



# Sensibilisation des Utilisateurs à la Sécurité Informatique

## SUSI 2017

PROJET SENSIBILISATION SPECIAL  
CODIR, SALARIES & UTILISATEURS

Hacking,  
Cyberattaque, Phishing,  
Ransomware, Social  
Engineering...



+33 685 965 972



[www.afsoftware.fr](http://www.afsoftware.fr)



Aix-en-Provence FRANCE



[afalck@afsoftware.fr](mailto:afalck@afsoftware.fr)

L'ensemble des collaborateurs doivent être sensibilisés, initiés, voire formés à la cyber-sécurité sans qu'il soit pour autant nécessaire d'en faire des experts du domaine

## **NO HACKING !!!**

"Acte de malveillance, piratage de données, utilisation abusive de droits ... La cyber-sécurité est une chaîne et sa solidité dépend de l'implication conjointe du service juridique, de la DSI et de la DRH" selon Jean-François Faye, directeur industriel chez Verlingue.

Le plus dur à convaincre n'est plus le directeur général, qui a compris ce que la responsabilité pénale et perte de valeur en cas d'attaques veulent dire, mais toutes les personnes ayant accès à INTERNET.

L'utilisateur est le maillon faible en sécurité de l'information. Les hackers le savent bien.

## **QUI EST AF SOFTWARE?**

Axel Falck, créateur d'AF Software est expert depuis plus de 18 ans en cyber-sécurité et spécialiste dans l'aide et le conseil aux entreprises. Agréé Cyberdéfense par le Ministère de la Défense Paris.

Notre objectif est de sensibiliser vos collaborateurs durant une journée pour mieux comprendre, analyser ce qu'est une cyberattaque et vous aider à mettre en place une politique de sécurité. Nous resterons en contact avec vous pour les menaces de demain.



# SENSIBILISATION A LA SECURITE DE L'INFORMATION

La session est basée sur une présentation Microsoft Powerpoint en français. Les quelques démonstrations seront faites sur un ordinateur.

Certains chapitres sont animés de vidéos explicatives et ludiques. En complément divers documents sont distribués durant la session.

~4 heures en fonction de l'interaction des stagiaires.

Maximum de 12 participants par session.

Cette journée de sensibilisation à la sécurité de l'information aborde le sujet sous deux aspects!

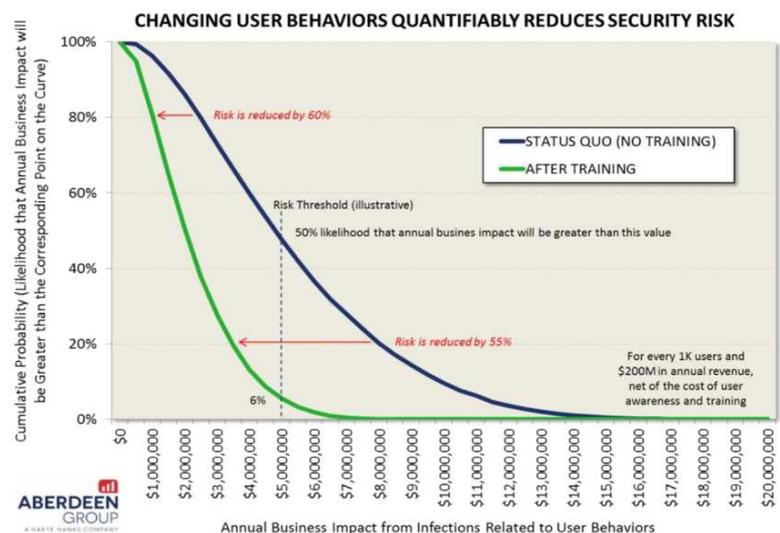
- technique et organisationnel

Le volet technique reste au niveau de la présentation des risques et des menaces pour l'entreprise au quotidien et le volet organisationnel s'attache à donner aux participants des bons réflexes et des bonnes pratiques en parallèle des éléments techniques présentés. Il s'agit donc d'impliquer les participants dans la sécurité du système d'information en étant acteur et non pas simple spectateur.

**Une session SUSI se déroule avec un maximum de 12 participants .**

**Un agenda sera défini entre les deux parties pour optimiser les sessions.**

**Les frais de transport et hébergement sont à votre charge.**



Source: Aberdeen Group, October 2014

Ci dessus une étude montrant la réduction de coûts et de risques avec de la sensibilisation



# THIS YEAR IN NUMBERS



En novembre 2016, Symantec estimait qu'un email sur 85 contenait un malware, qu'un email sur 2620 était une tentative de phishing (l'email vous invite à cliquer vers un faux site afin de voler vos identifiants, mots de passe, etc...) et que plus de la moitié des emails (54,3%) étaient non sollicités (spam).

En 2015, Symantec estimait que 429 millions de personnes dans le monde s'étaient faites voler des données personnelles, un chiffre en hausse de 23% par rapport à l'année précédente.

## INTERNET

CYBERATTAQUES, VOLS DE DONNÉES, SPAMS... LES CHIFFRES CLÉS

### La cybercriminalité en hausse en France

**13,7** millions de personnes touchées en France en 1 an

Faits les plus fréquents en France

Vol de mot de passe



**14%** des cas

Fraude à la carte bancaire



**10%**

Coût estimé (en 2015)

**2,88** milliards d'€  
soit 0,11% du PIB

### Dans le monde...

... coût de la cybercriminalité

**445** milliards de \$ en 2016

... vols de données personnelles

2014

**348** millions de personnes touchées

2015

**429** millions (+23%)

### Dans le monde, de plus en plus de malwares

Logiciels malveillants qui accèdent à l'appareil d'un utilisateur à son insu (logiciel espion, virus, cheval de Troie, rootkits, etc.)



**75%** des sites internet étaient vulnérables en 2015\*\*.

En novembre 2016

■ **1** email sur **85** contenait un malware.

■ **1** email sur **2620** était une tentative de phishing\*\*\*\*

■ **54,3%** des emails étaient du spam.

\*nouveaux malwares et variantes découverts. \*\*failles de sécurité connues et non corrigées. \*\*\*l'email vous invite à cliquer vers un faux site afin de voler vos identifiants, etc. Sources: Symantec, Avast, Norton, World Economic Forum, CNBC.

VISACTU

# Global Review



**A qui le tour ?** Un million de comptes Yahoo piratés, tout comme les banques centrales de Russie et du Bangladesh, Sony Pictures, Tesco mais aussi TV5 monde, Areva, Airbus, Schneider Electric, JP Morgan, New York Times... et Orange. Tous furent victimes de cyberattaques, la question n'est plus "est ce que je vais être attaqué" mais **"quand et suis je prêt ?"**

