



IFT101 - La sécurité informatique

Domaine de formation Bureautique/Informatique

Description sommaire Ce cours de formation en ligne de Sécurité informatique vous permettra d'identifier les risques et de mieux protéger votre outil informatique

Objectifs Appréhender la notion de Sécurité Informatique. Détecter et identifier les risques liés à l'utilisation de l'outil Informatique. Apprendre à protéger son matériel et ses données. S'initier au Droit de l'Informatique.

Contenu Notion de Sécurité Informatique

Prendre conscience de la gravité des conséquences qu'une attaque informatique peut avoir sur une entreprise.

Connaître les types d'attaques les plus courants

Prendre conscience du fait que la sécurité informatique est souvent une question de comportement et de bonnes habitudes

Les entreprises concernées (PME, TPE ...)

Les différents types d'attaques (internes, externes) et leur caractère (volontaire, involontaire)

Les conséquences d'une attaque informatique (financières, techniques, commerciales...)

Les bonnes habitudes (protection du système informatique par antivirus), maintenance de base (mise à jour logicielles, enregistrements des logiciels, authenticité des messages...), maintenance régulière (sauvegarde régulière des fichiers sur différents supports, analyse des fichiers, modification des mots de passe...), planification de la maintenance (manuelle ou automatique). Protéger son matériel

Apprendre à protéger son parc informatique des dommages physiques et du vol

Apprendre à voyager avec son ordinateur portable en toute sécurité

Les bases de protection matérielle : Protection incendie, inondation, effractions, protection des unités centrales, mise sous clés des ordinateurs portables et supports d'information...

La protection des serveurs : fonction des serveurs, emplacements réservés et sécurisés, marquages, limitation des autorisations d'accès aux informations...

Les clés USB, CD-ROM et disquettes : risques liés à introduction de virus par l'intermédiaire des différents supports physiques et nécessité de verrouiller les informations contenues sur ces supports faciles à dérober.

Les déplacements professionnels : principe de protection du portable et de son contenu (Verrouillage par mot de passe, cryptage, surveillance...)

Protéger ses données

Connaître les attaques dont on peut être victime.

Connaître les principes à mettre en pratique pour protéger les données informatisées

Connaître les trucs et astuces de la sauvegarde de données

Les attaques : se préserver des attaques de provenance diverse (interne, externe) et d'origine variée (malveillance, négligence)



Sécurité en entreprise

- La gestion des droits d'accès des utilisateurs : définir le niveau d'accès de chaque utilisateur en fonction de la tâche qu'il occupe au sein de l'entreprise, limiter les droits d'« Administrateurs », définir le rôle de l'Administrateur
- La protection par mot de passe : mot de passe renforcé : (choix du mot de passe, règle de sûreté, cryptage des dossiers sensibles, système EFS)
- La sauvegarde des données : détermination des fichiers à sauvegarder, de la fréquence des sauvegardes, des supports à utiliser (CD-ROM, disquette, disque dur externe...), Se protéger des attaques extérieures (virus, vers, chevaux de Troie spywares, WI-FI, VPN)
- Connaître les types d'attaques informatiques auxquelles vous pouvez être confronté
- Apprendre à déjouer ces attaques
- Les programmes malveillants (virus, vers et chevaux de Troie): mode d'infection, de propagation, dommages causés, origine, détection, conduite à adopter pour contrer ces programmes
- Les spywares (ou logiciels espions): origine, mode d'infection, détection, désinstallation, suppression, blocage à l'installation - pare-feux, mise à jour des logiciels anti-spyware...
- Les risques liés au WI-FI: évaluation des risques liés à ce type de connexion, conseils de sécurisation
- Les risques liés au VPN: définition du « réseau virtuel privé »,
- Communiquer en toute sécurité (messagerie électronique, instantanée, spams, canulars)
 - Utiliser l'e-mail en limitant au maximum les risques
- Se protéger des spams et des canulars
 - Sécuriser votre messagerie instantanée
 - Recevoir et envoyer des e-mails en toute sécurité : règles de sécurité liées à la réception de mails, à l'ouverture des pièces jointes, au lancement de fichiers exécutables « .exe », à l'envoi de mail (signature numérique, destinataires, contenu)
 - Les spams et canulars (appelés également hoax) : définition, identification, règles de sécurité, méthode d'éradication
 - La sécurisation de l'adresse e-mail : conseils liés à la divulgation de l'adresse, appréciation des politiques de confidentialité des différents sites WEB
 - Les dangers de la messagerie instantanée (ou IM) : présentation des attributs et mesures de prudence spécifiques à cette messagerie
- Surfer prudemment (cookies, achats en ligne, phishing, spoofing, téléchargement)
 - Apprendre à assurer la confidentialité de vos données sur internet
- Sécuriser vos achats en ligne
 - Déjouer les pièges du phishing et du spoofing
 - Conseils de sécurité pour le téléchargement
 - Régler son navigateur pour contrôler les cookies : définition, réglages d'Internet Explorer, détermination du niveau de confidentialité adapté, paramétrages de navigateurs autres, suppressions des cookies enregistrés sur le disque dur ENTREPRISE



Les achats en ligne : présentation des risques et des technologies de sécurisation des transactions en ligne, repérage des sites sécurisés (charte de confidentialité), conseils liés aux achats (assurance, commande, retour, frais, livraison...)

protéger du phishing : définition et principes, méthode de détection des sites WEB « falsifiés »

Télécharger en toute sécurité : conseils de sécurité : analyse anti-virus, choix des sites WEB Initiation au droit de l'informatique

Connaître les grandes lignes de ce que l'utilisateur de l'outil informatique a le droit de faire ou pas (les droits de l'utilisateur en matière d'informatique)

Se familiariser avec la Loi LCEN

Se familiariser avec la Loi Informatique et Libertés

La notion de licence d'utilisation : définition, termes et conditions de l'utilisation, notion de contrefaçon, de fraude logicielle, sanctions applicables en cas de non respect de cette licence par l'utilisateur ; précautions liées à l'achat de logiciel(s) (méthodes d'authentification de logiciels originaux)

La propriété intellectuelle : distinction « propriété industrielle » / « droit d'auteur »

La loi pour la Confiance dans l'Economie Numérique dite LCEN : présentation et définition

Informatique et Liberté : présentation, définition, application aux domaines de la cybersurveillance, de la collecte et diffusion des données, des droits des utilisateurs

Notions élémentaires

Compétences acquises Maîtrise des principales notions de sécurité Informatique.

Approche pédagogique La formation individualisée en ligne, disponible 24h/24 - 7 jours/7, vous permet d'acquérir de nouvelles connaissances à votre rythme, à l'endroit qui vous convient. Nos formations sont créées de façon à vous permettre un cheminement autonome, graduel et souple. Des lectures peuvent vous être proposées pour approfondir un concept. L'Encadrement est disponible en ligne par un tuteur spécialisé.

Durée durée du crédit d'accès à la plateforme : **3 mois**

