Formations E-learning

certilience
EXPERTS EN SÉCURITÉ INFORMATIQUE

3 allée des Séquoias - 69760 LIMONEST
04 28 29 72 50 - contact@certilience.fr

www.certilience.fr

Nos formations

Les formations e-learning à lire

SEN-L1	10 minutes	*La messagerie d'entreprise*
SEN-L2	7 minutes	*Les Réseaux Sociaux*
SEN-L3	5 minutes	*Le bon comportement sur le poste de travail*
SEN-L4	5 minutes	*Surfer sur le web en toute sécurité*
SEN-L5	5 minutes	*Le bon comportement sur Smartphone*
SEN-L6	5 minutes	*Construire les mots de passe*

Les formations e-learning sonorisées

SEN-S1	8 minutes	*Ce que veulent les pirates*
SEN-S2	10 minutes	*Le phishing*
SEN-S3	10 minutes	*Les mots de passe*
SEN-S4	5 minutes	*L'ingénierie sociale, ou phishing ciblé*
SEN-S5	5 minutes	*Les clés USB*
SEN-S6	5 minutes	*Les hotSpots Wifi*
SEN-S7	5 minutes	*De l'importance de faire les mises à jour*
SEN-S8	6 minutes	*Le RGPD : quel impact pour l'entreprise et ses salariés*
SEN-S9	5 minutes	*La charte informatique*

SEN-L1

La messagerie d'entreprise

Niveau	Prérequis	Lieu	Durée
Utilisateurs du SI	Pas de prérequis	À distance	10 minutes

Le messagerie est aujourd'hui le **premier vecteur d'infection dans une entreprise**. Il est donc important de former les employés sur ce point.

De nombreux remparts sont présents dans une entreprise (antivirus / anti-spam / pares-feux) mais **l'utilisateur est la dernière et la meilleure défense du système.** Sa capacité d'analyse, son esprit critique et son jugement seront plus efficaces qu'un système de protection et pourront faire toute la différence en cas d'attaque ou de phishing.

OBJECTIFS DE LA FORMATION

- comprendre le fonctionnement de la messagerie
- connaitre les différents types d'attaques
- identifier les emails dangereux
- acquérir les bons réflexes

PROGRAMME

1/. Présentation du fonctionnement de la messagerie

Nous présenterons ici le fonctionnement d'une chaine de messagerie standard dans une entreprise.

2/. Exemples d'attaques sur la messagerie et présentation des scénarios

Présentation des différentes techniques d'attaques utilisées par des personnes malveillantes : mail de phishing, pièces jointes pièges, spear-phishing, etc., pour récupérer votre compte de messagerie.

Il devient ensuite possible d'usurper votre identité ou récupérer des données sensibles dans votre boite.

3/. Techniques d'identifications de emails malveillants

Dans cette partie, nous vous enseignons des méthodes pour identifier des emails suspects et vous permettre d'évaluer rapidement le risque associé à un email avant d'utiliser le lien ou d'ouvrir la pièce jointe.

4/. Évaluation

Pour valider la bonne compréhension de cette formation, nous terminons par un Quiz.

SEN-L2

Les Réseaux Sociaux

Niveau	Prérequis	Lieu	Durée
Utilisateurs du SI	Pas de prérequis	À distance	7 minutes

Les réseaux sociaux peuvent être utilisés aussi bien dans un cadre personnel que professionnel. Mais ils regorgent d'informations qui, utilisées par les cyberpirates, peuvent vous **nuire personnellement** mais peuvent également **nuire à votre entreprise**.

Cette formation vous présente les différentes utilisations des réseaux sociaux et les risques induits à son exploitation.

Comprendre leur fonctionnement et les dangers qui s'y cachent vous permettront de **mieux vous protéger.**

OBJECTIFS DE LA FORMATION

- comprendre le fonctionnement des réseaux sociaux
- faire le point sur les avantages et les risques
- apprendre à gérer ses données personnelles
- différencier usage perso et usage professionnel

PROGRAMME

1/. Introduction

Présentation des réseaux sociaux :

- les différentes utilités et utilisations,
- les différents types de réseaux sociaux.

2/. Les risques

Une mauvaise utilisation des réseaux sociaux pourra avoir des conséquences sur l'activité et même sur la sécurité de l'entreprise.

3/. Usage professionnel / usage personnel

Quelles informations sur quels réseaux ; gérer ses données personnelles ; les sanctions pénales ; apprendre à ne pas mettre l'entreprise en danger.

4/. Apprendre les bons réflexes

Exemples et conseils pour changer son comportement sur les réseaux sociaux : se protéger et protéger son entreprise.

5/. Évaluation

Pour valider la bonne compréhension de cette formation, nous terminons par un Quiz.

SEN-L3

Le bon comportement sur le poste de travail

Niveau	Prérequis	Lieu	Durée
Utilisateurs du SI	Pas de prérequis	À distance	5 minutes

Les attaques informatiques récentes montrent que **les pirates s'intéressent en premier lieu aux utilisateurs et à leurs terminaux** plutôt qu'à l'infrastructure d'entreprise.

Leurs buts sont variés : du simple vol de données personnelles à l'utilisation de votre terminal, ils peuvent aller jusqu'à **bloquer tout le réseau de l'entreprise et demander une rançon**.

Dans tous les cas, **ils s'appuient sur le comportement des utilisateurs**. Cette formation vous permet d'acquérir un comportement sain afin de limiter les risques d'intrusions.

OBJECTIFS DE LA FORMATION

- comprendre quels sont les risques réels
- être capable de les identifier
- acquérir les réflexes nécessaires à un bon comportement

PROGRAMME

1/. Les risques
Présentation des dangers liés à l'utilisation d'un ordinateur et de la valeur que votre poste peut avoir aux yeux d'un pirate.

2/. Les vecteurs d'attaques
Présentation des différentes méthodes et vecteurs utilisés par les pirates pour accéder à votre poste.

3/. Les conséquences d'une contamination
Présentations des conséquences, du niveau du poste de travail à l'échelle de l'entreprise.

4/. Les bonnes pratiques
Explications simples des bonnes pratiques et des réflexes à avoir dans votre utilisation quotidienne de votre poste de travail.

5/. Évaluation
Pour valider la bonne compréhension de cette formation, nous terminons par un Quiz.

SEN-L4

Surfer sur le web en toute sécurité

Niveau	Prérequis	Lieu	Durée
Utilisateurs du SI	Pas de prérequis	À distance	5 minutes

Surfer sur le web est une activité quotidienne qui nécessite un peu de prudence.

Une partie de la sécurité peut être assurée par des barrières techniques, mais **la prise de conscience et le comportement des utilisateurs sont primordiaux**.

Cette formation vous présente **les différentes menaces** impliquées par l'utilisation d'internet et **les réflexes nécessaires à un surf en toute sécurité** pour l'utilisateur comme pour l'entreprise.

OBJECTIFS DE LA FORMATION

- identifier les dangers
- prendre conscience des risques encourus
- connaitre ses droits et ses obligations
- apprendre les bonnes pratiques

PROGRAMME

1/. Introduction

Présentation de l'actualité concernant le comportement des utilisateurs sur internet.

2/. Les dangers du monde virtuel

Les conséquences d'un comportement inapproprié, pour l'individu et pour l'entreprise.

Quels sont les risques suite à du surf sans précaution.

3/. Internet et la loi

Quelles sont les infractions ; l'utilisation de mes données personnelles ; l'usurpation de mon identité et de mes informations.

Internet et l'entreprise.

4/. Conseils et solutions

Présentation de solutions techniques.
Conseils pour acquérir de bonnes pratiques et reconnaitre les arnaques.

5/. Évaluation

Pour valider la bonne compréhension de cette formation, nous terminons par un Quiz.

SEN-L5

Le bon comportement sur Smartphone

Niveau	Prérequis	Lieu	Durée
Utilisateurs du SI	Pas de prérequis	À distance	5 minutes

Peut-on imaginer une journée de travail sans Smartphone ?

L'utilisation de cet outil n'est pourtant pas sans risque. Cette formation fait le point sur **son fonctionnement** et sur **les dangers sous-jacents** à son utilisation. Le bon comportement sur smartphone permet **d'éviter la contamination du téléphone mais également de toute l'entreprise !**

OBJECTIFS DE LA FORMATION

- identifier les dangers
- prendre conscience des risques encourus
- apprendre les bonnes pratiques pour se protéger et protéger son entreprise

PROGRAMME

1/. Introduction

Présentation de faits d'actualité : les cyberpirates et les smartphones.

2/. Les risques

Ce que cherchent les pirates et jusqu'où ils peuvent aller ;
Les risques pour l'individu et pour l'entreprise.

3/. Conseils et bonnes pratiques

Les gestes simples pour limiter les risques,
Les points à surveiller,
Acquérir les bonnes pratiques et les bons réflexes.

4/. Évaluation

Pour valider la bonne compréhension de cette formation, nous terminons par un Quiz.

SEN-L6

Construire les mots de passe

Niveau	Prérequis	Lieu	Durée
Utilisateurs du SI	Pas de prérequis	À distance	5 minutes

Le mot de passe est aujourd'hui une clef d'entrée sur votre SI !

Cette formation vous **présente les risques associés à un mot de passe faible**, mais vous donne également des techniques ou des conseils pour **construire et stocker** un mot de passe.

Comprendre l'intérêt d'un mot de passe et identifier les risques n'auront plus de secret pour vous.

OBJECTIFS DE LA FORMATION

- comprendre l'importance du mot de passe
- les dangers d'un mot de passe faible
- acquérir les méthodes pour construire un mot de passe
- apprendre à le stocker en toute sécurité

PROGRAMME

1/. Introduction
Qu'est-ce qu'un « bon » mot de passe.
Présentation de l'actualité concernant des incidents de sécurité liés à des mots de passe.

2/. Présentation des erreurs
Présentation des erreurs classiques de construction d'un mot de passe : suite logique de chiffres ou de nombres, utilisateur du TOP25 des mauvais mots de passe (password / azerty /etc.).

3/. Méthode de construction d'un mot de passe
Nos experts vous donnent des conseils et des astuces pour construire un mot de passe ou comment utiliser des d'outils adaptés.

4/. Comment conserver un mot de passe
Comment stocker un mot de passe de manière sécurisée ;
le conserver dans le temps et maintenir un bon niveau de sécurité.

5/. Évaluation
Pour valider la bonne compréhension de cette formation, nous terminons par un Quiz.

SEN-S1

Ce que veulent les pirates

Niveau	Prérequis	Lieu	Durée
Utilisateurs du SI	Pas de prérequis	À distance	8 minutes

Le but de cette formation est de vous montrer **les techniques qu'utilisent les pirates** pour compromettre vos PCs et vos données d'entreprise, et pourquoi cela concerne **chaque collaborateur de l'entreprise.**

La sécurité informatique est accessible à tous, et **chacun participe à son niveau** à la sécurité de l'entreprise.

Voici ce qui intéresse réellement les pirates et comment se protéger de leurs attaques.

Cette formation est **sonorisée**.

OBJECTIFS DE LA FORMATION

- comprendre le rôle et le potentiel de sécurisation des collaborateurs
- comprendre la valeur des données et de l'infrastructure pour le pirate
- comprendre la démarche des pirates
- acquérir les bons réflexes

PROGRAMME

1/. Introduction

Différencier la valeur des données à mes yeux / aux yeux des pirates.

Quelles sont les motivations des pirates.

2/. Les risques

Quelles sont les conséquences d'une attaque de pirate : sur mes données / sur mon matériel / pour l'entreprise.

3/. Ce que le pirate peut faire de mon ordinateur

Quelles sont les différentes façons d'exploiter un ordinateur pour un pirate.

4/. Évaluation

Pour valider la bonne compréhension de cette formation, nous terminons par un Quiz.

SEN-S2

Le phishing

Niveau	Prérequis	Lieu	Durée
Utilisateurs du SI	Pas de prérequis	À distance	10 minutes

Les mails de phishing (ou hameçonnage) interviennent dans **73 % des attaques.** Savoir reconnaitre un mail de phishing permet donc d'**éviter de tomber dans les pièges lancés par les pirates.**

Cette formation décortique **les techniques utilisées par les pirates** pour déjouer l'attention des utilisateurs.

Cette formation est **sonorisée**.

OBJECTIFS DE LA FORMATION

- savoir ce que les pirates recherchent
- comprendre leur démarche et leurs techniques
- acquérir les bons réflexes pour se protéger
- reconnaitre les tentatives de phishing

PROGRAMME

1/. Introduction
La valeur du mot de passe et des identifications ; pourquoi les pirates les recherchent.

2/. Le fonctionnement du phishing
Les étapes et les risques associés.
Comment le pirate vous vole vos données à partir d'un mail.
Les leviers psychologiques.

3/. Exemples « classiques » de phishing
Testez vos réflexes. Saurez-vous reconnaitre un mail ou un site de phishing ?

4/. Les dangers et les points à surveiller
Le format des pièces jointes, les extensions de fichier, les liens.
Comment se protéger : les points à contrôler, acquérir les bons réflexes et le bon comportement.

5/. Évaluation
Pour valider la bonne compréhension de cette formation, nous terminons par un Quiz.

SEN-S3

Les mots de passe

Niveau	Prérequis	Lieu	Durée
Utilisateurs du SI	Pas de prérequis	À distance	10 minutes

Le mot de passe est aujourd'hui une clef d'entrée sur votre SI !

Cette formation vous permet de **comprendre l'intérêt d'un bon mot de passe** et **d'identifier les risques** associés à un mot de passe faible.

Apprenez ensuite à **construire et stocker** un mot de passe fort grâce aux techniques et conseils de nos experts.

Cette formation est **sonorisée**.

OBJECTIFS DE LA FORMATION

- comprendre l'importance du mot de passe
- les dangers d'un mot de passe faible
- acquérir les méthodes pour construire un mot de passe
- apprendre à le stocker en toute sécurité

PROGRAMME

1/. Introduction
Les nombreuses utilisations des mots de passe ;
ce que recherchent les pirates.

2/. L'utilisation des identifiants et des mots de passe
Informations publiques / privées : les informations que l'on peut divulguer / les informations confidentielles.
Conseils et bons réflexes sur l'utilisation des mots de passe.

3/. Qu'est-ce qu'un « bon » mot de passe
Les différents critères et les règles « classiques » ;
Exemples de mots de passe : sont-ils assez forts ?
Comment fonctionnent les pirates.

4/. Créer et stocker un mot de passe
Méthodes et outils pour créer et sécuriser ses mots de passe.

5/. Évaluation
Pour valider la bonne compréhension de cette formation, nous terminons par un Quiz.

SEN-S4

L'ingénierie sociale, ou phishing ciblé

Niveau	Prérequis	Lieu	Durée
Utilisateurs du SI	Pas de prérequis	À distance	5 minutes

L'ingénierie sociale est un procédé par lequel le pirate vise **une personne** ou **une entreprise en particulier**, et il tente de manipuler sa victime par un contact direct.

Cette formation vous explique les différentes étapes et les processus utilisés par les pirates pour vous soutirer des informations, la manière dont elles sont utilisées, et la finalité visée.

Cette formation est **sonorisée**.

OBJECTIFS DE LA FORMATION

- savoir ce que les pirates recherchent
- comprendre leur démarche et leurs techniques
- acquérir les bons réflexes pour se protéger
- reconnaitre les tentatives de phishing

PROGRAMME

1/. Introduction
L'ingénierie sociale, une attaque par phishing ciblé.

2/. Le fonctionnement du phishing
La démarche des pirates et les scénarios mis en place.
Le type d'information recherchée.
Comment le pirate vous convainc de lui donner les informations qu'il recherche.

3/. Exemples de l'actualité
Cas concret d'entreprises qui ont subi des attaques.

4/. Comment se protéger dans les lieux publics
Toutes les informations sont bonnes à prendre pour les pirates…
Apprendre à changer ses habitudes dans les lieux publics afin de préserver ses informations sensibles.

5/. Évaluation
Pour valider la bonne compréhension de cette formation, nous terminons par un Quiz.

SEN-S5

Les clés USB

Niveau	Prérequis	Lieu	Durée
Utilisateurs du SI	Pas de prérequis	À distance	5 minutes

Les clés USB sont des médias amovibles très pratiques pour transporter des fichiers. Mais quels sont **les risques liés à ce support** ?

Cette formation met en lumière les dangers liés à ce support et vous apprend **les bons gestes** pour limiter les risques. Comment utiliser les clés USB en toute tranquillité.

Cette formation est **sonorisée**.

OBJECTIFS DE LA FORMATION

- quels sont les risques lorsqu'on utilise une clé USB
- les données et le stockage
- acquérir les bons réflexes pour se protéger

PROGRAMME

1/. Introduction
Utilisation des clés USB.

2/. Les risques
Quelles données stocker sur une clé,
quels réflexes à adopter.

3/. Les dangers
Les différents types de virus et d'attaques transmises via clés USB.
Quelles conséquences pour mon ordinateur / pour mon entreprise.

4/. Exemple de l'actualité
Stuxnet, histoire d'un virus qui se transforme en arme de guerre.
Ce qu'on trouve sur internet.

5/. Évaluation
Pour valider la bonne compréhension de cette formation, nous terminons par un Quiz.

SEN-S6

Les hotSpots Wifi

Niveau	Prérequis	Lieu	Durée
Utilisateurs du SI	Pas de prérequis	À distance	5 minutes

Lorsque vous vous connectez à **internet dans un café ou un lieu public**, la connexion WiFi est-elle vraiment sécurisée ? Quelqu'un pourrait-il être en train d'intercepter les données que vous partagez ?

Cette formation met en **lumière les dangers liés à l'utilisation de ces connexions publiques** et vous apprend les bons gestes pour limiter les risques.

Cette formation est **sonorisée**.

OBJECTIFS DE LA FORMATION

- connaitre les risques liés à l'utilisation d'une connexion publique
- comprendre ce que recherchent les pirates et par quels moyens
- acquérir les bons réflexes pour naviguer en toute sécurité

PROGRAMME

1/. Introduction
Les points d'accès publics.

2/. La bonne attitude sur les lieux publics
Dans un restaurant, un hôtel ou un train, quel comportement adopter.

3/. Les données personnelles
Quelles informations puis-je faire transiter lorsque j'utilise un hotSpot Wifi.

4/. La connexion automatique
Comment fonctionne-t-elle ?
Quels sont les avantages et les risques à activer cette option ?

5/. Évaluation
Pour valider la bonne compréhension de cette formation, nous terminons par un Quiz.

SEN-S7

De l'importance de faire les mises à jour

Niveau	Prérequis	Lieu	Durée
Utilisateurs du SI	Pas de prérequis	À distance	5 minutes

Vous avez certainement déjà vu apparaitre sur votre écran un message vous indiquant qu'une mise à jour est en cours d'installation.

Cette formation vous explique **pourquoi il est important de faire les mises à jour** des logiciels, particulièrement des systèmes d'exploitation. Elle vous montre aussi **les risques encourus** si vous ne suivez pas ces mises à jour.

Cette formation est **sonorisée**.

OBJECTIFS DE LA FORMATION

- connaitre les risques liés à la non mise à jour des applications, logiciels et systèmes
- comprendre les failles utilisées par les pirates et ce qu'ils peuvent en faire
- acquérir les bons réflexes

PROGRAMME

1/. Introduction
Le fonctionnement de Windows.

2/. Les risques et les vulnérabilités
Quelles failles utilisent les pirates.

3/. Les smartphones
Les risques liés aux smartphones.

4/. Actualité
L'exemple de Wannacry ;
D'où venait ce virus, son fonctionnement, les coûts et les dégâts dans le monde entier.

5/. Évaluation
Pour valider la bonne compréhension de cette formation, nous terminons par un Quiz.

SEN-S8

Le RGPD : quel impact pour l'entreprise et ses salariés

Niveau	Prérequis	Lieu	Durée
Utilisateurs du SI	Pas de prérequis	À distance	6 minutes

Le RGPD, ou Règlement Général de Protection des Données, a été mis en place par l'Europe pour **forcer les sites à sécuriser les données** des utilisateurs.

Cette formation fait le point sur le **processus de traitement des données personnelles** et sur **ce qu'il implique** pour les entreprises et pour les utilisateurs.

Cette formation est **sonorisée**.

OBJECTIFS DE LA FORMATION

- connaitre les risques liés à la non mise à jour des applications, logiciels et systèmes
- comprendre les failles utilisées par les pirates et ce qu'ils peuvent en faire
- acquérir les bons réflexes

PROGRAMME

1/. Introduction
Définition et explication du principe de fonctionnement du RGPD.

2/. Les sanctions
Ce que prévoit le règlement en cas de manquement.

3/. Exemples de l'actualité
Ce qui s'est passé et les sanctions
Bilan des amendes depuis la mise en application du règlement.

4/. Les implications
Ce qui change pour les entreprises ;
Ce qui change pour les utilisateurs.

5/. Évaluation
Pour valider la bonne compréhension de cette formation, nous terminons par un Quiz.

SEN-S9

La charte informatique

Niveau	Prérequis	Lieu	Durée
Utilisateurs du SI	Pas de prérequis	À distance	5 minutes

Quel est **le rôle de la charte informatique** en entreprise ?

Cette formation met en avant **les points importants** de la charte informatique et **ce qu'elle implique** pour les entreprises aussi bien que pour les collaborateurs.

Cette formation est **sonorisée**.

OBJECTIFS DE LA FORMATION

- comprendre à quoi sert une charte informatique
- comprendre ses avantages, pour l'entreprise comme pour les utilisateurs
- savoir analyser son contenu

PROGRAMME

1/. Introduction
Définition, rôle et règles d'utilisation de la charte informatique.

2/. Le contenu
Quels sont les principaux thèmes abordés dans une charte informatique.

3/. Le point sur l'utilisation du système d'information de l'entreprise
Ce que le salarié peut / ne peut pas faire avec les ressources de l'entreprise.

4/. Évaluation
Pour valider la bonne compréhension de cette formation, nous terminons par un Quiz.

Conférences et Ateliers

certilience
EXPERTS EN SÉCURITÉ INFORMATIQUE

3 allée des Séquoias - 69760 LIMONEST
04 28 29 72 50 - contact@certilience.fr

www.certilience.fr

Nos formations

Les conférences

SEN02	1h45 à 2h	*Je participe à l'amélioration du niveau de sécurité de mon entreprise*

Les ateliers

SEN-AT1	1h45 à 2h	*Les Applis malveillantes*
SEN-AT2	1h45 à 2h	*Les Cyber-Risques*
SEN-AT3	1h45 à 2h	*Les Mots de passe*
SEN-AT4	1h45 à 2h	*Les Clés USB*

SEN02

Conférence : Je participe à l'amélioration du niveau de sécurité de mon entreprise

Niveau	Prérequis	Lieu	Durée
Utilisateurs du SI	Pas de prérequis	Dans vos locaux	1h45 à 2h

30% des incidents de sécurité sont attribuables à l'erreur humaine.

Les conséquences d'une cyberattaque sont toujours impactantes pour votre entreprise (pertes financières, arrêt de production, déclin de l'image de marque, amendes à payer, etc.). **Pourtant, se protéger de ces attaques est à la portée de chacun !**

La sensibilisation des salariés, c'est **l'apprentissage des bonnes pratiques** sur l'utilisation du système d'information de l'entreprise. **Chacun devient acteur de la sécurité de l'entreprise.**

OBJECTIFS DE LA FORMATION

- démystifier les risques informatiques pour les salariés
- vulgariser les attaques sur la messagerie (mail de phishing, mail piégé) et les attaques sur certains médias USB
- présenter les bonnes pratiques pour une utilisation professionnelle et personnelle

PROGRAMME

Déroulement :

- en session participative : jusqu'à 25 personnes
- en mode « amphithéâtre : illimité

1/. Entrez dans la tête d'un pirate
Cas d'utilisations frauduleuses du système d'information et pourquoi un attaquant est intéressé par votre poste ou vos comptes.

2/. Le phishing
Les étapes d'un phishing et exemples de scénarios ; les points vigilances.

3/. Les mots de passe
Principes du mot de passe ; les attaques et des bonnes pratiques.

4/. L'ingénierie sociale
Principe et démonstration des méthodes utilisées.

5/. Les dangers des clés USB
Fonctionnement et explication sur le détournement possible de ces médias.

6/. Les risques du réseau Wifi
Principe et démonstration des méthodes utilisées.

7/. Les mises à jour
L'utilité des mises à jour ; quels sont les risques à ne pas les faire.

8/. Le RGDP pour votre entreprise et vos salariés
Les bonnes pratiques concernant les données manipulées.

9/. La charte informatique
Présentation de votre charte informatique et d'illustration de certains points.

SEN-AT1

Atelier : Les Applis malveillantes

Niveau	Prérequis	Lieu	Durée
Utilisateurs du SI	Pas de prérequis	Dans vos locaux	1h45 à 2h

30 % des incidents de sécurité en entreprise sont attribuables à l'erreur humaine.

Grâce à des **démonstrations réalisées en direct** par un expert, nos ateliers font **prendre conscience** des risques réels aux participants. Notre expert explique les risques liés à la sécurité informatique, et les sensibilise à l'importance de cet apprentissage.

Ces ateliers interactifs permettent **l'apprentissage des bonnes pratiques** et des connaissances nécessaires à un comportement sain.

OBJECTIFS DE LA FORMATION

- comprendre les risques liés à l'utilisation d'applis
- comprendre ce qui intéresse les pirates et comment ils procèdent
- adopter les bons gestes dans l'utilisation d'applis pour limiter les risques
- pouvoir interagir directement avec un expert pour personnaliser les informations reçues

PROGRAMME

Déroulement :

- en session participative : jusqu'à 25 personnes

1/. Démonstration :
utilisation d'une appli mobile malveillante

2/. Les risques et les conséquences

3/. Les bonnes pratiques

SEN-AT2

Atelier : Les Cyber-Risques

Niveau	Prérequis	Lieu	Durée
Utilisateurs du SI	Pas de prérequis	Dans vos locaux	1h45 à 2h

30 % des incidents de sécurité en entreprise sont attribuables à l'erreur humaine.

Grâce à des **démonstrations réalisées en direct** par un expert, nos ateliers font **prendre conscience** des risques réels aux participants. Notre expert explique les risques liés à la sécurité informatique, et les sensibilise à l'importance de cet apprentissage.

Ces ateliers interactifs permettent **l'apprentissage des bonnes pratiques** et des connaissances nécessaires à un comportement sain.

OBJECTIFS DE LA FORMATION

- démystifier les risques informatiques
- vulgariser les attaques sur la messagerie
- apprendre les bonnes pratiques pour une utilisation professionnelle et personnelle des d'internet
- apprendre à utiliser le Wifi de manière sécurisée

PROGRAMME

Déroulement :

- en session participative : jusqu'à 25 personnes

1/. L'ingénierie sociale

2/. Le phishing

3/. Les réseaux sociaux

4/. Le Wifi

SEN-AT3

Atelier : Les Mots de passe

Niveau	Prérequis	Lieu	Durée
Utilisateurs du SI	Pas de prérequis	Dans vos locaux	1h45 à 2h

30 % des incidents de sécurité en entreprise sont attribuables à l'erreur humaine.

Grâce à des **démonstrations réalisées en direct** par un expert, nos ateliers font **prendre conscience** des risques réels aux participants. Notre expert explique les risques liés à la sécurité informatique, et les sensibilise à l'importance de cet apprentissage.

Ces ateliers interactifs permettent **l'apprentissage des bonnes pratiques** et des connaissances nécessaires à un comportement sain.

OBJECTIFS DE LA FORMATION

- comprendre l'importance d'un mot de passe fort
- comprendre ce qui intéresse les pirates et comment ils procèdent
- apprendre à créer des mots de passe forts
- pouvoir interagir directement avec un expert pour personnaliser les informations reçues

PROGRAMME

Déroulement :

- en session participative : jusqu'à 25 personnes

1/. Démonstration :
vol d'un mot de passe

2/. Les risques et les conséquences

3/. Les bonnes pratiques

SEN-AT4

Atelier : Les Clés USB

Niveau	Prérequis	Lieu	Durée
Utilisateurs du SI	Pas de prérequis	Dans vos locaux	1h45 à 2h

30 % des incidents de sécurité en entreprise sont attribuables à l'erreur humaine.

Grâce à des **démonstrations réalisées en direct** par un expert, nos ateliers font **prendre conscience** des risques réels aux participants. Notre expert explique les risques liés à la sécurité informatique, et les sensibilise à l'importance de cet apprentissage.

Ces ateliers interactifs permettent **l'apprentissage des bonnes pratiques** et des connaissances nécessaires à un comportement sain.

OBJECTIFS DE LA FORMATION

- comprendre les risques liés à l'usage des clés USB
- comprendre ce qui intéresse les pirates et comment ils procèdent
- apprendre les bonnes pratiques pour utiliser les clés USB
- pouvoir interagir directement avec un expert pour personnaliser les informations reçues

PROGRAMME

Déroulement :

- en session participative : jusqu'à 25 personnes

1/. Démonstration :
connexion d'une clé "trouvée"

2/. Les risques et les conséquences

3/. Les bonnes pratiques