ASTEK

SMI

Information Security Awareness Structure Module

François FEVRIER – CISO – ffevrier@groupeastek.fr

C2 – CONTROLLED DIFFUSION / 30.12.2021 / SMI-000469-DOC

SUMMARY

APPLICABLE SECURITY RULES

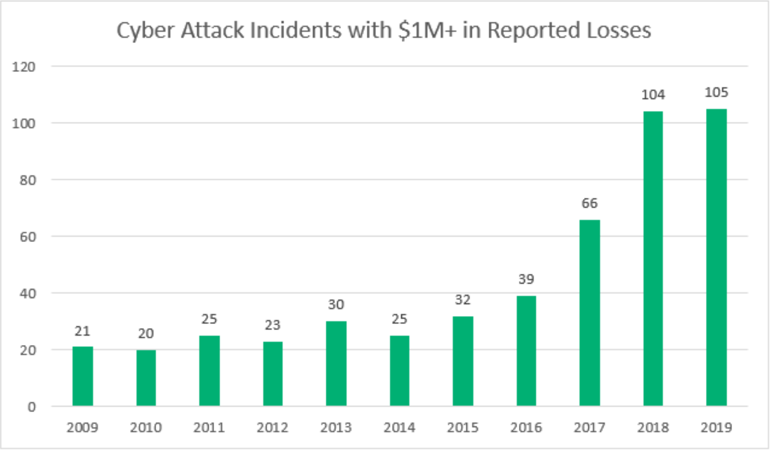
DATA CONFIDENTIALITY

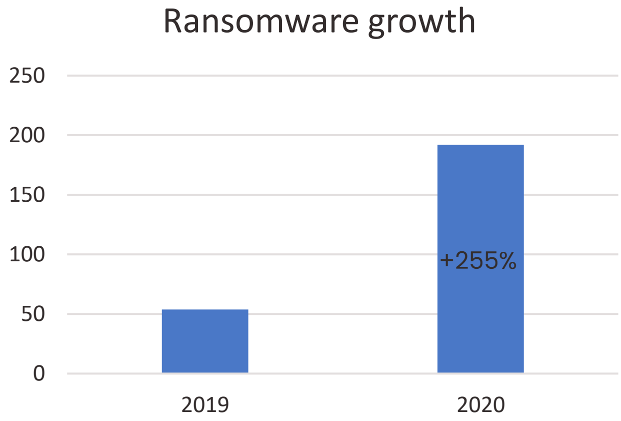
BEST PRACTICES

USEFUL CONTACTS

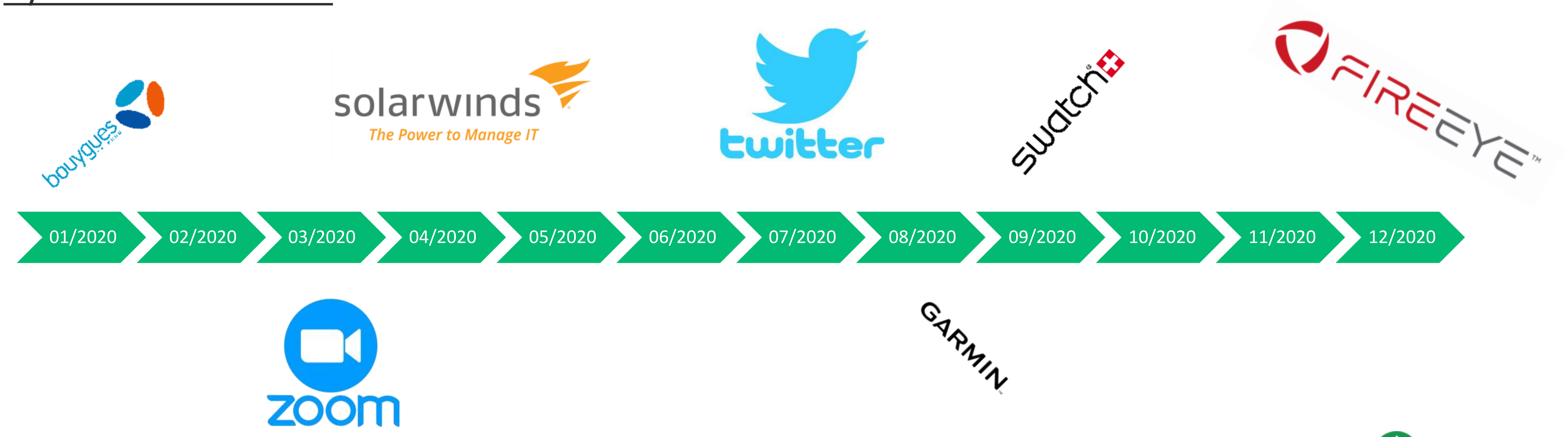
WHY THERE ARE RULES ?

Increasing threats:





Cyber attacks in 2020



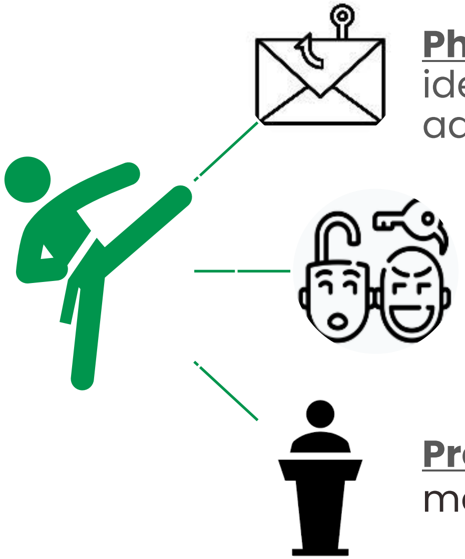
WHY THERE ARE RULES ?

The Structure population: a prime target for attackers

You may be involved in handling financial or contractual documents.

You are in contact at several levels with decision-makers within the company.

The most frequent techniques



Phishing : A technique used to obtain personal information in order to perpetrate identity theft. The technique consists in making the victim believe that he/she is addressing a trusted third party (bank, administration, etc.)

Social engineering: psychological manipulation for the purpose of fraud.

President scam: scammers ask the company to send them a large sum of money, pretending to be the company director

THE ISSP

The reference document

The Information Systems Security Policy (ISSP) reflects ***the strategic vision of the organisation's management about Information Systems Security****. It is the* ***reference document*** *for an organisation in Information Systems Security.*

Who is concerned ?

- All employees must respect the **ISSP**

What is the scope?

- All aspects of the IS (organisation, physical environment, development, operation, maintenance, etc.)
- During the entire life cycle of the IS and the information.

It is available for reading on: https://welcome.groupeastek.com

Reading the ISSP will allow you to work better on a daily basis.

OTHER DOCUMENTS TO BE AWARE OF

Other applicable documents

Internal Regulations

Document specifying the obligations, particularly in terms of safety, that the collaborator must comply within the company

IT charter

Document regulating the use of IT equipment and services made available by ASTEK

Physical Access Management Procedure

Procedure specifying access and security rules in the agencies. (Reference SMI-000377-PROC)

Safe Area Management Procedure

Procedure specifying the access rules to the different areas within a branch (Reference SMI-000310-PROC)

ℹ All these documents are available at **https://welcome.groupeastek.com**

SUMMARY

APPLICABLE SECURITY RULES

DATA CONFIDENTIALITY

BEST PRACTICES

USEFUL CONTACTS

DATA CONFIDENTIALITY

Classification, why?

The classification defines the expected level of security in accordance with the criticality of the information. You must apply the classification defined in the applicable ISSP.

The classification of documents and the application of the rules could have prevented these data leaks

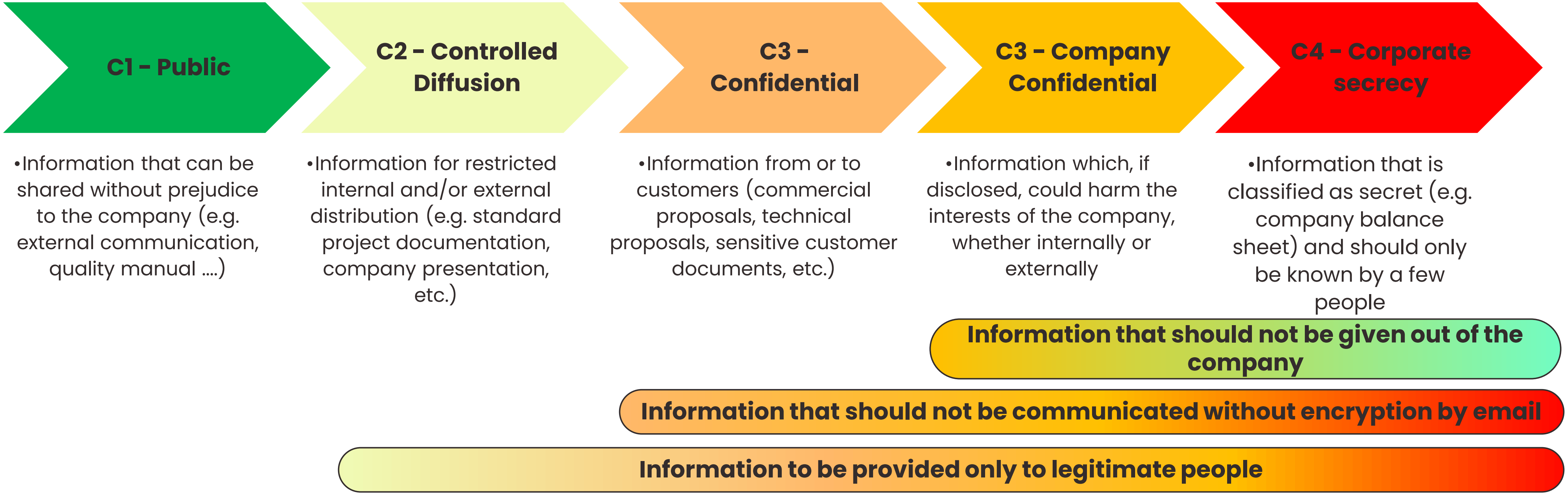
List of data leaks (non-exhaustive list):

Date	Company	Leak
08/2021	T-Mobile	50 million accounts
06/2021	Volkswagen, Audi	3.3 million accounts
06/2021	Linkedin	700 million accounts
04/2020	Facebook	267 million accounts
04/2020	Zoom	500 thousand accounts
04/2020	Nitendo	160 thousand accounts
01/2020	Microsoft	250 million accounts
11/2019	Alibaba	1.1 billion of data
05/2019	Canva	130 millions of data

Financial consequences and impact on the company's image

DATA CONFIDENTIALITY

classify information



C1 - Public

- Information that can be shared without prejudice to the company (e.g. external communication, quality manual ….)

C2 - Controlled Diffusion

- Information for restricted internal and/or external distribution (e.g. standard project documentation, company presentation, etc.)

C3 - Confidential

- Information from or to customers (commercial proposals, technical proposals, sensitive customer documents, etc.)

C3 - Company Confidential

- Information which, if disclosed, could harm the interests of the company, whether internally or externally

C4 - Corporate secrecy

- Information that is classified as secret (e.g. company balance sheet) and should only be known by a few people

Information that should not be given out of the company

Information that should not be communicated without encryption by email

Information to be provided only to legitimate people

A tag should identify the classification of any document

The default classification is "C2 - Controlled Release".

The document « ***Guide pratique de classification et manipulation des documents*** » on https://welcome.groupeastek.com will help you to make the right choice

CLASSIFICATION LEVELS

ASTEK classification: data storage and transfer

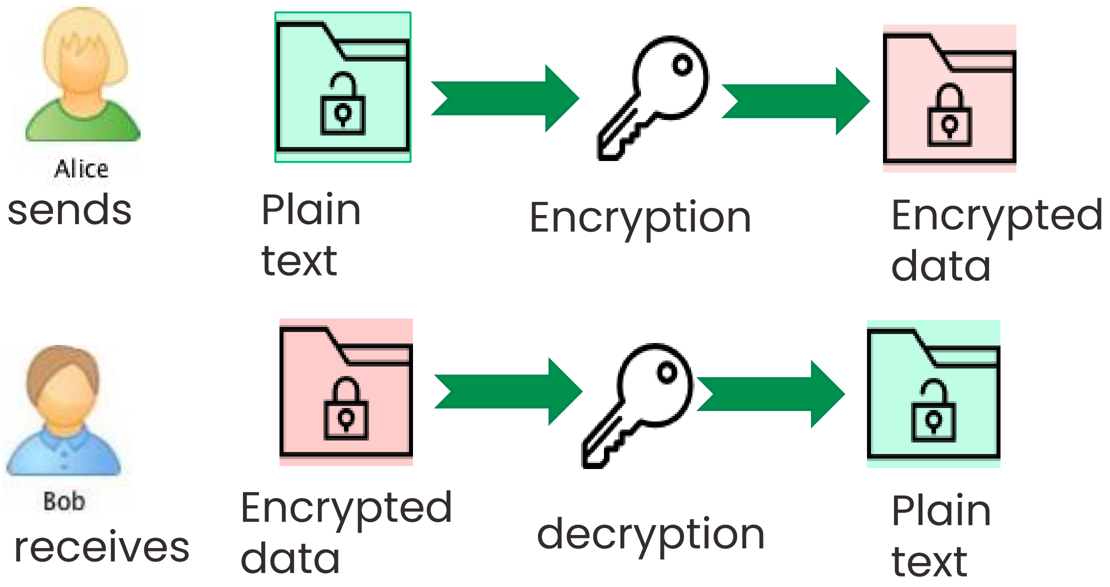
	in-company transfer	transfer outside the company	personal PC	ASTEK PC	IGUANE	SAAS (*)
C1 - PUBLIC	ALLOWED	ALLOWED	ALLOWED	ALLOWED	ALLOWED	ALLOWED
C2 – CONTROLED DIFFUSION	ALLOWED (specific persons)	ALLOWED (specific persons)	FORBIDDEN	ALLOWED	ALLOWED (specific persons)	ALLOWED (specific persons)
C3 – CONFIDENTIAL	ALLOWED (specific persons) if contractual clause : must be encrypted (e.g: Zedmail)	ALLOWED (specific persons) if contractual clause : must be encrypted (e.g: Zedmail)	FORBIDDEN	ALLOWED	ALLOWED (specific persons)	ALLOWED EXCEPT if contractual clause
C3 – COMPANY CONFIDENTIAL	ALLOWED encrypted (e.g: Zedmail) OR by using a **shared link**	FORBIDDEN (except NDA)	FORBIDDEN	ALLOWED	ALLOWED (specific persons)	ALLOWED (specific persons)
C4 – CORPORATE SECRECY	ALLOWED encrypted (e.g: Zedmail) OR by using a **shared link**	FORBIDDEN (except NDA)	FORBIDDEN	ALLOWED not recommended	ALLOWED (specific persons)	FORBIDDEN

(*) O365 (Sharepoint On Line, OneDrive, Teams), BOOND, SIMUS

DATA PROTECTION

One solution: encryption

Encryption means making data readable only if the user has the key.



Alice sends → Plain text → Encryption → Encrypted data

Bob receives → Encrypted data → decryption → Plain text

What can and should be encrypted?

- Communications
- Data
- Computing devices

DATA PROTECTION

How to encrypt a confidential document to be sent by email ?

It is advisable to encrypt all your confidential data so that it become unreadable and ***can be sent*** *securely.*
7 - Zip is the solution recommended by Astek internally

How to encrypt with 7Zip?

- ❑ Right click on the file and select the "7-Zip" menu then "Add to archive...".
- ❑ Select "Compress shared files".
  - ❑ Choose the "AES-256" encryption method
  - ❑ Choose a password.

Decryption is carried out by entering the key when opening the file. The data is then restored to its original state.

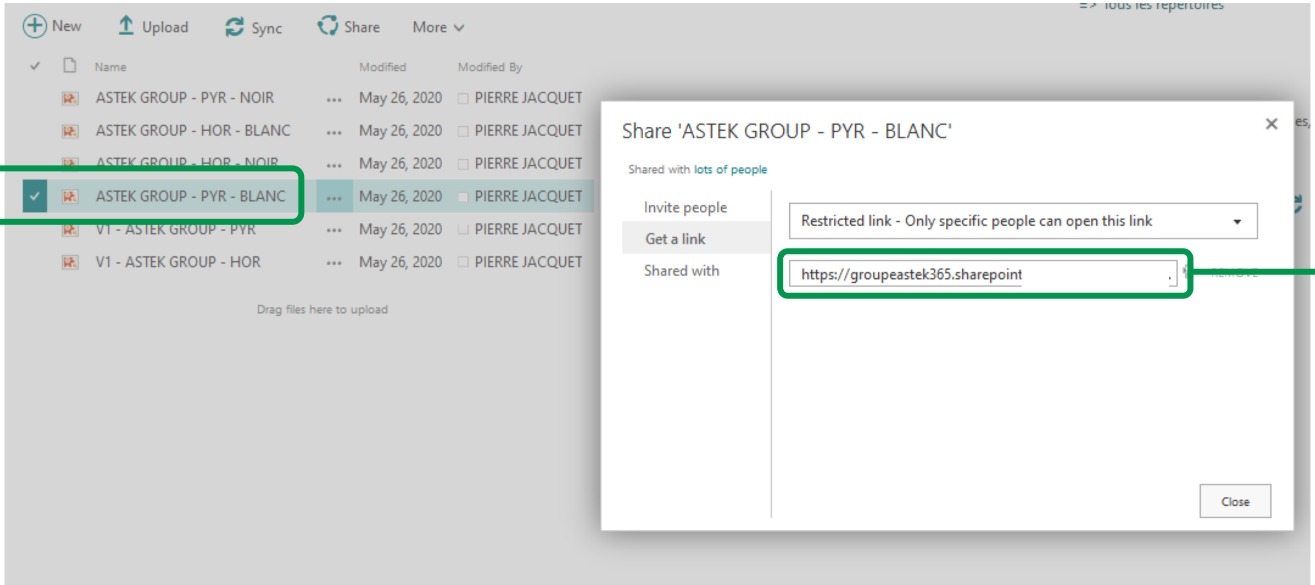
The password must be transferred through another channel than the one used to send the document.
Example: if the encrypted file is sent by email, the password should be sent by SMS.

DATA PROTECTION

Secure information sharing

- **You want to <u>share a document internally</u>**
  - ✓ The right way : **sharing an Office365® document through a link sent by email**
  - ✓ For what types of documents?
    - ✓ All documents except for contractual restrictions with your client
  - ✓ Advantage : **only users with the appropriate authorisation to access the file will be able to access the document** (this avoids the risks associated with an incorrect recipient)
  - ✓ Procedure

Right click on the document to share "Get a link



✓	Name		Modified	Modified By
	ASTEK GROUP - PYR - NOIR	•••	May 26, 2020	PIERRE JACQUET
	ASTEK GROUP - HOR - BLANC	•••	May 26, 2020	PIERRE JACQUET
	ASTEK GROUP - HOR - NOIR	•••	May 26, 2020	PIERRE JACQUET
✓	ASTEK GROUP - PYR - BLANC	•••	May 26, 2020	PIERRE JACQUET
	V1 - ASTEK GROUP - PYR	•••	May 26, 2020	PIERRE JACQUET
	V1 - ASTEK GROUP - HOR	•••	May 26, 2020	PIERRE JACQUET

Drag files here to upload

Share 'ASTEK GROUP - PYR - BLANC'

Shared with lots of people

Restricted link - Only specific people can open this link

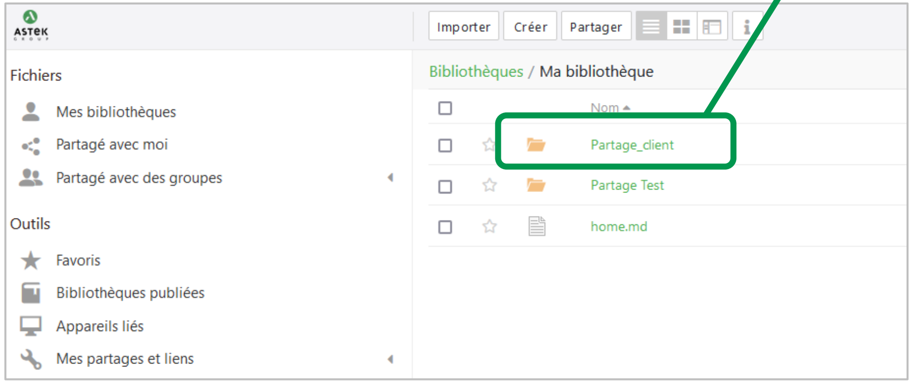
https://groupeastek365.sharepoint

Copy and paste the link into an email

DATA PROTECTION

Secure information sharing

- **You wish to send a group of documents to a contact outside the company**
  - ✓ One possibility: the use of **https://share.groupeastek.com**
  - ✓ Authentication with your Astek account/password
  - ✓ Advantage: share an encrypted folder with a large number of files
  - ✓ How it works
    - ✓ Create a folder and upload files to it
    - ✓ Right click on the folder then "Share".



ASTEK GROUP

Importer | Créer | Partager

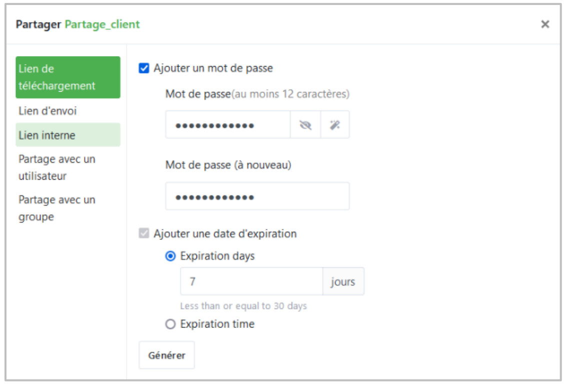
Fichiers
- Mes bibliothèques
- Partagé avec moi
- Partagé avec des groupes

Outils
- Favoris
- Bibliothèques publiées
- Appareils liés
- Mes partages et liens

Bibliothèques / Ma bibliothèque

			Nom ▲
□			
□	☆		Partage_client
□	☆		Partage Test
□	☆		home.md

    - ✓ Add a password and an expiry date



Partager Partage_client ×

- Lien de téléchargement
- Lien d'envoi
- Lien interne
- Partage avec un utilisateur
- Partage avec un groupe

☑ Ajouter un mot de passe

Mot de passe(au moins 12 caractères)

••••••••••••

Mot de passe (à nouveau)

••••••••••••

☑ Ajouter une date d'expiration

● Expiration days

7 jours

Less than or equal to 30 days

○ Expiration time

Générer

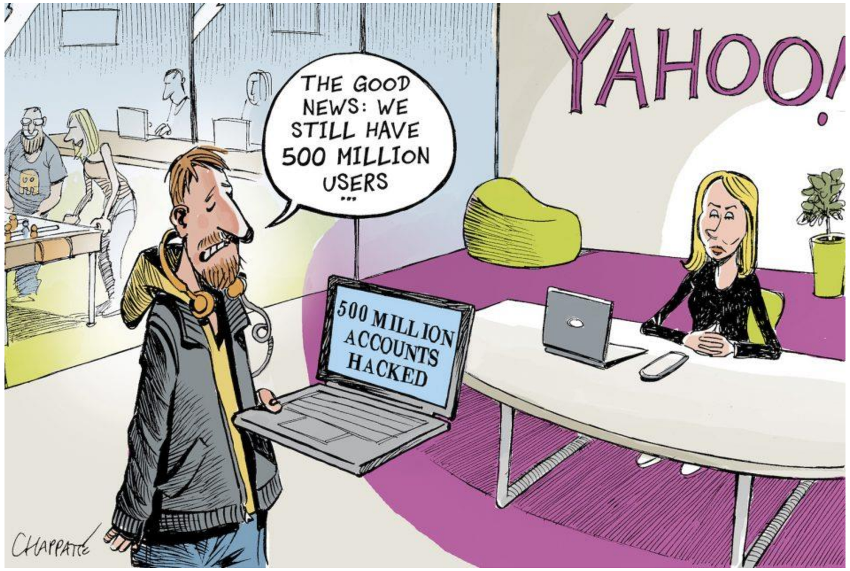
    - ✓ Copy the download link and paste it into an email

The document "***Guide d'utilisation de l'outil de partage de fichiers***" at **https://welcome.groupeastek.com** details how this service works.

DATA CONFIDENTIALITY

What is the GDPR and what are its objectives?

❑ The General Data Protection Regulation (GDPR) is the new European law for the processing and circulation of personal data.


YAHOO!
THE GOOD NEWS: WE STILL HAVE 500 MILLION USERS ...
500 MILLION ACCOUNTS HACKED
CHAPPATTE

❑ What are personal data?

Informations relating to:

- a physical person
- identified directly or indirectly

It can be:

- a name
- a photograph
- an IP address
- a phone number
- a login ID

- a street address
- a fingerprint
- a voice record
- a social security number
- an e-mail, etc.

ℹ You must complete the dedicated GDPR awareness course from https://welcome.groupeastek.com

DATA CONFIDENTIALITY

The GDPR : what applications for me ?

❑ If I am developing a website, a mobile application, etc.

- **PRIVACY BY DESIGN** : requires companies to take preventive rather than corrective measures. They must find solutions upstream, in the products' design and services, without waiting for the existence of a security breach to act.
- **PRIVACY BY DEFAULT** : requires companies to set their products by default with a high level of protection before any use. In other words, when using it for the first time, the user should not need to change any stings to enhance the protection of their data; everything should already be preconfigured.

❑ **The right to be forgotten**
Whether it is an embarrassing photo on a website or information collected by an organization that you deem unnecessary, you can obtain the erasure of personal data in certain specific cases such as if the data is used for prospecting purposes, if the data is not or no longer necessary for the purposes for which it was initially collected or processed or if you withdraw your consent to the use of your data.

GOOGLE GLASS, A SMARTPHONE, A SMARTWATCH... I NOW HAVE EVERYTHING.
...EXCEPT PRIVACY.
DATA MINING
News
U-T San Diego CREATORS.COM

SUMMARY

APPLICABLE SECURITY RULES

DATA CONFIDENTIALITY

BEST PRACTICES

USEFUL CONTACTS

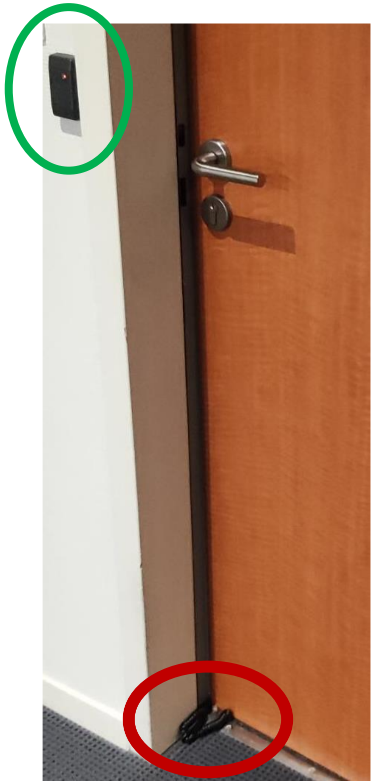
ASTEK

IN ASTEK BUILDINGS

Physical access

Every persons present in ASTEK buildings must be identified.

➡ This allows for easy identification of potential intruders.



A visitor must be accompanied by a resident staff member for the duration of his or her presence in the building.

The neck band with its badge must be worn by each employee
This badge allows access to the offices and the use of printers.

⚠ Doors with access control must remain closed to perform their function. **Any method of keeping a physical access open is prohibited!**

BEST PRACTICES

When you work on an ASTEK site

Information must be protected ➔ you must not facilitate the theft of information

IT equipment security

- ❑ When you are away, your laptop **should be tied down**.
- ❑ Similarly, your computer session should be **locked** (this also applies when you are away in any location).
  - ➔ A keyboard shortcut to use without moderation:

⊞ + L

If you don't have a cable, report it to madsi@groupeastek.fr

Exposure of paper documents

- ❑ When you leave the office in the evening, do not leave papers on the desk.
- ❑ Store confidential documents in locked boxes or rooms.
- ❑ When you no longer need confidential documents, shred them or put them in a secure container.

TELEWORKING

Maintain a good level of confidentiality

SECURE ACCESS TO THE NETWORK

- Better use a wired link to connect to your box.
- Use a strong password if you use the WIFI of the box.
- Use VPN if you need to access the company network.

MAINTAIN PROTECTION OF APPLICATIONS AND SERVICES

- Restart your computer frequently so that **security updates** can be installed.
- Use **complex and unique passwords per account** if you need to authenticate to new services.

USE THE COMPANY'S SHARING SPACES

- Put your work on the company's storage spaces so that it is saved and not only present on your computer (and so avoid any loss of data).
- **Do not use a USB key.**

CONFIRM ALL TRANSACTIONS AND INFORMATION REQUESTS BY PHONE

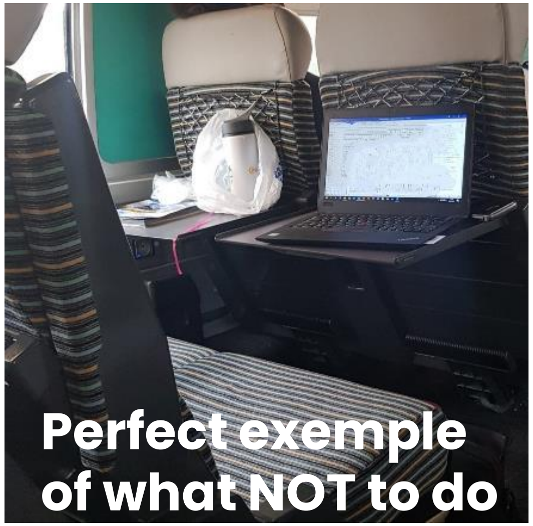
- Avoid email scams by verbally verifying that requests are legitimate and that the transmission of sensitive data is authorised.

ON THE ROAD

Don't let your guard down

In transport (train, plane) and waiting areas (station, airport):

- Use your **privacy filter** on your laptop screen.
- Do **not leave** your workstation alone.
- Do **not use public WIFI**, use your 4G access coupled with the company's VPN



Perfect exemple of what NOT to do

In hotels and restaurants:

- Use the hotel's WIFI **if and only if** you can activate the Company's VPN
- Do not discuss confidential matters over lunch in a loud and pronounced manner

In your vehicle:

- Do not leave visible documents in your vehicle
- Do not leave your computer overnight, even in the trunk.

AND WHEN I AM ON HOLIDAY?

NO

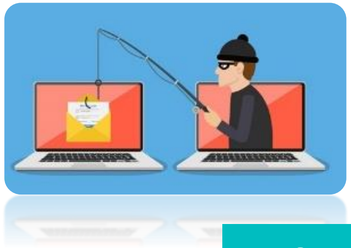
- ✗ Going on holiday abroad with your PC / Pro phone
- ✗ Giving your login details to a friend or colleague

YES

- ✓ Enjoy your holiday

PHISHING

Beware of phishing



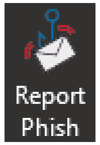
I have a suspicion about the origin of an e-mail...

✗ Do not open attachments
Do not click on the links

✗ Do not provide personal information or passwords

✗ Do not forward the e-mail to colleagues

✓ Report the security incident using Outlook OR from the web browser (office mail)



I have already clicked on a fraudulent link...

✓ I disconnect my computer from the network (wired and WIFI)

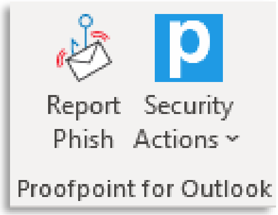
✓ I immediately contact the support team at madsi@groupeastek.fr and give my phone number to be called back

✓ I send an email to securite@groupeastek.fr

EMAILS

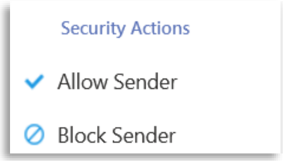
A solution to help you against phishing: Proofpoint©.

Services fromOutlook



A "**Report Phish**" button allows you to easily report a suspected phishing email.

By your action, the e-mail is automatically forwarded to Proofpoint for analysis.



You also have the possibility, from an email, to :

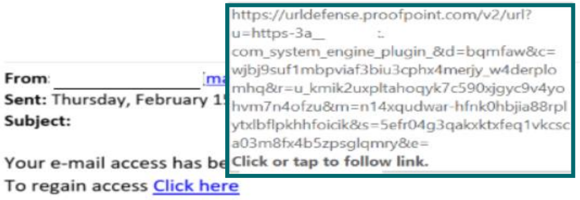
- Block a sender
- Allow a sender

This solution is an ally in the fight against phishing but should not replace your awareness.

URL rewriting

Every URL that is sent to you by e-mail is automatically checked for phishing or malware.

You will notice that these URLs are transparently rewritten for this purpose.



From: ________________ ma
Sent: Thursday, February 1
Subject:

Your e-mail access has be
To regain access Click here

https://urldefense.proofpoint.com/v2/url?u=https-3a__ :
com_system_engine_plugin_&d=bqmfaw&c=wjbj9suf1mbpviaf3biu3cphx4merjy_w4derplomhq&r=u_kmik2uxpltahoqyk7c590xjgyc9v4yohvm7n4ofzu&m=n14xqudwar-hfnk0hbjia88rplytxlbflpkhhfoicik&s=5efr04g3qakxktxfeq1vkcsca03m8fx4b5zpsglqmry&e=
Click or tap to follow link.

Managing spammy emails

Every day, you receive a "Spam Summary" email that shows you the emails received and identified as spam.

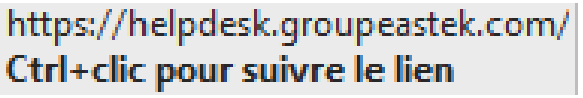
You can access the list and take action by simply clicking to receive one of the spammed emails in your inbox: Deliver / Release

EMAILS

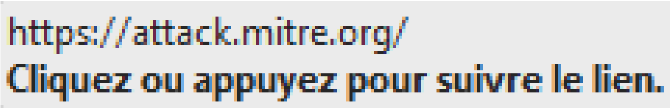
How to check the links received by email?

ASTEK internal mail

Links in emails sent from an **internal mailbox** are **not modified** by Proofpoint



https://helpdesk.groupeastek.com/
Ctrl+clic pour suivre le lien



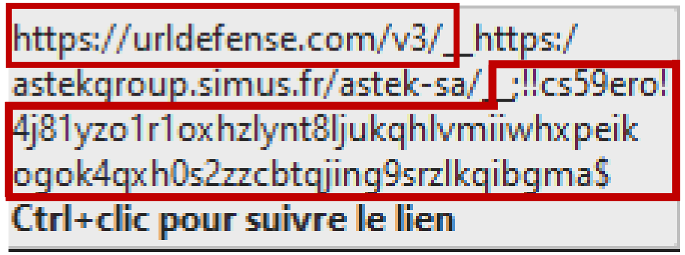
https://attack.mitre.org/
Cliquez ou appuyez pour suivre le lien.

External mail

Links in emails sent from an **external mailbox** are **modified** by Proofpoint. Original links are included between "*https://urldefense.com/v3_*" and "_;" followed by a random text.

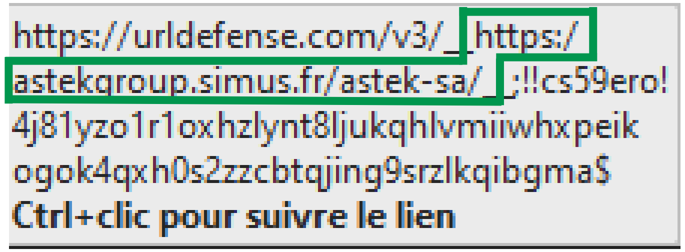
Exemple:

Added part by Proofpoint :



https://urldefense.com/v3/__https:/
astekgroup.simus.fr/astek-sa/__;!!cs59ero!
4j81yzo1r1oxhzlynt8ljukqhlvmiiwhxpeik
ogok4qxh0s2zzcbtqjing9srzlkqibgma$
Ctrl+clic pour suivre le lien

True original link :



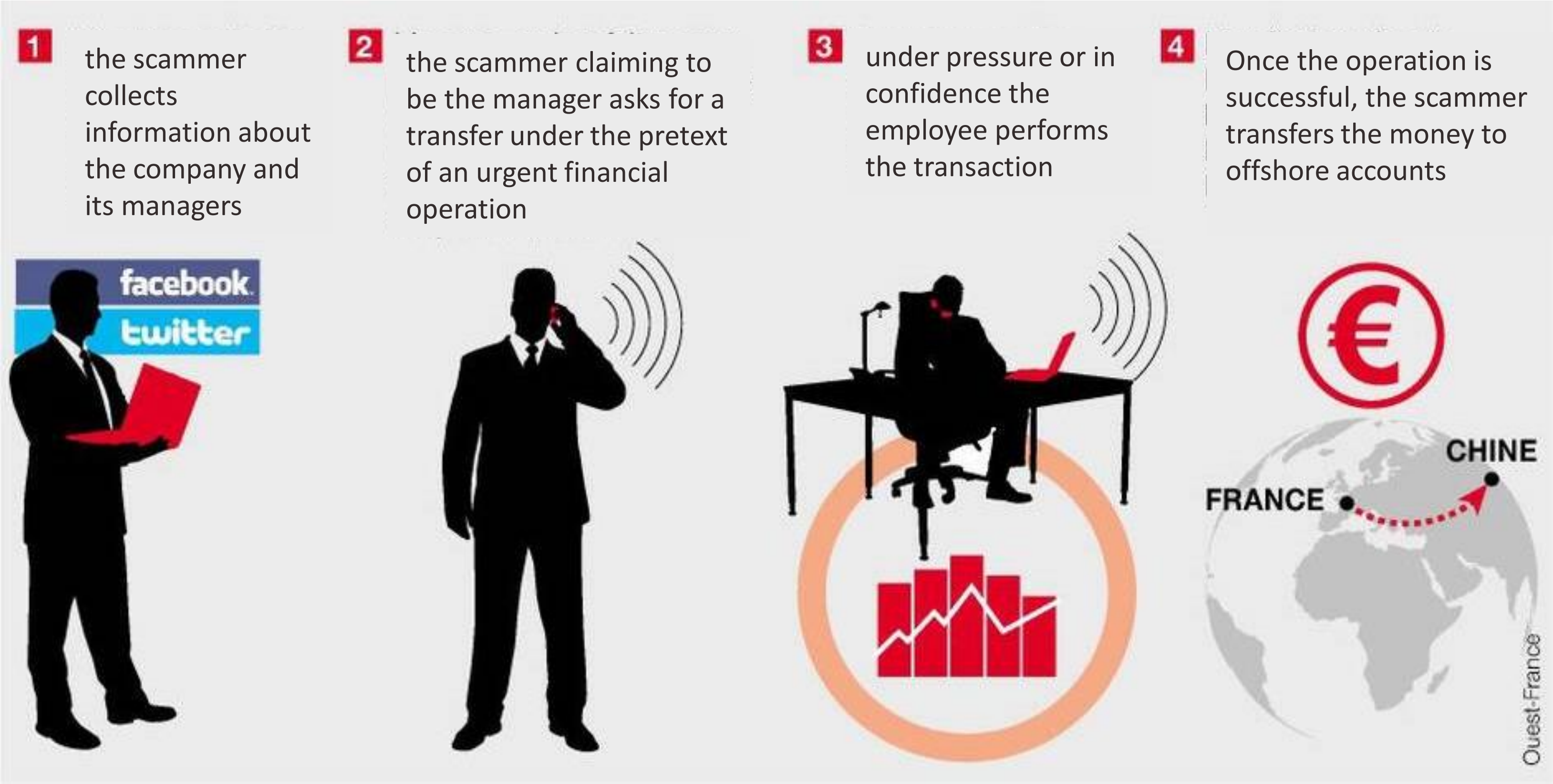
https://urldefense.com/v3/__https:/
astekgroup.simus.fr/astek-sa/__;!!cs59ero!
4j81yzo1r1oxhzlynt8ljukqhlvmiiwhxpeik
ogok4qxh0s2zzcbtqjing9srzlkqibgma$
Ctrl+clic pour suivre le lien

Always hover, with your mouse, over the links in emails (internal and external) to make sure they are authentic

THE PRESIDENT'S SCAM

The scammer presents himself as a company executive and solicits an employee with responsibilities to perform an **urgent and confidential action** (typically a transfer for an acquisition). This approach can be used for other purposes, such as an IS intrusion.

- According to the Office central for the repression of serious financial delinquency, fraud against the president has **cost French companies nearly 500 million euros** in 5 years.
- In 2021, Sefri-Cime was the victim of a fraud of more than 33 million euros



1 the scammer collects information about the company and its managers

2 the scammer claiming to be the manager asks for a transfer under the pretext of an urgent financial operation

3 under pressure or in confidence the employee performs the transaction

4 Once the operation is successful, the scammer transfers the money to offshore accounts

SUMMARY

APPLICABLE SECURITY RULES

DATA CONFIDENTIALITY

BEST PRACTICES

USEFUL CONTACTS

USE CASE

My laptop was stolen

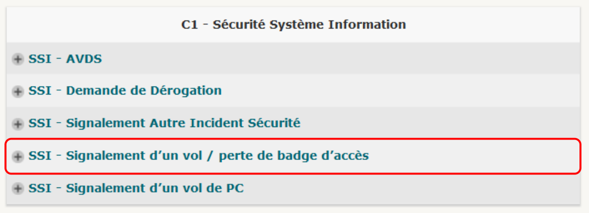
- ❑ I send an e-mail to securite@groupeastek.fr to report the theft, giving my contact details and the circumstances of the theft.

  ➔You will be called back by a member of the security team.

- ❑ I report the theft to the nearest police station.

I lost or had my badge stolen

- ❑ I report the event through https://helpdesk.groupeastek.com (only available in the agency or from outside through VPN)

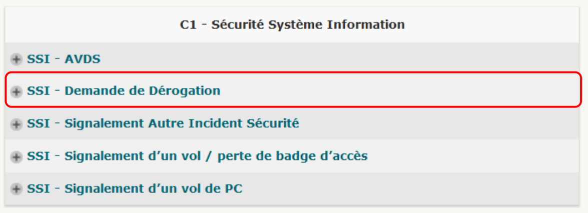


C1 - Sécurité Système Information

- ⊕ SSI - AVDS
- ⊕ SSI - Demande de Dérogation
- ⊕ SSI - Signalement Autre Incident Sécurité
- ⊕ SSI - Signalement d'un vol / perte de badge d'accès
- ⊕ SSI - Signalement d'un vol de PC

I need to derogate from the ISSP for operational constraints

- ❑ I fill in and sign the document specifying the request (To be downloaded here : *https://helpdesk.groupeastek.com/front/knowbaseitem.form.php?id=11*)
- ❑ I send my request through https://helpdesk.groupeastek.com



C1 - Sécurité Système Information

- ⊕ SSI - AVDS
- ⊕ SSI - Demande de Dérogation
- ⊕ SSI - Signalement Autre Incident Sécurité
- ⊕ SSI - Signalement d'un vol / perte de badge d'accès
- ⊕ SSI - Signalement d'un vol de PC

CONTACTS UTILES

Useful contacts

Email contacts

- **madsi@groupeastek.fr**
  For all IT requests or incident’s declaration
- **securite@groupeastek.fr**
  For all question or request relating to security

Le site Welcome

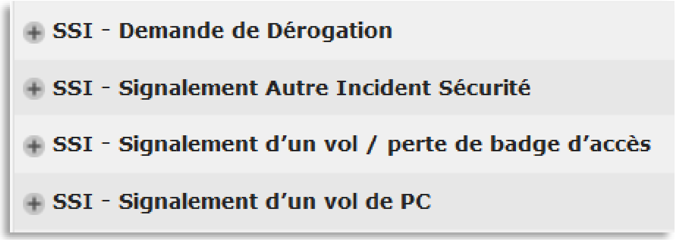
To access all management system documentation, including security guides and policies:

https://welcome.groupeastek.com

An online helpdesk to access all your requests through forms.

For all your online requests concerning IT and IS security:

https://helpdesk.groupeAstek.com (reachable through Intranet)



- SSI - Demande de Dérogation
- SSI - Signalement Autre Incident Sécurité
- SSI - Signalement d’un vol / perte de badge d’accès
- SSI - Signalement d’un vol de PC

THANK YOU FOR YOUR ATTENTION