Introduction à la Sécurité pour les Utilisateurs

Filière : **Soft Skills & Utilisateurs** Sous-filière : **Sécurité - Utilisateurs**

RÉFÉRENCE	DURÉE	PRIX UNITAIRE HT
USER-AWAR	**1 JOUR (7H)**	**480 €**

Description

Cette formation pour utilisateurs à pour but l'éveil aux problématiques de sécurité des systèmes d'information.

Les sujets traités sont

- L'utilisation des mots de passe,
- Le phishing,
- Les appareils mobiles,
- Les Réseaux Sociaux.

Objectifs pédagogiques

- Acquérir des notions de base en sécurité pour éviter les attaques
- Acquérir les bons réflexes

Public cible

- Utilisateurs

Programme de la formation

Les mots de passe

- Pourquoi un mot de passe est-il important?
- Comment créer un mot de passe fort?
- Quel genre d'attaques sont possibles pour récupérer les mots de passe?
- Exemples et erreurs classiques
- L' enjeux et les impacts du partage de mot de passe

- Démo d'une attaque par masque et dictionnaire.
- Verrouiller son ordinateur en absence

Le Phishing

- Qu'est-ce qu'une attaque de phishing?
- Pourquoi une attaque de phishing est-elle dangereuse?
- Comment détecter le phishing? (du point de vue de l'utilisateur)
- Que faire en cas de doute?
- Les arnaques téléphoniques (logiciel de control à distance)

Les différents types de malwares

- Spywares
- Keyloggeurs
- Dialeurs
- Downloaders
- Virus et worms
- Trojans et backdoors
- Macros
- Rootkits
- Flooders
- Crypteurs et ransonneurs
- Vidéo
    - https://www.youtube.com/watch?v=bjYhmX_OUQQ

Comment se protéger des malwares ?

- « Le meilleur antivirus, c'est l'être humain », Kevin Mitnick
- Tenir le système d'exploitation (OS) (Windows,linux, Mac...) à jour
- Tenir son navigateur et tous les logiciels du PC à jour
- Savoir identifier les services et programmes lancés au démarrage de son ordinateur
- Connaître les extensions utiles à son navigateur
- Éviter les pièges les plus connu du net (cracks, warez, sites pornographiques, P2P)
    - https://www.youtube.com/watch?v=uquRzrcwA18
- Scanner les clefs USB
- Désactiver l'exécution automatique de programmes
- Utiliser des logiciels de protection
- Attirer l'attention sur ce sujet chaud

- Avoir une idée de l'impact potentiel pour son entreprise
- Les risques pénaux encourus en cas d'usage abusif (pour l'entreprise ou l'employé)
- Les clauses de bonne conduite

La sécurité physique des appareils portables

- Les risques du « Bring Your Own Device » (BYOD) pour le réseau de l'entreprise
- Le verrouillage d'écran
- Les réseaux sans fil
- Les communications via réseaux non chiffrés – lorsqu'on est connecté à un réseau WiFi public

La sécurité des réseaux sociaux

- Les paramètres de sécurité et de confidentialité des réseaux sociaux principaux (Linkedin, Facebook, Twitter, Google+)
- Les comportements à adopter et à prescrire

Qualité

Cette formation est accessible aux personnes en situation de handicap, nous contacter en cas de besoin d'informations complémentaires.

Programme mis à jour le **15 novembre 2023**