V1CT0R PR0UFF
Formation

01 avril 2026

PROGRAMME DE FORMATION

Cybersécurité : Comprendre pour mieux se protéger

INFORMATIONS GÉNÉRALES

Profils des stagiaires : Travailleur indépendant utilisant quotidiennement des outils numériques

Prérequis : utiliser quotidiennement des outils numériques — aucune compétence technique requise

Durée : 7 heures — 5 modules de 1h à 1h30 sur 5 semaines

Modalité : formation à distance (visioconférence) — 1 séance par semaine

Format : Individuel ou petit groupe (4 personnes maximum)

Accessibilité : Sous 2 semaines — entretien préalable de positionnement inclus

Modalité d'accès : Entretien téléphonique ou visio de 30 minutes pour analyser les besoins et adapter le programme

Coût : Sur devis — prise en charge OPCO possible

Date : à fixer avec le formateur / Accessibilité sous 2 semaines

OBJECTIFS PÉDAGOGIQUES GÉNÉRAUX

À l'issue de la formation, le stagiaire sera capable de :

- identifier les principales méthodes utilisées par les cybercriminels ciblant les indépendants ;
- reconnaître et déjouer une tentative de phishing ou d'ingénierie sociale ;
- installer et utiliser un gestionnaire de mots de passe pour sécuriser ses accès professionnels ;
- activer la double authentification sur ses outils et comptes critiques ;
- appliquer les bonnes pratiques de sécurité au quotidien (sauvegardes, mises à jour, partage de données) ;
- mettre en œuvre une procédure de réaction adaptée en cas d'incident.

CONTENU DE LA FORMATION

MODULE 1 — Comprendre les cyberattaques *(1h30)*

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

- distinguer les deux grands types d'attaques (opportunistes et ciblées) et leur mécanisme ;
- expliquer comment ses informations personnelles et professionnelles sont collectées et exploitées ;
- évaluer sa propre exposition aux risques dans le cadre de son activité.

Contenu :

- Tour de table : profil, outils utilisés, incidents vécus
- Le parcours d'un attaquant : de la collecte d'informations à la compromission
- Les attaques opportunistes : fuites de données, credential stuffing, campagnes de phishing de masse
- Les attaques ciblées : OSINT, ingénierie sociale, usurpation d'identité
- L'intelligence artificielle comme amplificateur d'attaques : deepfake vocal, phishing ultra-personnalisé
- Se rechercher soi-même : démonstration Have I Been Pwned et recherche OSINT basique

Méthodes pédagogiques :

- Démonstrations en direct (Have I Been Pwned, exemples d'OSINT)
- Étude de cas : scénarios d'attaques adaptés au profil d'indépendant
- Questions-réponses interactives

MODULE 2 — Phishing et ingénierie sociale *(1h30)*

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

- identifier les indices caractéristiques d'un mail ou SMS de phishing ;
- reconnaître les techniques de manipulation psychologique utilisées dans les attaques d'ingénierie sociale ;
- appliquer le réflexe de vérification avant de cliquer, répondre ou transférer une information sensible.

Contenu :

- Anatomie d'un mail de phishing : les 5 indices à vérifier systématiquement (expéditeur, liens, urgence, pièces jointes, demandes inhabituelles)
- Les attaques spécifiques aux indépendants : fausse urgence client, arnaque au faux virement, usurpation de comptable ou d'avocat, faux support technique
- Les leviers psychologiques exploités : urgence, autorité, peur, confiance — et comment y résister
- Le réflexe anti-manipulation : douter → raccrocher ou ne pas cliquer → rappeler le vrai contact → signaler

Pratique :

- Exercice de détection : analyse commentée de 4 à 6 exemples réels (mails anonymisés)
- Mise en situation : simulation d'un scénario d'ingénierie sociale adapté au profil du stagiaire

Méthodes pédagogiques :

- Analyse collective de cas réels
- Jeu de rôle / simulation en visio
- Auto-évaluation : quiz "phishing ou légitime ?"

MODULE 3 — Gestionnaire de mots de passe *(1h30)*

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

- expliquer pourquoi la réutilisation de mots de passe expose l'ensemble de ses clients et partenaires ;
- installer et configurer un gestionnaire de mots de passe adapté à un usage professionnel ;
- migrer ses identifiants critiques vers un coffre-fort numérique sécurisé.

Contenu :

- Pourquoi les mots de passe actuels ne suffisent pas : attaques par dictionnaire, réutilisation, partage non sécurisé
- Le cas des accès clients partagés : risque de compromission en cascade, responsabilité de l'indépendant
- Critères de choix d'un gestionnaire : Bitwarden (gratuit, open source, recommandé ANSSI, RGPD compatible)
- Ce qu'est un mot de passe fort : longueur vs complexité, phrase de passe

Pratique :

- Installation et configuration de Bitwarden ensemble en direct
- Création du mot de passe maître et sauvegarde du code de secours
- Migration des 5 à 10 comptes les plus critiques pendant la séance
- Paramétrage de l'extension navigateur et de l'application mobile

Méthodes pédagogiques :

- Démonstration en partage d'écran
- Manipulation en direct par le stagiaire, guidée par le formateur
- Résolution des difficultés en temps réel

Travail entre les séances : migrer progressivement tous les comptes restants

MODULE 4 — Double authentification (2FA) *(1h)*

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

- expliquer pourquoi un mot de passe seul ne suffit pas à protéger un compte ;
- installer et utiliser une application d'authentification (Authenticator) ;
- activer la double authentification sur ses outils et comptes professionnels prioritaires.

Contenu :

- Pourquoi le SMS seul ne suffit pas : SIM swapping, interception — cas réels
- Les différentes formes de 2FA : SMS, application Authenticator, clé physique (FIDO2)
- La 2FA comme bouclier même en cas de vol de mot de passe

Pratique :

- Installation de l'application Authenticator (Aegis sur Android, Raivo ou Apple Passwords sur iOS)
- Activation en direct sur les comptes critiques : messagerie professionnelle, outil de stockage cloud, accès bancaire
- Sauvegarde des codes de récupération
- Discussion : comment recommander la 2FA à ses clients comme valeur ajoutée

Méthodes pédagogiques :

- Démonstration en partage d'écran
- Manipulation en direct par le stagiaire

MODULE 5 — Sécurité au quotidien et procédure d'urgence *(1h30)*

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

- mettre en œuvre les pratiques essentielles de sécurité au quotidien (mises à jour, sauvegardes, partage sécurisé) ;
- identifier et comprendre sa responsabilité en cas d'incident impliquant des données clients ;
- appliquer une procédure structurée de réaction en cas de cyberattaque.

Contenu :

- Les incontournables : mises à jour automatiques, antivirus actif, verrouillage automatique, séparation pro/perso
- Les sauvegardes : règle 3-2-1, comment tester une sauvegarde, fréquence adaptée à l'activité
- Partage sécurisé de données sensibles : alternatives à l'email non chiffré, envoi de documents confidentiels
- Wifi public et clés USB : pourquoi éviter et quelles alternatives
- Responsabilité de l'indépendant : RGPD, accès aux données clients, assurance RC Pro cyber
- Que faire en cas d'incident : cybermalveillance.gouv.fr, CNIL (si données clients exposées), assureur

Pratique :

- Construction de la fiche procédure d'urgence personnalisée du stagiaire
- Vérification et test de la sauvegarde existante
- Évaluation finale : QCM de 15 questions couvrant l'ensemble des modules

Méthodes pédagogiques :

- Co-construction de la fiche d'urgence personnalisée
- QCM d'évaluation finale avec correction commentée

- Bilan individuel et plan d'action pour les semaines suivantes

Livrable remis : fiche procédure d'urgence personnalisée (contacts, accès de secours, étapes à suivre)

ORGANISATION PÉDAGOGIQUE

Déroulé sur 5 semaines

Semaine	Module	Durée
Semaine 1	Module 1 — Comprendre les cyberattaques	1h30
Semaine 2	Module 2 — Phishing et ingénierie sociale	1h30
Semaine 3	Module 3 — Gestionnaire de mots de passe	1h30
Semaine 4	Module 4 — Double authentification	1h
Semaine 5	Module 5 — Sécurité au quotidien et procédure d'urgence	1h30
Total		**7h**

Moyens pédagogiques

- Formation à distance par visioconférence (kMeet)
- Partage d'écran formateur pour les démonstrations
- Manipulation en direct par le stagiaire sur ses propres outils, guidée par le formateur
- Exercices pratiques sur des outils réels (Gestionnaire de mdp, 2FA, Have I Been Pwned)
- Études de cas et exemples réels adaptés au profil d'indépendant

Dispositif d'évaluation des acquis

Moment	Modalité
Avant la formation	Questionnaire de positionnement (identification des acquis initiaux et des besoins)
En cours de formation	Questions orales à chaque séance — reformulation, mise en situation
Entre les modules	Travaux pratiques entre les séances (migration des comptes, activation de la 2FA)
Fin de formation	QCM de 15 questions couvrant tous les modules + correction commentée

ACCESSIBILITÉ AUX PERSONNES EN SITUATION DE HANDICAP

La formation en visio facilite l'accès aux personnes à mobilité réduite ou ne pouvant pas se déplacer. N'hésitez pas à nous contacter avant l'inscription pour que nous puissions analyser ensemble les aménagements nécessaires à votre situation.

Retrouvez des informations complémentaires sur les sites de l'Agefiph, Cap emploi, Fiphfp et des MDPH.

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

V1CT0R PR0UFF
Formation

01 avril 2026

CONTACT ET INFORMATIONS

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

Ce programme est adapté au profil de chaque stagiaire suite à l'entretien de positionnement préalable. Le contenu peut être ajusté en fonction des niveaux, des outils utilisés et des priorités identifiées.