ECDL STANDARD – Securité informatique – SM4

Description

Ce cours fournit des connaissances élémentaires sur la sécurité dans l'utilisation des TIC (Technologies de l'Information et de la Communication) au quotidien. Cela inclut la connexion sécurisée à un réseau, la sécurité sur Internet et la sécurisation des données et des informations.

Contenu du cours
Chapitre 1 : Concepts de base liés à la sécurité

- Module 1 : Menaces sur les données
  - Faire la différence entre les données et les informations
  - Comprendre les termes « Cybercriminalité », « Piratage » (hacking)
  - Connaître les menaces pour la sécurité des données causées par des individus, des fournisseurs d'accès, des organisations externes
  - Connaître les menaces majeures pour la sécurité des données comme : les incendies, les inondations, les guerres, les tremblements de terre
  - Connaître les menaces principales pour les données lors de l'utilisation de l'informatique dans le nuage : prise de contrôle sur les données, risque de perte de sa vie privée
- Module 2 : Valeur de l'information
  - Comprendre les caractéristiques de base de la sécurisation de l'information comme : la confidentialité, l'intégrité, la disponibilité des données
  - Comprendre pourquoi il est important de protéger les informations personnelles, notamment : pour éviter le vol d'identité, pour éviter les fraudes, pour conserver une vie privée
  - Comprendre pourquoi il est important de protéger les données professionnelles présentes sur les ordinateurs ou sur les dispositifs numériques mobiles pour éviter notamment : le vol ou l'utilisation frauduleuse des données, la perte accidentelle de données, le sabotage
  - Identifier les principales règles de protection, de conservation et de contrôle des données/ données privées, notamment : la transparence, les dispositions légales, la proportionnalité
  - Comprendre les expressions « données concernant des personnes physiques » et « contrôleurs des données » et comment les principes de protection, de conservation et de contrôle des données /données privées peuvent leur être appliqués
  - Comprendre l'importance de créer et d'adopter des directives (lignes de conduite/guidelines) et des réglementations (policies) en matière d'utilisation des TIC. Savoir si elles sont connues et accessibles
- Module 3 : Sécurité personnelle
  - Comprendre le terme « Ingénierie sociale/Social engineering » et ses implications comme : la collecte non-autorisée d'informations sur des ordinateurs ou dispositifs numériques mobiles, la fraude
  - Identifier les méthodes employées pour l'ingénierie sociale comme : les appels téléphoniques, l'hameçonnage, l'espionnage par-dessus l'épaule (shoulder surfing)
  - Comprendre le terme « Vol d'identité » et ses implications dans les domaines : personnels, financiers, des affaires, légaux
  - Identifier les méthodes de vol d'identité comme : escroquerie exploitant d'anciens matériels et/ou informations (information diving), escroquerie à la carte de paiement (skimming), escroquerie par abus de confiance (pretexting)
-

© Copyright ITTA – Tous les contenus sont protégés par le droit d'auteur.

Module 4 : Sécurité des fichiers
    - Comprendre les effets de l'activation/de la désactivation des paramètres de sécurité des macros dans les applications
    - Comprendre les avantages et les limites du cryptage des données. Savoir pourquoi il ne faut pas communiquer ou perdre le mot de passe de chiffrement, la clé ou le certificat
    - Comprendre comment crypter un fichier, un dossier, un lecteur
    - Appliquer un mot de passe aux fichiers comme : des documents, des classeurs/feuilles de calculs, des fichiers compressés

Chapitre 2 : Logiciels malveillants

- Module 1 : Types et fonctionnements
    - Comprendre le terme « Logiciel malveillant ». Reconnaître les différentes techniques adoptées par les logiciels malveillants pour rester masqués comme : le cheval de Troie (Trojan), le logiciel malveillant furtif (rootkit) et la porte dérobée (backdoor)
    - Reconnaître les différents types d'infections produits par les logiciels malveillants et comprendre comment ils agissent, notamment : les virus, les vers informatiques
    - Reconnaître les types de vols de données, les bénéfices produits par l'emploi de logiciels malveillants de vol de données et comprendre comment ils fonctionnent notamment : le logiciel publicitaire (adware), le logiciel de rançonnement (ransomware), le logiciel espion (spyware), la machine zombie (botnet), l'enregistreur de frappe (keylogger) et le composeur de numéros téléphoniques (dialler)
- Module 2 : Protection
    - Comprendre comment fonctionne un logiciel anti-virus et identifier ses limites
    - Comprendre qu'un logiciel anti-virus devrait être installé sur les ordinateurs et dispositifs numériques mobiles
    - Comprendre l'importance d'installer régulièrement les mises-à-jour des logiciels comme : l'anti-virus, les navigateurs Web, les modules d'extension (plug-in), les applications et le système d'exploitation
    - Analyser/scanner des lecteurs, dossiers, fichiers spécifiques avec un anti-virus. Planifier les analyses en utilisant un logiciel anti-virus
    - Comprendre les risque lors de l'utilisation de logiciels obsolètes ou dont le support n'est plus assuré par leurs éditeurs comme : la prolifération des logiciels malveillants, les incompatibilités de communication entre logiciels
- Module 3 : Résolution et suppression
    - Comprendre le terme « Quarantaine » et l'effet d'une quarantaine sur des fichiers infectés ou suspects
    - Comprendre l'intérêt de la mise en quarantaine, de la suppression des fichiers infectés ou suspects
    - Comprendre qu'une attaque de logiciel malveillant peut être diagnostiquée et résolue en utilisant des ressource en ligne comme : des sites de systèmes d'exploitation, des antivirus, les fournisseurs de navigateurs Web, les sites Web des autorités/organisations compétentes

Chapitre 3 : Sécurité réseau

- Module 1 : Réseaux et connectivité
    - Comprendre le terme « Réseau » et reconnaître les principaux types de réseaux comme : réseau local (Local Area Network (LAN)), réseau local sans fil (Wireless Local Area Network (WLAN)), réseau étendu (Wide Area Network (WAN)), réseau privé virtuel (Virtual Private Network (VPN))
    - Comprendre que le fait de se connecter à un réseau peut entraîner des problèmes de sécurité comme : apparition de logiciels malveillants, accès non autorisés à vos données, failles de protection de vos données personnelles
    - Comprendre le rôle de l'administrateur réseau dans la gestion des comptes utilisateurs, des droits

© Copyright ITTA – Tous les contenus sont protégés par le droit d'auteur.

d’accès et autorisations, des installations et mises à jour des correctifs de sécurité, de la surveillance du trafic sur le réseau, du traitement des logiciels malveillants trouvés sur le réseau
    - Comprendre l’utilité et les limites d’un pare-feu (firewall) dans un environnement de travail personnel Mettre en service/hors service le contrôle du flux entre votre machine et un réseau à l’aide un pare-feu personnel, bloquer une demande d’accès par un logiciel/service grâce au pare-feu
- Module 2 : Sécurité en environnement sans fil
    - Connaître les différents types de sécurisation d’un réseau sans fil comme : Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Wi-Fi Protected Access 2 (WPA2), filtrage par adresse MAC (Media Access Control address), masquage du nom du réseau sans fil (SSID Hiding)
    - Être conscient que l’utilisation d’un réseau sans fil non-protégé peut entraîner des risques comme : l’espionnage des données transmises (eavesdropping), le détournement de réseau (network hijacking), l’attaque de l’homme du milieu (man in the middle attack)
    - Comprendre ce qu’est un point d’accès (hotspot) personnel
    - Activer/désactiver un point d’accès personnel sécurisé et y connecter des dispositifs numériques mobiles de manière sécurisée

Chapitre 4 : Contrôle d’accès

- Module 1 : Méthodes
    - Identifier les mesures à prendre pour empêcher les accès non-autorisés aux données comme : un nom d’utilisateur, un mot de passe, un code PIN, le cryptage des données, l’authentification multi-facteurs
    - Comprendre le terme « Mot de passe à usage unique » et savoir dans quels cas il peut être utile
    - Comprendre l’utilité d’un compte utilisateur pour se connecter à un réseau
    - Comprendre que l’accès à un réseau devrait toujours passer par la saisie d’un nom d’utilisateur et d’un mot de passe. Savoir pourquoi il est important de verrouiller sa machine ou de se déconnecter du réseau quant le travail est terminé
    - Connaître les principales possibilités de contrôle d’accès biométrique comme : lecteur d’empreintes digitales, scanner rétinien, reconnaissance faciale, analyse de morphologie de la main
- Module 2 : Gestion des mots de passe
    - Connaître les bonnes pratiques en matière de mot de passe comme : le choisir de longueur suffisante, y mélanger des caractères très variés (lettres, chiffres et caractères spéciaux), ne pas le partager avec d’autres personnes, le modifier régulièrement, ne pas utiliser le même pour accéder à différents services/ logiciels/réseaux/ sites
    - Comprendre à quoi sert un logiciel de gestion de mots de passe et quelles sont ses limites

Chapitre 5 : Utilisation sécurisée du Web

- Module 1 : Paramètres du navigateur
    - Choisir les réglages appropriés pour activer, désactiver la fonction de remplissage automatique de formulaire/de sauvegarde automatique des données de formulaire lors du remplissage d’un formulaire sur le Web
    - Savoir supprimer les données personnelles dans un navigateur comme : l’historique de navigation, l’historique de téléchargement, les fichiers Internet temporaires (cache), les mots de passe, les cookies, les données de remplissage automatique de formulaires Web
- Module 2 : Naviguer en toute sécurité
    - Savoir que certaines activités en ligne (achats, transactions bancaires) ne devraient être effectuées que sur des pages Web sécurisées depuis un réseau sécurisé
    - Connaître les critères d’évaluation de la fiabilité d’un site Web comme : la qualité et l’actualisation du contenu, la validité/légitimité de l’URL, les informations concernant la société ou le propriétaire, les informations de contact, le certificat de sécurité, le contrôle du propriétaire de domaine
    - Comprendre le terme pharming

© Copyright ITTA – Tous les contenus sont protégés par le droit d’auteur.

- Comprendre le but, la fonction et les types de logiciels de contrôle de contenus comme : les logiciels de filtrage Web, les logiciels de contrôle parental

Chapitre 6 : Communications

- Module 1 : E-Mail
  - Comprendre le rôle du cryptage/décryptage d'un e-mail
  - Comprendre le terme « Certificat numérique »
  - Identifier des e-mails potentiellement frauduleux et/ou non-sollicités
  - Identifier les principales caractéristiques de l'hameçonnage (phishing) comme : utiliser le nom d'entreprises connues/de personnes connues, proposer des liens Internet falsifiés, afficher des logos et des marques réputés, pousser à la divulgation d'informations personnelles
  - Savoir qu'il est possible de signaler les tentatives d'hameçonnage à des organisations adaptées, aux autorités concernées
  - Être conscient du risque d'infecter l'ordinateur ou un dispositif numérique mobile par des logiciels malveillants en ouvrant une pièce-jointe (contenant une macro ou un fichier exécutable) dans un e-mail reçu
- Module 2 : Réseaux sociaux
  - Comprendre l'importance de ne pas diffuser d'informations confidentielles ou qui permettraient de vous identifier sur des sites de réseaux sociaux
  - Comprendre l'importance d'appliquer puis de vérifier régulièrement les bons réglages de confidentialité pour les comptes de réseaux sociaux comme : visibilité, emplacement
  - Savoir appliquer les bons réglages de confidentialité pour un compte de réseau social comme : visibilité, emplacement
  - Comprendre les risques potentiels lors de l'utilisation de sites de réseaux sociaux comme : la cyberintimidation (cyberbullying), la manipulation psychologique (grooming), la divulgation malveillante d'informations personnelles, les identités falsifiées, les liens ou contenus ou messages frauduleux
  - Savoir qu'il est possible de signaler les utilisations et comportements inappropriés sur des réseaux sociaux aux fournisseurs de services, aux autorités concernées
- Module 3 : VoIP et messagerie instantanée
  - Comprendre les failles de sécurité des messageries instantanées (MI/IM) et des logiciels utilisant le protocole de voix sur IP (VoIP) comme : les logiciels malveillants (malware), les portes dérobées (backdoor access), les accès non- autorisés aux fichiers, l'espionnage des données transmises (eavesdropping)
  - Connaître les méthodes pour assurer la confidentialité lors de l'utilisation des messageries instantanées et de la voix sur IP comme : le cryptage, ne pas diffuser d'informations importantes, limiter le partage des fichiers
- Module 4 : Dispositifs numériques mobiles
  - Comprendre les implications possibles lors de l'utilisation d'applications provenant de boutiques (application stores) non-officielles comme : logiciels malveillants pour dispositifs numériques mobiles, sur utilisation de ressources, accès aux données personnelles, qualité médiocre, coûts cachés
  - Comprendre ce que signifie gérer les permissions des applications
  - Savoir que les applications pour dispositifs numériques mobiles sont capables d'extraire des données de votre appareil comme : vos coordonnées, votre historique de localisation, des images
  - Connaître les mesures et précautions à prendre d'urgence lors de la perte de votre dispositif numérique mobile comme : désactiver l'accès à l'appareil à distance, supprimer les données de l'appareil à distance, localiser l'appareil à distance

Chapitre 7 : Gestion de la sécurité des données

© Copyright ITTA – Tous les contenus sont protégés par le droit d'auteur.

- Module 1 : Sécuriser et sauvegarder les données
    - Connaître les méthodes pour s'assurer de la sécurité physique des ordinateurs et dispositifs numériques mobiles comme : ne pas les laisser sans surveillance, se connecter de manière sécurisée au matériel, utiliser un câble de verrouillage, limiter les accès aux appareils
    - Connaître l'importance de maîtriser la procédure de sauvegarde (backup) en cas de perte de données sur un ordinateur ou dispositif numérique mobile
    - Identifier les caractéristiques d'une procédure de sauvegarde comme : fréquence, planification des tâches de sauvegarde, emplacement de stockage de la sauvegarde, compression prévue pour la sauvegarde
    - Sauvegarder des données vers des emplacements comme : lecteur local, lecteur/support externe, stockage dans le nuage
    - Restaurer des données en provenance d'emplacements comme : lecteur local, lecteur/support externe, stockage dans le nuage
- Module 2 : Suppression sécurisée et destruction de données
    - Faire la distinction entre un effacement et une suppression /destruction définitive de données
    - Comprendre pourquoi il peut être nécessaire de détruire de manière définitive des données qui se trouvent dans un lecteur ou dans un dispositif numérique mobile
    - Comprendre que la suppression de contenus n'est pas une destruction définitive sur des services comme : réseaux sociaux, blogs, forums Internet, stockage dans le nuage
    - Identifier les méthodes habituelles de suppression définitive de données comme : utiliser un logiciel de suppression de données (shredding), détruire le lecteur /support, démagnétiser le support de données, utiliser un utilitaire de destruction de données

Lab / Exercices

- Des exercices pratiques seront proposés durant et à la fin de chaque module

Documentation

- Support de cours numérique inclus

Examen

- Cette formation prépare à l'examen ECDL STANDARD - Securité informatique (SM2). Si vous souhaitez passer cet examen, merci de contacter notre secrétariat qui vous communiquera son prix et s'occupera de toutes les démarches administratives nécessaires pour vous

Profils des participants

- Personnes amenées à maîtriser les concepts essentiels et les techniques assurant une sécurité dans l'utilisation des TIC et souhaitant obtenir la certification ECDL

Connaissances Préalables

- Connaissances de bases sur la sécurité informatique
- Avoir les connaissances couvertes par les formations : ECDL BASE - L'essentiel sur le Web et la Communication (BM2) et ECDL BASE - L'essentiel sur l'ordinateur (BM1)

Objectifs

- Comprendre l'importance d'assurer la sécurité des informations et des données, identifier les principes fondamentaux de protection, de stockage et de gestion des données/données personnelles
- Identifier la menace concernant la sécurité personnelle que constitue l'usurpation d'identité, connaître les

© Copyright ITTA – Tous les contenus sont protégés par le droit d'auteur.

risques potentiels pour les données utilisées dans le cadre de l’informatique dans le nuage
- Mettre en place une politique de mots de passe et un cryptage afin de sécuriser des fichiers/données Comprendre les menaces représentées par les logiciels malveillants (malware) et être capable de protéger un ordinateur, un dispositif numérique mobile ou un réseau contre ces menaces
- Connaître les différents types de protection pour réseaux et réseaux sans fil, être capable d’utiliser un pare-feu (firewall) personnel et de mettre en place un point d’accès personnel (hotspot) sécurisé
- Protéger un ordinateur ou un dispositif numérique mobile contre les accès non-autorisés et être capable de définir de manière sécurisée les mots de passe (sans oublier leur mise à jour)
- Choisir les réglages appropriés pour un navigateur Web et comprendre comment identifier les sites Web de confiance pour s’assurer une navigation sécurisée
- Comprendre les problèmes de sécurité liés à la communication par e-mail, par réseaux sociaux, par protocole de voix sur IP (VoIP), par messagerie instantanée (MI/IM/Instant messaging) ou bien encore par applications disponibles sur un dispositif numérique mobile
- Sauvegarder des données vers des emplacements locaux ou dans le nuage, restaurer ou supprimer des données depuis ces mêmes emplacements. Manipuler les données et les dispositifs numériques mobiles en toute sécurité

Niveau
Intermédiaire
Prix de l'inscription en Présentiel (CHF)
1300
Prix de l'inscription en Virtuel (CHF)
1200
Durée (Nombre de Jours)
2
Reference
ECDL2-SM4

© Copyright ITTA – Tous les contenus sont protégés par le droit d’auteur.