Introduction

Sécurité des TI

CCe module expose les concepts essentiels et les techniques à maîtriser pour comprendre les principaux éléments qui assurent une sécurité dans l'utilisation des TIC (Technologies de l'Information et de la Communication) au quotidien. Ceci passe notamment par la maîtrise des techniques et applications appropriées pour conserver une connexion sécurisée au réseau, pour utiliser Internet en toute sécurité et pour manipuler les données et les informations de manière adaptée.

Objectifs du module

Les candidats qui réussiront ce module seront capables de :

- comprendre les concepts clés relatifs à l'importance d'assurer la sécurité des informations et des données, d'assurer leur sécurité physique, d'éviter le vol de données personnelles et de protéger leur vie privée,
- protéger un ordinateur, un dispositif numérique mobile, un réseau contre les logiciels malveillants (malware) et les accès non-autorisés,
- connaître les différents types de réseaux, de connexions et les composants spécifiques tels 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,
- comprendre les problèmes de sécurité liés à la communication, notamment en matière de courrier électronique et de messagerie instantanée (MI – IM/Instant messaging),
- sauvegarder et restaurer des données de manière appropriée et sécurisée, entreposer ses données et ses dispositifs numériques mobiles en toute sécurité.

Test et Evaluation du module « Sécurité des TI »

Temps alloué : 35 minutes.

Nombre de questions : 36.

Barre de succès : 75% de bonnes réponses.

Beaucoup de questions demandent une réflexion sur les objets présents dans l'écran, et permettent un autoapprentissage des bonnes pratiques ou des fonctions usuelles du domaine couvert.

Quelques conseils pour réaliser son test avec le maximum de chances de succès :

- Bien prendre son temps à chaque question : la lire deux fois posément et complètement.
- Ne jamais répondre trop vite (bien qu'il n'y ait jamais de piège dans les questions).
- Pour les questions QCM : lire complètement les réponses, et travailler par élimination.
- Pour les questions à zones sensibles : examiner l'image en détail, utiliser les éléments de la question.
- Analyser et retenir le sens des questions et des réponses quand il s'agit de bonnes pratiques ou de règles de productivité.

Catégorie	Domaine	Réf.	Dif.	Connaissances requises
1. Concepts de sécurité	1.1 Menaces sur les données	1.1.1		Faire la différence entre les données et les informations
		1.1.2		Comprendre le terme : cybercriminalité
		1.1.3		Comprendre la différence entre hacker (hacking), cracker (cracking) et pirater dans un but éthique (ethical hacking)
		1.1.4		Connaître les menaces majeures pour la sécurité des données comme : les incendies, les inondations, les guerres, les tremblements de terre
		1.1.5		Connaître les menaces pour la sécurité des données causées par : les employés, le fournisseur d'accès, les personnes externes
	1.2 Valeur de l'information	1.2.1		Comprendre pourquoi il est important de protéger les informations personnelles, notamment : pour éviter le vol d'identité, pour éviter les fraudes
		1.2.2		Comprendre pourquoi il est important de protéger des données commerciales sensibles, notamment : pour éviter le vol ou le détournement d'informations sur les clients, pour éviter le vol de données financières
		1.2.3		Identifier les mesures à prendre pour empêcher les accès non-autorisés aux données comme : le cryptage des données, l'utilisation de mots de passe
		1.2.4		Comprendre les caractéristiques de base de la sécurisation de l'information comme : la confidentialité, l'intégrité, la disponibilité des données
		1.2.5		Identifier les principales règles de protection, de conservation et de contrôle des données / données privées en vigueur dans votre pays
		1.2.6		Comprendre l'importance de créer et d'adopter des directives (lignes de conduite / guidelines) et des réglementations (policies) en matière d'utilisation des TIC
	1.3 Sécurité personnelle	1.3.1		Comprendre le terme : ingénierie sociale (social engineering) et ses implications comme : la collecte d'informations, la fraude, l'accès au système informatique

Catégorie	Domaine	Réf.	Dif.	Connaissances requises
		1.3.2		Identifier les méthodes employées pour l'ingénierie sociale comme : les appels téléphoniques, l'hameçonnage, l'espionnage par-dessus l'épaule (shoulder surfing)
		1.3.3		Comprendre le terme : vol d'identité et ses implications dans les domaines : personnels, financiers, des affaires, légaux
		1.3.4		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)
	1.4 Sécurité des fichiers	1.4.1		Comprendre les effets de l'activation / la désactivation des macros dans les options de sécurité des applications
		1.4.2		Utiliser un mot de passe pour les fichiers comme : les documents, les fichiers compressés, les classeurs / feuilles de calculs
		1.4.3		Comprendre les avantages et les limites du cryptage des données
2. Logiciels malveillants	2.1 Définition et fonctionnement	2.1.1		Comprendre le terme : logiciel malveillant (malware)
		2.1.2		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)
	2.2 Types	2.2.1		Reconnaître les différents types d'infections produits par les logiciels malveillants et comprendre comment ils agissent, notamment : les virus, les vers informatiques
		2.2.2		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 espion (spyware), la machine zombie (botnet), l'enregistreur de frappe (keystroke logging) et le composeur de numéros téléphoniques (dialler)

Catégorie	Domaine	Réf.	Dif.	Connaissances requises
	2.3 Protection	2.3.1		Comprendre comment fonctionne un logiciel anti-virus et identifier ses limites
		2.3.2		Analyser/scanner des lecteurs, dossiers, fichiers spécifiques avec un logiciel anti-virus. Planifier les analyses en utilisant un logiciel anti-virus
		2.3.3		Comprendre le terme : quarantaine et l'effet d'une quarantaine sur des fichiers infectés ou suspects
		2.3.4		Comprendre l'importance de télécharger et d'installer régulièrement les mises-à-jour des logiciels anti-virus et les nouvelles signatures de virus reconnues par votre anti-virus
3. Sécurité réseau	3.1 Réseaux	3.1.1		Comprendre le terme : réseau et reconnaître les principaux types de réseaux comme : réseau local (Local Area Network (LAN)), réseau étendu (Wide Area Network (WAN)), réseau privé virtuel (Virtual Private Network (VPN))
		3.1.2		Comprendre le rôle de l'administrateur réseau dans la gestion des comptes utilisateurs, des droits d'accès, des autorisations et des espaces disques alloués aux utilisateurs
		3.1.3		Comprendre l'utilité et les limites d'un pare-feu (firewall)
	3.2 Connexions réseaux	3.2.1		Connaître les différentes façons de se connecter à un réseau comme : par câble, sans-fil (wireless)
		3.2.2		Comprendre que le fait de se connecter à un réseau peut entraîner des problèmes de sécurité comme : apparition de logiciels malveillants, accès non autorisés aux données privées, failles de protection des données personnelles
	3.3 Sécurité en environnement sans fil	3.3.1		Connaître l'importance d'imposer la saisie d'un mot de passe pour protéger l'accès à un réseau sans fil
		3.3.2		Connaître les différents types de sécurisation d'un réseau sans fil comme : Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Media Access Control (MAC)

Catégorie	Domaine	Réf.	Dif.	Connaissances requises
		3.3.3		Être conscient que l'utilisation d'un réseau sans fil non-protégé peut permettre l'espionnage de vos données personnelles
		3.3.4		Se connecter à un réseau sans fil protégé / non-protégé
	3.4 Contrôle d'accès	3.4.1		Comprendre l'utilité d'un compte utilisateur pour se connecter à un réseau et l'importance de toujours passer par la saisie d'un nom d'utilisateur et d'un mot de passe pour accéder au réseau
		3.4.2		Connaître les bonnes pratiques en matière de mot de passe comme : ne pas le partager avec d'autres utilisateurs, le changer régulièrement, le choisir de longueur suffisante, y mélanger des caractères très variés (lettres, chiffres et caractères spéciaux)
		3.4.3		Connaître les principales possibilités de contrôle d'accès biométrique comme : lecteur d'empreintes digitales, scanner rétinien
4. Utilisation sécurisée du Web	4.1 Navigation Web	4.1.1		Savoir que certaines activités en ligne (achats, transactions bancaires) ne devraient être effectuées que sur des pages Web sécurisées
		4.1.2		Reconnaître un site Web sécurisé : https, symbole de cadenas
		4.1.3		Etre conscient des risques de redirection vers des sites malveillants (pharming)
		4.1.4		Comprendre le terme : certificat numérique. Mettre en fonction un certificat numérique
		4.1.5		Comprendre le terme : mot de passe à usage unique
		4.1.6		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
		4.1.7		Comprendre le terme : mouchard électronique (cookie)
		4.1.8		Choisir les réglages appropriés pour autoriser, bloquer les mouchards électroniques (cookies)

Catégorie	Domaine	Réf.	Dif.	Connaissances requises
		4.1.9		Supprimer les données personnelles dans un navigateur comme : l'historique de navigation, les fichiers Internet temporaires, les mots de passe, les mouchards électroniques (cookies), les données de remplissage automatique de formulaires Web
		4.1.10		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
	4.2 Réseaux sociaux	4.2.1		Comprendre l'importance de ne pas diffuser d'informations confidentielles sur des sites de réseaux sociaux
		4.2.2		Etre attentif à l'importance d'appliquer les bons réglages de confidentialité pour les comptes de réseaux sociaux
		4.2.3		Comprendre les risques potentiels lors de l'utilisation des réseaux sociaux comme : le harcèlement par le Web (cyberbullying), la manipulation psychologique (grooming), les informations trompeuses / dangereuses, les identités falsifiées, les liens ou messages frauduleux
5. Communications	5.1 E-Mail	5.1.1		Comprendre le rôle du cryptage, décryptage d'un e-mail
		5.1.2		Comprendre le terme : signature numérique
		5.1.3		Créer et ajouter / importer un certificat numérique
		5.1.4		Être conscient de la possibilité de recevoir des e-mails frauduleux et non-sollicités
		5.1.5		Comprendre le terme : hameçonnage (phishing). Identifier les principales caractéristiques d'hameçonnage comme : utiliser le nom d'entreprises connues, de personnes connues, proposer des liens Internet falsifiés
		5.1.6		Etre conscient du risque d'infecter l'ordinateur par des logiciels malveillants en ouvrant une pièce jointe (contenant une macro ou un fichier exécutable)

Catégorie	Domaine	Réf.	Dif.	Connaissances requises
	5.2 Messagerie instantanée (MI/IM)	5.2.1		Comprendre le terme : messagerie instantanée (MI/IM) et ses utilisations possibles
		5.2.2		Comprendre les failles de sécurité liées aux messageries instantanées comme : les logiciels malveillants (malware), les portes dérobées (backdoor access), les accès non-autorisés aux fichiers
		5.2.3		Connaître les méthodes pour assurer la confidentialité lors de l'utilisation des messageries instantanées comme : le cryptage, ne pas diffuser d'informations importantes, limiter le partage des fichiers
6. Gestion de la sécurité des données	6.1 Sécuriser et sauvegarder les données	6.1.1		Connaître les méthodes pour s'assurer de la sécurité physique des dispositifs numériques mobiles comme : gérer efficacement les emplacements et les caractéristiques des appareils, utiliser un câble de verrouillage, limiter les accès aux appareils
		6.1.2		Connaître l'importance de maîtriser la procédure de sauvegarde (backup) en cas de perte de fichiers, de données comptables, d'historique de navigation et de signets
		6.1.3		Identifier les paramètres d'une procédure de sauvegarde comme : régularité/fréquence, planification des tâches de sauvegarde, emplacement de stockage de la sauvegarde
		6.1.4		Sauvegarder des données
		6.1.5		Restaurer et valider la restauration de données en provenance d'une sauvegarde
	6.2 Destruction sécurisée	6.2.1		Comprendre l'importance de pouvoir détruire de manière définitive des données qui se trouvent dans un lecteur ou dans un dispositif numérique mobile
		6.2.2		Faire la distinction entre un effacement et une totale destruction (définitive) de données

Catégorie	Domaine	Réf.	Dif.	Connaissances requises
		6.2.3		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