Cybersécurité au quotidien : Les bons réflexes de l'agent de l'Etat

PROGRAMME DE LA FORMATION

3 heures

13 octobre 2026

9h30 – 12h30

IRA de Nantes

Gabriel TOLLAFIELD

OBJECTIFS PEDAGOGIQUES

- ✓ Identifier les menaces
- ✓ Comprendre le fonctionnement des malwares
- ✓ Appliquer l'hygiène informatique
- ✓ S'inscrire dans la stratégie nationale de cyberdéfense

PUBLICS

✓ Agents de la fonction publique d'Etat

PREREQUIS

Pas de prérequis

METHODES PEDAGOGIQUES

✓ Alternance d'exposé et d'ateliers pratiques

Phase 1 : Introduction

- **Enjeux :** Pourquoi l'Etat est-il la cible ?
- **Le coût de l'attaque** : Au-delà de l'argent, c'est la continuité du service public qui est menacée.

Phase 2 : Panorama des menaces et l'univers des Malwares

Objectif : Comprendre que l'email n'est qu'un « vecteur » et que le malware est « l'arme ».

- **Le Malware (logiciel malveillant) : L'ennemi invisible**
  - Définition
  - Typologie simplifiée
    - Le Rançongiciel (Ransomware) : Verrouillage de fichiers et demande de rançon
    - L'Espion (Spyware/Keylogger) : Enregistrement des écrits et capture d'écran à votre insu
    - L'Infostealer : vol des identifiants
  - Comment s'installe-t-il ? Via une pièce-jointe, un lien vers un site infecté, une clé USB compromise
- **L'hameçonnage (Phishing)**
  - Comment on vous incite à installer ces malwares.
- **Atelier pratique** : La chasse aux indices (Analyse de mails suspects

Phase 3 : Les bonnes pratiques et l'hygiène numérique

Objectif : Barrer la route aux malwares.

- **La gestion des accès**
  - Fin des mots de passe sur Post-it
  - Créer un mot de passe robuste
  - Gestionnaires de mots de passe validés par l'administration
  - Double authentification

- **La sécurité matérielle et logicielle**
  - Mises à jour. Permet de corriger les failles que les malwares utilisent pour entrer.
  - Clés USB
  - Télétravail : Utiliser uniquement le VPN ou matériel fourni par l'administration
  - Focus outils de l'État : Outils sécurisés à privilégier
  - En préventif et en cas de doute : https://jecliqueoupas.cyber.gouv.fr/accueil

- **Réaction en cas d'infection**
  - Signaux d'alerte
  - Le réflexe « Débrancher le réseau » : Empêcher le malware de se propager aux collègues
  - Règle d'or : Signaler une fausse alerte plutôt que cacher une vraie erreur
  - Qui contacter ?
  - La procédure d'urgence

Phase 4 : Synthèse et Conclusion Institutionnelle

- **Quiz final**
  Validation des réflexes et récapitulatif.

- **La vision de l'État**
  - Le constat de Sébastien LECORNU
  - La réponse souveraine : Plan de 200 M€, fusion DINUM/DITP pour une autorité forte.
  - Le rôle majeur de l'ANSSI
  - Mot de la fin : L'agent est le maillon fort de la nouvelle « doctrine de protection » de l'État.