
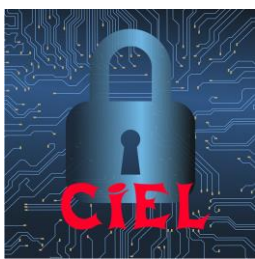







2 nd e BAC Pro CIEL	<p>Identifier les attaques courantes</p> <p>Le phishing</p>	 <p>Année 2025/2026</p>
		

Nom		
Prénom		
Date		
<div><u>Matériel</u> <u>Outillage</u> </div>	⇒ Mail	<div><u>Durée : 3H</u> </div>
<div><u>Travaux à réaliser</u> </div>	⇒ Recherche phishing ⇒ Analyse mail ⇒ Préconisation	
<u>Pôle d'activité</u> : Valorisation de la donnée et cybersécurité		
<u>Activités</u> : ⇒ D1 : Elaboration et appropriation d'un cahier des charges		
<u>Taches</u> : ⇒ T1 : Collecte des informations ⇒ T2 : Analyse des informations		
<u>Compétences</u> : ⇒ C01 : Communiquer en situation professionnelle (Français/Anglais) ⇒ C04 : Analyser une structure matérielle et logicielle		
		
Lorsque le logo  apparaît, il est indispensable d'appeler l'enseignant pour vérification.		

A. Mise en contexte

À la suite de la phase de découverte des enjeux de la cybersécurité, l'entreprise CyberABE Solutions constate une augmentation significative des tentatives d'escroquerie par courrier électronique (phishing) auprès de ses clients.

Plusieurs entreprises accompagnées par CyberABE Solutions signalent la réception de messages électroniques suspects demandant :

- ⇒ la communication d'informations personnelles ou professionnelles
- ⇒ la saisie d'identifiants de connexion
- ⇒ l'ouverture de liens et de pièces jointes potentiellement malveillants

Ces messages exploitent souvent :

- ⇒ l'urgence
- ⇒ la peur
- ⇒ l'imitation de services connus (banques, fournisseurs, administrations)

Avant toute mise en place de solutions techniques ou de procédures de traitement d'incidents, le responsable de CyberABE Solutions souhaite s'assurer que les techniciens juniors sont capables de :

- ⇒ reconnaître une tentative de phishing
- ⇒ analyser les risques associés à ce type de message
- ⇒ adopter et recommander les bonnes pratiques de sécurité à destination des utilisateurs

Vous êtes donc chargé, en tant que technicien junior en cybersécurité, d'analyser plusieurs exemples de messages électroniques afin d'identifier les tentatives de phishing et de formaliser vos conclusions dans un rapport professionnel destiné à votre responsable.

B. Problématique

Comment reconnaître une tentative de phishing et analyser les risques afin de prévenir les utilisateurs et limiter les incidents de sécurité au sein d'une organisation ?



C. Compétences

C01 COMMUNIQUER EN SITUATION PROFESSIONNELLE (ANGLAIS/FRANÇAIS)	
La présentation (typographie, orthographe, illustration, lisibilité) est soignée et soutient le discours avec des enchaînements cohérents	X
La présentation orale (support et expression) est de qualité et claire	
L'argumentation développée lors de la présentation et de l'échange est de qualité	X
L'argumentation tient compte des éventuelles situations de handicap des personnes avec lesquelles il interagit	
C03 PARTICIPER A UN PROJET	
Les rôles et tâches de chacun sont identifiés ; le cas échéant, les besoins spécifiques des personnes en situation de handicap sont pris en compte	
Le planning prévisionnel est compris	
Le suivi du projet est respecté	
L'espace collaboratif est correctement utilisé	
C04 ANALYSER UNE STRUCTURE MATÉRIELLE ET LOGICIELLE	
Le besoin est identifié ainsi que les ressources matérielles, logicielles et humaines	X
Les logiciels d'analyse et de tests sont utilisés selon les procédures de traitement d'incidents	
Les informations nécessaires sont extraites des documents réglementaires et/ou constructeurs	X
Les indicateurs de fonctionnement sont interprétés	
Les fiches de test ou d'intervention sont renseignées	
C06 VALIDER LA CONFORMITÉ D'UNE INSTALLATION	
Les exigences du cahier des charges sont respectées	
Les tests sont effectués	
Les résultats attendus sont vérifiés	
La procédure de test est respectée	
C07 RÉALISER DES MAQUETTES ET PROTOTYPES	
Le placement et routage sont conformes au cahier des charges	
La génération des fichiers de fabrication du PCB est conforme aux attentes	
Le PCB est réalisé, contrôlé et conforme aux IPC (tolérances mécaniques, finition de surface, propreté, ESD etc.)	
Les composants sont conformes à la nomenclature (marquage, étiquetage)	
La nomenclature des composants est respectée	
Le brasage de la carte est conforme à la nomenclature et aux IPC	
Les contraintes liées aux impacts environnementaux sont intégrées	
Le contrôle visuel de la carte assemblée est conforme au dossier de fabrication	
Les risques d'une situation de travail sont repérés et les mesures appropriées pour sa santé, sa sécurité et celle des autres sont adoptées	
C08 CODER	
Les environnements de développement et de test sont mis en oeuvre en tenant compte des contraintes de fonctionnalités et de sécurité	
Le module logiciel est débogué et syntaxiquement correct	
Les composants logiciels individuels sont développés et testés conformément aux spécifications du cahier des charges et des bonnes pratiques	
La solution (logicielle et matérielle) est intégrée et testée conformément aux spécifications du cahier des charges et des bonnes pratiques	
Le code est commenté et le logiciel est documenté	

C09 INSTALLER LES ÉLÉMENTS D'UN SYSTÈME ÉLECTRONIQUE OU INFORMATIQUE	
L'ensemble des éléments pour l'installation du système est complet et vérifié par rapport au cahier des charges	
Les éléments du système sont installés et raccordés selon une procédure	
La configuration est réalisée	
La mise en service est réalisée	
L'état de l'installation est renseigné de manière écrite ou orale	
Les risques d'une situation de travail sont repérés et les mesures appropriées pour sa santé, sa sécurité et celle des autres sont adoptées	
C10 EXPLOITER UN RÉSEAU INFORMATIQUE	
Les alertes et problèmes rencontrés sont renseignés	
Les différents éléments d'un réseau ou d'un système à partir d'un schéma fourni sont identifiés	
La mise à jour des équipements (iOS, OS, logiciel, firmware) est effectuée	
Les optimisations nécessaires sont effectuées	
C11 MAINTENIR UN SYSTÈME ÉLECTRONIQUE OU RÉSEAU INFORMATIQUE	
L'intervention est préparée	
Le dysfonctionnement est constaté	
La maintenance ou la réparation est réalisée	
La fiche d'intervention est correctement renseignée	
Les risques d'une situation de travail sont repérés et les mesures appropriées pour sa santé, sa sécurité et celle des autres sont adoptées	

Nature de complexité de l'activité :

Découverte	X
Intermédiaire	
Bac Pro	

D. Comprendre le phishing (30 min)

Créer un nouveau document Word « *NOM*Phising.docx » avec *NOM* votre nom de famille.

Créer un titre de niveau 1 intitulé « Qu'est-ce que le phishing ? »

A l'aide de vos connaissances et du « Livre Blanc : Phishing Votre guide ultime », **rédiger** un paragraphe structuré expliquant :

- ⇒ Ce qu'est le phishing
- ⇒ Son objectif principal
- ⇒ Pourquoi il fonctionne encore aujourd'hui

E. Analyse de mails (1H30)

Créer un titre de niveau 1 intitulé « Analyse de mails ».

Vous disposez de plusieurs exemples de mails.

Pour chaque mail, vous devez :

- ⇒ Déterminer s'il est légitime ou frauduleux
- ⇒ Repérer les indices suspects

Réaliser le tableau suivant :

Mail N°	Légitime / Phishing	Indices observés	Risque pour l'entreprise

F. Bonnes pratiques et prévention (30 min)

Créer un titre de niveau 1 intitulé « Bonnes pratiques face au phishing »

A partir de vos analyses, **rédiger** une liste de bonnes pratiques à destination des employés.

Enregistrer le document au format pdf et déposer sur le NAS64.