Formation Cyber Sécurité

Pour tous collaborateurs de l’entreprise

Sommaire

Pourquoi la sécurité de l'information est-elle stratégique pour votre entreprise ?

La perte, le vol ou l'altération d'informations affaiblissent l'entreprise

Pourquoi former vos collaborateurs à la cybersécurité de l'information ?

De nouveaux usages et modes de travail à risques pour la sécurité de l'information

Le point le plus vulnérable des systèmes d'information est souvent l'humain

Formation Cyber Sécurité pour les collaborateurs

Modalités et objectifs de la formation

Programme de formation

Comment se passe une formation chez Resource Lab ?

Les différentes étapes de la formation

Pourquoi la sécurité de l’information est-elle stratégique pour votre entreprise ?

La perte, le vol ou l'altération d'informations affaiblissent l'entreprise

CHIFFRES CLÉS* 2014

Le « hacking » de données dans le monde n'est plus un mythe. Le nombre d'incidents est en nette progression.

- **42,8 millions** d'incidents
  En hausse de 48% par rapport à 2013
- **2,7 millions** coût annuel des incidents
  En hausse de 34% par rapport à 2013
- **20 millions** coût des pertes
  Chiffre pratiquement multiplié par 2

PRINCIPALES ATTAQUES - TOP 3

- Virus
- Spam
- Phishing

CONSÉQUENCES - TOP 3

- Pertes financières
- Atteinte à la réputation et à l'image
- Baisse de performance

En Europe, **les incidents de cybersécurité** ont progressé de 41 % en 2014.
Ceux-ci ne concernent pas uniquement les grandes entreprises, les PME et TPE sont également ciblées.

Les cyberattaques en tout genre donnant lieu à la **perte d'informations critiques** affaiblissent l'entreprise (espionnage industriel, pannes, ralentissement de l'activité, perte de contrats et de marchés…) et peuvent la paralyser jusqu'à provoquer la fermeture pour les plus vulnérables d'entres elles.

Ceci est d'autant plus critique que **les collaborateurs** utilisateurs du système d'information souvent visés par ces attaques représentent **la première faille de sécurité.**

Il est urgent de sensibiliser les collaborateurs aux enjeux de la cybersécurité et aux bonnes pratiques pour éviter les pièges faciles.

Source : Etude mondiale de PWC, CIO et CSO - 2014

Pourquoi former vos collaborateurs à la cybersécurité de l’information ?

De nouveaux usages et modes de travail à risque pour la sécurité de l'information

Des salariés de plus en plus connectés

Utilisation de l'équipement personnel au travail

Home office

Co-working et espaces de travail modernes

Ces nouveaux usages comme le développement des dispositifs mobiles ou le nomadisme des collaborateurs sont particulièrement exposés aux pertes de données

Le point le plus vulnérable des systèmes d'information est souvent l'humain

82% des français n'ont jamais entendu parler des plus grandes failles de sécurité*

62% des français déclarent qu'ils n'ont toujours pas de mots de passe différents pour chaque site ou chaque application*

47% des français ne changent pas de mots de passe suite à la révélation des failles de sécurité *

*Source : Etude CISCO- 2014

Ces comportements à risques ont des conséquences sur la sécurité de l'information en entreprise. D'autant plus que l'**ingénierie sociale** qui consiste à récupérer des codes d'accès auprès des collaborateurs est de plus en plus fréquente.

Destinée aux collaborateurs, notre formation Cybersécurité est centrée sur la menace afin de donner aux utilisateurs internes à l'entreprise le moyen de s'en prémunir et d'adopter les réflexes pour réduire les risques.

Bénéfices de la formation : répondre à des enjeux de management et de business :

- Valorisation des équipes
- Employabilité
- Gage de confiance pour les clients
- Conformité aux appels d'offres
- Sûreté des personnes et des biens
- Protection commerciale
- Protection des actifs
- Préservation de l'investissement Intelligence Economique

Formation Cyber Sécurité pour les collaborateurs

Modalités et objectifs de la formation

Description

Ce stage d'une journée **sensibilise aux dangers** des cyberattaques pour limiter les comportements à risques et **présente des techniques informatiques** pour intégrer des réflexes d'autodéfense vis-à-vis de ces attaques :

Prévention • Détection • Réaction

Le stage doit permettre des échanges de vues et d'expériences.

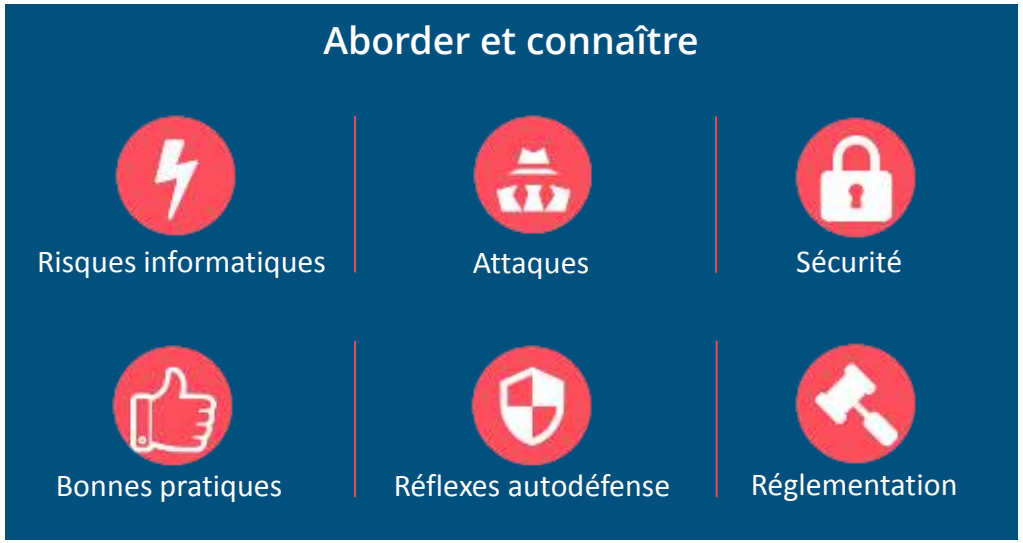
PRÉREQUIS

Niveau du stage : Base
Public : Collaborateurs : fonctions support, office manager, commerciaux…

ANIMATEUR

Jean DOUAT : Ingénieur, expert cyberdéfense, Référent Cyber à Eurosaé. Précédemment chef du service de la sécurité de défense et des systèmes d'information de la DGA

Objectifs



Les Plus

Exemples concrets choisis dans les domaines étatiques ou industriels.
Mises en situation à travers divers scénarii.
Formateurs expérimentés et référents dans le domaine.

Programme de formation

L'environnement

- Internet
- Le réseau d'entreprise
- Le poste utilisateur

Les attaques

- Les principaux scénarios
- Les objectifs poursuivis
- Les conséquences

Les mises en situation

- Scénarios de base
- Scénarios à risques
- Identifier les problèmes

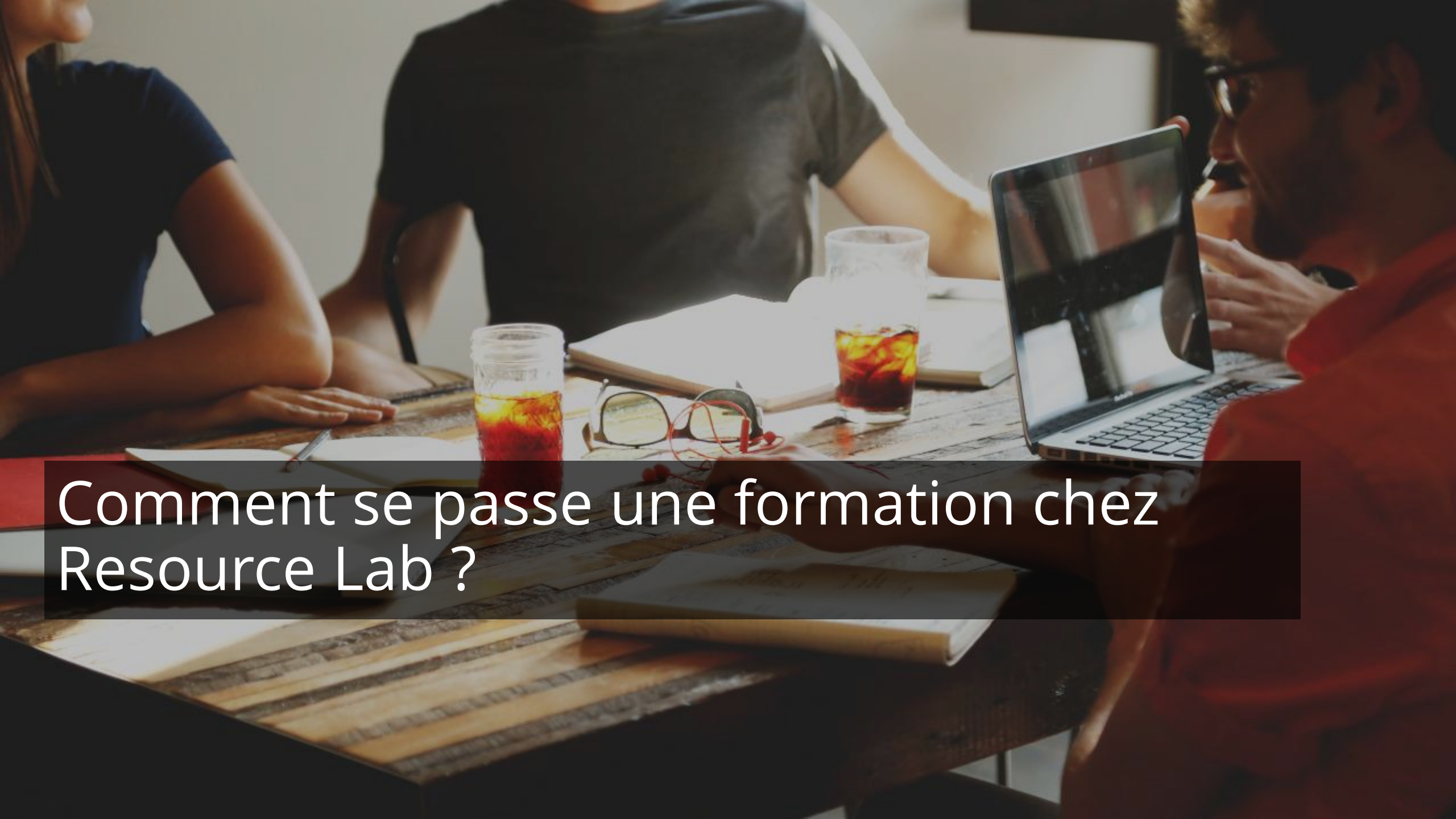
Les moyens de limiter les risques

- Le poste de travail
- La messagerie
- Les téléchargements
- Les clés USB
- Les imprimantes

La sécurité

- L'organisation sécurité de l'entreprise
- Le RSSI
- Les collaborateurs

Conclusion



Comment se passe une formation chez Resource Lab ?

Les différentes étapes de la formation

Avant la formation

Inscription et constitution des dossiers de formation, notamment les documents nécessaires à une prise en charge par une OPCA.

7 jours avant la formation, les participants recevront une invitation par mail rappelant l'intitulé du stage et indiquant le lieu et les horaires de la session.

Le jour J

Accueil sur le lieu de la formation.
L'intervenant indiquera aux participants les informations nécessaires au bon déroulement du stage.

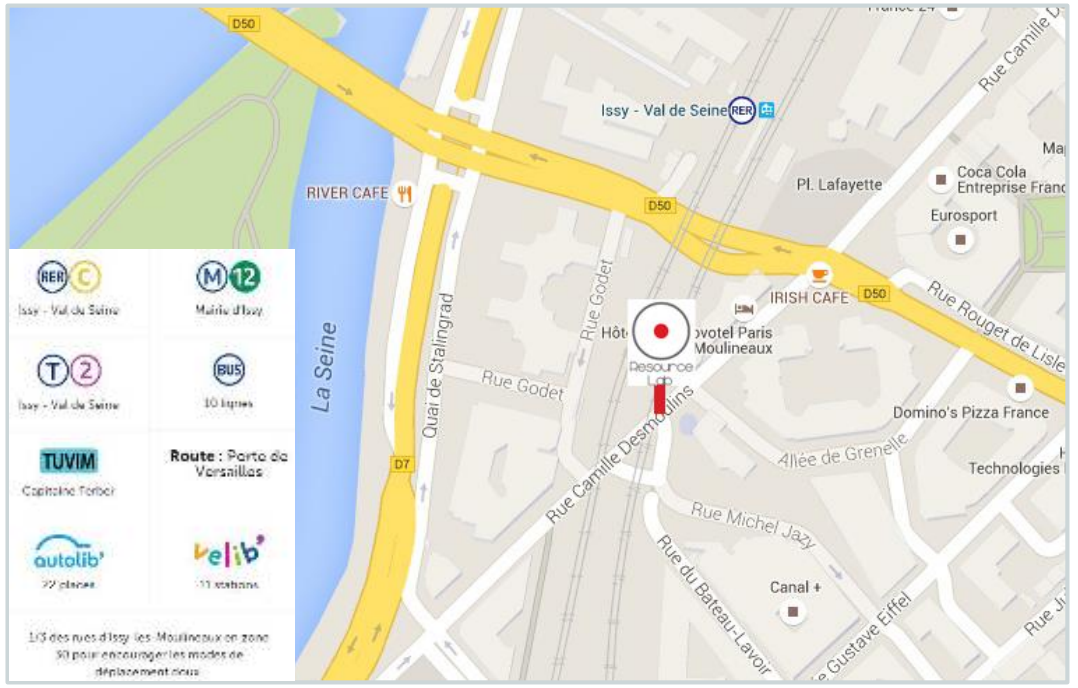
Les horaires : 9h30 – 17h30 incluant une pause repas.
Le formateur peut aménager la journée en fonction de son programme, et dans la mesure du possible, en fonction des contraintes et spécificités du groupe.

Les jours suivants

Les jours suivant la formation nous transmettrons :

- Une attestation nominative
- Les documents nécessaires si une demande de prise en charge a été effectuée.
- Un questionnaire d'évaluation en ligne afin de nous permettre de mieux répondre à vos besoins et d'améliorer notre prestation.

Nous contacter



Resource Lab

Immeuble Nextdoor
43, rue Camille Desmoulins
92130 ISSY LES MOULINEAUX

Contact formation

Gladys JACQUES
Directrice des Projets et Opérations
06 60 40 61 76

Suivez-nous sur le Web !

www resourcelab.fr

@ResourceLab