FORMATION - LES BASES EN CYBERSÉCURITÉ

DURÉE : 1h30 à 2h
LIEU : Dans votre entreprise ou nos locaux
PRÉREQUIS : Aucun

En 2026, 1 cyberattaque a lieu toutes les 39 secondes en France (source : ANSSI), et 90% d'entre elles débutent par un simple email de phishing. Une fuite de données coûte en moyenne 4,45 millions d'euros à une entreprise, sans compter les amendes RGPD (jusqu'à 4% du chiffre d'affaires mondial) ou la perte de confiance des clients.

Cette formation pratique et accessible permet à tous les collaborateurs – sans prérequis technique – de :

- Identifier les cybermenaces (phishing, ransomware, fuites de données).
- Appliquer les bonnes pratiques au quotidien
- Rappeler les solutions mises en place par l'entreprise
- Réagir efficacement en cas d'incident (procédures d'urgence, signalement).

Notre valeur ajoutée :

- Pédagogie active : Exercices concrets (repérage de phishing, création de mots de passe sécurisés, activation du 2FA…).
- Impact immédiat : Réduction des risques de 80% grâce à des gestes simples.
- Adaptée à tous : Dirigeants, équipes métiers, télétravailleurs…

Pour qui ?

Toutes les entreprises, quelle que soit leur taille, souhaitant :

- Sécuriser leurs données et éviter les amendes RGPD.
- Sensibiliser leurs équipes sans jargon technique.

Volcanis

MODULE	CONTENU	TEMPS
Introduction	Définitions et état de la cybersécurité	10 min
Les menaces courantes	Phishing Ransomware Fuites de données BruteForce Social engenering	20 min
Bonnes pratiques	Mot de passe	10 min
	Emails	10 min
	Wifi et connexions réseau	5 min
	Poste de travail	5 min
	Médias amovibles	10 min
Gestion des incidents	Comment réagir	20 min
Q & A		30 min

Introduction :

Rappel des chiffres : 1 attaque toutes les 39 secondes en France selon l'ANSSI en 2024.

Qu'est ce que la cybersécurité : ce sont des moyens de protection numérique.

Faire un rappel de ce qui existe déjà dans l'entreprise (FW, contrôles d'accès, antivirus, ...)

Les exigences/instances française : RGPD par exemple, ANSSI, cyber17, etc

Les menaces courantes :

Phishing :

- Définition : Il s'agit d'une technique d'usage de faux : faux email, faux site internet, faux SMS
- But : Il permet de récupérer : des identifiants de connexion, des coordonnées bancaires, des données personnelles, ...
- S'en prémunir : faire attention aux noms de domaines, adresses email, les liens, ...

Ransomware :

- Définition : Chiffrement des données et demande de rançons. Diffusé via un lien frauduleux, installation d'un logiciel, ouverture d'une PJ, ...
- But : bloquer l'activité d'une entreprise et les forcer à payer un rançon pour récupérer les données compromises.
- S'en prémunir : première analyse par l'antivirus vérifier le lien de téléchargement ou l'expéditeur, obtenir un média amovible de confiance, station blanche.

Fuite de données :

- Définition : vol ou revente de données. Dû à un vol de PC, session restée ouverte, média amovible, failles de sécurité
- But : les revendre sur des sites pirates qui peuvent ensuite servir à du phishing, revente concurrence, chantage ou rançon.
- S'en prémunir : surveiller son matériel, fermer sa session, faire attention aux médias amovibles, faire les mises à jours de sécurité, ...

BruteForce :

- Définition : essayer toutes les combinaisons de mot de passe
- But : voler des identifiants de connexion à des logiciels métiers, à des machines, la banque, ...
- S'en prémunir : avoir des mots de passes forts, si possible activer la double authentification, , 1 mot de passe par site/application, pas de mélange de mot de passe et email pro et perso,

Ingénierie sociale :

- Définition : manipulation psychologique d'une personne pour arriver à ses fins.
- But : obtenir des informations confidentielles, des accès sur des applications, planifier un vol
- S'en prémunir : identifier la source. Est-elle habilité ?

Bonnes pratiques :

- Poste de travail :
  - Verrouillage de session quand on est plus à son poste
  - Pas d'enregistrement des mots de passes dans le navigateur
- Mots de passes :
  - Utilisation d'un gestionnaire de mot de passe
  - Utilisation d'un mot de passe robuste
  - Mots de passes différents sur tous les sites
  - Ne pas utiliser les mots de passes personnels pour ses accès professionnels
  - Activer la double authetification (éviter le SMS si possible)
- Emails :
  - Ne pas utiliser sa boite email professionnelle pour des usages personnelles
  - Vérifier l'expéditeur (faire une vérification du nom de domaine / recherche Google), son nom, l'entreprise
  - Vérifier les liens hover (vérification nom de domaine / recherche Google), réputation du site
- Médias amovibles :
  - Eviter au maximum l'utilisation des médias amovibles (clés USB / disques durs)
  - Ne pas accepter de clés USB pour récupérer des documents
  - Ne pas utiliser de clés USB dont on ne connait pas la provenance (récupérés sur un salon/expo, ou ailleurs)
  - Au besoin faire une vérification sur une station blanche, à défaut passage antivirus
- Wifi et point de connexion :
  - Ne pas se connecter sur des réseaux inconnus avec ses équipements professionnels : hôtel, aéroport, gare, hotspots gratuits, ...
  - Utiliser un VPN pour se connecter aux ressources de l'entreprise

Que faire en cas d'incident :

- **AVERTIR** : Il est nécessaire dans tous les cas de contacter la personne en charge de l'informatique et lui expliquer la chronologie des événements. Signalement 17cyber
- **PHISING** : Avertir puis changer ses mots de passe. Si ce mot de passe est utilisé sur un autre site, le changer également
- **RANSOMWARE** : débrancher l'accès au réseau / couper wifi puis avertir. Ne pas payer la rançon (que ce soit dans le milieu professionnel ou personnel)
- **FUITE DE DONNÉES** : avertir les autorités (sur 17cyber) qui sauront vous expliquer la marche à suivre. Il est ensuite nécessaire, en fonction des données impactées de prévenir ses clients ou fournisseurs,

Adaptation de la formation à votre entreprise selon:

- les dispositifs et outils mis en place en matière de cybersécurité
- l'existence d'un gestionnaire de mot de passe ou d'une politique de mots de passes
- la personne a contacter en cas d'incident
- la mobilité des agents (télétravail, déplacements professionnels, voyage à l'étanger)
- l'utilisation d'un VPN pour vos connexions sécurisées

Annexe - exercices :

- Introduction : identification des risques potentiels dans l'entreprise
- Détection d'email : quizz sur la détéction d'emails frauduleux et non frauduleux
- Tests de mot de passe : test de robustesse de mot de passe des agents (sans divulgation)
- Ecriture de mot de passe sécurisé : passPhrase, utilisation de mots de passes générés aléatoirement
- Démo de clé USB / ransomware