BLOC 2

Formation en cybersécurité, gestion et protection de ses données personnelles (SP48)

Objectifs

- sensibiliser aux enjeux de la cyber sécurité
- prévenir les attaques cyber
- sécuriser les activités sur internet
- sécuriser les communications
- protéger la confidentialité des données

Contenu

- 1. ingénierie sociale : le maillon faible est souvent l'humain
- 1. analyse de l'attaquant et des conséquences : individu, entreprise, état
- 1. analyse de l'attaqué et des conséquences : individu, entreprise, état
- 2. sécurité sur internet : VPN, TOR, Darkweb ;
- 2. failles systèmes ;
- 2. failles d'application ;
- 2. virus (ransomware, spyware, worms, trojan...) ;
- 3. mots de passe ;
- 3. failles réseau (Dos, DDoS) ;
- 3. télécommunications : attaque Man-in-the-Middle ;
- 3. emails ;
- 3. appels téléphoniques ;
- 3. SMS ;
- 4. applications de messageries sécurisées ;
- 4. appareils mobiles ;
- 4. sécurité bancaire ;
- 4. véhicules et objets connectés ;
- 4. surveillance VS vie privée (révélations Snowden, plans de l'UE, lutte anti-terrorisme) ;

Méthodes

- Parties théoriques, vulgarisation de notions cryptographiques ;
- Parties pratiques avec prise en main des logiciels de sécurité comme des gestionnaires de mots de passe ou de chiffrements de mails ;
- Mises en pratiques collectives, en groupe, en binôme.

Modalités

Langue : Français

Public cible : Tout doctorant

Prérequis : Niveau B1 en Français minimum.

Intervenant : Frédéric HAYEK

Durée : 12 heures

Nombre maximum de participants : 20 participants

Validation : 1 module

S'inscrire via ADUM ici