Université de Bordeaux

Rapport de sensibilisation à la cybersécurité

Cybersécurité : comment se protéger au quotidien ?

Comprendre les menaces, leurs conséquences et les bons réflexes

Rapport destiné à un public non spécialiste

Objectif : expliquer simplement la cybersécurité, illustrer des attaques courantes et proposer des mesures concrètes de protection du quotidien.

Participants :

DIAZ Lucas

MAYSOUETE Justin

Année universitaire : 2025–2026

Soutenance : avril 2026

Résumé

La cybersécurité est devenue une question de la vie quotidienne. Nous utilisons tous des services numériques pour communiquer, payer, stocker des documents, travailler, étudier, effectuer des démarches administratives ou partager des contenus. Cette dépendance croissante rend nos appareils, nos comptes et nos données plus précieux, donc plus attractifs pour les attaquants. Or les cyberattaques ne concernent pas uniquement les grandes entreprises : un particulier peut lui aussi perdre l'accès à sa messagerie, voir ses données bancaires compromises, être victime d'usurpation d'identité ou subir le blocage de ses fichiers par un rançongiciel.

Ce rapport vise à présenter de <d façon claire et pédagogique les bases de la cybersécurité, ses objectifs fondamentaux, les principaux types d'attaques, leurs conséquences et les gestes à adopter pour réduire les risques. Il insiste sur un point central : il n'est pas nécessaire d'être informaticien pour mieux se protéger. Une grande partie des menaces les plus courantes peut déjà être freinée par des mesures simples : mots de passe robustes et uniques, double authentification, mises à jour régulières, sauvegardes, vérification des liens et prudence face aux messages alarmants ou trop pressants [14, 3, 12].

Le rapport contient également un exemple complet de cyberattaque, rédigé sous forme de scénario réaliste et accompagné de schémas. Le but est de montrer comment une attaque peut réussir non pas grâce à une technique spectaculaire, mais à cause d'un enchaînement de petites faiblesses : confiance, précipitation, réutilisation de mot de passe et absence de seconde barrière de sécurité [9, 15].

Mots-clés

— **Cybersécurité** : ensemble des pratiques, méthodes et outils destinés à protéger systèmes, réseaux, services et données numériques.
— **Phishing / hameçonnage** : technique consistant à tromper la victime pour lui faire révéler des informations ou réaliser une action dangereuse [9].
— **Malware** : logiciel malveillant ayant pour but de nuire, bloquer, espionner ou voler des données [16].
— **Rançongiciel** : malware qui bloque ou chiffre des fichiers afin d'exiger une rançon [13].
— **2FA / MFA** : authentification renforcée ajoutant une seconde preuve après le mot de passe [12].
— **Sauvegarde 3-2-1** : stratégie consistant à conserver trois copies sur deux supports différents dont une hors ligne [4].

Table des matières

1 Introduction : pourquoi la cybersécurité est devenue un sujet de tous les jours

1.1 L'arrivée de la menace

La menace informatique n'est pas nouvelle. Dès les débuts de l'informatique, les chercheurs ont compris qu'un programme pouvait, en théorie puis en pratique, se reproduire, se déplacer et perturber d'autres machines. IBM rappelle que l'histoire des logiciels malveillants remonte aux années 1960 sur le plan conceptuel, avant de prendre de l'ampleur avec l'évolution des réseaux et d'Internet [16]. Cette ancienneté est importante : elle montre que la cybersécurité n'est pas un effet de mode. Dès que des systèmes stockent des informations de valeur et communiquent entre eux, des personnes cherchent à détourner ces fonctions pour espionner, voler, saboter ou extorquer.

Avec la généralisation du numérique, l'échelle a changé. Les attaques qui relevaient autrefois de l'expérimentation ou de l'exploit technique se sont transformées en phénomènes industriels : campagnes massives de phishing, revente d'identifiants volés, rançongiciels, escroqueries bancaires, faux supports, usurpations d'identité, compromissions de comptes en ligne et exploitation de failles logicielles [15, 8]. Le sujet dépasse donc très largement le cadre des spécialistes.

1.2 Pourquoi cela concerne maintenant tout le monde

Aujourd'hui, la majorité des usages quotidiens passent par des outils numériques : messagerie, comptes bancaires, dossiers administratifs, achats en ligne, stockage de documents, réseaux sociaux, services de santé, cours et plateformes universitaires. La conséquence est simple : chaque personne transporte une part de sa vie sur un téléphone, un ordinateur ou dans des comptes accessibles à distance.

Cela signifie qu'une attaque numérique peut produire des effets très concrets : perte d'argent, blocage administratif, divulgation de messages privés, disparition de travaux importants, indisponibilité d'un compte essentiel, ou détérioration de l'image d'une personne ou d'une organisation. Le numérique n'est donc pas séparé du réel ; il en est devenu une composante directe [14, 6].

1.3 Cadre légal et prise de conscience collective

La société a progressivement reconnu la gravité de ces risques. En France, le Code pénal sanctionne l'accès frauduleux ou le maintien frauduleux dans un système de traitement automatisé de données, ainsi que l'entrave à son fonctionnement [20, 21]. À l'échelle européenne, la directive NIS 2 renforce le cadre commun de cybersécurité pour de nombreux secteurs critiques et essentiels [22]. Cette évolution juridique montre que le sujet n'est pas

uniquement technique. Il relève aussi de la protection des personnes, des organisations et de la confiance collective dans le numérique.

1.4 Problématique et objectif

Problématique : comment un utilisateur courant peut-il se protéger efficacement au quotidien face aux menaces numériques sans être un professionnel de l'informatique ?

Objectif : présenter une vision claire, structurée et accessible de la cybersécurité, expliquer les attaques les plus courantes et proposer des gestes simples à forte efficacité.

2 Comprendre la cybersécurité

2.1 Définition générale

La cybersécurité désigne l'ensemble des moyens destinés à protéger les systèmes, les réseaux, les données et les services numériques. Elle concerne donc à la fois :

- les appareils : ordinateurs, smartphones, serveurs, tablettes ;
- les réseaux : Wi-Fi, Internet, services de communication ;
- les données : documents, identifiants, photos, messages, informations personnelles ;
- les comptes et services : messagerie, banque, plateformes administratives, outils professionnels ou universitaires.

La cybersécurité n'est pas juste un antivirus. C'est un ensemble de pratiques techniques et humaines : configuration, mises à jour, mots de passe, sauvegardes, surveillance, organisation, réaction en cas d'incident, et formation des utilisateurs [14, 3].

2.2 Un processus permanent plutôt qu'un produit

Une erreur fréquente consiste à croire qu'un seul outil suffit à être protégé. En réalité, la cybersécurité ressemble davantage à l'hygiène ou à la sécurité routière qu'à un objet magique. Un appareil à jour mais avec un mot de passe réutilisé partout reste fragile. Une machine très bien configurée peut être compromise si son utilisateur donne lui-même son code à un faux support ou clique sur un faux lien. La sécurité repose donc sur la combinaison de plusieurs couches : des outils, des habitudes, des règles et une capacité à réagir.

2.3 Les objectifs fondamentaux : le triptyque CIA

La cybersécurité est souvent présentée à l'aide du triptyque **CIA** : **Confidentialité**, **Intégrité**, **Disponibilité**. Il s'agit d'un cadre simple et très utile pour comprendre ce que l'on cherche à protéger.

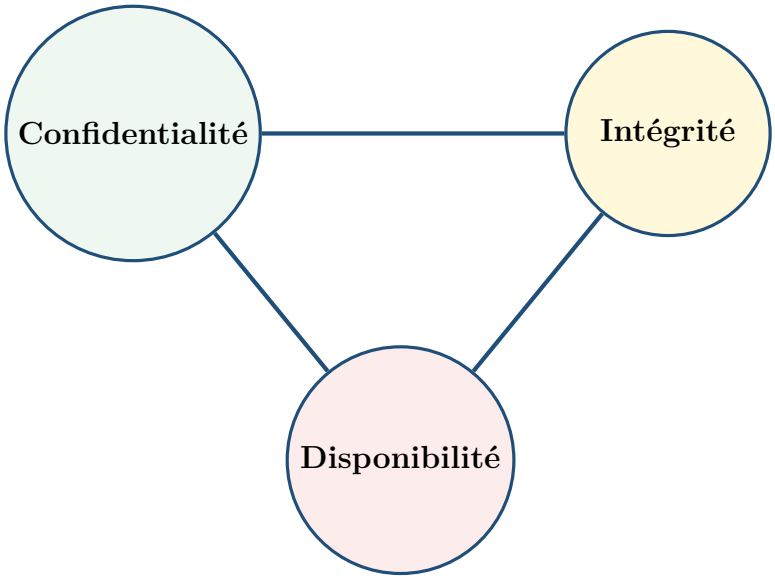

FIGURE 1 – Le triptyque CIA : trois objectifs fondamentaux de la cybersécurité.

2.3.1 Confidentialité

La confidentialité signifie que seules les personnes autorisées doivent pouvoir accéder à une donnée. L'exemple le plus évident est celui d'une boîte mail ou d'un compte bancaire : si un tiers non autorisé lit les messages ou accède aux opérations, la confidentialité est rompue. Les mesures associées sont notamment les mots de passe, l'authentification forte, le chiffrement et la limitation des droits d'accès.

2.3.2 Intégrité

L'intégrité signifie que l'information ne doit pas être modifiée de manière non autorisée. Une donnée fausse peut être aussi problématique qu'une donnée volée : faux RIB sur une facture, altération d'un document, modification d'une note, changement d'une configuration ou d'une information de profil. Les sauvegardes, les journaux d'activité, l'historique des versions et certains mécanismes de contrôle contribuent à préserver l'intégrité.

2.3.3 Disponibilité

La disponibilité signifie que les ressources doivent rester accessibles au bon moment. Un site inaccessible, un compte bloqué, un service saturé par une attaque DDoS ou des fichiers chiffrés par un rançongiciel posent tous un problème de disponibilité [19, 13]. Cette dimension rappelle que la cybersécurité ne sert pas uniquement à empêcher le vol ; elle sert aussi à garantir la continuité d'usage.

2.4 Les quatre piliers d'une approche simple

Le site cyber.gouv.fr propose de structurer les mesures de sécurité autour de quatre piliers : **gouvernance**, **protection**, **défense** et **résilience** [1]. Cette grille a l'avantage d'être compréhensible par un non-spécialiste tout en restant pertinente.

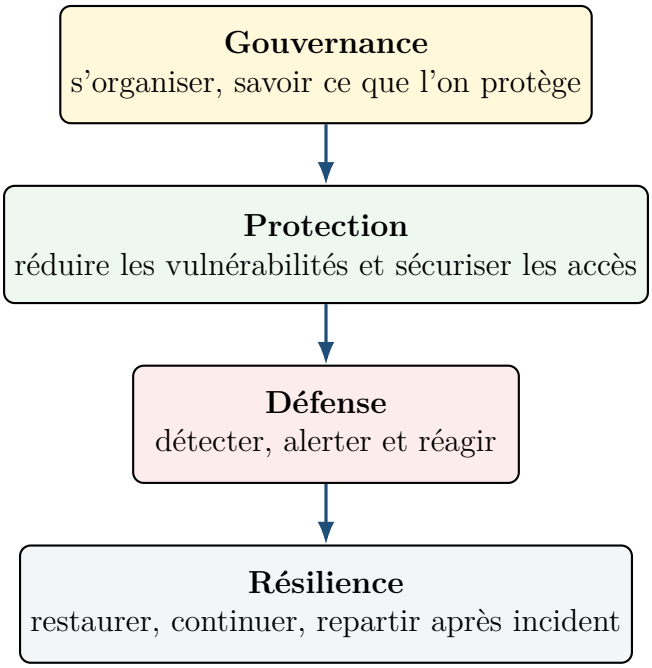

FIGURE 2 – Quatre piliers pour structurer simplement la cybersécurité.

2.4.1 Gouvernance

Même pour un particulier, la gouvernance a du sens. Elle consiste à savoir quels comptes on possède, quels appareils on utilise, quelles données sont importantes, et où elles se trouvent. Sans cette vision d'ensemble, la sécurité devient improvisée.

2.4.2 Protection

La protection correspond aux mesures qui réduisent les risques avant l'incident : mises à jour, mots de passe robustes, double authentification, verrouillage des appareils, téléchargement depuis des sources fiables, précaution sur le Wi-Fi, chiffrement quand il est disponible.

2.4.3 Défense

La défense consiste à détecter qu'un problème est en cours : alerte de connexion inhabituelle, activité anormale sur un compte, ralentissement anormal d'un appareil, demande de validation inattendue, message suspect, ou comportement étrange d'une application.

2.4.4 Résilience

La résilience est la capacité à se relever après l'incident. Pour un particulier, cela repose surtout sur les sauvegardes, la récupération des comptes, la possibilité de réinstaller proprement un appareil et l'existence de solutions de secours [2, 4].

2.5 Les grands domaines cachés derrière un seul mot

Quand on parle de cybersécurité, on parle en réalité de plusieurs spécialités : sécurité système, sécurité réseau, sécurité web, cryptographie, audit, forensic, réponse à incident. Cette diversité est importante car elle montre qu'une personne peut être bien protégée sur un aspect et fragile sur un autre. Un site peut être techniquement solide mais ses utilisateurs peuvent être ciblés par phishing. Inversement, un utilisateur prudent peut être affecté par une faille d'un service tiers. La cybersécurité doit donc être pensée comme un ensemble, pas comme un point isolé.

2.6 Pourquoi cela concerne tout le monde

Beaucoup d'attaques cherchent simplement le chemin le plus facile. L'attaquant n'a pas besoin d'une technique très rare si la victime réutilise le même mot de passe, clique dans l'urgence ou ne sauvegarde jamais ses documents. C'est pourquoi les gestes de base ont une valeur stratégique : ils ferment les portes les plus simples à exploiter [11, 6].

Table 1 – Quelques idées reçues fréquentes.

Idée reçue	**Pourquoi elle est fausse ou incomplète**
Je ne suis pas une cible intéressante.	Un compte mail, un accès bancaire, des documents d'identité ou de simples informations personnelles ont déjà une valeur.
Un antivirus suffit.	L'antivirus est utile, mais ne protège ni contre toutes les arnaques, ni contre la réutilisation de mots de passe, ni contre la manipulation psychologique.
Les cyberattaques sont trop techniques pour moi.	Beaucoup d'attaques réussissent justement parce qu'elles s'appuient sur des gestes ordinaires : cliquer, saisir un mot de passe, payer, rappeler un numéro.
La cybersécurité concerne surtout les entreprises.	Les particuliers sont ciblés pour l'argent, les identifiants, les données personnelles et la confiance qu'ils représentent auprès d'autres personnes.

3 Quels sont les types de cyberattaques ?

Cette partie présente les principales familles d'attaques, avec une logique volontairement pédagogique : que cherche l'attaquant, comment procède-t-il, qu'observe la victime et quels sont les impacts les plus courants ?

3.1 L'ingénierie sociale : attaquer la personne plutôt que la machine

L'ingénierie sociale consiste à contourner la sécurité technique en manipulant l'utilisateur. L'attaquant joue sur l'urgence, la peur, la confiance, l'habitude ou l'autorité. Cette famille d'attaques est centrale car elle touche directement le grand public.

3.1.1 Le phishing ou hameçonnage

Le phishing imite un tiers de confiance : banque, administration, université, plateforme de livraison, réseau social, opérateur, support technique. Le but est de faire cliquer sur un lien, saisir des identifiants, transmettre un code, ou télécharger un document piégé. Les messages jouent souvent sur la pression temporelle : compte suspendu, paiement refusé, colis bloqué, quota dépassé, dossier incomplet [9].

3.1.2 Le smishing et le vishing

Le **smishing** applique la même logique par SMS ; le **vishing** par téléphone. Dans les deux cas, la communication paraît plus directe, donc parfois plus crédible. La victime a moins de temps pour analyser calmement la situation.

3.1.3 Le faux support technique

Le faux support annonce un problème grave : virus détecté, compte compromis, abonnement suspendu, anomalie sur l'ordinateur ou besoin de validation urgente. L'objectif est de faire paniquer la victime pour qu'elle paie, qu'elle fournisse des codes ou qu'elle installe un outil de prise en main à distance.

3.1.4 Le quishing

Le quishing est un phishing passant par un QR code. L'utilisateur scanne souvent sans lire immédiatement le lien complet, ce qui diminue sa vigilance. Cette technique a gagné en visibilité avec les faux QR codes collés sur des affiches, des menus, des bornes ou des documents imprimés [10].

3.2 Les logiciels malveillants : infecter l'appareil

Le mot **malware** recouvre différents logiciels malveillants : certains espionnent, d'autres volent, d'autres bloquent, d'autres utilisent la machine à l'insu de l'utilisateur [16].

3.2.1 Virus et vers

Le virus se propage en général via un fichier ou une action de l'utilisateur. Le ver, lui, peut se diffuser plus automatiquement via un réseau ou une faille. Cette différence est importante car elle explique pourquoi certaines infections se propagent très rapidement dans un environnement mal protégé.

3.2.2 Cheval de Troie

Le cheval de Troie se présente comme un programme utile ou anodin, alors qu'il exécute une action cachée. Pour le grand public, c'est une image simple et parlante : l'utilisateur installe lui-même ce qu'il croit être un outil légitime, alors qu'il introduit un programme malveillant.

3.2.3 Spyware, keylogger, infostealer

Ces programmes servent à espionner. Le spyware collecte des informations sur l'activité, le keylogger enregistre les frappes clavier et l'infostealer tente de récupérer identifiants, cookies, mots de passe enregistrés ou documents. Ils sont particulièrement dangereux parce qu'ils peuvent rester discrets un certain temps.

3.2.4 Botnet et cryptojacking

Un botnet est un ensemble d'appareils compromis et contrôlés à distance. Ces machines peuvent être utilisées pour lancer d'autres attaques, envoyer du spam ou saturer des services. Le cryptojacking, lui, détourne la puissance de calcul de la machine pour miner de la cryptomonnaie.

3.3 Les attaques techniques contre les applications et services

Certaines attaques visent directement les faiblesses techniques d'un site, d'une application ou d'un service.

3.3.1 Injection SQL

Une injection SQL consiste à faire exécuter à une application une requête non prévue vers sa base de données, en exploitant une mauvaise gestion des entrées utilisateur. Une injection réussie peut permettre de lire, modifier ou supprimer des informations [17].

3.3.2 XSS (Cross Site Scripting)

Le XSS consiste à injecter un code qui sera ensuite exécuté dans le navigateur d'autres utilisateurs. Il peut servir à afficher de faux contenus, voler des sessions ou rediriger vers des pages malveillantes [18].

3.3.3 Déni de service (DoS / DDoS)

Les attaques DoS ou DDoS cherchent à rendre un service indisponible en le saturant de requêtes. Le DDoS mobilise souvent plusieurs machines sources. Pour la victime, le résultat est simple : le site ralentit ou devient inaccessible [19].

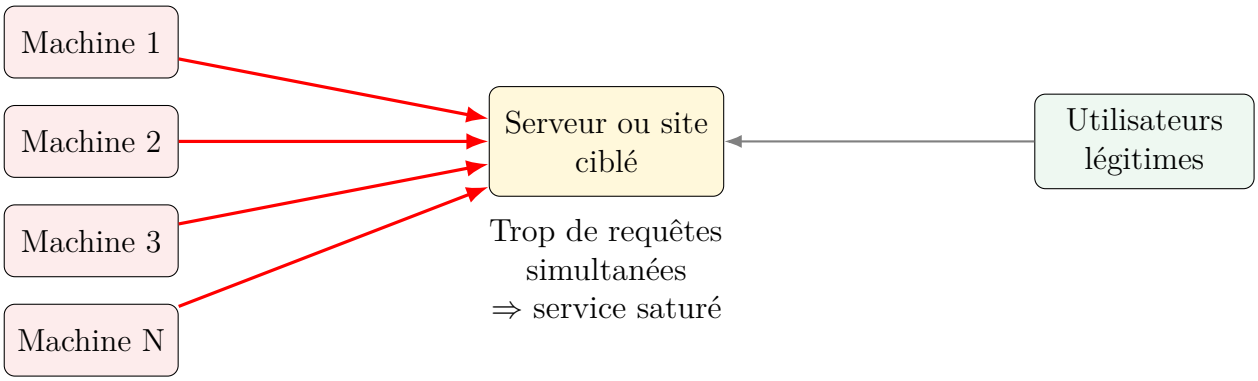

FIGURE 3 – Principe simplifié d'une attaque DDoS.

3.4 Les attaques sur les comptes

3.4.1 Force brute et mots de passe faibles

La force brute consiste à tester automatiquement de nombreuses combinaisons. En pratique, les attaquants utilisent aussi des listes de mots de passe courants ou des informations personnelles faciles à deviner. C'est pourquoi la longueur, l'unicité et l'imprévisibilité du mot de passe sont essentielles [11].

3.4.2 Réutilisation d'identifiants

Lorsqu'une fuite de données touche un service, les identifiants récupérés peuvent être essayés ailleurs. Cette technique est redoutable parce qu'un très grand nombre d'utilisateurs réutilisent le même mot de passe sur plusieurs services.

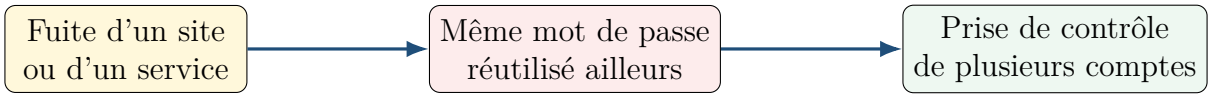

FIGURE 4 – Pourquoi la réutilisation des mots de passe est particulièrement dangereuse.

3.5 Les rançongiciels

Les rançongiciels sont l'une des formes d'attaque les plus connues du grand public. Ils bloquent ou chiffrent les fichiers, puis exigent le paiement d'une rançon pour permettre une récupération supposée. De plus en plus souvent, ils s'accompagnent aussi d'un vol de données destiné à faire pression sur la victime [13]. Pour comprendre leur pouvoir de nuisance, il faut retenir une idée simple : plus les données sont importantes et moins elles sont sauvegardées, plus l'attaquant dispose d'un moyen de pression.

3.6 Vue d'ensemble

TABLE 2 – Synthèse des principales cyberattaques.

Type	**Principe**	**Ce que voit la victime**	**Conséquence fréquente**
Phishing	Faux message ou faux site imitant un tiers de confiance	Mail urgent, SMS, page de connexion inhabituelle	Vol d'identifiants, fraude, compromission de compte
Faux support	Mise en scène d'un problème critique	Appel, alerte, demande de paiement ou de code	Paiement, prise en main à distance, vol d'accès
Quishing	Redirection via QR code malveillant	QR code apparemment banal	Saisie d'identifiants sur un faux site
Malware / cheval de Troie	Fichier ou programme piégé	Installation d'un outil supposé utile	Espionnage, vol, prise de contrôle
Rançongiciel	Chiffrement ou blocage des données	Fichiers inaccessibles, note de rançon	Indisponibilité, extorsion
Force brute / réutilisation d'identifiants	Essais massifs ou exploitation de fuites	Alerte de connexion, changement de mot de passe	Compte compromis
DDoS	Saturation d'un service	Site lent ou inaccessible	Interruption de service
Injection SQL / XSS	Exploitation d'une faille d'application	Souvent invisible pour l'usager	Vol, altération ou redirection

4 Quelles sont les conséquences des cyberattaques ?

4.1 Des effets bien réels

Une cyberattaque n'est pas un problème virtuel au sens de secondaire ou sans conséquence. Les effets sont souvent très concrets : perte d'argent, perte de temps, stress, blocage d'un appareil, suppression ou diffusion de contenus privés, arrêt d'une activité, embarras vis-à-vis de proches ou de collègues, atteinte à la réputation, voire conséquences administratives ou juridiques.

4.2 Conséquences matérielles et techniques

Même si ce n'est pas toujours le but principal, un incident cyber peut provoquer : ralentissement extrême, plantages, perte de configuration, saturation d'un appareil, impossibilité d'utiliser certains services, réinstallation complète d'un système, ou usure anormale des ressources. Ces conséquences sont importantes parce qu'elles représentent du temps, de la compétence et parfois de l'argent pour remettre l'environnement en état.

4.3 Conséquences sur les données

Les données constituent la cible centrale de nombreuses attaques. Elles peuvent être volées, modifiées, copiées, détruites, rendues indisponibles ou publiées. Plusieurs types de préjudices en découlent :

— **perte financière** : fraude bancaire, achat non autorisé, détournement de paiement ;
— **usurpation d'identité** : un attaquant agit au nom de la victime ;
— **atteinte à la vie privée** : messages, photos, documents ou historiques diffusés ;
— **perte d'intégrité** : documents falsifiés ou informations modifiées ; Cybersécurité
— **indisponibilité** : impossibilité d'accéder à ses fichiers ou à un compte essentiel.

4.4 Conséquences psychologiques

Le stress, la honte, la culpabilité, la panique ou le sentiment d'impuissance sont fréquents après un incident cyber. Beaucoup de victimes pensent avoir été naïves alors que les attaques sont précisément conçues pour exploiter les réflexes humains. Il est donc important de rappeler qu'un incident n'est pas un échec moral. C'est un problème à traiter méthodiquement.

4.5 La logique d'effet domino

Une cyberattaque fonctionne souvent en cascade. Une première faiblesse ouvre un accès ; cet accès permet de collecter de nouvelles informations ; ces informations servent à compromettre

d'autres comptes ou d'autres personnes.

FIGURE 5 – Exemple d'effet domino à partir d'une seule compromission initiale.

4.6 Le rôle décisif des sauvegardes

La différence entre un incident sérieux et une catastrophe se joue souvent sur la présence de sauvegardes. Une personne qui dispose de copies récentes et séparées de ses documents peut restaurer plus vite son activité et limiter les effets d'un rançongiciel ou d'une panne. Sans sauvegarde, la victime perd beaucoup plus de contrôle [4, 5].

5 Exemple détaillé d'une cyberattaque : le faux message universitaire

Cette partie propose un scénario pédagogique, fictif mais réaliste, destiné à montrer comment une attaque courante peut réussir. Le but n'est pas de fournir une méthode offensive, mais d'expliquer le raisonnement de l'attaquant et les points où l'utilisateur peut reprendre l'avantage.

5.1 Contexte du scénario

Un étudiant reçoit un message semblant provenir du service informatique de son université. Le mail annonce que sa boîte mail va être suspendue dans la journée à cause d'un dépassement de quota. Le logo paraît familier, le texte est crédible et un bouton se reconnecter est présent. L'étudiant est en période de rendu de dossier ; il ne veut pas perdre l'accès à ses échanges ni rater un message important.

5.2 Étape 1 : attirer l'attention et provoquer l'urgence

L'attaquant n'a pas besoin d'un message parfait. Il lui suffit d'un message plausible, envoyé au bon moment, avec un ressort psychologique simple : la peur d'un blocage imminent. Trois leviers sont généralement utilisés :

— l'**urgence** : votre compte sera suspendu aujourd'hui ;
— l'**autorité** : le message semble venir d'un service officiel ;
— la **routine** : se reconnecter à un compte est une action ordinaire.

FIGURE 6 – Première phase : faire sortir la victime de sa routine normale.

5.3 Étape 2 : la fausse page de connexion

Le lien renvoie vers une page qui imite le portail habituel. Le logo, les couleurs et la structure générale rassurent. La victime pense régler un problème de compte. En réalité, la page appartient à l'attaquant. Lorsque l'étudiant saisit son identifiant et son mot de passe, ceux-ci sont enregistrés.

FIGURE 7 – Vol d'identifiants via une fausse page de connexion.

5.4 Étape 3 : la messagerie devient le compte pivot

Une fois le mot de passe obtenu, l'attaquant tente de se connecter à la vraie boîte mail. Si la double authentification n'est pas activée, l'accès peut être immédiat. Or la messagerie est souvent le compte le plus stratégique, car elle permet de recevoir les liens de réinitialisation d'autres services.

5.5 Étape 4 : effet domino sur d'autres comptes

L'attaquant peut alors :

— tester le même mot de passe sur d'autres comptes ;
— demander la réinitialisation du mot de passe d'un réseau social, d'un cloud ou d'une plateforme d'achat ;
— utiliser la messagerie compromise pour envoyer d'autres messages frauduleux.

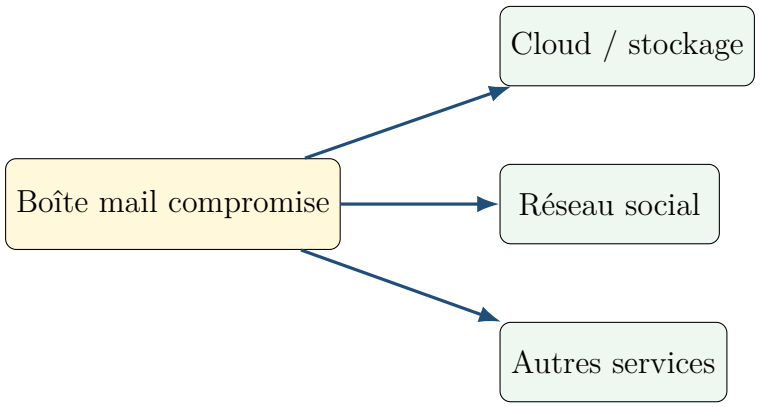

FIGURE 8 – La messagerie comme point de pivot vers d'autres comptes.

5.6 Étape 5 : exploitation de la confiance

Une fois dans la messagerie, l'attaquant peut envoyer de nouveaux messages à la place de la victime. Cette étape est redoutable car les destinataires voient une adresse connue. La crédibilité de l'arnaque augmente fortement.

5.7 Ce que la victime aurait pu remarquer

Plusieurs signaux faibles sont possibles : nom de domaine inhabituel, lien étrange, urgence exagérée, demande de reconnexion hors contexte, alerte de connexion, messages marqués comme lus, réinitialisations inattendues. Aucun signal n'est toujours présent, mais la combinaison de plusieurs d'entre eux doit alerter.

5.8 Comment la chaîne aurait pu être interrompue

Ce scénario aurait pu être stoppé à plusieurs endroits :

- en retapant soi-même l'adresse officielle au lieu de cliquer ;
- en vérifiant le nom de domaine ;
- avec un mot de passe unique pour la messagerie ;
- avec la double authentification ;
- en réagissant immédiatement à l'alerte de connexion ;
- en changeant vite les mots de passe et en fermant les sessions.

5.9 Variante aggravée : du faux document au rançongiciel

Dans une version plus grave, le faux message ne renvoie pas vers une page de connexion mais vers une pièce jointe ou un faux logiciel. L'ouverture du document déclenche alors l'installation d'un malware qui peut ensuite voler des données, télécharger d'autres composants ou préparer le chiffrement des fichiers.

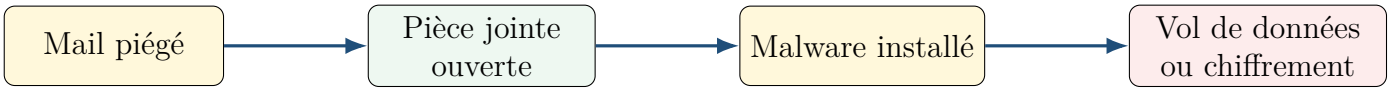

FIGURE 9 – Variante simplifiée d'une attaque menant à un rançongiciel.

5.10 Ce que cet exemple montre

Une cyberattaque réussie repose souvent sur un enchaînement de petites faiblesses plutôt que sur une technique impressionnante : contexte crédible, urgence, erreur de vérification, absence de double authentification, réutilisation de mot de passe, faible capacité de détection. C'est précisément pour cela que les gestes simples ont autant de valeur.

6 Comment se protéger au quotidien ?

Cette section se concentre sur les mesures les plus utiles pour un particulier, un étudiant ou tout public non spécialiste. L'idée n'est pas d'atteindre une sécurité parfaite, mais d'obtenir le meilleur rapport effort / protection [3, 6, 8].

6.1 Protéger en priorité le compte mail principal

L'adresse mail principale est souvent la clé de voûte de la vie numérique. Elle sert à recevoir les notifications, à réinitialiser les mots de passe et à prouver son identité auprès de nombreux services. Si ce compte est compromis, de nombreux autres comptes deviennent plus faciles à attaquer.

Les actions prioritaires sont donc : mot de passe unique, double authentification, vérification des appareils connectés, et conservation séparée des moyens de récupération.

6.2 Mots de passe : robustes, uniques et gérables

Un mot de passe utile est avant tout unique et suffisamment long. La réutilisation représente un danger majeur. Cybermalveillance.gouv.fr recommande notamment d'utiliser un mot de passe différent pour chaque service important, long, complexe et impossible à deviner [11].

Table 3 – Bonnes pratiques relatives aux mots de passe.

À faire	À éviter
Un mot de passe différent pour chaque service critique	Le même mot de passe partout
Une phrase de passe longue ou un mot de passe généré	Des suites simples comme 123456 ou azerty
Un gestionnaire de mots de passe si besoin	Un fichier non protégé contenant tous les codes
Des références non liées à la vie personnelle	Date de naissance, prénom, club favori, etc.

6.3 Double authentification : la seconde barrière

La double authentification ajoute une preuve supplémentaire après le mot de passe : code temporaire, validation sur téléphone, application d'authentification, parfois clé physique. Son intérêt est très fort : même si un mot de passe a été volé, l'accès n'est pas accordé automatiquement [12].

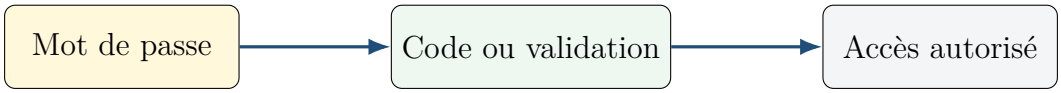

FIGURE 10 – Principe simplifié de la double authentification.

6.4 Mises à jour : fermer les failles connues

Les mises à jour corrigent régulièrement des vulnérabilités identifiées. Les retarder durablement revient à laisser ouvertes des portes déjà connues. L'un des réflexes les plus rentables consiste donc à activer les mises à jour automatiques quand c'est possible, et à ne pas repousser indéfiniment celles qui concernent le système, le navigateur, les applications ou les outils de communication [3, 6].

6.5 Sauvegardes : la meilleure réponse aux pannes et aux rançongiciels

La règle 3-2-1 est un repère pédagogique très efficace : trois copies, deux supports différents, une copie hors ligne ou hors site [4]. L'objectif n'est pas de compliquer la vie de l'utilisateur, mais d'éviter que l'unique copie d'un document important ne se trouve sur l'appareil compromis.

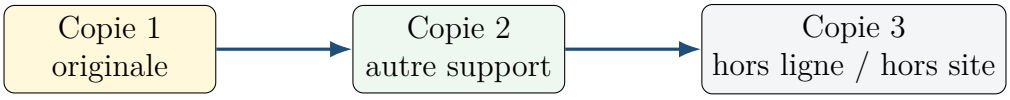

FIGURE 11 – Principe de la sauvegarde 3-2-1.

6.6 Vérifier avant d'agir

Ce réflexe universel a une efficacité remarquable. Avant de cliquer, de payer, de télécharger ou de saisir un mot de passe, il faut prendre quelques secondes pour vérifier.

6.6.1 Vérifier l'origine

Qui envoie le message ? Le nom de domaine est-il cohérent ? L'adresse est-elle orthographiée correctement ? Le service demande-t-il habituellement ce type d'action par ce canal ?

6.6.2 Vérifier la demande

Une demande étrange reste étrange même si sa présentation est soignée. Les demandes de code, de validation urgente, de paiement immédiat ou de communication d'identifiants doivent être considérées avec prudence.

6.6.3 Vérifier par un canal indépendant

En cas de doute, le meilleur réflexe est de taper soi-même l'adresse officielle dans le navigateur, d'utiliser l'application habituelle, ou de contacter le service par un moyen déjà connu. Il faut éviter de répondre directement au message suspect.

6.7 Téléchargements, liens et QR codes

Télécharger depuis des sources officielles ou connues réduit fortement le risque de malware. Il faut se méfier des cracks, des installateurs non officiels, des pièces jointes inattendues et des QR codes provenant d'affiches, de messages ou de documents peu fiables. Le QR code n'est pas sûr par nature ; il est simplement plus rapide à utiliser. Cette rapidité peut devenir une faiblesse.

6.8 Limiter l'exposition sur les réseaux sociaux

Plus un attaquant connaît des détails sur une personne, plus il peut construire un message crédible. Date de naissance, établissement, habitudes, voyages, documents montrés en photo, numéros partiellement visibles : ces éléments peuvent servir à rendre une arnaque plus convaincante ou à deviner des réponses à des questions de sécurité.

6.9 Checklist du quotidien

Table 4 – Checklist simple de cybersécurité personnelle.

Action	Fait	À revoir
Mot de passe unique sur la messagerie principale	☐	☐
Double authentification activée sur les comptes critiques	☐	☐
Mises à jour activées ou vérifiées régulièrement	☐	☐
Sauvegarde récente des documents importants	☐	☐
Habitude de vérifier les liens avant de cliquer	☐	☐
Téléchargements limités aux sources officielles	☐	☐
Verrouillage des appareils activé	☐	☐
Informations sensibles peu exposées publiquement	☐	☐
Moyens de récupération des comptes conservés séparément	☐	☐

7 Bien réagir en cas d'incident

Se protéger est indispensable, mais il faut aussi savoir réagir lorsqu'un incident survient. Une bonne réaction limite fortement la gravité du problème.

7.1 Face à un message suspect

Si un message semble frauduleux, il ne faut pas agir dans l'urgence. Il est conseillé de vérifier l'expéditeur, le nom de domaine, la cohérence de la demande et, si besoin, d'utiliser un canal indépendant pour confirmer. Conserver le message peut aussi être utile si un signalement devient nécessaire [9].

7.2 Si un mot de passe a été saisi sur un faux site

Il faut agir immédiatement : changer le mot de passe du compte concerné, changer aussi les autres comptes si le mot de passe était réutilisé, activer la double authentification, révoquer les sessions actives et surveiller les alertes de connexion. Si le compte a servi à envoyer des messages, il faut prévenir les contacts.

7.3 Si l'appareil paraît infecté

En cas de comportement anormal (ralentissement extrême, fenêtres inconnues, fichiers renommés, blocages, note de rançon), il faut éviter de continuer à saisir des mots de passe, isoler l'appareil du réseau si nécessaire, ne pas payer une rançon et chercher une aide fiable [13].

7.4 Le rôle du 17Cyber

Le Gouvernement français présente 17Cyber comme un service public d'assistance en ligne destiné aux victimes de cybermalveillance, accessible à tout moment [7]. Pour un public non spécialiste, l'existence d'un point d'entrée officiel est précieuse : cela permet de ne pas rester seul face à un incident et d'obtenir une première orientation adaptée.

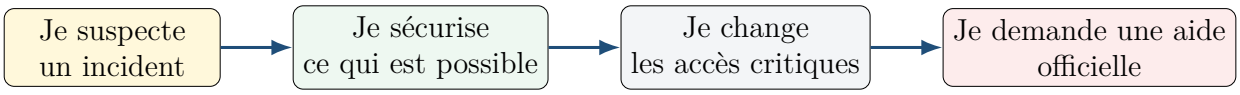

FIGURE 12 – Réaction simplifiée face à un incident cyber.

7.5 Pourquoi il ne faut pas paniquer

La panique favorise les erreurs. Or beaucoup d'attaques sont précisément conçues pour provoquer une réaction rapide et mal contrôlée. En cas d'incident, ralentir, vérifier, isoler, changer les accès essentiels et demander une aide fiable sont des réflexes bien plus utiles que d'agir dans la précipitation.

8 Conseils ciblés pour un public étudiant et grand public

8.1 Pour les étudiants

Les étudiants manipulent souvent des comptes universitaires, des documents de cours, des mémoires, des plateformes d'examen, des outils collaboratifs et des services cloud. Les réflexes essentiels sont : protéger la messagerie universitaire, sauvegarder les travaux, se méfier des faux mails liés à la scolarité, aux bourses, aux stages ou aux services informatiques, éviter les téléchargements douteux et séparer autant que possible les usages personnels et académiques.

8.2 Pour les particuliers

Pour le grand public, les comptes les plus sensibles sont souvent la messagerie, la banque, les services administratifs, les réseaux sociaux et le téléphone lui-même. Il faut donc prioriser ces accès, surveiller les alertes, limiter les informations partagées et conserver des sauvegardes simples mais régulières.

8.3 Pour la famille et l'entourage

La cybersécurité a aussi une dimension collective. Une personne prudente peut être exposée par un proche moins informé, ou au contraire aider son entourage à éviter certaines erreurs. Expliquer calmement les bons réflexes à des parents, à des amis ou à des collègues est déjà une véritable action de prévention.

8.4 L'importance de la pédagogie

Un public non spécialiste n'a pas besoin d'un discours trop technique. Il a surtout besoin de comprendre les mécanismes, de reconnaître les signaux d'alerte, de connaître les priorités et de savoir quoi faire en cas de problème. C'est pourquoi un bon rapport de sensibilisation doit rester concret, progressif et relié aux usages réels.

9 Ouverture : le risque zéro n'existe pas, mais la marge de sécurité oui

Même en appliquant de bonnes pratiques, aucune personne ni aucune organisation ne peut garantir un risque nul. Les outils évoluent, de nouvelles failles apparaissent, les usages changent, et l'être humain reste faillible. Cependant, cette réalité ne doit pas conduire au fatalisme. En cybersécurité, l'objectif n'est pas d'éliminer complètement le risque, mais de :

— diminuer la probabilité d'une attaque réussie ;
— limiter la gravité de ses effets ;
— raccourcir le temps de reprise ;
— empêcher l'effet domino entre plusieurs comptes ou appareils.

Cette logique est fondamentale. Une personne bien préparée peut encore subir un incident, mais elle réduit fortement ses conséquences. À l'inverse, une faible préparation transforme souvent une erreur mineure en problème majeur.

10 Conclusion

La cybersécurité n'est pas réservée aux spécialistes. Elle repose avant tout sur une compréhension claire des enjeux, sur quelques gestes réguliers et sur la capacité à reconnaître les situations à risque. À travers la définition générale du domaine, le triptyque CIA, les quatre piliers de structuration des mesures de sécurité, les grandes familles d'attaques, leurs conséquences et l'exemple détaillé du faux message universitaire, ce rapport montre qu'une cyberattaque est souvent une chaîne logique plus qu'un acte mystérieux.

Le message principal est donc simple : une grande part des risques peut déjà être réduite par des actions à la portée de tous. Protéger sa messagerie, utiliser des mots de passe uniques, activer la double authentification, mettre à jour ses appareils, sauvegarder ses fichiers et vérifier avant d'agir constituent un socle de protection solide [11, 12, 4, 6].

La cybersécurité du quotidien n'exige pas d'être expert ; elle demande surtout d'être attentif, organisé et régulier. Dans un monde où nos vies numériques prennent une place de plus en plus importante, cette vigilance est devenue une compétence essentielle.

A Annexe A : résumé visuel des réflexes essentiels

1. Protéger en priorité la messagerie principale.
2. Utiliser un mot de passe différent pour chaque compte important.
3. Activer la double authentification quand elle existe.
4. Mettre à jour les appareils et applications.
5. Sauvegarder régulièrement les fichiers importants.
6. Se méfier des messages urgents, alarmants ou trop pressants.
7. Taper soi-même l'adresse officielle en cas de doute.
8. Réagir vite mais calmement en cas d'incident.

B Annexe B : mini-glossaire

Authentification
Vérification de l'identité d'un utilisateur avant de lui accorder un accès.

Base de données
Espace structuré où sont stockées les informations exploitées par une application.

Botnet
Ensemble de machines compromises contrôlées à distance.

Chiffrement
Transformation d'une information pour la rendre illisible sans clé adaptée.

DDoS
Attaque visant à saturer un service avec un volume massif de requêtes.

Faille
Faiblesse technique exploitable par un attaquant.

Forensic
Analyse réalisée après incident pour comprendre ce qu'il s'est passé.

Session
Connexion ouverte et reconnue par un service en ligne.

Infostealer
Malware spécialisé dans le vol d'informations.

Hameçonnage
Technique consistant à imiter un service de confiance pour tromper la victime.

Références

[1] ANSSI / cyber.gouv.fr, *Gouvernance, protection, défense, résilience : comment structurer ses mesures de sécurité ?*, consulté le 17 mars 2026.
`https://cyber.gouv.fr/securisation/gestion-de-crise/anticiper-gerer-une-crise-cyber/structurer-ses-mesures-de-securite/`

[2] ANSSI / cyber.gouv.fr, *Anticiper et gérer une crise cyber*, consulté le 17 mars 2026.
`https://cyber.gouv.fr/securisation/gestion-de-crise/anticiper-gerer-une-crise-cyber/`

[3] CNIL, *Sécurité des données : les règles essentielles pour démarrer*, 2018, consulté le 17 mars 2026.
`https://www.cnil.fr/fr/securite-des-donnees-les-regles-essentielles-pour-demarrer`

[4] CNIL, *Sécurité : Sauvegarder*, 2024, consulté le 17 mars 2026.
`https://www.cnil.fr/fr/securite-sauvegarder`

[5] CNIL, *Guide de la sécurité des données personnelles 2024*, 2024, consulté le 17 mars 2026.
`https://www.cnil.fr/sites/cnil/files/2024-03/cnil_guide_securite_personnelle_2024.pdf`

[6] Gouvernement français, *Cybersécurité : conseils pratiques pour les usagers*, 2023, consulté le 17 mars 2026.
`https://www.info.gouv.fr/risques/cyber-conseils-aux-usagers`

[7] Gouvernement français, *17Cyber, guichet unique pour les victimes de cybermalveillance*, 18 décembre 2024, consulté le 17 mars 2026.
`https://www.info.gouv.fr/actualite/17cyber-gouv-fr-le-guichet-unique-pour-les-victimes-de-cyberm`

[8] Cybermalveillance.gouv.fr, *Assistance aux victimes de cybermalveillance*, consulté le 17 mars 2026.
`https://www.cybermalveillance.gouv.fr/`

[9] Cybermalveillance.gouv.fr, *Que faire en cas de phishing ou hameçonnage ?*, consulté le 17 mars 2026.
`https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/hameconnage-phishing`

[10] Cybermalveillance.gouv.fr, *Le quishing : l'hameçonnage par QR code*, 2024, consulté le 17 mars 2026.
`https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/quishing-hameconnage-qr-code`

[11] Cybermalveillance.gouv.fr, *Pourquoi et comment bien gérer ses mots de passe ?*, 2019, consulté le 17 mars 2026.
`https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mots-de-passe`

[12] Cybermalveillance.gouv.fr, *Comment protéger ses comptes en ligne avec la double authentification ?*, 2023, consulté le 17 mars 2026.
`https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/double-authentification`

[13] Cybermalveillance.gouv.fr, *Rançongiciel ou ransomware, que faire ? (particuliers)*, 2025, consulté le 17 mars 2026.
`https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/rancongiciel-ransomware-particuliers`

[14] Microsoft Security, *What is cybersecurity ?*, consulté le 17 mars 2026.
`https://www.microsoft.com/fr-fr/security/business/security-101/what-is-cybersecurity`

[15] Microsoft Security, *What is a cyberattack ?*, consulté le 17 mars 2026.
`https://www.microsoft.com/fr-fr/security/business/security-101/what-is-a-cyberattack`

[16] IBM, *L'histoire des logiciels malveillants*, consulté le 17 mars 2026.
`https://www.ibm.com/fr-fr/think/topics/malware-history`

[17] OWASP Foundation, *SQL Injection*, consulté le 17 mars 2026.
`https://owasp.org/www-community/attacks/SQL_Injection`

[18] OWASP Foundation, *Cross Site Scripting (XSS)*, consulté le 17 mars 2026.
`https://owasp.org/www-community/attacks/xss/`

[19] Cloudflare, *Qu'est-ce qu'une attaque DDoS ?*, consulté le 17 mars 2026.
`https://www.cloudflare.com/fr-fr/learning/ddos/what-is-a-ddos-attack/`

[20] Légifrance, *Article 323-1 du Code pénal*, version consultée le 17 mars 2026.
`https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000047052655`

[21] Légifrance, *Des atteintes aux systèmes de traitement automatisé de données*, consulté le 17 mars 2026.
`https://www.legifrance.gouv.fr/codes/id/LEGISCTA000006149839`

[22] Union européenne, *Directive (UE) 2022/2555 dite NIS 2*, 2022, consulté le 17 mars 2026.
`https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=fr`