Diplôme : Bac Pro Ciel			Option : Ciel
Nom:	Prénom:	Classe:	Date:

0 — 1 an — 2 ans — 3 ans

TP Cybersécurité : 91% des cyberattaques commencent comme ça

Objectifs pédagogiques (référentiel Bac Pro CIEL)

Compétence C04 : Analyser une structure matérielle et logicielle
Compétence C06 : Valider la conformité d'une installation
(mises à jour, antivirus, pare-feu, sauvegardes) et justifier chaque mesure.
Compétence C10 : Exploiter un réseau informatique
sur un réseau public (Wi-Fi partagé, mode avion des clés USB inconnues).
Compétence C11 : Maintenir un système électronique ou réseau informatique
Compétence C01 : Communiquer en situation professionnelle



Ce qui est attendu de l'élève

1. Regarder la vidéo interactive (étape 2) et répondre à ses activités (définitions et QCM).
2. Compléter ce livret : cours à trous, glossaire (étape 3), glisser-déposer (étape 5), résumé (étape 9) et questions ouvertes (étape 8).
3. Faire les 9 étapes du livre interactif dans l'ordre (glossaire, flashcards, glisser-déposer, 6 QCM, quiz d'entraînement, questions ouvertes, fiche de synthèse).
4. Terminer par le QUIZ noté de 10 questions : seuil de validation 60 % (12/20).
5. Savoir expliquer avec ses mots pourquoi 91 % des cyberattaques commencent par un hameçonnage, et citer trois réflexes de protection.

BOUNGAB



TP Cybersécurité : 91% des cyberattaques commencent comme ça



Activité 1 — Le cours à compléter

Complète les pointillés en écoutant la vidéo. Mots à placer (un mot peut servir plusieurs fois) :

DDoS • email • ingénierie sociale • malware • mot de passe • Ransomware

1. Donc ce qu'il faut faire c'est toujours vérifier l'adresse ..... de l'expéditeur.
2. Vous téléchargez un fichier infecté, le ..... se lance, il crypte tous vos fichiers.
3. Pour se protéger ici, les entreprises utilisent des services anti-..... qui filtrent le trafic et bloquent les fausses requêtes, comme par exemple Cloudflare, AWS Shield, Akamai, etc.
4. Un ....., c'est un programme conçu pour nuire, voler vos données, détruire vos fichiers, espionner vos actions, prendre le contrôle de votre machine.
5. Parce que oui, parfois un ..... essaie d'envoyer vos données vers l'extérieur.
6. En fait c'est un ..... qui se fait passer pour un logiciel légitime.
7. Vous téléchargez un logiciel gratuit, un jeu, un outil ou n'importe quoi, mais caché à l'intérieur il y a un .....
8. Niveau stats, c'est 98% des cyberattaques qui impliquent une forme d'.....
9. C'est-à-dire de ne jamais, au grand jamais, donner des infos sensibles par téléphone ou par .....
10. Vous entrez votre ..... puis le système vous demande une deuxième preuve.

Activité 2 — Je complète le glossaire (étape 3 du cours)

Écris la définition de chacun des 6 termes ci-dessous (avec un exemple quand c'est possible) :

- **Attaque par déni de servic**

- **Hameçonnag**

- **Logiciel de rançon**

- **Logiciel malveillan**

- **Pare-fe**

BOUNGAB



- **Réseau privé virtuel**

Activité 3 — Je complète le glisser-déposer (étape 5 du cours)

Replace les 6 termes techniques en face de leur définition :

Attaque par déni de service

- ..... : Attaque visant à rendre un service en ligne indisponible en le surchargeant avec un grand nombre de requêtes.

Activité 4 — Je complète le résumé (étape 9 du cours)

Retrouve le terme qui correspond à chaque définition, puis rédige le résumé avec tes mots :

Hameçonnage (phishing) • Rançongiciel (ransomware) • Attaque par déni de service (DDoS) • Logiciel malveillant (malware) • Cheval de Troie • Ingénierie sociale • Faille zero-day • Pare-feu (firewall) • VPN • 2FA (double authentification)

- ..... : email ou message qui imite un organisme officiel pour voler vos identifiants. 91 % des cyberattaques commencent comme ça.
- ..... : logiciel qui chiffre vos fichiers et réclame une rançon
- ..... : le site est submergé de fausses requêtes et devient inaccessible
- ..... : programme nuisible (virus, ver, cheval de Troie, rançongiciel, espion)
- ..... : logiciel en apparence utile qui cache un programme malveillant
- ..... : manipulation de la personne (peur, urgence, confiance) — le maillon faible, c'est l'humain.
- ..... : défaut de sécurité encore inconnu de l'éditeur, donc pas corrigé
- ..... : filtre le trafic réseau et bloque les accès non autorisés
- ..... : tunnel chiffré qui protège la connexion, indispensable sur un Wi-Fi public
- ..... : un second code en plus du mot de passe : il bloque la plupart des attaques

Avec mes mots, je résume le thème en trois phrases :

BOUNGAB



Activité 5 — Questions ouvertes d'approfondissement (étape 8 du cours)

1. Expliquez, en utilisant une analogie simple, comment fonctionne une attaque par phishing et pourquoi c'est une méthode si courante parmi les cybercriminels.

2. Décrivez comment un ransomware fonctionne et proposez une méthode simple pour s'en protéger.

3. Pourquoi les attaques DDoS sont-elles si efficaces pour rendre un site web inaccessible ? Utilisez une comparaison pour illustrer votre réponse.

4. Qu'est-ce que l'ingénierie sociale et pourquoi est-elle considérée comme l'une des techniques les plus dangereuses en cybersécurité ?

5. Expliquez ce qu'est une faille zero-day et pourquoi elle est si dangereuse pour les utilisateurs et les entreprises.

BOUNGAB

FICHE SYNTHESE

91% Des Cyberattaques Commencent Comme Ça



➢ **A RETENIR** *Compléter*

Aide-mémoire — à retenir

1. Hameçonnage (phishing) : email ou message qui imite un organisme officiel pour voler vos identifiants. 91 % des cyberattaques commencent comme ça.
2. Rançongiciel (ransomware) : logiciel qui chiffre vos fichiers et réclame une ranço
3. Attaque par déni de service (DDoS) : le site est submergé de fausses requêtes et devient inaccessible.
4. Logiciel malveillant (malware) : programme nuisible (virus, ver, cheval de Troie, rançongiciel, espion).
5. Cheval de Troie : logiciel en apparence utile qui cache un programme malveillan
6. Ingénierie sociale : manipulation de la personne (peur, urgence, confiance) — le maillon faible, c'est l'humain.
7. Faille zero-day : défaut de sécurité encore inconnu de l'éditeur, donc pas corrigé.
8. Pare-feu (firewall) : filtre le trafic réseau et bloque les accès non autorisés.
9. VPN : tunnel chiffré qui protège la connexion, indispensable sur un Wi-Fi public.
10. 2FA (double authentification) : un second code en plus du mot de passe : il bloque la plupart des attaques.

Réflexes professionnels CIEL :
- Vérifier l'adresse de l'expéditeur avant de cliquer — ne jamais ouvrir une pièce jointe douteuse.
- Mots de passe longs et uniques + double authentification.
- Mettre à jour le système, le navigateur et l'antivirus.
- Sauvegarder régulièrement les données (disque externe ou cloud professionnel).
- Signaler tout incident au référent informatique et sur cybermalveillance.gouv.fr