Navigation Web, sensibilisation à la sécurité

Cours Synthèse de 1 jour - 7h
Réf : SWZ - Prix 2024 : nous consulter

Le web est un formidable outil pour la communication et l'échange de ressources. Nous y constatons aussi un nombre grandissant de menaces ces dernières années. L'objectif de cette synthèse est d'appréhender les risques auxquels les internautes sont exposés afin d'apprendre à utiliser le web en toute sécurité.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Appréhender les menaces et concepts de sécurité autour de l'utilisation du web

Utiliser Internet en étant conscient des risques

Naviguer avec un niveau de sécurité satisfaisant

Contrôler la diffusion de ses informations personnelles

Acquérir les bonnes pratiques de sécurité pour la navigation web

ECHANGES

Échanges pédagogiques avec l'intervenant, qui illustre techniquement les concepts avec des outils variés.

LE PROGRAMME

dernière mise à jour : 10/2023

1) Les principales menaces rencontrées sur le web

- Bulle de filtrage et ciblage publicitaire.
- Fake news et canular (hoax).
- Le phishing (hameçonnage) : e-mails et sites frauduleux.
- Les pièces jointes à un courriel.
- Piratage de compte et d'identité.

Exemple : Analyse des contenus et des liens d'e-mails de phishing.
Recueil d'information avec le logiciel Altengo.

2) Données personnelles et bonnes pratiques de navigation

- Le contrôle de la diffusion des données personnelles sur le web.
- Gestion des mots de passe et moyens d'authentification.
- Bloqueurs de pubs et de sites malveillants.
- Mise à jour des logiciels et désactivation de composants.
- La sauvegarde régulière de ses données.
- Les réglementations française, européenne et nord-américaine relatives à la protection des données.
- Signalement des pratiques frauduleuses.

Exemple : Démonstration de recueil de metadonnées diverses (jpeg, exif, champs d'en-tête HTTP et User-Agent). Présentation des cookies.

3) Les mécanismes de confiance pour le web

- HTTPS : le web sécurisé.
- Focus sur les clés de chiffrement : cryptage, hachage et vérification d'intégrité.
- Les certificats SSL/TLS : présentation et typologie.
- Organismes de certification et certificats auto-signés.

PARTICIPANTS

Tout public ayant une utilisation de la navigation web et des services d'e-mail.

PRÉREQUIS

Aucune connaissance particulière.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

- Le paiement en ligne.
Génération de clés asymétriques, chiffrement et signature de contenu textuel.
Démonstration du hashage de mots de passe.

4) Approche technique des attaques sur le web

- Typologie des pirates et leurs objectifs.
- Doxxing, hot-reading, stalking.
- Malware : les pièces jointes infectées dans les e-mails.
- Le cas particulier des ransomwares (rançongiciels).
- JavaScript : clickjacking, cross-site scripting (XSS) et CSRF.
- Les types d'attaques directes et par rebond.
- Man in the middle.
- Déni de service et DDoS.

LES DATES

Nous contacter