Avantages Formation

SENSIBILISATION A LA CYBERSECURITE	Durée : 7 heures

Objectifs de la formation
L'utilisation des ressources du système d'information n'est pas sans risque. Cette sensibilisation présente à l'aide de très nombreux exemples les bonnes pratiques de l'utilisateur sédentaire, nomade ou en télétravail pour limiter les risques d'erreur ou de malveillance. L'approche méthodologique participative de ce module permet des échanges entre les participants et le formateur sur des retours d'expériences.

Public concerné et prérequis
Tout le personnel, pas de prérequis

Méthodologie et Conditions de formation
Formateur professionnel expert Informatique Réseaux et Sécurité Internet
Formation intra entreprise par petit groupe de 6 maximum.
Evaluations par tests et étude de cas.

Contenu de la formation

1 - Introduction
- Les préjugés à surmonter
- Les valeurs essentielles à protéger
- Les périmètres
- Les menaces

2 - L'organisation et les responsabilités
- La direction générale – le service informatique
- Les sous-traitants
- Les administrateurs techniques et fonctionnels
- Les utilisateurs

3 - Les référentiels SSI et vie privée
- Les guides et manuels
- Les procédures

4 - Vision synthétique des obligations légales
- Disciplinaire
- Contractuelle
- Civiles
- Pénales
- Le cas du contrôle par l'employeur : utilisation professionnelle et non-professionnelle

5 - Les menaces
- La divulgation d'information "spontanée"
- L'ingénierie sociale et l'incitation à dire ou faire
- Le lien avec l'intelligence économique
- Le lien avec l'espionnage industriel

6 - Les risques
- Vol, destruction
- Virus
- Les aspirateurs à données
- Le phishing /l'hameçonnage
- Les malwares
- Les spywares
- L'usurpation
- Le cas des réseaux sociaux

7 - Les bonnes pratiques d'évaluation de la sensibilité de l'information
- La classification par les impacts, (juridiques, opérationnels, financiers, image, sociaux)
- L'échelle d'impact
- Les pièges

8 - Les bonnes pratiques pour les comportements généraux
- A l'intérieur des établissements
- A l'extérieur des établissements

9 - Les bonnes pratiques d'utilisation des supports d'information sensible pour les phases de conception, stockage, échanges et fin de vie
- Papier
- Environnement partagé
- Environnement individuel sédentaire
- Environnement individuel mobile

10 - Les bonnes pratiques d'utilisation des ressources du système d'information
- Installation et maintenance : postes fixes, équipements nomades, portables, ordiphones
- Identification et authentification
- Échanges et communications : intranet, internet, contrôle des certificats serveurs, les échanges de fichiers via la plate-forme "institutionnelle", le nomadisme, les télétravailleurs et le VPN de télé accès, email, la consultation en Web mail, signature, chiffrement, Cloud, réseaux sociaux et forums thématiques professionnels et privés, téléphonie
- Stockages et sauvegardes (clés usb, locales, serveurs, ...)
- Archivages
- Anonymisation
- Destruction ou recyclage

11 - Conclusion