INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

# Comprendre les cybermenaces des PME

**MODULE N°1 · LIVRET DU PARTICIPANT**

## FORMATION À LA CYBERSÉCURITÉ POUR LES PME

Cas réels · attaques courantes · DIC · mises en situation

Robert Tomczak

Université Polytechnique HAUTS-DE-FRANCE

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

# Ce que vous saurez faire à la fin du module

### 1. Comprendre

Pourquoi une PME peut intéresser des cybercriminels.

### 2. Reconnaître

Quatre types d’attaques et leurs principaux signaux d’alerte.

### 3. Mesurer

Les risques pour vos données, vos outils et votre activité.

### 4. Réagir

Trois réflexes simples face à une demande suspecte.

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

# Une attaque réelle : le centre hospitalier Sud-Francilien

## CE QUI S'EST PASSÉ

- Une cyberattaque rend une grande partie du système informatique inaccessible.
- Messagerie, pharmacie, comptabilité et équipements de laboratoire perturbés.
- Des nouveau-nés sont transférés ; les équipes réorganisent les soins.

## CONSÉQUENCES ET EXTORSION

- Rançon demandée : 10 millions de dollars.
- Des données sont aussi volées puis divulguées.
- L'impact dépasse largement la seule informatique.

**QUESTION AU GROUPE** **Comment les attaquants ont-ils pu entrer ?**

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

# Et dans une PME ? L’exemple Octave

## Octave

Éditeur de logiciels de 38 salariés touché par un rançongiciel : systèmes chiffrés et services clients en panne.

## Lyophilise & Co

Client de 20 salariés à Lorient : activité paralysée, près de 20 000 € perdus par jour.

**La suite :** Un nouveau site en quatre jours pour le client. Octave : redressement judiciaire (nov. 2024), puis liquidation (mars 2025).

**QUESTION AU GROUPE** **Qu’aurions-nous à perdre si nos outils ne fonctionnaient plus ?**

# Pourquoi les PME intéressent les attaquants

### Attaques opportunistes

Une campagne massive peut toucher une PME sans qu'elle ait été choisie personnellement.

### Relations commerciales

L'accès à une PME peut servir à atteindre ses clients, fournisseurs et partenaires.

### Moyens limités

Pas toujours d'équipe dédiée, de sauvegardes testées ou de règles d'accès formalisées.

**453 900 crimes et délits liés au numérique enregistrés en France en 2025 (périmètre large).**

# 1. Des attaques massives et automatisées

## UN SCÉNARIO CLASSIQUE

- Un escroc envoie 50 000 faux courriels de livraison.
- Les destinataires sont invités à saisir leurs identifiants professionnels.
- L’attaquant ne connaît pas forcément les entreprises destinataires.
- Un seul compte compromis peut suffire à ouvrir une porte.

**QUESTION AU GROUPE** **Faut-il que l’attaquant connaisse votre entreprise ?**

# 2. Le risque de la chaîne d’approvisionnement

**VOTRE PME EST CONNECTÉE AUX AUTRES**

- Échanges de courriels, de factures, de fichiers et d’accès informatiques.
- Un prestataire compromis peut mettre en danger son client ; l’inverse est également possible.
- Solware (2021) : données de 1 500 garages clients chiffrées après une attaque du fournisseur.

**NIS 2 :** en novembre 2026, transposition française encore en cours selon le livret ; des exigences peuvent déjà venir des clients par contrat.

# 3. Des protections parfois incomplètes

## SIX VULNÉRABILITÉS POSSIBLES

- Logiciels non mis à jour
- Mots de passe partagés
- Sauvegardes jamais testées
- Absence de double authentification
- Accès conservés par d’anciens salariés
- Pas de procédure en cas d’incident

## À RETENIR

La cybersécurité commence par l’organisation, les protections adaptées et des habitudes simples appliquées régulièrement.

# Que recherchent les cybercriminels ?

## L’argent

Rançon, fausse facture, détournement de virement.

## Les données

Plans industriels, recettes, fichiers clients, informations commerciales.

## La pression sur l’activité

Production bloquée, système de facturation inaccessible.

## La nuisance

Sabotage, dégradation de la réputation, perturbation du fonctionnement.

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

# Quelques chiffres sur les TPE-PME

**16 %**

Un incident déclaré sur 12 mois

**43 %**

Des entreprises touchées : hameçonnage cité

**49 %**

Des petites entreprises non préparées

**26 %**

Utilisent la double authentification

**+170 %**

Demandes d’aide pour fraude au virement en 2025

# Qui peut attaquer une PME ?

| Profil | Motivation principale |
|---|---|
| **Organisation criminelle** | Argent à grande échelle ; systèmes d'affiliés |
| **Personne interne ou ex-salariée** | Conflit, vengeance ou récupération de données |
| **Amateur** | Test d'outils d'attaque facilement accessibles |
| **Activiste** | Faire passer un message ou nuire à une image |
| **État espion** | Renseignement stratégique, savoir-faire |
| **Mercenaire** | Attaquer pour le compte d'un tiers |

**Réflexe : gérer les droits d'accès de tous, notamment lors des départs.**

# Mini-cas : une PME de mécanique

## Entreprise de 15 salariés

- Plans techniques pour ses clients
- Fichiers clients et logiciel de gestion commerciale
- Machines indispensables à la fabrication

**QUESTION AU GROUPE** **Quels sont les risques encourus par cette PME ?**

# Les quatre attaques à connaître

**01** **Rançongiciel**

Chiffrement et blocage des systèmes.

**02** **Hameçonnage**

Faux message, vol d’identifiants ou piège.

**03** **Fraude financière**

Faux dirigeant, faux fournisseur ou RIB.

**04** **Fuite de données**

Copie ou divulgation d’informations.

# Le rançongiciel : comment ça marche ?

## LE MÉCANISME

- Un programme malveillant chiffre les fichiers ou bloque les systèmes.
- L'attaquant demande une rançon pour la récupération.
- Il peut aussi menacer de divulguer des données volées.

## LES PORTES D'ENTRÉE

- Compte ou mot de passe compromis
- Accès distant insuffisamment protégé
- Logiciel vulnérable
- Pièce jointe ou fichier malveillant

**Payer ne garantit ni la récupération des fichiers ni leur confidentialité.**

# Cas réel : Fondouest (2024)

## 1er FÉVRIER 2024

- Pièce jointe d'un courriel ouverte par un salarié, d'après le prestataire informatique.
- Huit serveurs, deux tiers des postes et la téléphonie hors service.
- Des imprimantes diffusent une demande de rançon.

## LA SUITE

- L'entreprise ne paie pas.
- Sauvegardes intactes : redémarrage après quatre jours.
- Quinze jours de fonctionnement dégradé.
- Pertes estimées : ≈ 105 000 € au total.

**QUESTION AU GROUPE** **Votre entreprise pourrait-elle tenir quatre jours sans serveurs ni téléphonie ?**

BUREAU D'ÉTUDES GÉOTECHNIQUES • ≈ 60 SALARIÉS

# Rançongiciel : trois conséquences à anticiper

### Indisponibilité

Plus de devis, de facturation, de production ou de réponses aux clients.

### Coût de reprise

Arrêt de l'activité, intervention de prestataires, reconstruction des systèmes.

### Perte de données

Possibilité d'exfiltration et de publication de documents confidentiels.

**La sauvegarde ne suffit pas : il faut aussi tester sa restauration.**

# L’hameçonnage ou phishing

## DÉFINITION

- Un attaquant se fait passer pour une personne ou un service légitime.
- Le piège peut arriver par courriel, SMS, appel, messagerie ou faux site.
- Objectifs : obtenir des identifiants, provoquer un paiement ou installer un logiciel malveillant.

**Attention :** un message frauduleux peut être bien rédigé et venir d’un vrai compte piraté.

# Phishing : un faux message Microsoft 365

**« Votre mot de passe Microsoft 365 expire aujourd'hui. Pour éviter la suspension de votre compte professionnel, veuillez confirmer immédiatement vos identifiants. »**

## CE QUE L'ATTAQUANT CHERCHE À FAIRE

- Faire cliquer sur un bouton « Vérifier mon compte ».
- Afficher une fausse page d'authentification.
- Récupérer le mot de passe, puis accéder à la messagerie.

# Phishing : quels signaux observer ?

### Urgence

« Votre compte sera suspendu aujourd’hui ».

### Pression

Demande de secret, menace ou autorité inhabituelle.

### Lien trompeur

Le domaine n’est pas exactement celui attendu.

### Vérification indépendante

Se connecter par le site habituel, jamais par le lien du message.

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

# Cas réel : André Laurent (2023)

## L'INCIDENT

- Une salariée ouvre un courriel frauduleux.
- Le cybercriminel récupère son carnet d'adresses professionnel.
- Il envoie de fausses factures à une quinzaine de clients.

## LA DIMENSION COMMERCIALE

- L'entreprise devient malgré elle un point de départ pour escroquer ses clients.
- Il faut réagir vite et alerter chaque destinataire.

**QUESTION AU GROUPE** **Comment prévenir quinze clients qu'une fausse facture circule à votre nom ?**

# La fraude au président

## LE PRINCIPE

- Le fraudeur usurpe l'identité du dirigeant ou d'un responsable.
- Il demande un virement urgent, confidentiel et inhabituel.
- Il joue sur l'autorité hiérarchique et la pression temporelle.

## EXEMPLE DE MESSAGE

*« Nous devons effectuer aujourd'hui un virement confidentiel de 18 500 €. Merci de ne pas en parler. »*

**QUESTION AU GROUPE** **Que doit faire la comptable avant de payer ?**

# Cas réel : BRM Mobilier (2015–2016)

**1,6 M€**

Montant des virements frauduleux obtenus en quelques semaines

**UNE USURPATION DU PDG**

- Fabricant de mobilier pour bibliothèques à Bressuire ; 44 salariés.
- Des escrocs adressent à la comptable des demandes très confidentielles.
- Virements vers l'Asie durant l'été 2015.

**Conséquence : redressement judiciaire en septembre 2015, liquidation en janvier 2016.**

# La fraude au faux fournisseur

## LE SCÉNARIO

- Une facture habituelle arrive avec un « nouveau RIB ».
- Le courriel reprend le logo et parfois le fil de discussion du fournisseur.
- La comptabilité modifie les coordonnées et paie l'escroc.

## LE BON RÉFLEXE

- Vérifier chaque changement de RIB par un canal connu à l'avance.
- Appeler un numéro déjà enregistré, pas celui du message.
- Prévoir une double validation des coordonnées bancaires.

**QUESTION AU GROUPE** **Un fournisseur annonce un nouveau RIB : que vérifiez-vous ?**

# Fraude financière : ce qu’il faut retenir

### Signaux

Virement inhabituel, urgence, secret, nouveau RIB, impossibilité de rappeler.

### Dommages

L’argent part sur un compte contrôlé par l’escroc ; le récupérer peut être difficile.

### Protection

Vérification indépendante + validation des changements bancaires.

**En cas de transfert frauduleux : avertir la banque immédiatement.**

# Le vol et la fuite de données

## LES DONNÉES VISÉES

- Fichiers clients et fournisseurs
- Données bancaires et informations RH
- Contrats, devis, plans de fabrication
- Recettes, produits et procédés industriels

## CONSÉQUENCES POSSIBLES

- Perte de confiance et atteinte à la réputation
- Fraudes ciblées visant les clients
- Perte d'un avantage commercial
- Obligations légales en cas de données personnelles

# Cas réel : Le Slip Français (2024)

## Données dérobées

Noms, coordonnées et, pour certains clients, numéros de commande.

## Données non concernées

Selon le communiqué : mots de passe et données de carte bancaire.

**Réaction de l'entreprise :** information des clients, dépôt de plainte et signalement à la CNIL.

**QUESTION AU GROUPE** **Pourquoi des coordonnées seules peuvent-elles intéresser un fraudeur ?**

# Données personnelles : obligations RGPD

**UNE VIOLATION DOIT ÊTRE ÉVALUÉE**

- Documenter l'incident et mesurer les risques pour les personnes.
- Notifier la CNIL si la violation présente un risque pour leurs droits et libertés.
- Faire la notification, si possible, dans les 72 heures suivant la prise de connaissance.
- Informer aussi les personnes en cas de risque élevé.

**Toutes les fuites de données ne nécessitent pas automatiquement une notification à la CNIL.**

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

# Une attaque, étape par étape

| Étape | Ce que fait l'attaquant | Où casser la chaîne |
|---|---|---|
| **1. Repérage** | Identifie l'acheteur et le fournisseur | Limiter les informations exposées |
| **2. Préparation** | Crée une adresse ressemblante | Vigilance sur l'expéditeur |
| **3. Envoi** | Annonce un nouveau RIB par courriel | Appel au numéro connu |
| **4. Exploitation** | Fait modifier le RIB dans le logiciel | Double validation |
| **5–6. Suivi** | Relance, surveille les paiements | Contrôle des anomalies |
| **7. Action** | Deux factures vers le mauvais compte | Signalement immédiat à la banque |

# Mesurer les dégâts : le modèle DIC

**D**

## Disponibilité

Puis-je encore travailler ?

**I**

## Intégrité

Puis-je encore faire confiance à mes données ?

**C**

## Confidentialité

Qui peut voir mes informations ?

# D : Disponibilité : puis-je travailler ?

**EXEMPLE : FONDOUEST**

- Huit serveurs sont bloqués après un rançongiciel.
- Les fichiers sont devenus inaccessibles : devis, production et facturation perturbés.
- Même sans suppression de données, l'activité ne peut plus fonctionner normalement.

**La disponibilité est indispensable à la continuité de l'activité.**

# I : Intégrité : puis-je faire confiance ?

**EXEMPLE : BOUTIQUE-RHUM.COM (MAI 2023)**

- Un pirate remplace l'IBAN sur la page de paiement du site.
- Le site reste accessible et les clients continuent de commander.
- Mais les virements sont dirigés vers le compte de l'attaquant.
- Un robot de surveillance finit par signaler l'anomalie.

**Une information modifiée sans autorisation = atteinte à l'intégrité.**

# C : Confidentialité : qui accède aux données ?

**EXEMPLE : LE SLIP FRANÇAIS**

- Des attaquants copient des informations sur des clients.
- Les fichiers d’origine peuvent rester présents, intacts et accessibles.
- Pourtant, des tiers non autorisés disposent désormais des données.

**Une copie non autorisée suffit à porter atteinte à la confidentialité.**

# DIC : une même attaque peut toucher plusieurs critères

| Critère | Question simple | Exemple |
|---|---|---|
| **Disponibilité** | Puis-je travailler ? | Serveur chiffré, activité bloquée |
| **Intégrité** | Puis-je me fier aux données ? | RIB modifié dans une facture |
| **Confidentialité** | Qui peut accéder aux données ? | Plans industriels volés |

**Exemple :** un rançongiciel qui chiffre ET vole des fichiers touche la disponibilité ET la confidentialité.

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

# Atelier : votre PME face à une cyberattaque

| 03 MIN | 07 MIN | 08 MIN | 02 MIN |
|---|---|---|---|
| Lecture du scénario | Analyse en groupe | Restitution et correction | Synthèse |

**Objectif : reconnaître l'incident, identifier les conséquences et proposer les premières mesures.**

20 MINUTES • TRAVAIL EN TROIS GROUPES

INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

# Scénario A : Une entreprise paralysée

Une entreprise industrielle de 20 salariés ne peut plus accéder aux dossiers de fabrication, devis et factures. Un message réclame une rançon. La dernière sauvegarde vérifiée date de plusieurs semaines.

## QUESTIONS À TRAITER

1. Quel type d'attaque ?
2. Quels éléments sont concernés ?
3. Quels critères DIC ?
4. Quelles conséquences ?
5. Quelles premières actions ?

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

# Scénario B : Un virement détourné

Une PME reçoit un courriel de son fournisseur habituel annonçant un nouveau RIB. Une facture de 12 000 € est réglée. Trois jours plus tard, le vrai fournisseur réclame son paiement : il n'a jamais changé de banque.

## QUESTIONS À TRAITER

1. Quel type de fraude ?
2. Quelle information a été falsifiée ?
3. Quel critère DIC ?
4. Quelles conséquences possibles ?
5. Quelle vérification aurait évité le risque ?

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

# Scénario C : Un fichier clients accessible

Un tableau contenant noms, courriels, téléphones et historiques de commandes est accessible sur Internet par un lien de partage sans authentification. Ce lien circule depuis plusieurs jours.

## QUESTIONS À TRAITER

1. Quel type d'incident ?
2. Quelles données sont exposées ?
3. Quel critère DIC surtout ?
4. Quelles conséquences ?
5. Que faire après la découverte ?

# Atelier : mise en commun

## A — Rançongiciel

Disponibilité d’abord. Isoler les systèmes touchés, alerter, préserver les preuves, organiser la reprise.

## B — Faux fournisseur

Intégrité du RIB. Alerter la banque immédiatement et vérifier le fournisseur par un contact indépendant.

## C — Partage public

Confidentialité. Fermer l’accès, documenter la fuite, évaluer le risque RGPD et notifier si requis.

# Ce qu’il faut retenir

## LES QUATRE MENACES

- Rançongiciel
- Hameçonnage
- Fraude au président ou au fournisseur
- Vol et fuite de données

## LES TROIS QUESTIONS DIC

- Puis-je encore travailler ?
- Mes informations sont-elles fiables ?
- Qui peut y accéder ?

**Face à une demande inhabituelle : je doute · je vérifie · je signale.**

# Dernière question pour votre entreprise

**Quel est l’élément numérique dont la perte ou l’indisponibilité mettrait aujourd’hui votre activité en difficulté ?**

Votre réponse servira à prioriser les protections dans les prochains modules.

# Fiche réflexe : « J’ai cliqué, chef ! »

| Ce qui s’est passé | Ce que je fais immédiatement |
|---|---|
| **J’ai cliqué sur un lien** | Je ferme la page et je préviens. |
| **J’ai saisi un mot de passe** | Je le change depuis un autre appareil et je préviens. |
| **J’ai ouvert un fichier malveillant** | J’isole l’appareil du réseau sans l’éteindre et j’alerte. |
| **J’ai donné des informations ou payé** | J’alerte la direction ; j’appelle la banque en urgence si virement. |

**Un signalement rapide facilite la réaction. L’erreur cachée peut coûter très cher.**

# Les trois réflexes essentiels

**1**

## JE DOUTE

Urgence, secret, autorité inhabituelle : je m’arrête.

**2**

## JE VÉRIFIE

Je rappelle au numéro déjà connu, pas à celui du message.

**3**

## JE SIGNALE

Je préviens aussitôt la personne désignée, même en cas de simple doute.

# En cas d’incident : qui prévenir ?

| Situation | Contact / premier réflexe |
|---|---|
| **Cyberattaque suspectée** | 17cyber.gouv.fr (service public, 24h/24 et 7j/7) |
| **Besoin technique** | Prestataire via Cybermalveillance.gouv.fr |
| **Virement frauduleux** | Banque immédiatement, puis plainte |
| **Données personnelles exposées** | Évaluation RGPD ; CNIL sous 72 h si notification requise |
| **Cyber-assurance** | Contacter l’assureur rapidement et vérifier son contrat |

# Les gestes qui évitent d’aggraver l’incident

## ALERTER VITE

Prévenir les personnes compétentes et conserver les informations utiles.

## ISOLER

Débrancher du réseau les machines touchées, sans les éteindre si possible.

## DOCUMENTER

Noter l’heure, les messages et les événements observés.

## DEMANDER CONSEIL

Ne pas payer une rançon sans être accompagné et vérifier les obligations applicables.

# Sources et ressources

- ANSSI : État de la menace informatique dans le secteur de la santé (2024) : attaque du centre hospitalier Sud-Francilien.
- ARS Île-de-France : Table ronde « PUI, faire face à une cyberattaque » (2023) : pharmacie de l'hôpital.
- LeMagIT : Centre hospitalier Sud-Francilien : ce que dit l'autopsie de la cyberattaque (2022) : mode d'entrée des attaquants.
- Cas Octave et Lyophilise & Co : Clubic (2025) ; Le Journal des Entreprises (2024).
- Cas Solware : Journal Auto (2022).
- Cas Fondouest : CCI France (2024) ; Ouest-France (2024).
- Cas André Laurent : Le Parisien (2024).
- Cas BRM Mobilier : ICI, ex-France Bleu (2016) ; cour d'appel de Poitiers (2025).

# Sources et références — suite


- Cas Le Slip Français : communiqué de l'entreprise (2024).
- Cas Boutique-rhum.com : Clubic, d'après Le Parisien (2024).
- Cybermalveillance.gouv.fr : Baromètre TPE-PME 2025 : incidents, préparation, double authentification et hameçonnage.
- Cybermalveillance.gouv.fr : Rapport d'activité 2025 : fraude au virement et tendances.
- Ministère de l'Intérieur : Bilan statistique 2025 : chiffres révisés des infractions numériques.
- CNIL : Notification des violations de données personnelles : obligations RGPD.
- ANSSI : NIS 2 et préparation des organisations : périmètre et situation réglementaire.

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

# Merci de votre attention

**Je doute. Je vérifie par un autre canal. Je signale.**