V1CT0R PR0UFF
Formation

01 avril 2026

PROGRAMME DE FORMATION

Cybersécurité : Comprendre pour mieux se protéger

INFORMATIONS GÉNÉRALES

Profils des stagiaires : salarié d'entreprise ou agent de collectivité utilisant quotidiennement un ordinateur.
Prérequis : utiliser quotidiennement des outils numériques (ordinateur, smartphone, navigateur web etc.).
Durée : 12 heures - 4 modules de 2h30 à 3h30
Dates : à fixer avec le formateur / Accessibilité sous 2 semaines.
Modalité d'accès : entretien téléphonique pour connaître et analyser les besoins.
Modalités pédagogiques : formation présentielle.
Coût: devis sur-mesure en fonction du nombre d'apprenants et de la localisation.

OBJECTIFS PÉDAGOGIQUES GÉNÉRAUX

À l'issue de la formation, l'apprenant sera capable de :

- identifier les méthodes et outils des pirates informatiques ;
- reconnaître et déjouer une tentative de phishing ou d'ingénierie sociale ;
- installer, configurer et utiliser un gestionnaire de mots de passe professionnel ;
- activer la double authentification sur ses comptes professionnels critiques ;
- appliquer les bonnes pratiques de sécurité au quotidien ;
- mettre en œuvre une procédure de réaction adaptée en cas d'incident cyber.

CONTENU DE LA FORMATION

Module 1 - Comprendre les attaquants (3h30)

Objectifs pédagogiques — À l'issue de ce module, l'apprenant sera capable de :

- distinguer les deux grands types d'attaques (opportunistes et ciblées) et leurs mécanismes respectifs ;
- expliquer pourquoi les PME sont des cibles prioritaires ;
- identifier son niveau d'exposition personnelle aux risques cyber.

Contenu :

- Introduction et échanges :
  - présentation des participants : parcours, profils, niveaux d'expérience ;
  - discussion sur l'exposition individuelle et collective aux risques cyber ;
- Comprendre les méthodes des attaquants :
  - mise en situation ludique à l'aide du Serious Game "Dans la tête d'un hacker" pour appréhender les techniques et outils des attaquants et apprendre à s'en défendre.
- OSINT – Recherche sur sources ouvertes :
  - les bons usages ;
  - l'utilisation par les cybercriminels (ciblage de sous-traitants via LinkedIn, site web, documents publics) ;
  - se rechercher soi-même.

Méthodes pédagogiques :

- Serious Game "Dans la tête d'un hacker"

- Démonstration OSINT en direct
- Questions-réponses interactives

Module 2 - Phishing, ingénierie sociale et bonnes pratiques (3h30)

Objectifs pédagogiques — À l'issue de ce module, l'apprenant sera capable de :

- reconnaître les techniques de manipulation psychologique utilisées dans les attaques d'ingénierie sociale ;
- identifier les indices caractéristiques d'un mail ou SMS de phishing et adopter le bon réflexe ;
- appliquer les bonnes pratiques de sécurité au quotidien (session, données sensibles, appareils) ;
- appliquer une procédure structurée de réaction en cas d'incident.

Contenu :

- Ingénierie sociale :
  - exploitation de la psychologie humaine par les attaquants : urgence, autorité, confiance, peur ;
  - les attaques ciblant les PME industrielles : fausse urgence fournisseur, arnaque au virement, usurpation d'identité dirigeant, faux support technique ;
  - techniques pour détecter et se prémunir contre ces attaques.
- L'intelligence artificielle :
  - ce qu'elle apporte aux cybercriminels : deepfake vocal, phishing ultra-personnalisé à partir de données publiques.
- Détection des mails/SMS de phishing :
  - les 5 indices à vérifier systématiquement (expéditeur, liens, urgence, pièces jointes, demandes inhabituelles) ;
  - réactions appropriées face à un mail ou SMS de phishing.
- Les incontournables de la sécurité :
  - verrouiller sa session ;
  - mises à jour : pourquoi ne pas les reporter ;
  - séparation appareils pro/perso ;
  - clés USB inconnues et réseaux wifi non maîtrisés : pourquoi les éviter ;
- Que faire en cas d'attaque ?
  - réflexes immédiats ;
  - qui alerter ;

Pratique :

- Quiz de détection : 10 exemples (légitime ou phishing ?) — correction commentée collective.
- Mise en situation : simulation d'un scénario d'ingénierie sociale adapté au contexte industriel.

Méthodes pédagogiques :

- Exposé interactif
- Analyse collective de cas réels anonymisés
- Quiz participatif

Module 3 — Atelier pratique : Gestionnaire de mots de passe *(2h30)*

Objectifs pédagogiques — À l'issue de ce module, l'apprenant sera capable de :

- expliquer pourquoi des mots de passe faibles ou partagés exposent l'ensemble de l'entreprise ;
- installer et configurer un gestionnaire de mots de passe professionnel ;

- enregistrer et organiser ses identifiants critiques dans un coffre-fort sécurisé.

Contenu :

- Pourquoi les mots de passe actuels ne suffisent pas :
  - attaques par dictionnaire, credential stuffing, fuites de bases de données ;
  - les mots de passe partagés au sein d'une équipe : risque de compromission en cascade, traçabilité impossible ;
  - pourquoi ne pas stocker ses mots de passe dans le navigateur, un fichier Excel ou sur papier.
- Ce qu'est un mot de passe fort : longueur vs complexité, phrase de passe.
- Pourquoi choisir un gestionnaire dédié plutôt que ceux des navigateurs ou GAFAM :
  - coffre individuel + coffre partagé par équipe ou service ;
  - console d'administration : gestion centralisée des accès, désactivation en cas de départ ;

Pratique :

- Installation et configuration du gestionnaire sur poste et mobile ;
- Création du mot de passe maître et sauvegarde du code de secours ;
- Enregistrement des 5 à 10 comptes les plus critiques pendant la séance (messagerie, VPN, outils métiers) ;
- Paramétrage de l'extension navigateur.

Méthodes pédagogiques :

- Démonstration en vidéoprojection
- Manipulation en direct par chaque apprenant sur son propre poste, guidée par le formateur
- Résolution des difficultés en temps réel

Livrable remis : guide de prise en main synthétique (format PDF)

Module 4 — Atelier pratique : Double authentification *(2h30)*

Objectifs pédagogiques — À l'issue de ce module, l'apprenant sera capable de :

- expliquer pourquoi un mot de passe seul ne suffit pas à protéger un compte ;
- installer et utiliser une application d'authentification ;
- activer la double authentification sur ses comptes et accès professionnels prioritaires ;
- appliquer le principe de séparation des rôles et du moindre privilège dans son usage quotidien.

Contenu :

- Pourquoi le SMS seul ne suffit pas : SIM swapping, interception.
- Les différentes formes de 2FA : SMS, application Authenticator, clé physique (FIDO2) — avantages et usages.
- La 2FA comme bouclier même en cas de vol de mot de passe.
- Gestion des rôles et droits d'accès :
  - principe du moindre privilège : chaque collaborateur accède uniquement à ce dont il a besoin ;
  - comptes nominatifs : pourquoi les comptes partagés sont un risque ;
  - procédure de départ : révocation immédiate des accès.

Pratique :

- Installation d'une application d'authentification ;
- Activation en direct sur les comptes critiques : messagerie, VPN ;
- Sauvegarde des codes de récupération.

Méthodes pédagogiques :

- Démonstration en vidéoprojection
- Manipulation en direct par chaque apprenant sur son propre appareil, guidée par le formateur

ORGANISATION DE LA FORMATION

Déroulé sur 1,5 jour

Session	Module	Durée
1	Module 1 — Comprendre les attaquants	3h30
2	Module 2 — Phishing, ingénierie sociale, pratiques	3h30
3	Module 3 — Atelier gestionnaire de mots de passe	2h30
4	Module 4 — Atelier double authentification	2h30
Total		**12h**

> *Pour un groupe de plus de 10 participants, la formation est dupliqué en sous-groupes (10 participants maximum).*

Moyens et méthodes pédagogiques

- Salle dédiée à la formation, un poste par participant ;
- Vidéoprojection ;
- Serious Game "Dans la tête d'un hacker" — mise en situation ludique ;
- Documents supports projetés et remis aux participants ;
- Exercices pratiques sur outils réels (gestionnaire de mots de passe, application 2FA) ;
- Études de cas et exemples contextualisés ;
- Formateur expert en cybersécurité.

Dispositif d'évaluation des acquis

Moment	Modalité
Avant la formation	Questionnaire de positionnement (acquis initiaux et besoins spécifiques)
Modules 1 et 2	Questions orales, quiz participatif, mises en situation — correction commentée collective
Modules 3 et 4	Évaluation pratique : chaque apprenant installe et configure les outils sur son appareil
Fin de formation	QCM couvrant l'ensemble des modules + correction commentée

Moyens et méthodes pédagogiques :

- accueil des stagiaires dans une salle dédiée à la formation ;
- documents supports de formation projetés ;
- Serious Game, mise en situation « Dans la tête dans un hacker » ;
- approche ludique ;
- exposés théoriques ;
- formateur expert en cybersécurité.

Dispositif de suivi de l'exécution de l'évaluation des résultats de la formation :

- questions orales tout au court de la formation
- QCM à la fin de la formation ;
- mises en situation ;
- certificat de réalisation.

Livrables et attestations

Document	Remise
Attestation de présence	À l'issue de la formation
Certificat de réalisation	À l'issue de la formation

ACCESSIBILITÉ AUX PERSONNES EN SITUATION DE HANDICAP

N'hésitez pas à nous contacter. Nous analyserons avec vous la meilleure formule de formation adaptée à votre situation. Retrouvez plus d'informations sur l'accès à la formation pour les personnes en situation d'handicap sur les sites de l'Agefiph, les Cap emploi, du Fiphfp ou des MDPH.

Ce programme sera adapté en fonction des niveaux et des attentes de chaque participant. Des moyens de compensation seront mis en place pour les personnes en situation de handicap.

Contacts

Téléphone : 06 87 06 18 35
E-mail : contact-pro@victorprouff.fr