

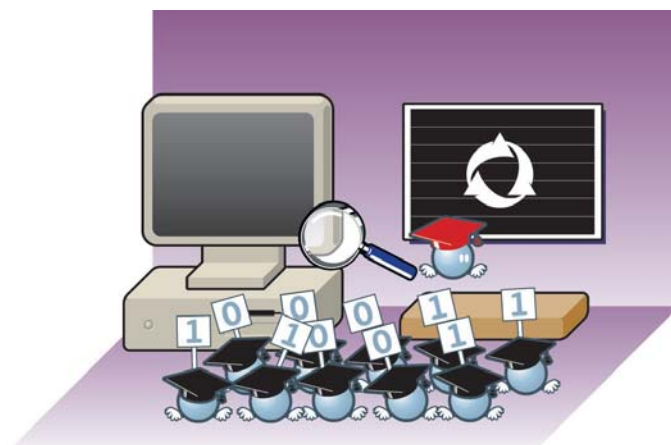
## Résumé

La formation et la sensibilisation à la sécurité des systèmes d'information et de communication forme un élément essentiel parmi les actions nécessaires pour que la sécurité devienne une réalité pour toute personne. La formation et la sensibilisation

peuvent s'expliquer par leurs différents buts d'apprentissage : connaissances de base, réflexes de protection, conduite à tenir. Ce document permet de comprendre et de mesurer toute l'importance de ce domaine.

## Table des matières

- 1 C'est quoi ? →
- 2 Qui est concerné ? →
- 3 Comment cela fonctionne-t-il ? →
- 4 Quel genre d'illustrations est utilisable lors des séances de sensibilisation ? →
- 5 Quelles recommandations peut-on suivre pour se protéger ? →



## 1 C'est quoi ?

**Formation et sensibilisation peuvent s'expliquer par leurs différents buts :**

- Donner aux utilisateurs, par exemple employés et management, les connaissances de base pour assurer la protection des informations dans les situations les plus courantes.
- Induire chez les utilisateurs des systèmes d'information et de communication, des réflexes de protection et les convaincre par rapport aux mesures de sécurité qui sont nécessaires, même si elles ont pour corollaire des contraintes et des inconvénients.
- Indiquer la conduite à tenir en cas de doute dans des situations particulières ainsi que les différentes procédures à suivre (par exemple, contacter des personnes spécifiques).

En l'absence de sensibilisation sur leur bien-fondé, les mesures de sécurité préconisées ne seront pas appliquées, par négligence ou manque de conviction, ou bien encore par refus d'en accepter les contraintes. Dans tous les cas, la formation et la sensibilisation sont un préalable à tout progrès dans le domaine de la sécurité.

## 2 Qui est concerné ?

Tous les citoyens, PME, et administrations confondus ayant des ressources ou informations avec de la valeur et qui sont exposés à différents types de menaces pouvant aller du vol et de la perte d'informations jusqu'à l'espionnage industriel.

## 3 Comment cela fonctionne-t-il ?

Le premier moyen de communication permettant de sensibiliser les utilisateurs, par exemple les employés, le management d'une organisation/entreprise, à travers des séances ou formations de sensibilisation.

Au-delà des séances de sensibilisation et de travail en groupes, qui sont souvent des préliminaires incontournables, la sensibilisation fait également appel à des moyens de communication qui rappellent aux utilisateurs la conduite à tenir pour protéger l'information.

Ces moyens de communication sont nombreux et doivent souvent être employés de manière complémentaire et innovante afin d'éviter également la banalisation de ceux-ci.

→ suite

Parmi les différents types de moyens peuvent être utilisés :

- La diffusion de notes internes, bulletins d'information, vidéos ou livrets de sécurité.
- L'utilisation de posters, tapis de souris et affiches.
- Des moyens techniques tels que des écrans de veille portant un message sécurité voire des fonds d'écran.

La volonté de sensibiliser les utilisateurs se traduit par un plan de sensibilisation continu, sur plusieurs années. Pour cela, il faudra prendre en compte plusieurs paramètres :

- Le bien-fondé des mesures de sécurité.
- L'attractivité et l'efficacité du message et du média utilisé.
- Des points permettant de mesurer l'efficacité du plan de sensibilisation.

4

## Quel genre d'illustrations est utilisable lors des séances de sensibilisation ?

Introduction	4
Internet and email	5
Internet routing	
Internet email	
Logins & passwords	8
Other security issues	10
Backup	
Physical security	
Security software	
Helpdesk contacts	14
Glossary & interesting sites	16
Conclusion	18
Helpful contacts	
Top 7 security rules	



### Pirates, hackers, ...

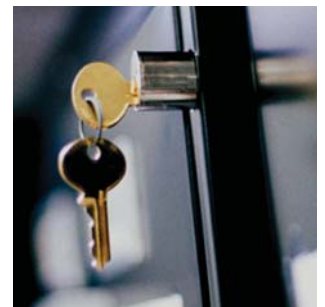


- Des personnes malintentionnées ayant comme but -
- De prendre la main sur votre machine ou le système d'information de la X afin de voler, modifier ou effacer des informations
- D'utiliser votre machine ou le système d'information de X afin d'attaquer une autre cible

L'ingénierie sociale est une technique de plus en plus courante même en Europe afin d'extraire des informations à des personnes uniquement à travers le téléphone

- le coup de téléphone de l'informaticien qui vous demande votre mot de passe
- « Bonjour je m'appelle Marc Dubois. Je fais partie de l'Institut ISO et nous faisons une enquête sur ... »

Si vous pensez avoir été victime d'ingénierie sociale, contactez un des RSSI. (cf. page Contact dans Chapitre 5 - Annexes)



5

## Quelles recommandations peut-on suivre pour se protéger ?

Afin de protéger l'investissement lors de la mise en place d'une campagne voire d'un plan de formation et sensibilisation, voici quelques recommandations :

- Impliquez et de coordonnez le plan avec les départements Ressources Humaines et Formations.
- Utilisez lors du plan de formation et sensibilisation des spécialistes en communication et sensibilisation afin de garantir l'efficacité du message à faire passer et surtout pour qu'il soit compris.

- Sensibilisez votre personnel aux aspects de sécurité dans leur vie privée, ceci peut faciliter et plus facilement justifier les besoins de protection des informations de l'organisation/entreprise.

CASES,

pour plus de sécurité dans l'utilisation des systèmes d'information électroniques. Une initiative européenne soutenue par l'Etat luxembourgeois

olas

OFFICE LUXEMBOURGEOIS  
D'ACCREDITATION ET DE  
SURVEILLANCE



LE GOUVERNEMENT  
DU GRAND-DUCHÉ DE LUXEMBOURG  
Ministère de l'Economie  
et du Commerce extérieur