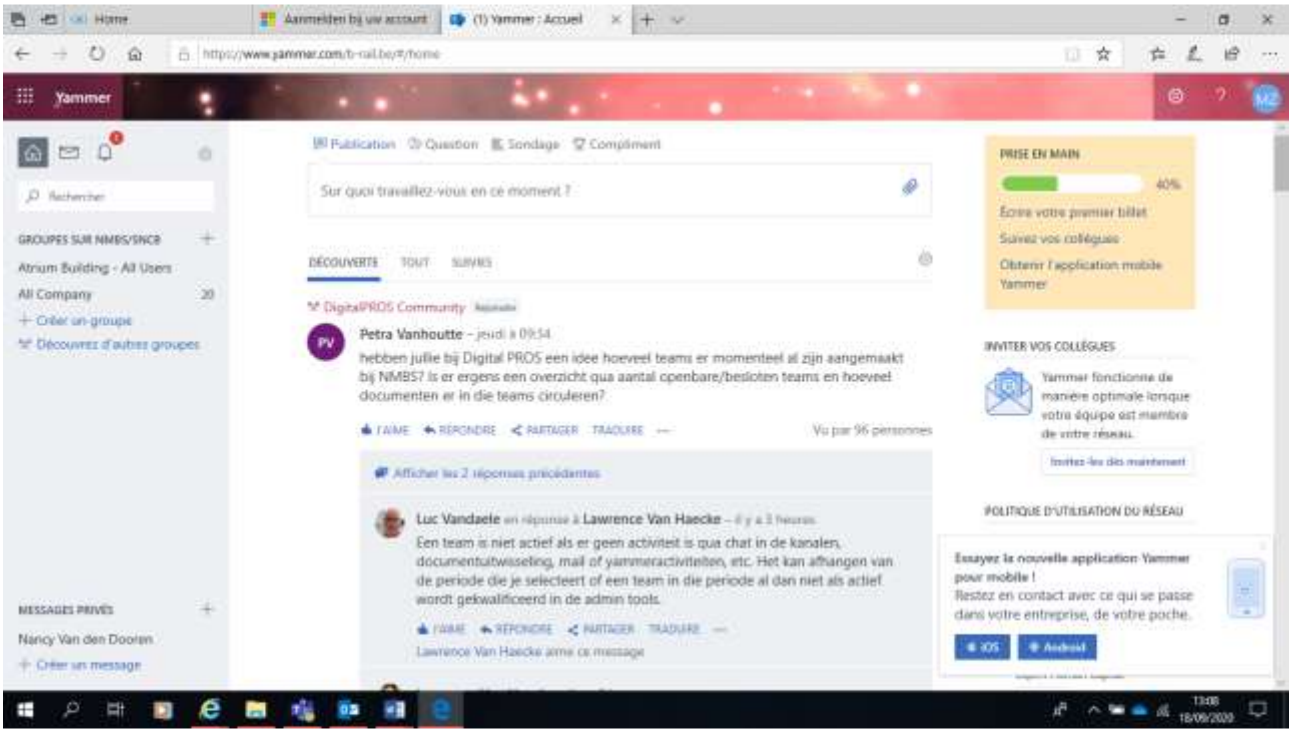
Heeft u een vraag over onze dienst? We beantwoorden ze met plezier! Vous avez ...

Ayrton Van Nevel – July 8 at 11:03 AM from Android

Not wearing a mask on Belgian trains will be fined this summer

www.brusselstimes.com

Add files or links that are important to this group.



Petra Vanhoutte – jeudi à 09:54

hebben jullie bij Digital PROS een idee hoeveel teams er momenteel al zijn aangemaakt bij NMBS? Is er ergens een overzicht qua aantal openbare/besloten teams en hoeveel documenten er in die teams circuleren?

Vu par 96 personnes

Luc Vandaele en réponse à Lawrence Van Haecke – il y a 3 heures

Een team is niet actief als er geen activiteit is qua chat in de kanalen, documentuitwiseling, mail of yammeractiviteiten, etc. Het kan afhangen van de periode die je selecteert of een team in die periode al dan niet als actief wordt gekwalificeerd in de admin tools.

Lawrence Van Haecke aime ce message

Yammer fonctionne de manière optimale lorsque votre équipe est membre de votre réseau.

Essayez la nouvelle application Yammer pour mobile !

Restez en contact avec ce qui se passe dans votre entreprise, de votre poche.

5.2.2. SNCF (France)

SNCF is present on a large number of social media platforms: Facebook, Twitter, Instagram and LinkedIn. SNCF is mentioned 5000 times a day on average. SNCF is present on social media 7 days a week from 7am to 10pm, all year round. As such, SNCF can be considered omnipresent and must know how to control its image.

This control requires a specific organization consisting of two teams: The e-reputation division – Located within the Communication and the Marketing Department of SNCF (Saint-Denis), which oversee institutional communication and the protection of the SNCF group's image on the web. These teams are in charge of:

- The Social Room, located within SNCF VOYAGES' external communication department (La Défense), provides community management and coordination with two major services: the traffic information center and the remote customer relations center.
- The traffic information center is located near the Gare de l'Est train station in Paris. The Traffic Information Center at the Gare de l'Est station in Paris, which is located within the national rail operations center. This pole's mission is to update traffic information in real time on the website and in the SNCF application, and on the other hand to answer questions about passenger traffic on digital channels.
- The remote customer relations center is located in Vannes and Nantes. The Remote Customer Relations Department of Vannes and Nantes. These teams are dedicated to commercial relations for ticket purchases, loyalty programs, questions about services, after-sales, etc.
- The e-reputation division is in charge of highlighting the expression channels of SNCF on all digital platforms. Sharing the values and the universe of the SNCF group allows to positively involve the public and to counterbalance the negative feedback from public opinion.
- The e-reputation division also handles web monitoring for the entire SNCF brand. It manages sensitive subjects in close collaboration with the SNCF group's crisis communication department.
- “The challenge for SNCF on social networks is to gather the speeches of carriers and other entities to respond with a single voice to Internet users who solicit us. Thanks to all our tools and the organization we have put in place, we are able to respond effectively to any type of request 7/7 from 7am to 10pm. [...] The multiplicity of channels through which SNCF customers can contact us greatly facilitates exchanges" explains Michaël Fleurbaey, head of the e-reputation division of the SNCF Group.

The theme of "security" is an integral part of the sensitive subjects handled by the e-reputation division. The connections between the e-reputation division, the SNCF Security Directorate and the Ministry of the Interior are essential in order to pass on sensitive messages about the security of goods and people as quickly as possible. These reports are made via the PHAROS platform. These information feedbacks are done by email, 7/7 24/24.

2 examples:

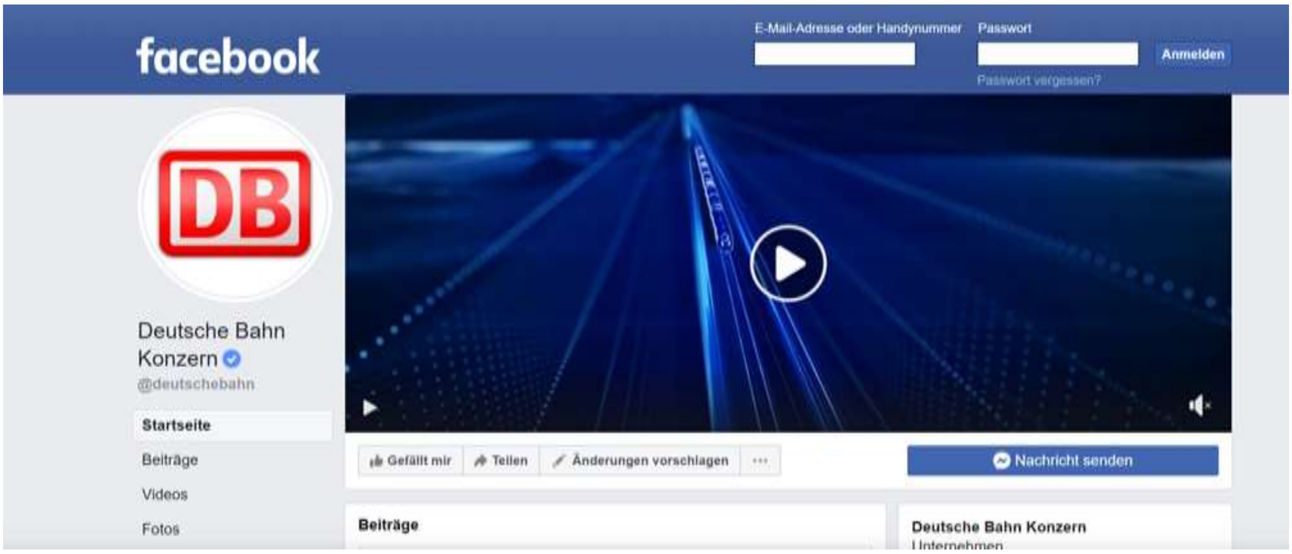
- During the attacks on the Bataclan, SNCF was at the disposal of the Ministry of the Interior and the Police Prefecture. All publications were stopped, and we relayed official messages. The connection between the DNcom (national director of crisis communication), the DNSF (national director of railway security) and the Ministry of the Interior is permanent. All messages related to security events are relayed from DNCOM to DNSF to the Ministry.
- During the Thalys attack, the communication department's crisis room was opened. It is the DNCOM that manages the 360 communication, including social networks. The e-reputation division put itself on standby throughout the crisis period and provided regular monitoring reports.

5.2.3. DB AG (Germany)

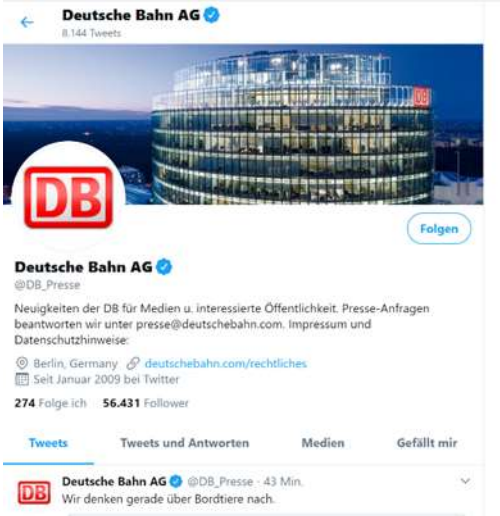
A social media strategy is an established part DB’s communication. Deutsche Bahn Group and Deutsche Bahn Passenger Transport Communication Departments coordinate the central dialogue channels with high user numbers and open dialogue. DB has been expanding online communication activities continuously. Thanks to a competence team working across the group and various channels, social media has been a fixed component of corporate communications since December 2011. The focus of DB's social media strategy is media- and other target group-oriented dialogue. Beyond Facebook, Twitter, YouTube and Instagram, Deutsche Bahn is now also active on WhatsApp, XING and Foursquare.

DB's social media activities are intended to create an open, transparent exchange and enable personal communication with users on the web. The Social Media teams of DB are aware of the critical environment, therefore deliberately seek dialogue and exchange with interested parties and travelers and offer their users a competent and fast response which is a confirmed, added value.

In establishing the DB Facebook presence, DB Group Communications acts as a kind of catalyst and online distribution of passenger transport is jointly and closely interlinked.



DB offers news for the media and the interested public, direct contact with Deutsche Bahn passenger transport, current transport news and information on career opportunities also on the short message service Twitter since January 2009.



Deutsche Bahn AG
8.144 Tweets

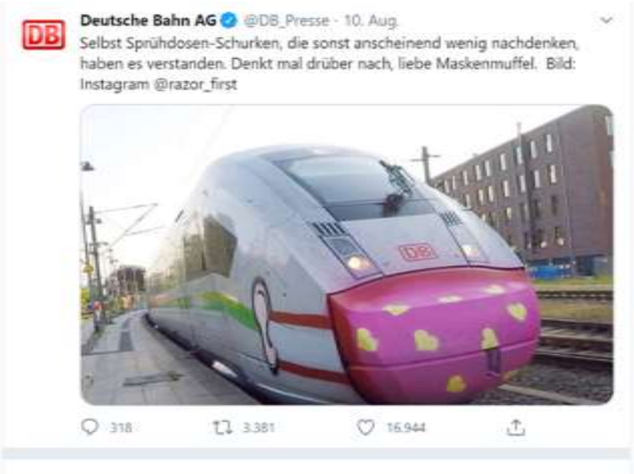
Deutsche Bahn AG
@DB_Presse

Neuigkeiten der DB für Medien u. interessierte Öffentlichkeit. Presse-Anfragen beantworten wir unter presse@deutschebahn.com. Impressum und Datenschutzhinweise:

Berlin, Germany deutschebahn.com/rechtliches
Seit Januar 2009 bei Twitter

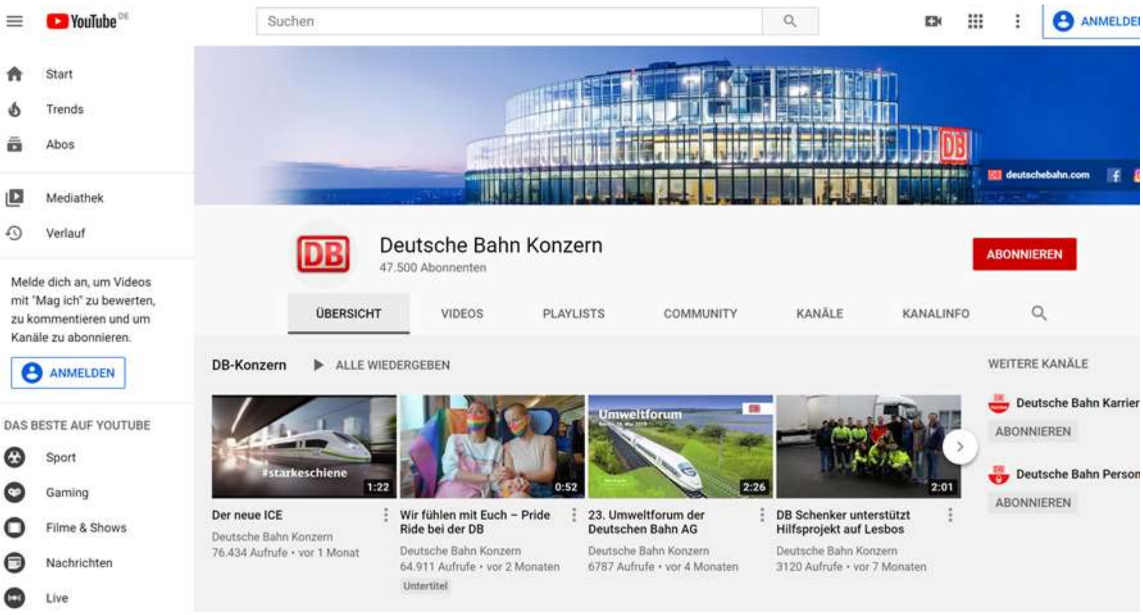
274 Folge ich 56.431 Follower

Deutsche Bahn AG @DB_Presse · 43 Min.
Wir denken gerade über Bordtiere nach.



Deutsche Bahn AG @DB_Presse · 10. Aug.
Selbst Sprühdosen-Schurken, die sonst anscheinend wenig nachdenken, haben es verstanden. Denkt mal drüber nach, liebe Maskenmuffel. Bild: Instagram @razor_first

As with Facebook, the content on DB Group' YouTube channel also reflects people's interests in the railway industry and also considers customers' and stakeholders' expectations. Complex interrelationships are presented here in moving image contributions clearly explained in order to gain a better understanding of the structures and fields of DB Groups' activities. The users can display the contents in different playlists such as "DB Group", "Logistics", "Infrastructure and Technology" or "Security and Safety at Railway Facilities” according to their interests.



Melde dich an, um Videos mit "Mag ich" zu bewerten, zu kommentieren und um Kanäle zu abonnieren.

Deutsche Bahn Konzern
47.500 Abonnenten

DB-Konzern

Der neue ICE
Deutsche Bahn Konzern
76.434 Aufrufe • vor 1 Monat

Wir fühlen mit Euch – Pride Ride bei der DB
Deutsche Bahn Konzern
64.911 Aufrufe • vor 2 Monaten
Untertitel

23. Umweltforum der Deutschen Bahn AG
Deutsche Bahn Konzern
6787 Aufrufe • vor 4 Monaten

DB Schenker unterstützt Hilfsprojekt auf Lesbos
Deutsche Bahn Konzern
3120 Aufrufe • vor 7 Monaten

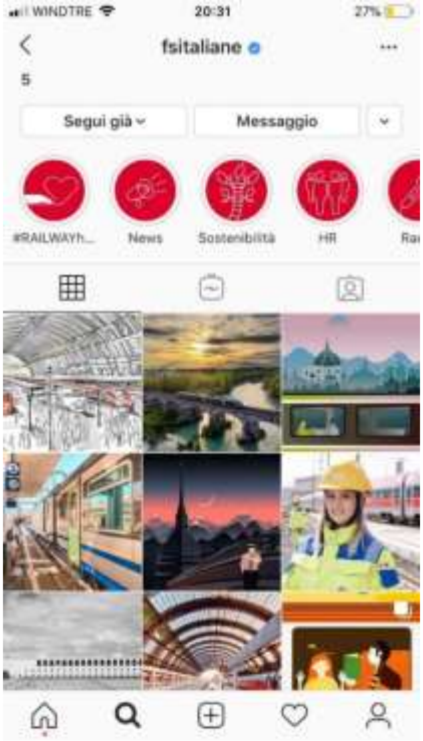
Deutsche Bahn Karrier
Deutsche Bahn Person

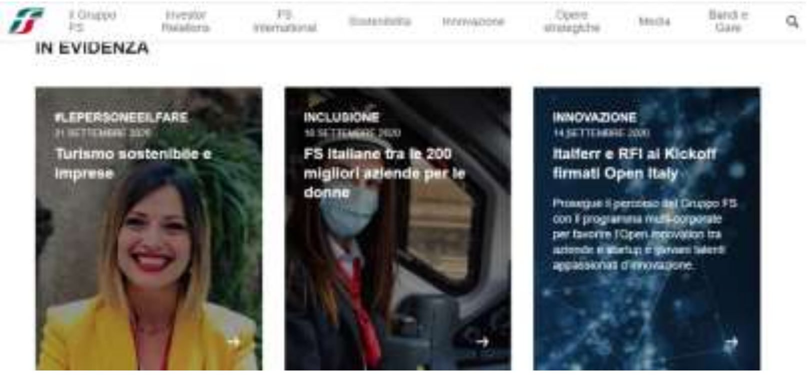
At the centre of the social media communication, however, topics such as innovation, technology, infrastructure, ecology, logistics and the social commitment of DB are presented. Security communication is in the hand of the close partnership with the federal police and cannot be found in isolated DB social media channels. The partners have, however, agreed to integrate information on security-relevant behaviour in social media in a more targeted and stronger direction in the future.

5.2.4. FS (Italy)

Social media are technologies designed for social interaction, exchange and cooperation, mainly aimed at sharing, promoting and socializing contents. Facebook, Twitter, Linkedin, Youtube, Instagram, Flicker, Foursquare, Wikipidia are good examples of platforms that allow the publication and sharing of texts**,** comments, reviews, photos, videos, audios, votes / "like". From a company point of view these tools can facilitate the definition of a direct and constant exchange/contact with customers and the promotion of core business activities and initiatives.

The FS Group, recognizing the crucial importance of being effectively present on these platforms, introduced a dedicated policy/procedure aimed at ensuring a full, legitimate and functional online activity and participation.





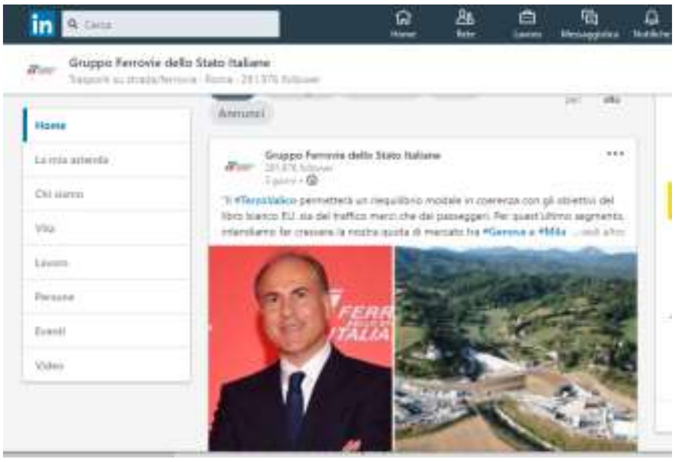
IN EVIDENZA

#LEPERSONEEILFARE
21 SETTEMBRE 2020
Turismo sostenibile e imprese

INCLUSIONE
18 SETTEMBRE 2020
FS Italiane tra le 200 migliori aziende per le donne

INNOVAZIONE
14 SETTEMBRE 2020
Italferr e RFI al Kickoff firmati Open Italy

Prosegue il percorso del Gruppo FS con il programma multi-corporate per favorire l'Open innovation tra aziende e startup e giovani talenti appassionati d'innovazione.



Gruppo Ferrovie dello Stato Italiane
Trasporti su strada/ferrovie · Roma · 281.376 follower

Gruppo Ferrovie dello Stato Italiane
281.376 follower
2 giorni •

"Il #TerzoValico permetterà un riequilibrio modale in coerenza con gli obiettivi del libro bianco EU, sia del traffico merci che dei passeggeri. Per quest'ultimo segmento, intendiamo far crescere la nostra quota di mercato fra #Genova e #Mila ...vedi altro

In this regard, following the mentioned internal regulations/guidelines, the FS Group uses its official profiles to share and communicate with customers information related to a restrict area of topics, such as:
Real time information, concerning rail traffic, also on customer request.
Services, promotions and commercial offers.
Press release, communication campaigns, images, official audios and videos.
Publications and social offers.
Job opportunities and social campaigns.
To facilitate and guarantee the effective fulfillment of these activities, the Fs Group has set up a specialized team, within the Central External Communication and Media Department, with the task of defining and managing the group online communication strategy,:

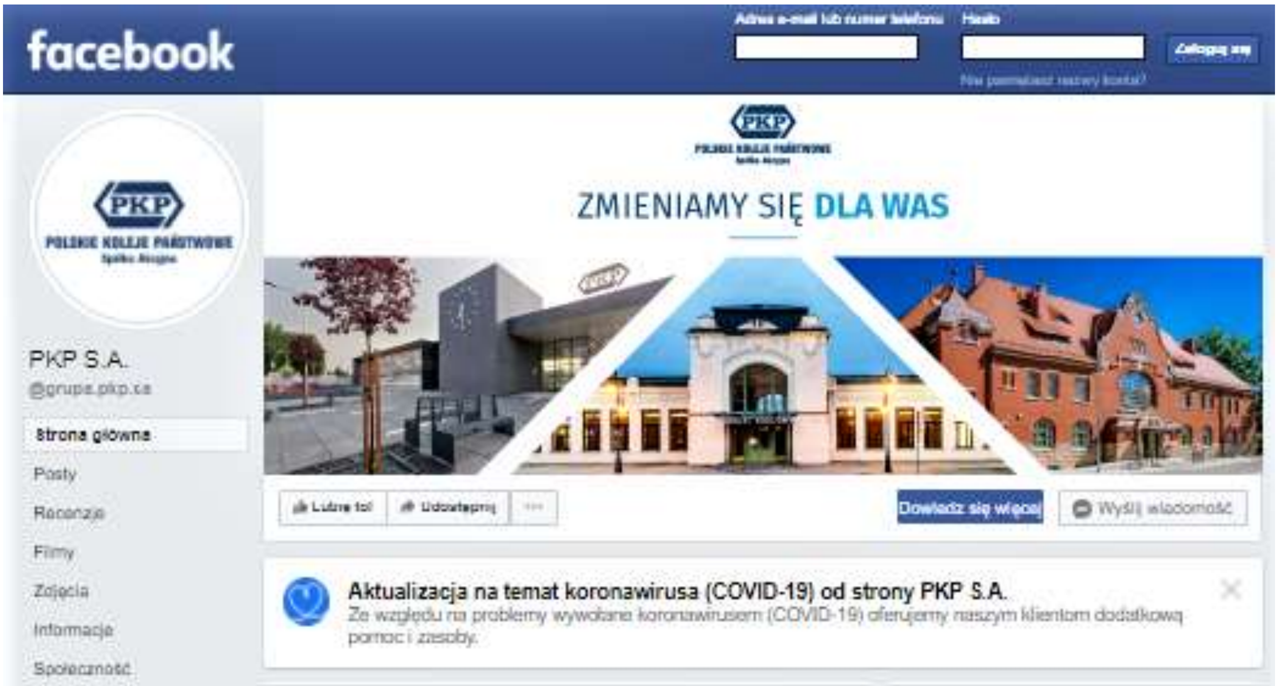
- creating accounts, profiles, pages and web spaces;
- publishing contents (texts, videos, images, audio, etc ...) on official social profiles;
- planning and implementing, initiatives for the companies of the Group;
- verifying the design and implementation of initiatives, for subsidiaries or investee companies, with a prevalent business content;
- responding to customer requests;
- moderating users in the official social spaces of the FS Italiane Group;
- participating in online discussions on behalf of the FS Italiane Group.

However, according to this communication strategy, FS Italiane does not use social media to share security information. The Group only refers to social media in case of emergency with the aim of informing customers on a specific event, affecting the regularity of railway services and activities and the measures adopted to face and manage the events (crisis, emergency ecc.). In this case the communication towards the public is organized on the basis of a dedicated strategy, internally defined, lead by an Emergency Committee and in strict accordance with public authorities prescriptions

5.2.5. PKP S.A. (Poland)

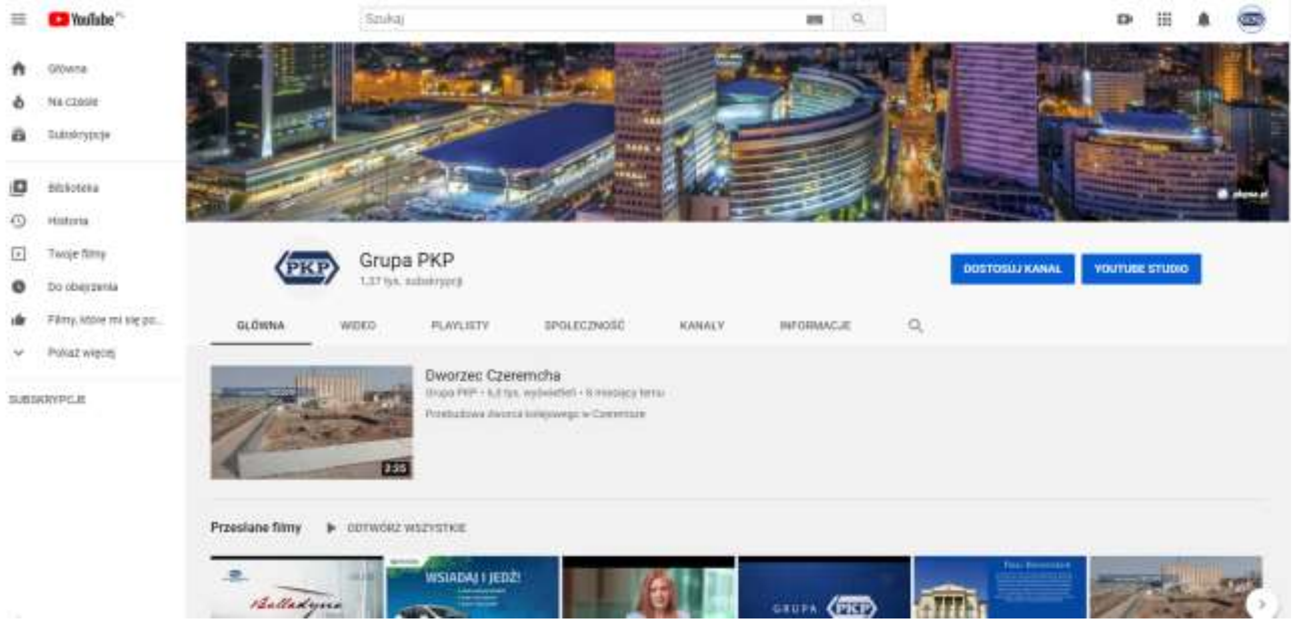
Social media is a part of the overall communication of PKP S.A. in public spaces, which is constantly being developed due to the changing reality, trends and popularity of these channels among society. PKP S.A. has profiles in the following social media: Twitter, Facebook, LinkedIn, YouTube and Instagram. These profiles are used to build a positive image of the company and to communicate about station investments and other events and activities of the group. Social media is the most effective tool for external communication and interaction with users.

As a rule, social media is not used to inform the public about the threats of terrorism. However, part of the communication strategy is to provide information that has an impact on raising passengers' awareness also in the area of security, such as providing information about the conducted "Aware=Safe" campaign.



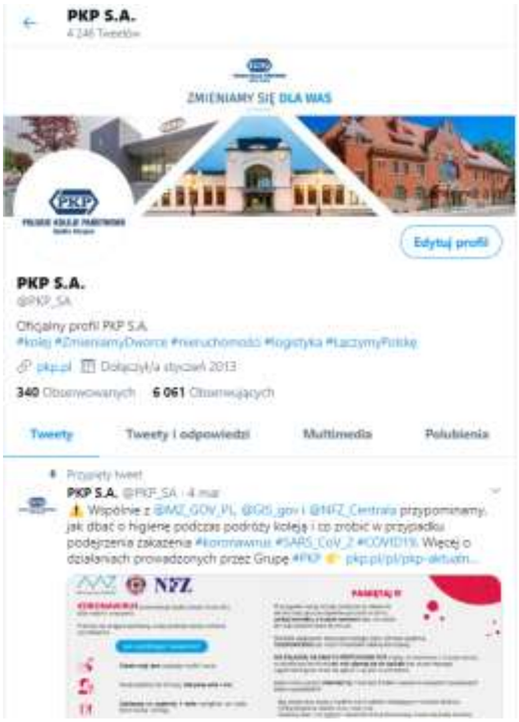
Aktualizacja na temat koronawirusa (COVID-19) od strony PKP S.A.
Ze względu na problemy wywołane koronawirusem (COVID-19) oferujemy naszym klientom dodatkową pomoc i zasoby.

At the same time it should be emphasized that other companies of the PKP Group such as PKP Intercity S.A., PKP Polskie Linie Kolejowe S.A. or PKP Cargo S.A. run their own social media profiles. However, they also do not focus on highlighting terrorist threats and use softer tools to raise awareness among passengers.



Grupa PKP
1,37 tys. subskrypcji

Dworzec Czeremcha
Grupa PKP • 6,8 tys. wyświetleń • 8 miesięcy temu
Przebudowa dworca kolejowego w Czeremsze



PKP S.A.
4 246 Tweetów

PKP S.A.
@PKP_SA

Oficjalny profil PKP S.A.
#kolej #ZmieniamyDworce #nieruchomości #logistyka #ŁączymyPolskę

pkp.pl Dołączył/a styczeń 2013

340 Obserwowanych 6 061 Obserwujących

Przypięty tweet
PKP S.A. @PKP_SA · 4 mar
⚠️ Wspólnie z @MZ_GOV_PL, @GIS_gov i @NFZ_Centrala przypominamy, jak dbać o higienę podczas podróży koleją i co zrobić w przypadku podejrzenia zakażenia #koronawirus #SARS_CoV_2 #COVID19. Więcej o działaniach prowadzonych przez Grupę #PKP 👉 pkp.pl/pl/pkp-aktualn…

Bezpieczeństwo na dworcach cz. 1

5.3. Potential Benefits and Negative Implications of Social Media

5.3.1. Advantages

- ***Emergency information via social media may help those who are ill-prepared for an incident:*** Providing lifesaving directives and information at the onset of an incident, or during an incident, could help underprepared citizens. It can provide for essential information such as evacuation details, food, water, and shelter locations etc. (…)

- ***Social media can provide for a two-way communication:*** Another potential benefit of social is that it enables public's ability to communicate with authorities or crisis management. Classic and current emergency communication seem to focus on a one-way communication—from the crisis management to the individuals. Social media has the ability to change that and provide for a communication also from the individual towards the crisis management. (…)

- ***Social media could be used as a supplement to the common telephone emergency lines:*** Landline phone networks might be unavailable or intermittently available, with the emergency service line rapidly becoming overwhelmed by the incoming volume of calls. This has been seen during a number of attacks as the Madrid train bombings, the London tube explosions or the Brussels attacks. Fiber-optic connectivity and mobile telephone networks are severely affected during a critical situation too but, in most of the crisis situations, they exhibit a more resilient performance, especially concerning the capacity to establish SMS and text messaging communication. (…)

- ***Citizens' journalism:*** Online social media has been instrumental in providing eye-witness accounts and first impressions from the affected areas, thus contributing to the enhancement of the general situational awareness. (…)

5.3.2. Negative Implications

- ***The "digital divide": not everyone uses social media:*** While the term 'digital divide' originally referred to whether people had access or not to digital technologies, today digital divides are defined by skills, frequency of use and how people are able (or not) to solve their problems thanks to technologies[27]. The recent Petersen et al. (2017) study found that young people were slightly more likely to expect critical infrastructure operators to use social media for crisis communication[20]. That said, young people are not the only ones using social media and it can be a useful tool to reach persons of

[27] Horrigan, J.B. (2016). Digital Readiness Gaps. *Pew Research Center*. http://www.pewinternet.org/2016/09/20/digital-readiness-gaps/

all ages, while keeping in mind the issue of a) having interest access and b) opting-in to the use of a given social media platform.

- ***Spread of false information:*** Social media can serve as instrument for rumor, misguidance and misinformation. Despite this, as stated in the introduction, it has still been found to be a worthwhile tool for situational awareness for responders. Further, studies have also demonstrated that once rumours have been negated by official sources, they quickly die down[28]. This further demonstrates the importance in spreading true information quickly as soon as an incident starts.

[28] Kaigo, M. (2012). Social media usage during disasters and social capital: Twitter and the great East Japan earthquake. *Keio Communication Review*, No. 24

PART C- RECOMMENDATIONS FOR CRISIS COMMUNICATION

1. RAILWAYS' CRISIS COMMUNICATION GUIDE TOWARDS THE PUBLIC FOR TERRORIST INCIDENTS

1.1. Setting up one's digital media strategy

The following are recommendations on how to set up one's digital media strategy for security awareness and terrorism related crisis communication:

- determine appropriate types of information for dissemination;
- identify target audiences for the applications;
- identify preferred medium of communication;
- identify when and why communication should be provided;
- determine the appropriate format of information for dissemination;
- set up an approval process;
- identify any negative consequences arising from the application;
- provide for a regularly response to posts and requests;
- provide accurate information;
- consider malicious or disruptive use of social media;
- proactively seek out and eliminate malicious posts and profiles;
- consider technological limitations;
- incorporate privacy law implications;
- plan for administrative efforts and costs;
- Perform regular security audits;
- Delete inactive accounts; and
- Invest in adequate security software.

1.2. Executing one's digital media strategy

1.2.1. Preparedness

Digital media should be used to communicate directly with the public during the preparedness phase of the crisis management cycle for increased security awareness. Awareness campaigns can take many forms, as was illustrated within this deliverable. It is important to keep in mind that the level of communication on security should be in line with national frameworks.

1.2.2. Response

During the response phase of the crisis management cycle, it is important to acknowledge the crisis and provide continuous updates, including updates that there is still no new information. During this phase, it is important to provide the public as soon as you are able to with information regarding how the terrorist attack might affect the railway transport offering/timetables. It is also a good time to make use of the crisis communication amplification potential of social media and other digital medias by repeating official information provided by official sources (e.g. law enforcement agencies). Indeed, studies have shown that the repetition of key messages as well as finding the same information from different sources helps the public to take the correct action. When a terrorist attack take place, people begin a search for information not only relating to what has happened, but also about how they should act. People want to be informed on this, and so it is a good opportunity to provide them with advice, such as those provided by national authorities.

1.2.3. Recovery

After the attack has happened and the security of all involved is once more assured, this is the prime time for the railway company to examine their crisis communication strategy to evaluate what worked and what didn't work. Another key aspect of crisis communication in the recovery phase of the crisis management cycle is to use digital media as a means to restore confidence in rail travellers. Indeed, people may be apprehensive to return to an area that was part of a terrorist attack. Communicating about new security measures put in place may help to recreate a feeling of security amongst travellers.

CONCLUSION

This deliverable has addressed the issue of how digital media can be used to both increase security awareness and improve crisis communication regarding terrorist attacks by railway companies. It has highlighted some of the difficulties involved in communicating about such security issues, namely, that this topic falls under the responsibility of the State and as such railway companies must comply with State undertakings. That said, the State has seen the value in collaborating with railway companies to increase security awareness and most railway companies share at least the information provided by their respective authorities.

Next, the deliverable presented the best practice examples from the SHERPA consortium partners regarding four different kinds of digital media: security awareness communication campaigns, mobile applications, social media and emergency numbers. The many examples demonstrated the important role the railways have to play in developing security awareness of the general population as well as their staff.

Finally, recommendations were presented on how to first, set-up a digital media for terrorism strategy and second, how to implement said strategy. To set up, one must take into consideration a plethora of elements, including which digital media, what kinds of information, who will be in charge, etc. The recommendations for implementing the strategy follow the three main stages of the crisis management cycle: preparedness, response and recovery.