SENSIBILISATION À LA SÉCURITÉ DU POSTE DE TRAVAIL

Public	Toute personne concernée par une démarche sécurité au sein de l'entreprise.
Durée	1 journée - 7 heures
Pré-requis	Savoir utiliser un ordinateur sous Windows ou macOS.
Objectifs	Décrire les concepts-clés relatifs à l'importance d'assurer la sécurité des informations et des données, d'assurer votre sécurité physique, d'éviter le vol de données personnelles et de protéger votre vie privée Protéger un ordinateur, un dispositif numérique mobile, un réseau contre les logiciels malveillants (malware) et les accès non-autorisés Décrire les différents types de réseaux, de connexions et les composants spécifiques tel que le pare-feu (firewall) qui peuvent poser problème lors des connexions Naviguer sur le World Wide Web et communiquer en toute sécurité sur Internet
Méthodes pédagogiques	Pour bien préparer la formation, le stagiaire remplit une évaluation de positionnement et fixe ses objectifs à travers un questionnaire. La formation est délivrée en présentiel ou distanciel (e-learning, classe virtuelle, présentiel et à distance). Le formateur alterne entre méthodes démonstratives, interrogatives et actives (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification. Cette formation est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par Audit Conseil Formation.
Moyens techniques	1 poste de travail complet par personne De nombreux exercices d'application Mise en place d'ateliers pratiques Remise d'un support de cours Passage de certification(s) dans le cadre du CPF Remise d'une attestation de stage
Modalité d'évaluation des acquis	Evaluation des besoins et objectifs en pré et post formation Evaluation technique des connaissances en pré et post formation Evaluation générale du stage
Délai d'accès	L'inscription à cette formation est possible jusqu'à 5 jours ouvrés avant le début de la session
Accessibilité handicapés	Au centre d'affaires ELITE partenaire d'ACF à 20 m. Guide d'accessibilité à l'accueil.

MENACES SUR LES DONNÉES

- Faire la différence entre données et informations
- Définir la cybercriminalité
- Expliquer la différence entre hacker (hacking), cracker (cracking) et pirater dans un but éthique (ethical hacking)
- Citer les menaces majeures pour la sécurité des données
- Comprendre l'importance de protéger les informations personnelles, notamment pour éviter : le vol d'identité, les fraudes

VALEUR DE L'INFORMATION

- Expliquer pourquoi il est important de protéger des données commerciales sensibles : vol d'informations client, données financières
- Identifier les mesures à prendre pour empêcher les accès non autorisés aux données : cryptage, mot de passe
- Comprendre les bases de la sécurisation de l'information : confidentialité, intégrité, disponibilité
- Identifier les principales règles de protection, de conservation et de contrôle des données en France
- Comprendre l'importance de créer et d'adopter des directives (lignes de conduite / guidelines) et des réglementations (policies) en matière d'utilisation des TIC

SÉCURITÉ PERSONNELLE

- Définir la notion d'ingénierie sociale et les méthodes utilisées
- Identifier les méthodes de vol d'identité : hameçonnage, "shoulder surfing", appels téléphoniques.

SÉCURITÉ DES FICHIERS

- Comprendre les effets de l'activation / désactivation des macros dans les options de sécurité des applications
- Comprendre les avantages et les limites du cryptage des données

LOGICIELS MALVEILLANTS

- Comprendre le terme "malware"
- Identifier les différentes techniques des logiciels malveillants
- Reconnaître les différents types d'infections
- Le logiciel publicitaire (adware)
- Le logiciel espion (spyware)
- La machine zombie (botnet)
- L'enregistreur de frappe (keystroke logging)
- Le composeur de numéros téléphoniques (dialler)

PROTECTION

- Comprendre le fonctionnement d'un antivirus et identifier ses limites
- Analyser / scanner des lecteurs, des dossiers et des clés USB avec un antivirus
- Planifier une analyse
- Comprendre et mettre en application une quarantaine
- Comprendre l'importance de télécharger et d'installer régulièrement les mises à jour des logiciels antivirus

SÉCURITÉ SUR DES RÉSEAUX

- Comprendre ce qu'est un réseau et reconnaître les principaux types de réseaux (LAN, WAN, VPN)
- Comprendre le rôle de l'administrateur réseau dans la gestion des utilisateurs, des droits et des espaces alloués
- Décrire l'utilité et les limites d'un pare-feu (firewall)
- Connaître les différentes solutions pour se connecter à un réseau : câble, sans fil
- Comprendre pourquoi la connexion à un réseau (filaire ou sans fil) peut entraîner des problèmes de sécurité
- Comprendre l'importance d'imposer un mot de passe pour se connecter
- Identifier les différents types de sécurisation d'un réseau sans fil
- Etre conscient que la connexion à un réseau Wi-Fi non protégé peut permettre l'espionnage des données

CONTRÔLE D'ACCÈS

- Comprendre l'utilité d'un identifiant et d'un mot de passe pour se connecter
- Connaître les bonnes pratiques en matière de mot de passe
- Reconnaître les différentes possibilités de contrôles d'accès biométrique

NAVIGATION WEB

- Identifier une page Web / site Web sécurisés pour les achats en ligne et les transactions bancaires
- Etre conscient des risques de redirection vers des sites malveillants
- Mettre en fonction un certificat numérique
- Comprendre ce qu'est un mot de passe à usage unique
- Choisir les réglages appropriés pour sécuriser son navigateur : remplissage automatique de formulaire, autorisation ou blocage des cookies, suppression des données personnelles et de l'historique de navigation
- Comprendre le but, les fonctionnalités et les différents types de logiciels de filtrage Web

RÉSEAUX SOCIAUX

- Comprendre l'importance de ne pas diffuser d'informations confidentielles sur les réseaux sociaux
- Vérifier le paramétrage des comptes des réseaux sociaux
- Comprendre les risques potentiels de l'usage des réseaux sociaux : harcèlement, manipulation psychologique, usurpation, lies / messages frauduleux

E-MAIL ET MESSAGERIES INSTANTANÉES

- Comprendre le rôle du cryptage de mail
- Comprendre le terme "signature numérique"
- Créer / ajouter un certificat numérique
- Identifier les différents mails frauduleux
- Prendre conscience des risques liés aux pièces jointes
- Comprendre ce qu'est l'hameçonnage (phishing)
- Comprendre ce qu'est une messagerie instantanée et leurs failles de sécurité
- Connaître les méthodes pour assurer la confidentialité des échanges

SÉCURISER, SAUVEGARDER LES DONNÉES

- Connaître les méthodes pour assurer une sécurité physique des dispositifs numériques mobiles
- Mettre en place des sauvegardes de données et les restaurer
- Comprendre l'importance de pouvoir détruire des données de manière définitive
- Faire la différence entre un effacement et une destruction définitive des données
- Identifier les méthodes de suppression définitives de données (shredding)

NOUS CONTACTER

Siège social
16, ALLÉE FRANÇOIS VILLON
38130 ÉCHIROLLES

Centre de formation
87, RUE GÉNÉRAL MANGIN
38000 GRENOBLE

Téléphone
04 76 23 20 50 - 06 81 73 19 35

E-mail
contact@audit-conseil-formation.com

Suivez-nous sur les réseaux sociaux, rejoignez la communauté !

ACF Audit Conseil Formation @ACF_Formation ACFauditconseilformation