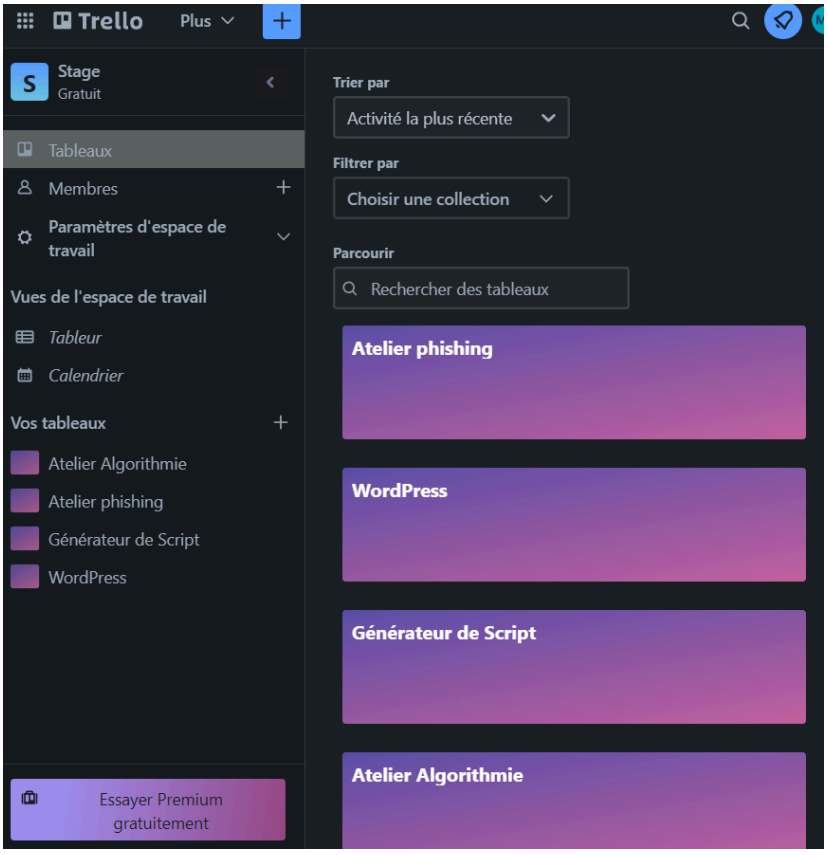
Synthèse - Première semaine

Travail 1 : Découverte de la méthodologie Agile

Ma première tâche à été la découverte de la méthodologie Agile permettant une meilleure organisation du travail en équipe lors d'une organisation en télétravail, cette méthodologie Agile permet de décomposer les projets en plusieurs petites parties courtes et de suivre l'avancement de manière plus précise.

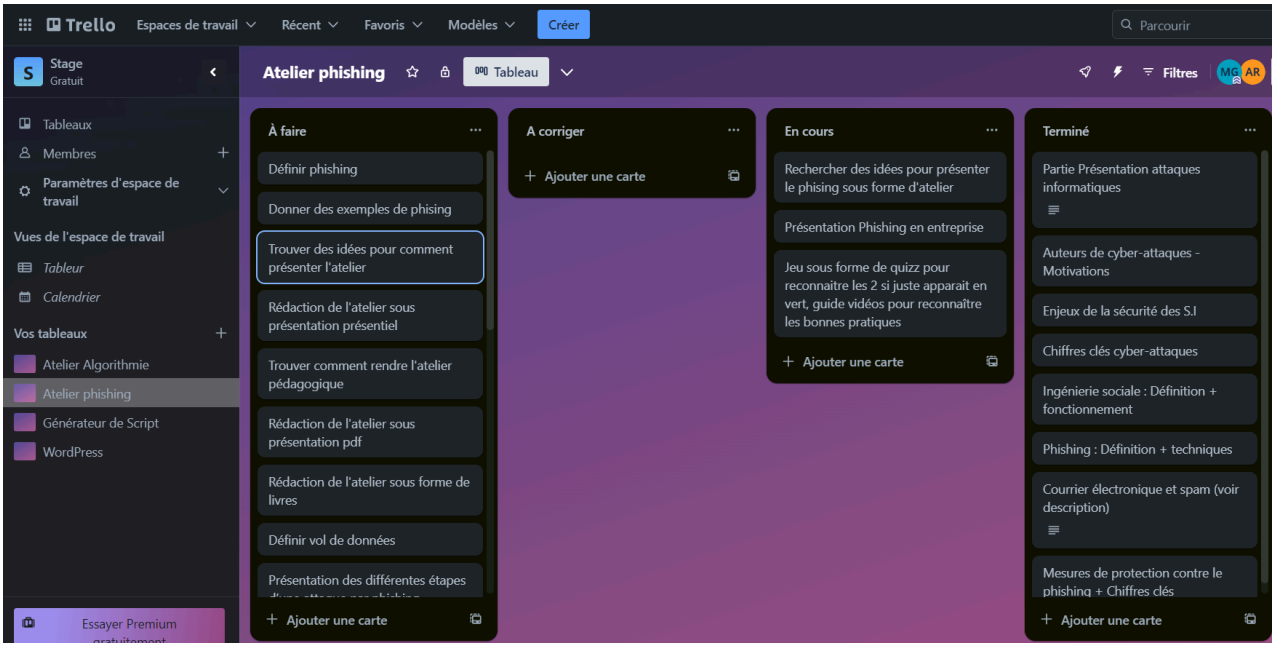
J'ai donc par la suite mis en place cette méthodologie Agile pour mon premier projet de Stage, à l'aide de l'outil de gestion de projet trello .

J'ai donc d'abord mis en place mon environnement de travail en créant 4 tableaux pour les 4 projets que j'aurais au cours de mon stage :

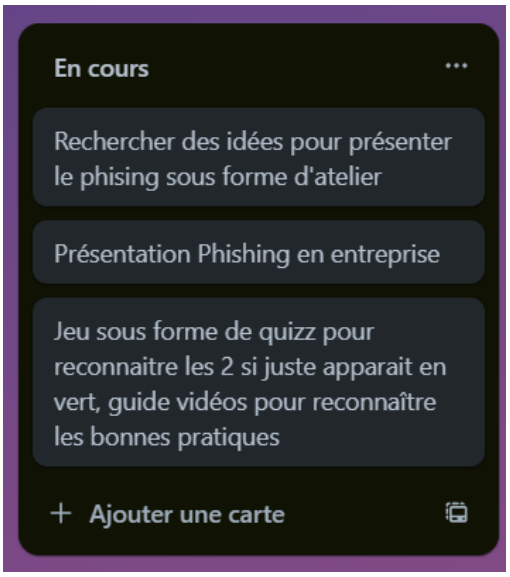


J’ai ensuite effectué des recherches d’idées pour mon premier projet, qui est la création d’un atelier de sensibilisation au Phishing, cet atelier sera par la suite dispensé, à toute sorte de public et de tout âges.

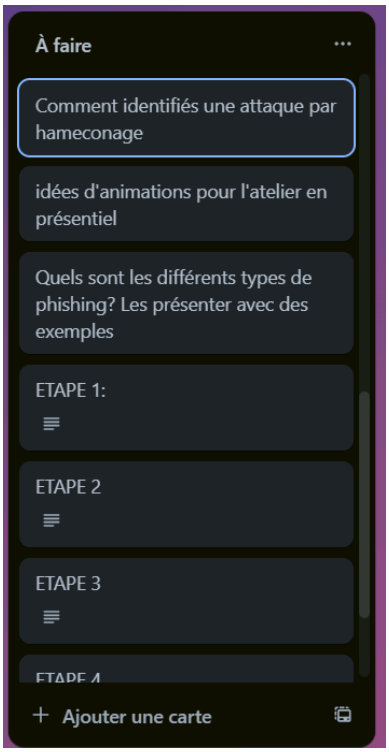
Présentation du tableau dans son ensemble avec les différentes cartes:



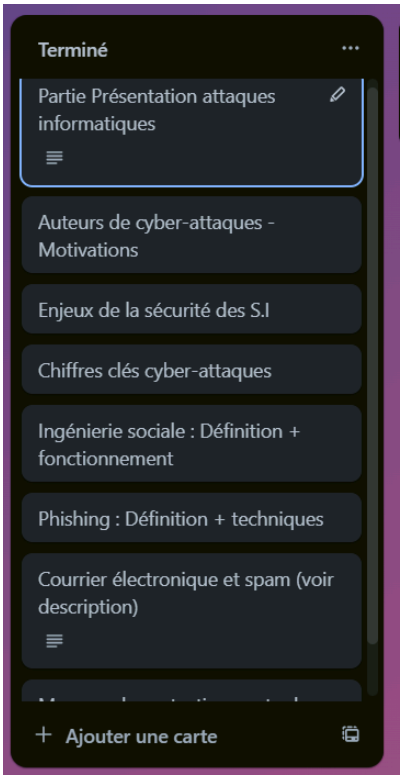
En cours :



A faire :



Terminé :



Travail 2 : Création d'un atelier de sensibilisation au Phishing

A la suite de cette découverte et mise en place de l'outil trello, j'ai commencé la création de l'atelier de sensibilisation au Phishing.

J'ai donc effectué de nombreuses recherches afin de trouver comment rendre un atelier pédagogique et compréhensible par le plus grand nombre du plus jeune au plus âgés, avec des explications simples mais également la mise en place de supports visuels tels que des schémas explicatifs réalisés à l'aide de Canva, par la suite je mettrais en place du contenu interactif sous forme de quiz .

Cette première semaine de stage j'ai donc effectué des recherches et rédiger du contenu pour les sujets suivant:

-Les attaques informatiques (Définition + présentation des principales attaques informatiques)

-Les auteurs de cyberattaques (Présentation + Présentation des principales motivations)

-Les enjeux de la sécurité des S.I (Définition + Enjeux)

-Les chiffres clés des cyberattaques

-L'ingénierie sociale (Définition + Fonctionnement)

-Le phishing (Définition + techniques)

-Courrier électronique et spam (Définition + Schéma d'une attaque + les techniques de spam et courrier électronique + types de spam les plus fréquents)

-Phishing par logiciel malveillant (Définition + Schéma d'une attaque)

-Phishing en entreprise (Définitions + Risques + Sensibilisation des salariés + Schéma d'une attaque)

-Les mesures de protection contre le Phishing + chiffres clés phishing

Suite du Stage:

A la suite de cet atelier je vais avoir plusieurs autres missions:

- L'amélioration du site internet de l'entreprise (wordpress)
- La création d'un Script générateur de projet de base (à l'aide d'angular et de git)
- Tester les applications créées par l'entreprise, vérifier que les différentes fonctionnalités fonctionnent.
- La création d'un atelier de sensibilisation à l'algorithmie

Je vais également pouvoir assister aux différentes réunions avec le client actuel, afin de voir le déroulement des réunions et le suivi de projet avec un client.

Afin de voir le travail fini pour l'atelier de sensibilisation au phishing et les différents schéma réalisés à l'aide de canva :

ATELIER INITIATION

AU

HAMEÇONNAGE

(partie 1 - Première Semaine)

Les attaques informatiques

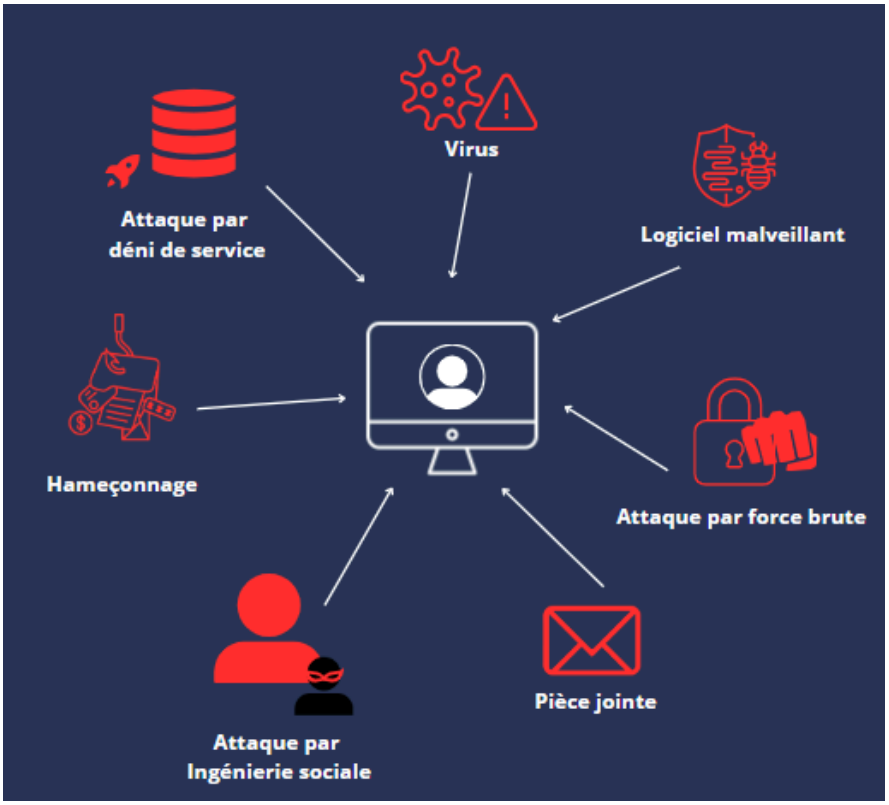
Les attaques informatiques sont des tentatives d'accès volontaires et malveillantes à un système informatique, un ordinateur ou un réseau informatique avec pour but de causer des dommages aux informations et aux personnes qui les traitent.

Il s'agit généralement de tentatives de vols, d'étalage, de modification ou de destruction des biens d'autrui par le biais d'un accès non autorisé à des systèmes informatiques.

Avec un cyberspace grandissant, les attaques malveillantes sont de plus en plus nombreuses et tout le monde peut en être la cible, que ce soit les particuliers, les entreprises, les institutions…

Ces attaques peuvent être réalisées par une personne seule (hacker), par un groupe de pirates, par une organisation criminelle ou bien même par un État .

Les principales attaques informatiques



Auteurs de cyber-attaques

Les cyber-attaquants peuvent avoir de multiples motivations, elles peuvent variées mais elles sont principalement de 3 types: criminel, politique et personnel.

Les attaquants ayant des motivations criminelles sont attirés par le souhait d'un gain financier grâce à un vol de données, d'argent ou une panne.

Les attaquant ayant une motivation politique sont associés à des idées politique, à la cyber-guerre, au cyber-terrorisme ainsi qu'au hacktivisme.

Les attaquants qui ont des motivations personnelles sont quant à eux le personnel actuel ou ancien d'une organisation, qui cherchent à se venger par le vol d'argent, de données sensibles voire en perturbant les systèmes de l'organisation.

Les motivations des cybers-attaquants

Des simples hackers aux actes de guerre, les cyber-attaques sont lancées pour de nombreuses raisons. Les auteurs de ces cyber-attaques et leurs motivations peuvent être catégorisés dans une certaine mesure, le plus souvent, chaque catégorie de cyber-attaquant est animée par une raison principale.

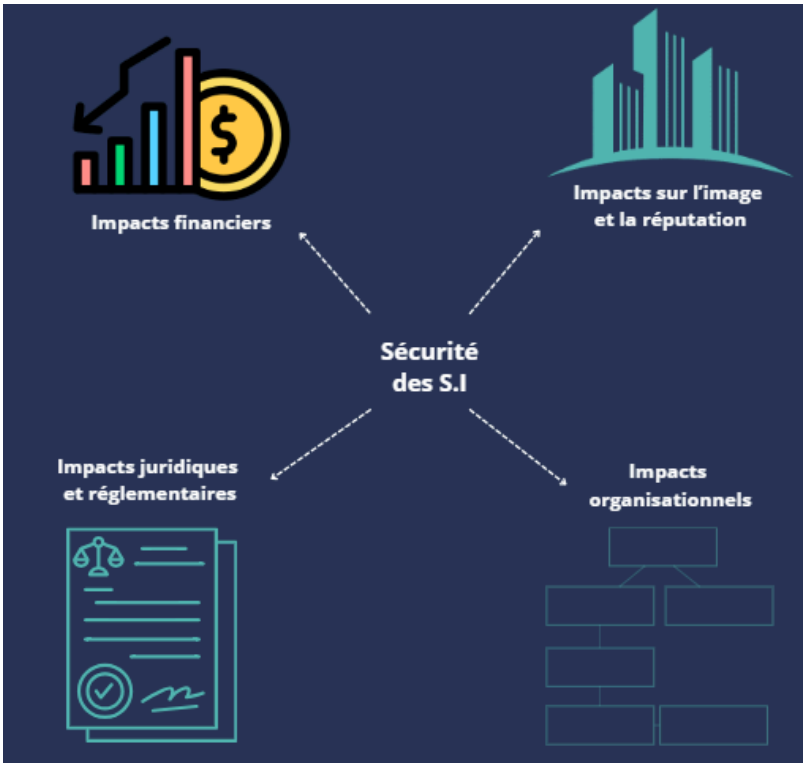
Enjeux de la sécurité des S.I

Pour les plus petites et les plus grandes entreprises, les conséquences d'une cyberattaque sont très importantes, elles ont un coût indirect et direct pour l'organisation qui en est victime.

Cela peut entraîner une perte d'argent ou de données (fichiers clients, contrats, comptabilité…), un arrêt de l'activité, une prise d'otage des données contre une rançon. Mais également un coût lié à la réputation de l'entreprise et une perte de confiance des acteurs de l'entreprise.

Les impacts d'une cyber-attaque se matérialisent en trois catégories: l'intégrité, la confidentialité et la disponibilité.

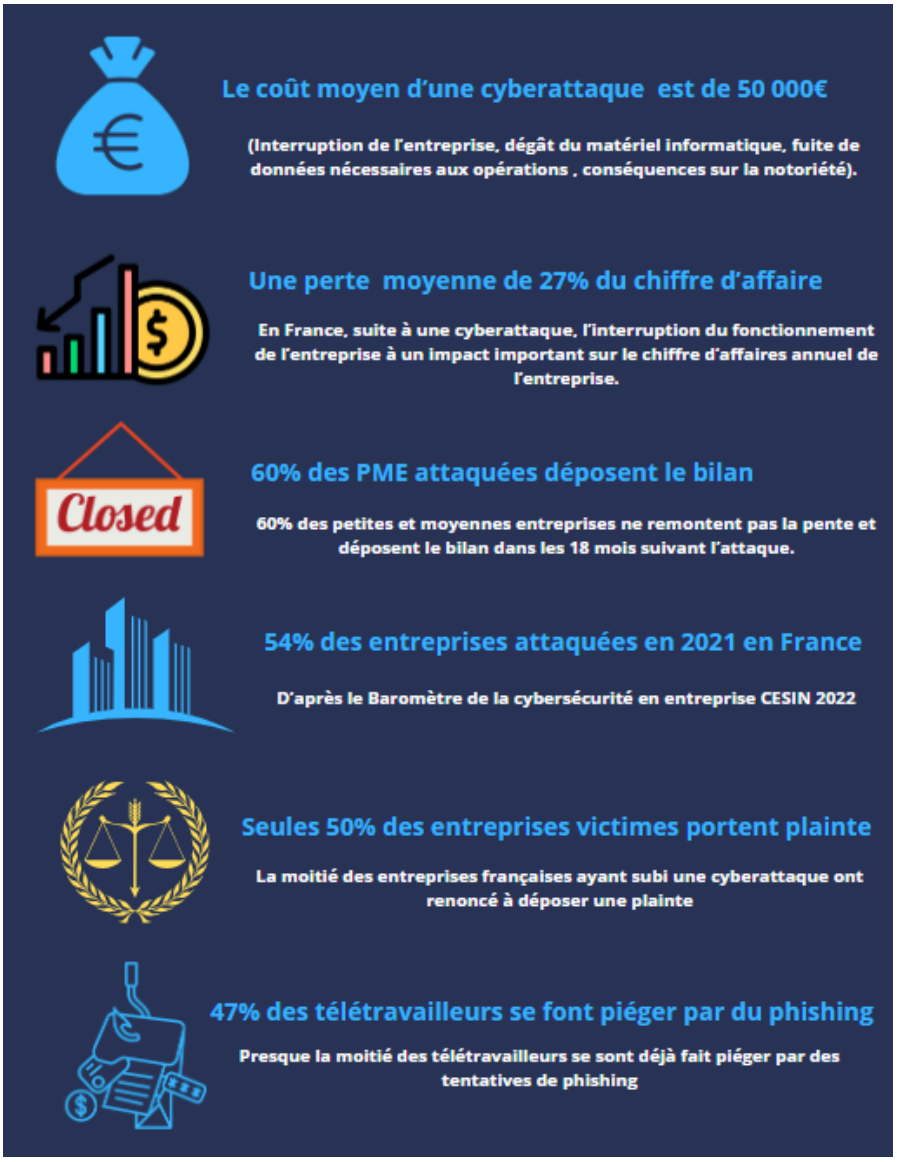
Enjeux de la sécurité des S.I



Chiffres clés Cyber-attaques

Les cyberattaques qui ont frappé la France sont de plus en plus nombreuses, que ce soit des attaques par ingénierie sociale, de l'hameçonnage (phishing), des logiciels malveillants… Voici les chiffres clés sur les évènements de cybersécurité ces dernières années.

Chiffres clés



L'ingénierie sociale

L'ingénierie sociale est une manipulation psychologique à des fins d'escroquerie. Elle exploite les faiblesses psychologiques, sociales et organisationnelles des individus afin d'obtenir de manière frauduleuse des informations confidentielles (un bien, un service, un virement bancaire, la divulgation d'informations confidentielles...).

L'attaquant cherche à abuser de la confiance, de l'ignorance et de la naïveté de sa cible pour obtenir ce qu'il veut.

L'ingénierie sociale prend appuie sur la manipulation psychologique et exploite les erreurs ou les faiblesses humaines plutôt que les vulnérabilités techniques ou numériques des systèmes.

Fonctionnement de l'ingénierie sociale

Les tactiques et les techniques de manipulation psychologiques utilisant l'ingénierie sociale reposent sur la manipulation des émotions et de l'instinct des victimes en les poussant à prendre des décisions qui ne sont pas dans leur intérêt.

En règle générale, l'ingénierie sociale fait appel à une ou plusieurs des tactiques suivants:

Le phishing

Face à la rapidité de la technologie, de nombreux consommateurs et employés ne réalisent pas l'importance des données personnelles et ne savent pas comment protéger ces informations de manière optimale.

Presque toutes les attaques contiennent un certain type d'ingénierie sociale, notamment le phishing.

Le phishing : une méthode d'ingénierie sociale

L'hameçonnage (phishing) repose sur des messages électroniques, semblant provenir de sources fiables, visant à manipuler les destinataires afin qu'ils partagent des données à caractère personnel, qu'ils transfèrent de l'argent ou des actifs, qu'ils téléchargent des logiciels malveillants.

Les messages sont conçus d'une manière à ce qu'ils aient l'air de provenir d'une personne connue par la victime ou d'une organisation.

Les techniques de phishing

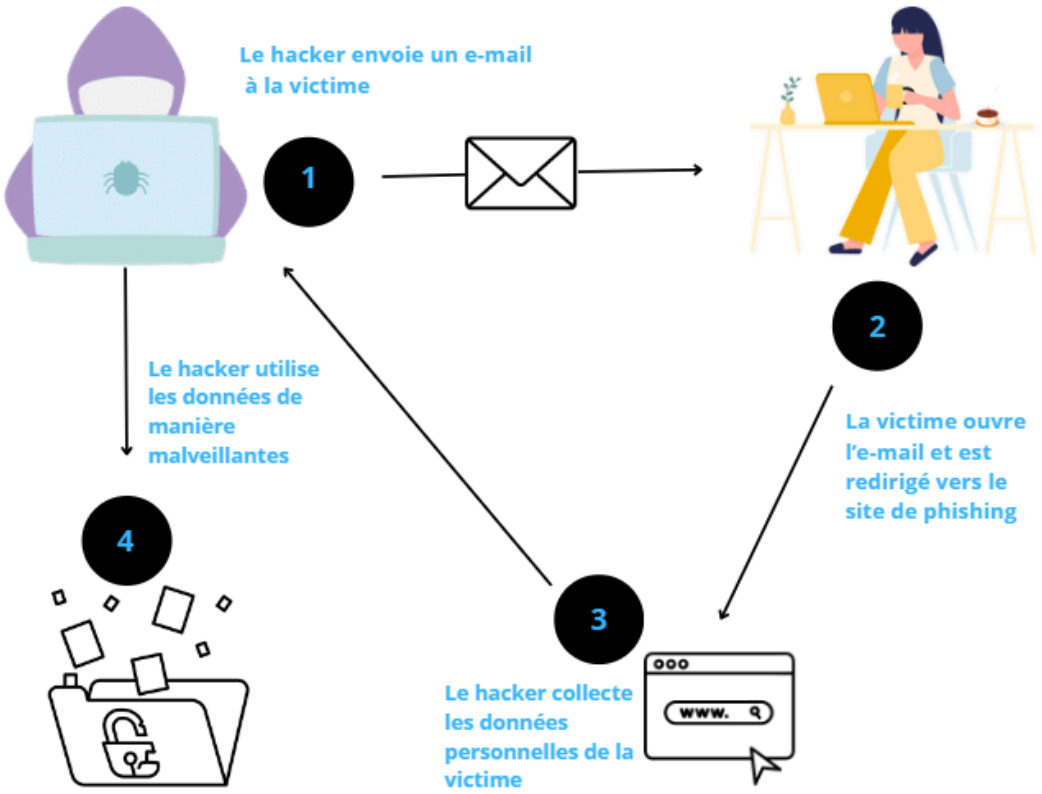
Courrier électronique et spam

Le pirate informatique envoie un message électronique similaire, souvent publicitaire, à un grand nombre de personnes sans leur consentement. Il s'agit d'une méthode d'hameçonnage très répandue.

Ce courrier contient un lien renvoyant vers un site prétendument de confiance pour l'internaute, ce site contenant un formulaire demandant la saisie d'informations personnelles à des fins d'utilisation illégales.

Généralement, l'objet du message évoque une situation urgente à régler (blocage de compte ou de carte de crédit, perte d'argent, vérification du propriétaire du compte…).

Schéma d'une attaque par hameçonnage



Les techniques de spam et courrier électronique

Les attaquants utilisent des techniques et des programmes spécifiques pour générer et diffuser les milliers de spams qui sont distribués chaque jour.

L'activité du spammeur peut se décomposer selon les étapes suivantes :

1. Collecte et vérification d'adresses e-mail, répartition des adresses par groupes de cibles
2. Création de plateformes pour du mailing de masse (serveurs et/ou ordinateurs particuliers)
3. Écriture de programmes de mailing de masse
4. Promotion d'offres de spammeurs
5. Création de textes pour des campagnes spécifiques
6. Envoi de spams

Collecte et création de listes d'adresses

La première mission du travail d'un spammeur est de se créer une base de données d'adresses mail. Derrière chaque adresse mail collectées, des informations complémentaires vont être stockées telles que l'emplacement géographique, le domaine d'activité (s' il s'agit d'une adresse mail d'entreprise) ou les centres d'intérêts (pour les internautes).

Afin de collecter des adresses les spammeurs vont la plupart du temps utiliser des scan de ressources publiques, telles que des sites web, des forums, des sites de discussion… En effet, elles comportent souvent des indications sur les préférences de l'utilisateur, ainsi que d'autres informations personnelles comme l'âge, le sexe, etc.

Types de spam les plus féquents

A travers le monde, les spams vont promouvoir une certaine gamme de services et de produits sans prendre en compte l'emplacement géographique ou la langue.

Ils vont cependant prendre en considération le changement de saison, par exemple, en hiver les spams auront pour objet des offres de cadeaux de Noël ou de chauffage, et l'été des offres de climatisation ou de vacances au soleil.

Les spammeurs diversifient de plus en plus leurs gammes de produits et de services, ils sont en recherche constante de nouveaux pièges pour les utilisateurs peu méfiants.

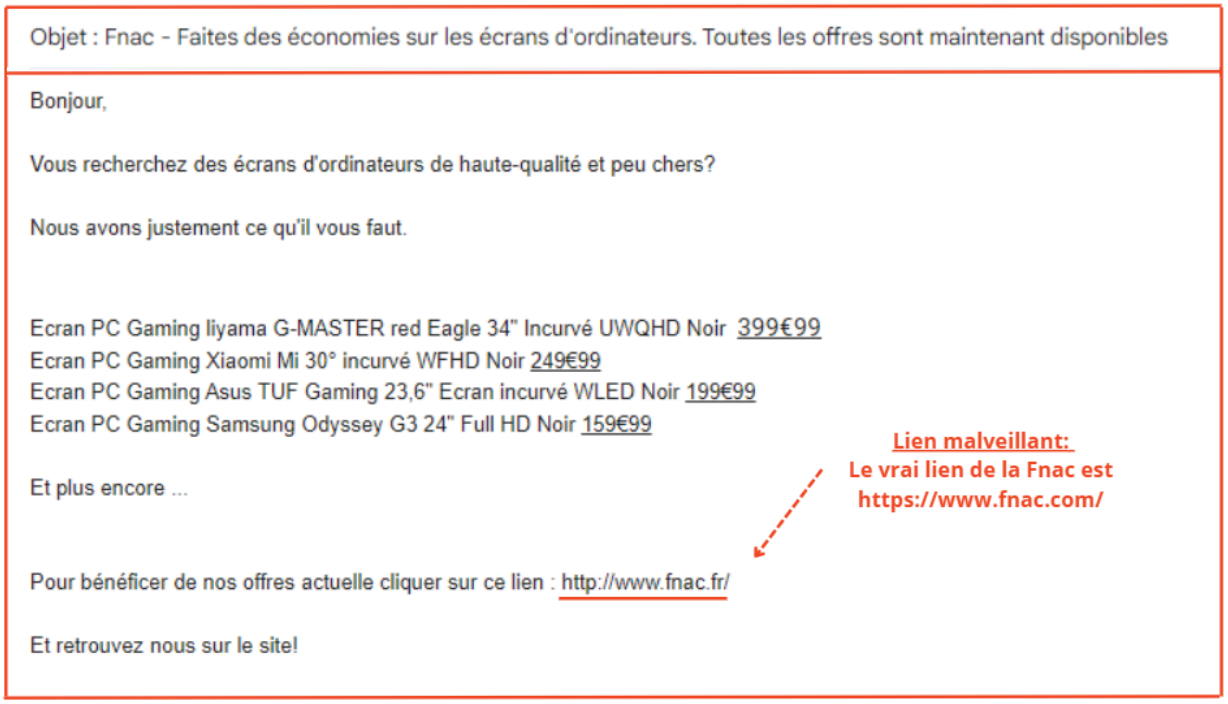
Cependant les types de spam les plus fréquents font partie des catégories suivantes:

- Informatique
- Santé
- Education et formation
- Finances

Informatique

Parmi cette catégorie, les spams proposent le plus souvent des logiciels et du matériel informatique à bas prix, mais également des services pour les propriétaires de sites tels que l'hébergement, les domaines d'enregistrement, etc.

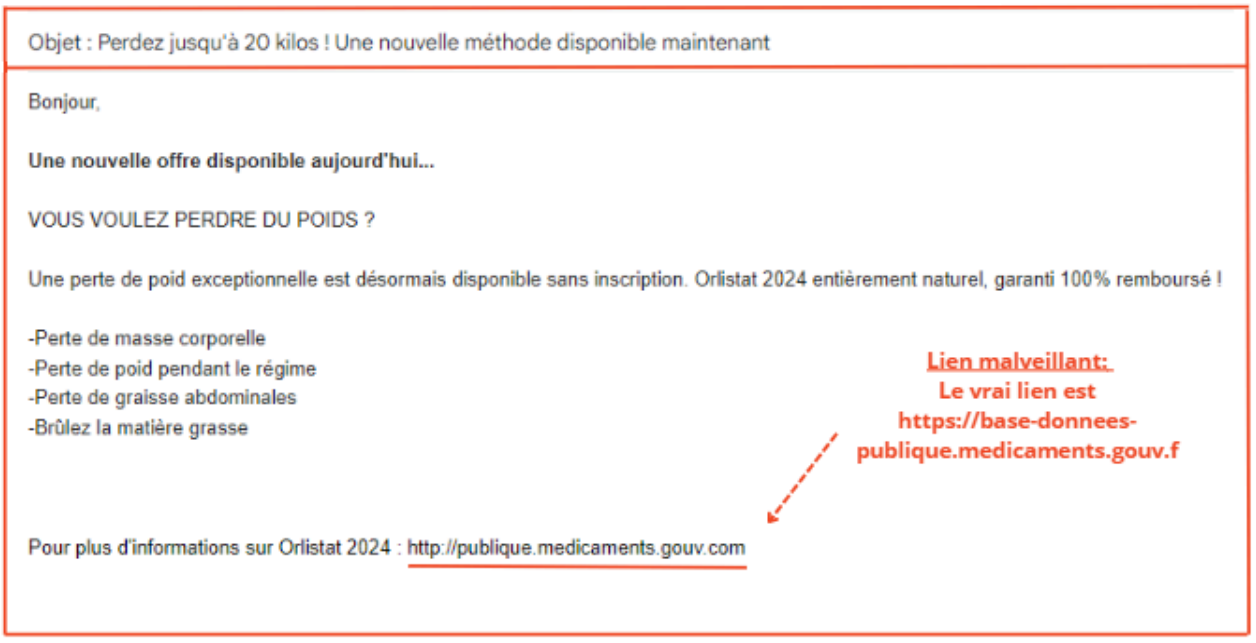
Exemple d'e-mail envoyé : (Phishing par Manipulation de lien)



Santé et médecine

La catégorie Santé et médecines inclut les spams de publicités pour les soins capillaires, les produits de beauté, les crèmes pour le corps, la perte de poids…

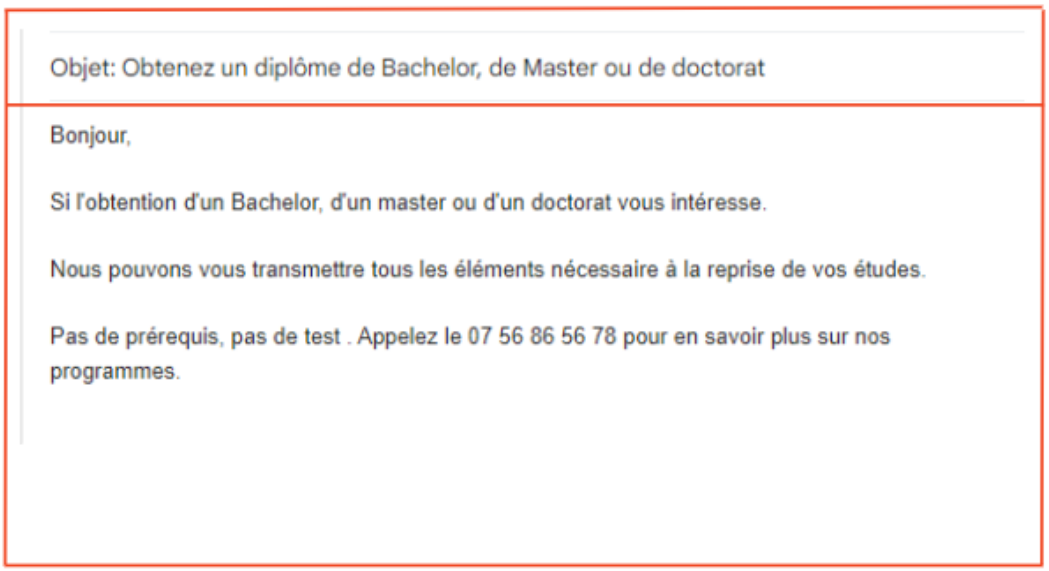
Exemple d'e-mail envoyé : (Phishing par Manipulation de lien)



Education et formation

La catégorie Éducation et formation regroupe toutes les offres de cours et formations en ligne mais également de séminaires.

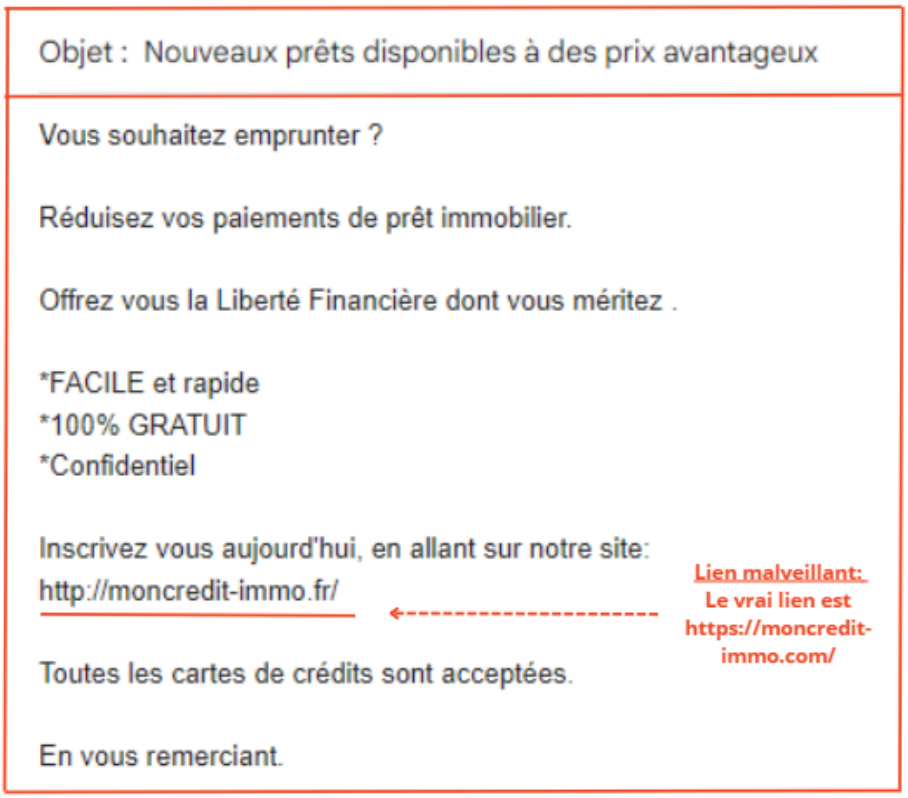
Exemple d'e-mail envoyé :



Finances personnelles

La catégorie Finances personnelles propose des spams de services de réductions de dettes, de prêts à des taux avantageux, des assurances.

Exemple d'e-mail envoyé : (Phishing par Manipulation de lien)



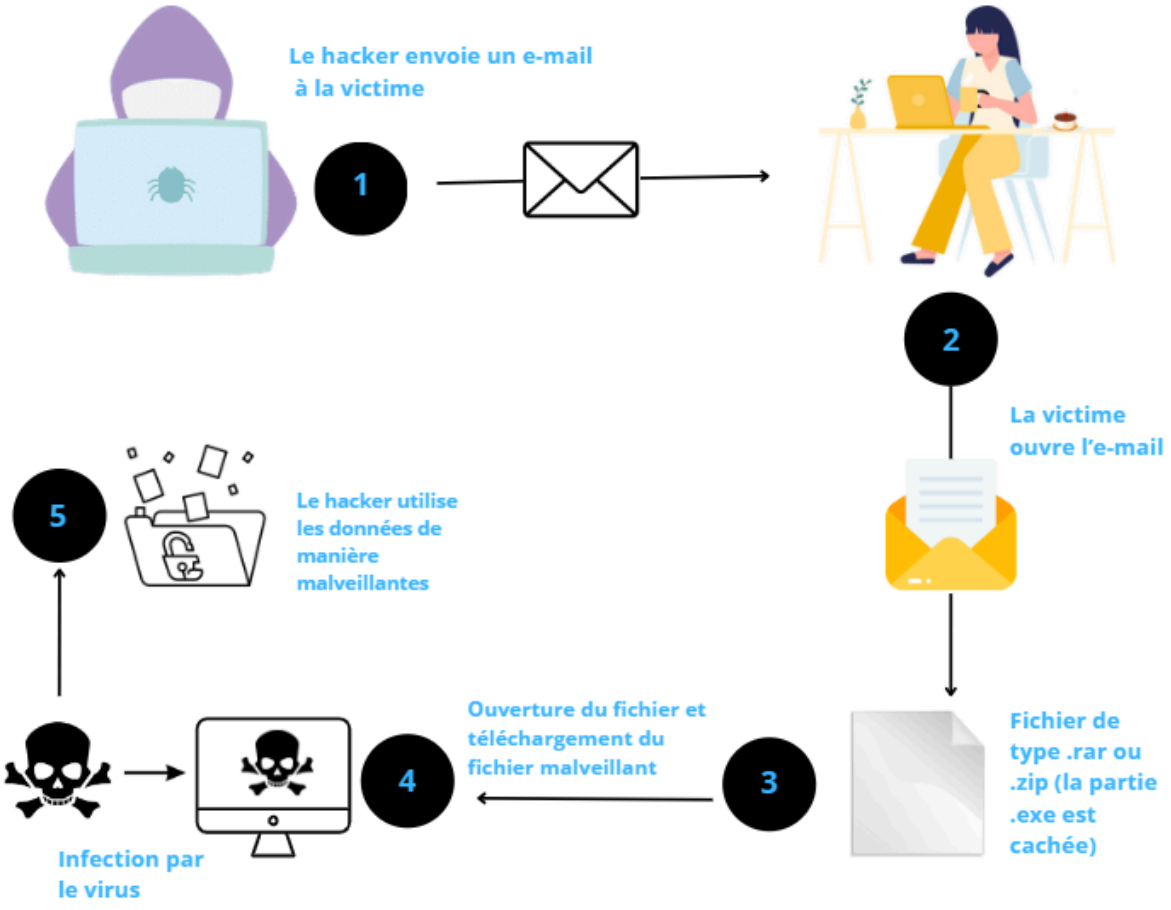
Phishing par logiciel malveillant

Une attaque de phishing par logiciel malveillant est une attaque qui nécessite l'installation de celui-ci sur l'ordinateur de la victime.

Le logiciel malveillant se présente généralement sous la forme d'une pièce jointe dans un courrier électronique, celle-ci est transmise par l'attaquant ou en tant que fichier téléchargeable à partir d'un site internet piraté.

Lorsque la victime clique sur le lien, le logiciel malveillant (malware) commence à fonctionner. Donc quand la victime tentera d'accéder à la véritable page web, en réalité, elle sera automatiquement renvoyée vers une page web falsifiée contre sa volonté.

Schéma d'une attaque par logiciel malveillant



PHISHING EN ENTREPRISE

L'attaque par hameçonnage en entreprise est une méthode employée par les attaquants afin de détourner des fonds et voler des informations sensibles.

Malgré les nombreuses mesures de sécurité et sensibilisation des salariés, le phishing reste une menace importante pour de nombreuses entreprises.

En entreprise, les attaquants utilisent massivement les méthodes de phishing tels que les emails frauduleux pour piéger leurs victimes, mais également la création de sites falsifiés usurpant l'identité de sites web légitimes.

Les risques du phishing en entreprise

Le phishing en entreprise présente 3 grands types de risque:

- Le vol de données sensibles
- La perte de confiance des tiers
- Les pertes financières

Le vol de données sensibles en entreprise

Lors d'une attaque de phishing réussie, un grand nombre de données sensibles peuvent être volées.

Il peut s'agir d'informations bancaires (comme l'identifiant de compte ou des codes d'accès), mais également des données à caractères personnelles ou alors des identifiants de connexion (tels que les noms d'utilisateurs et mots de passe, adresse mail, etc).

Les pirates vont utiliser ces informations afin de s'introduire dans les systèmes de l'entreprise. L'attaquant peut ensuite réaliser un virement vers un compte frauduleux, ou dans les cas les plus graves, engager un risque pour la sécurité nationale en cas de cyberattaques à l'encontre des aéroports, pouvant causer des perturbations néfastes par exemple.

Les pertes financières

Face à des attaques de phishing, les entreprises vont faire face à des coûts directs tels que d'importantes pertes financières, notamment des vols ou des fraudes financières directes, et des transactions non autorisées.

Mais elles vont également devoir faire face à des coûts indirects comme une perte de productivité, des frais juridiques, une perte de confiance des tiers, et un impact sur la réputation de l'entreprise.

Les coûts directs et indirects subis par l'entreprise suite à une attaque par phishing vont entraîner des pertes financières colossales.

La perte de confiance des tiers

Suite à des attaques informatiques, les entreprises peuvent subir en plus de pertes financières importantes, une perte de confiance des tiers.

La réputation de l'entreprise peut être impactée auprès des fournisseurs, clients, investisseurs, etc. Cette perte de confiance de l'entreprise va donc être difficile à rétablir.

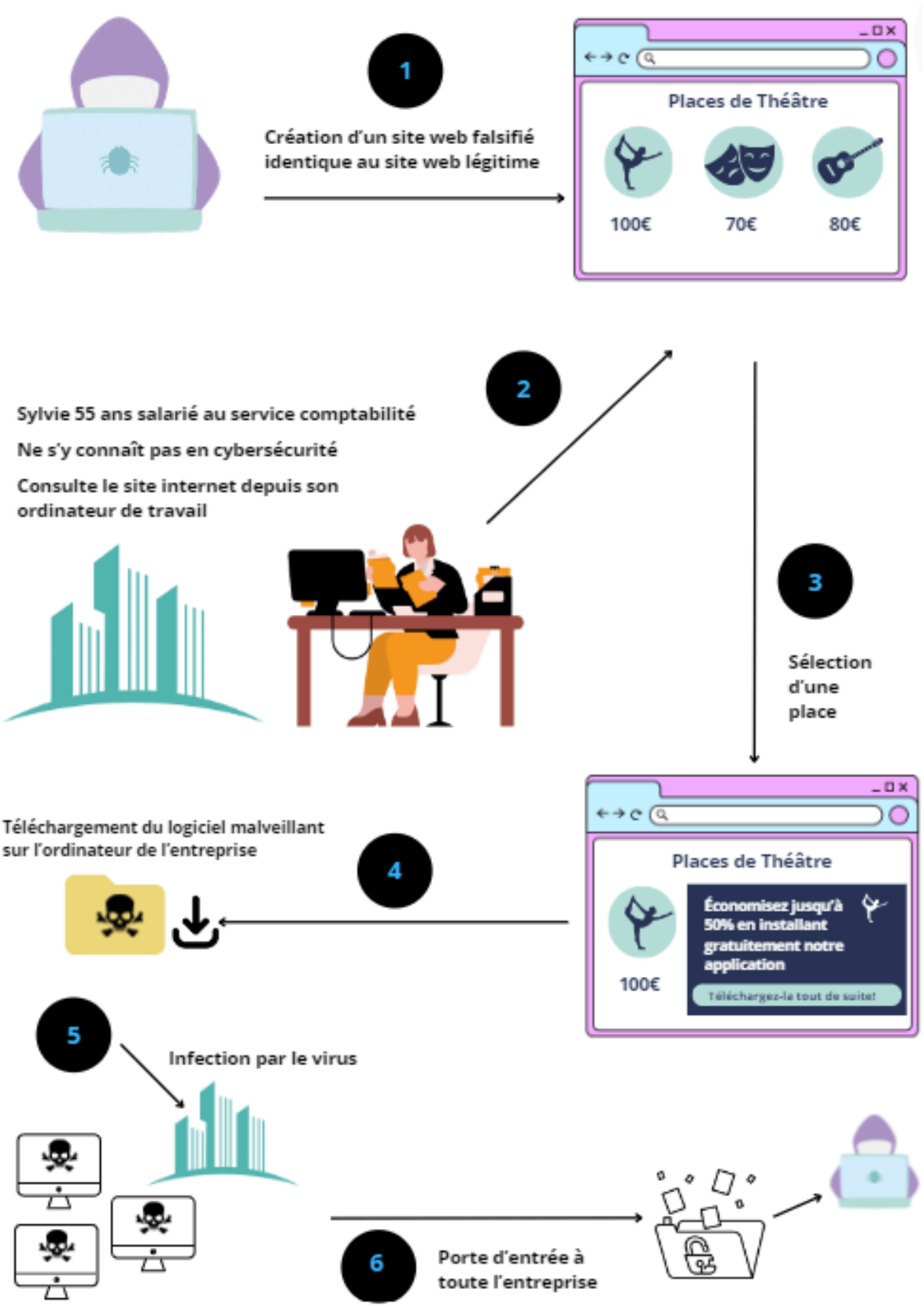
Sensibilisation des salariés aux attaques de phishing

Face à l'augmentation constante des attaques par phishing et des leurs conséquences, il est nécessaire pour les entreprises de mettre en place une formation à la cybersécurité pour leurs salariés.

Avec ces formations, les entreprises pourraient sensibiliser aux attaques par phishing, apprendre aux employés comment identifier et répondre aux e-mails ou messages suspects.

Les employés seraient donc formés à reconnaître et signaler les tentatives de phishing, permettant ainsi la réduction du risque d'en être victime.

Schéma d'une attaque par hameçonnage en entreprise



Les mesures de protection contre le phishing

Afin de se protéger contre le phishing, il est nécessaire d'adopter des mesures comportementales afin d'éviter toutes attaques qui pourraient s'avérer nuisibles.

Mesures comportementales

Il est désormais nécessaire de se tenir informé face aux nouvelles techniques de phishing utilisées dans la mesure où de nouvelles menaces apparaissent de jour en jour. En restant informé, le risque est nettement diminué.

Outre s'informer des nouvelles techniques de phishing , des mesures comportementales sont à adopter afin de diminuer le risque de se faire avoir.

Chiffres clés phishing

Dans cette époque en perpétuelle évolution, on constate de plus en plus de cyberattaques, notamment des attaques par hameçonnage, les chiffres clés des attaques par hameçonnage révèlent l'ampleur alarmante de cette menace.

26,2_milliards de dollars de pertes ont été occasionnées en 2019 par des attaques d'e-mails compromis."

42,8 %_des pièces jointes malveillantes se présentaient sous la forme de documents Microsoft Office

667 %_d'augmentation des attaques par hameçonnage en seulement 1 mois durant la pandémie de COVID-19

30 %_des messages d'hameçonnage ont été envoyés un lundi

32,5 %_de l'ensemble des attaques par courriels comprenaient dans l'objet du message le mot clé «paiement»