ATELIER INITIATION

AU

HAMEÇONNAGE

SOMMAIRE

Les attaques informatiques

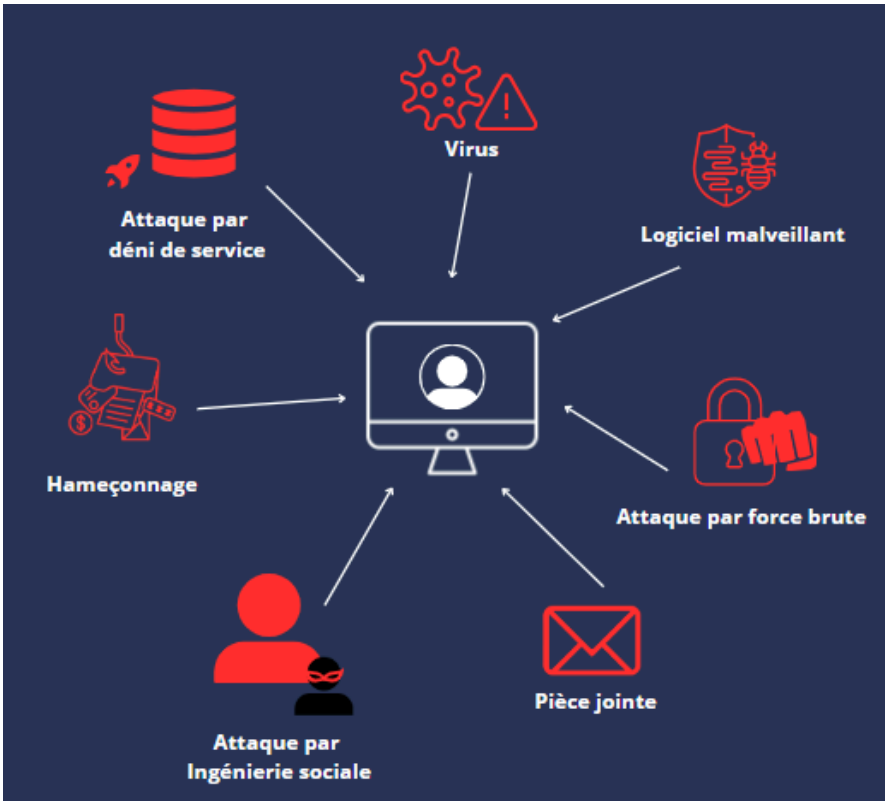
Les attaques informatiques sont des tentatives d'accès volontaires et malveillantes à un système informatique, un ordinateur ou un réseau informatique avec pour but de causer des dommages aux informations et aux personnes qui les traitent.

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.

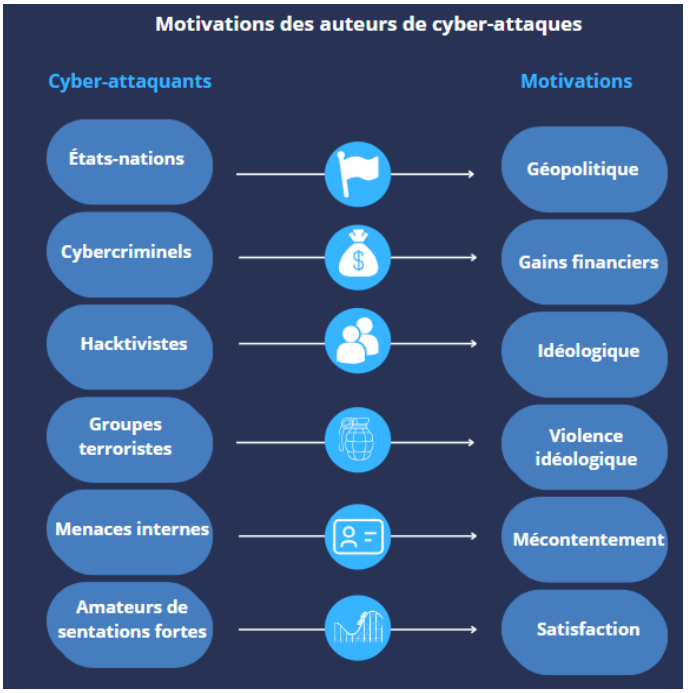
Les attaquants ayant des motivations criminelles sont attirés par le souhait d'un gain financier grâce à un vol de données, d'argent ou une panne.

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

Les attaquants qui ont des motivations personnelles sont quant à eux soit un membre du personnel actuel, soit un ancien membre 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.



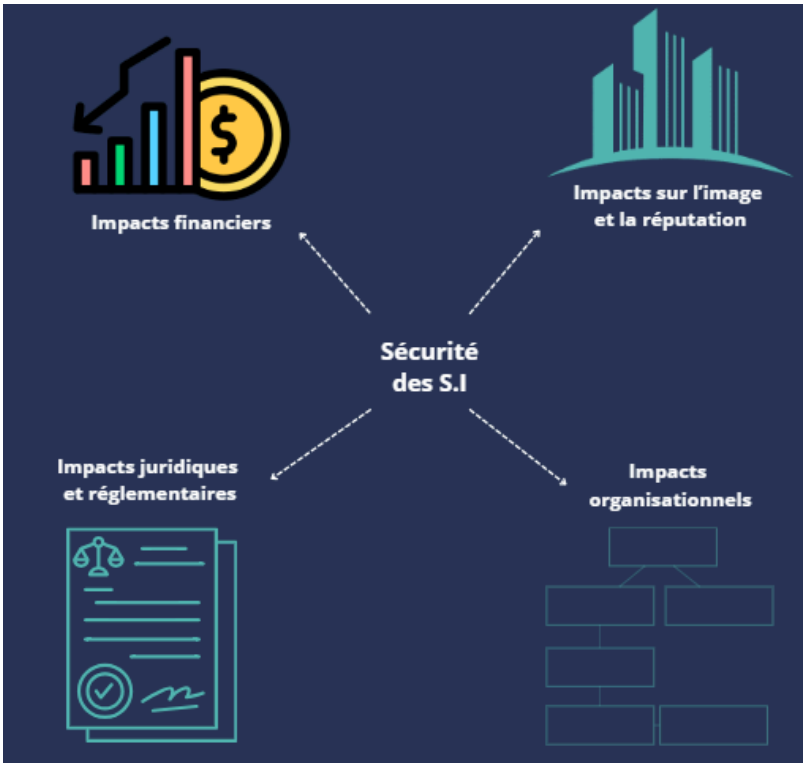
Enjeux de la sécurité des S.I

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 manipulations 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 suivantes :

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 de 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

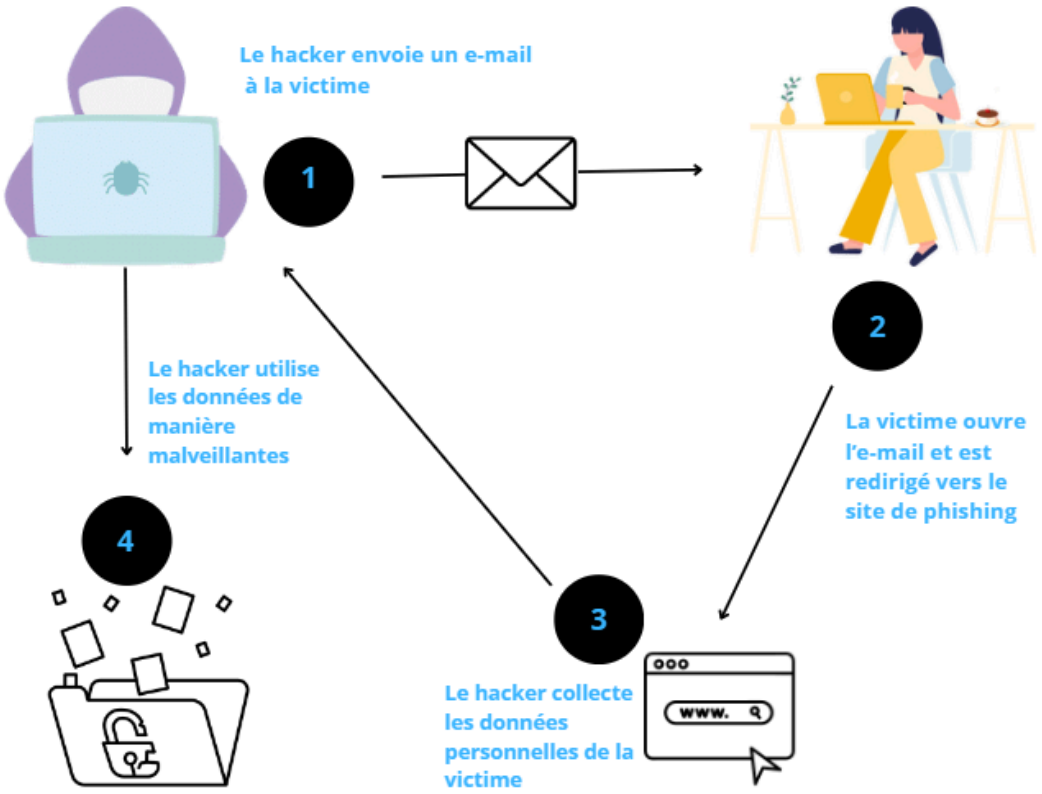
Courrier électronique et spam

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)

Objet : Fnac - Faites des économies sur les écrans d'ordinateurs. Toutes les offres sont maintenant disponibles

Bonjour,

Vous recherchez des écrans d'ordinateurs de haute-qualité et peu chers?

Nous avons justement ce qu'il vous faut.

Ecran PC Gaming Iiyama G-MASTER red Eagle 34" Incurvé UWQHD Noir 399€99
Ecran PC Gaming Xiaomi Mi 30° incurvé WFHD Noir 249€99
Ecran PC Gaming Asus TUF Gaming 23,6" Ecran incurvé WLED Noir 199€99
Ecran PC Gaming Samsung Odyssey G3 24" Full HD Noir 159€99

Et plus encore ...

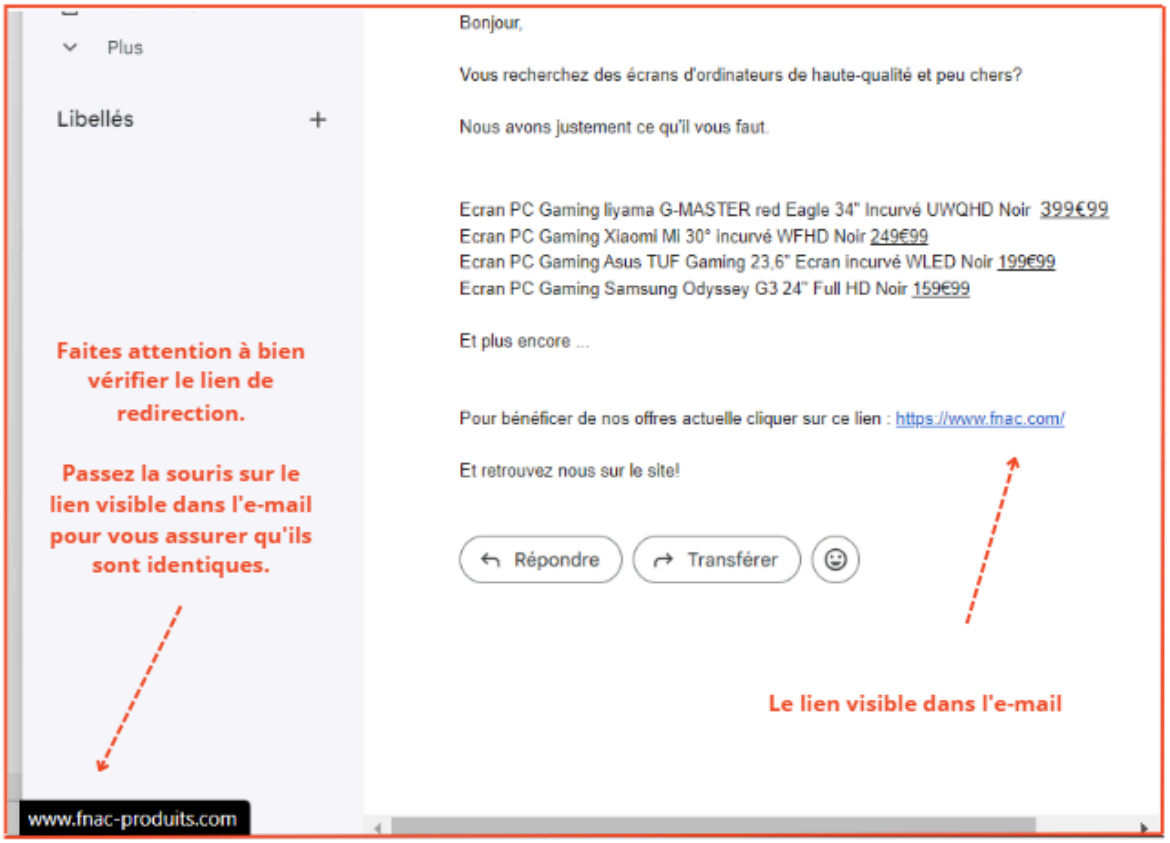
Véritable lien vers le vrai site de la fnac

Pour bénéficer de nos offres actuelle cliquer sur ce lien : https://www.fnac.com/

Accéder au lien : https://www.fnac-produits.com/ | Modifier | Supprimer

Et retrouvez nous sur le site!

Lien vers le site web falsifié



Santé et médecine

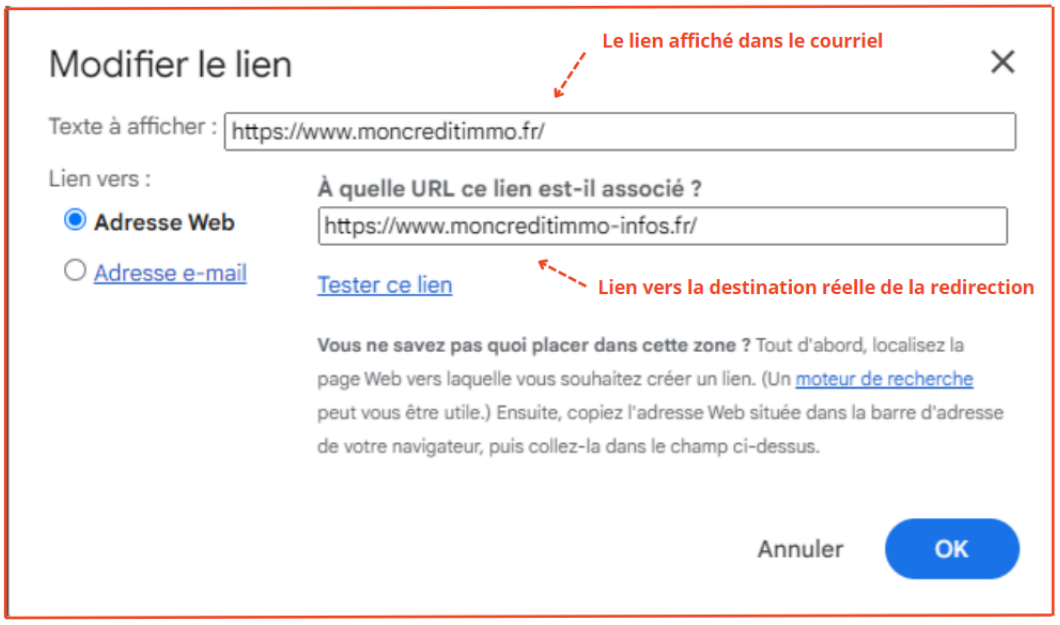
La catégorie Santé et médecines inclut les spams de publicités pour les soins capillaires, les produits de beauté, les crèmes pour le corps, la perte de poids…

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

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)



Nouveaux prêts disponibles à des prix avantageux

Vous souhaitez emprunter?

Réduisez vos paiements de prêt immobilier.

Offrez vous la Liberté Financière dont vous méritez.

*FACILE et rapide
*100% GRATUIT
*Confidentiel

Inscrivez vous aujourd'hui, en allant sur notre site:
https://www.moncreditimmo.fr/ **Véritable lien vers le vrai site**

Accéder au lien : https://www.moncreditimmo-infos.fr/ | Modifier | Supprimer

Lien vers le site web falsifié

Vous souhaitez emprunter?

Réduisez vos paiements de prêt immobilier.

Offrez vous la Liberté Financière dont vous méritez.

*FACILE et rapide
*100% GRATUIT
*Confidentiel

Inscrivez vous aujourd'hui, en allant sur notre site:
https://www.moncreditimmo.fr/

Le lien visible dans l'e-mail

Répondre Transférer

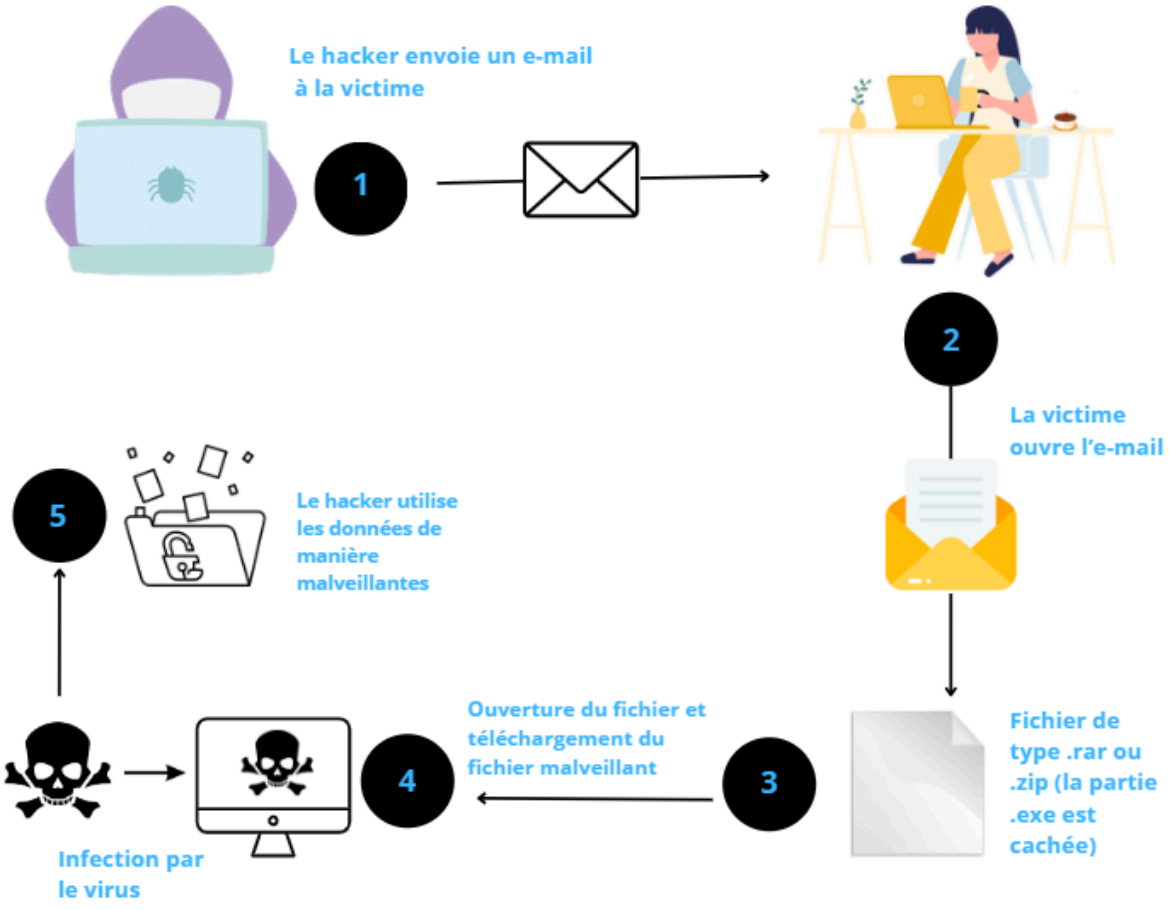
Phishing par logiciel malveillant

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.

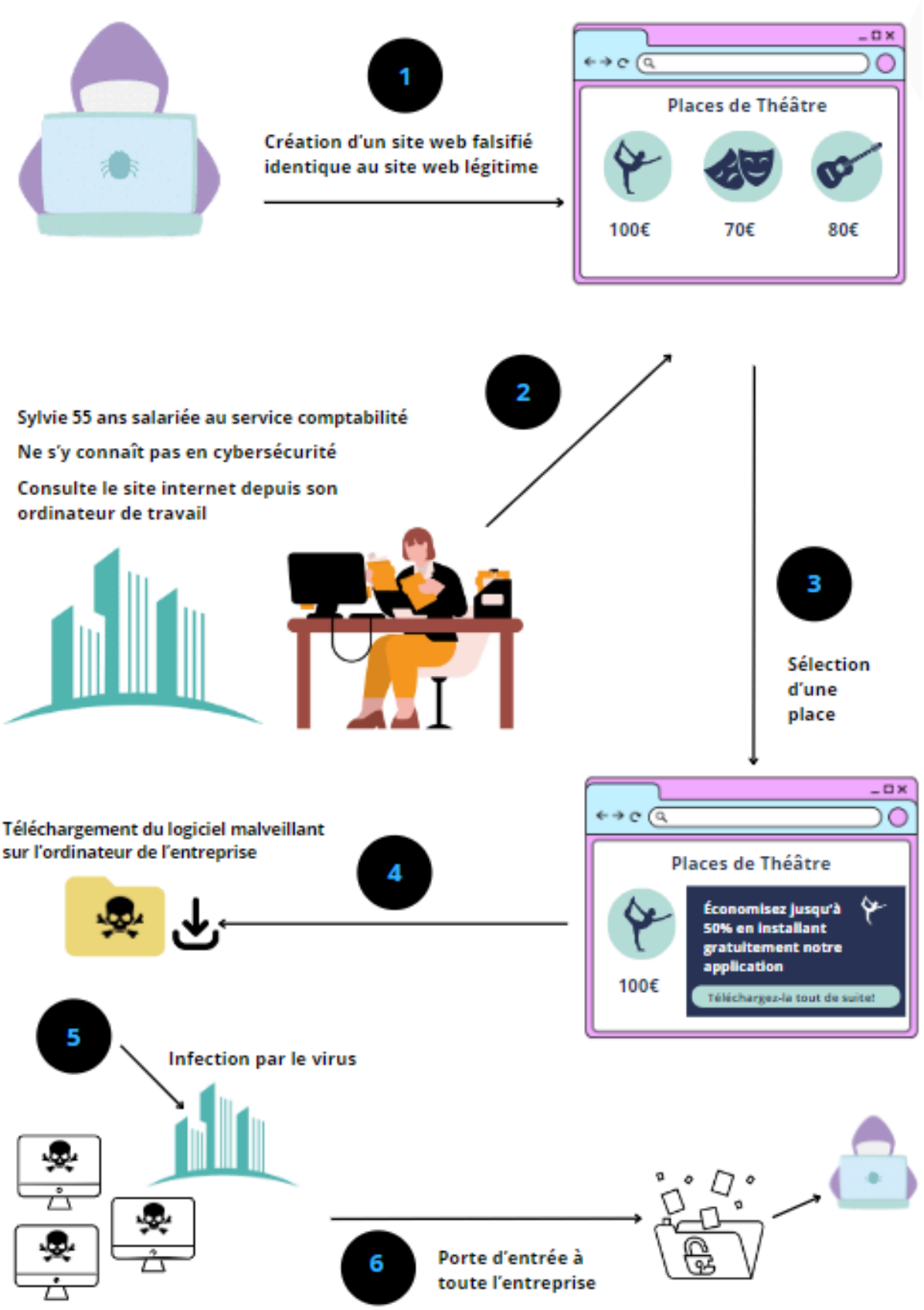
Sensibilisation des salariés aux attaques de phishing

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.

Procédures de Contact en Cas de Phishing : Qui Informer et Comment Réagir

Face à cette menace, la mise en place de procédures de contact appropriées est cruciale pour contrer les attaques et protéger les utilisateurs en ligne.

Les Entités à Contacter : Si vous pensez avoir été victime de phishing, commencez par contacter directement l'entreprise ou la plateforme en question. Signalez l'incident au service client en fournissant autant de détails que possible sur la tentative de phishing. Cette première étape est cruciale pour bloquer d'éventuelles attaques futures et protéger d'autres utilisateurs.

Les Organisations Gouvernementales : Les personnes confrontées au phishing peuvent également se tourner vers les organisations gouvernementales spécialisées dans la lutte contre la cybercriminalité. En France, par exemple, la Commission nationale de l'informatique et des libertés (CNIL) joue un rôle central dans la réception des plaintes liées à la cybercriminalité. Ces agences sont expertes dans la collecte d'informations sur les fraudes en ligne et offrent un moyen supplémentaire de signaler de tels incidents.

Organisations Spécialisées et Mécanismes de Signalement Intégrés :

Pour lutter contre le phishing, vous pouvez également faire appel à des organisations spécialisées telles que l'Anti-Phishing Working Group (APWG), qui œuvre à l'échelle internationale pour contrer cette menace. Parallèlement, de nombreuses plateformes en ligne proposent des options de signalement intégrées. Il est recommandé aux utilisateurs d'utiliser ces fonctionnalités pour signaler les activités malveillantes, que ce soit par le biais d'e-mails, de messages sur les réseaux sociaux ou d'autres plateformes.

Le Phishing sur les réseaux sociaux

De nos jours, le phishing est de plus en plus présent notamment sur les réseaux sociaux, ce type de phishing désigne une attaque réalisée sur des plateformes telles qu'Instagram, Linkedin, Facebook ou Twitter. Le but de ce type d'attaque étant de voler des données à caractères personnelles ou de prendre le contrôle de votre compte de réseaux sociaux.

Les réseaux sociaux sont devenus omniprésents, on les utilise pour prendre contact avec notre famille, nos amis mais également pour rester informé des dernières nouvelles, se connecter au monde.

Les entreprises utilisent également ces plateformes à des fins commerciales, ainsi que pour attirer des nouveaux clients, c'est pourquoi les réseaux sociaux sont devenus intéressant pour les pirates informatiques voulant réaliser des attaques de phishing.

Les attaquants cherchent à récupérer des informations comme les identifiants de connexion, des informations de cartes bancaires, ou encore des informations à caractères personnelles vous concernant, afin de les utiliser par la suite à des fins malveillantes pour lancer d'autres attaques et escroqueries par exemple.

Phishing sur Instagram

Instagram est une plateforme de partage de photographies, de vidéos et de messages, c'est le réseau social de l'esthétisme.

Il permet aux utilisateurs de partager leurs expériences et moments de vie en postant des photos et de courtes vidéos, comme une sorte de journal intime.

Une attaque de phishing sur Instagram débute par la création d'une page de connexion à Instagram falsifiée par un pirate informatique. Afin de vous tromper, les pages falsifiée sont conçues à l'identique du vrai site.

Lorsque vous renseignez un identifiant et un mot de passe Instagram sur le site falsifiée, l'attaquant récupère vos informations d'identifications.

Généralement, vous êtes redirigé vers la véritable page de connexion au site Instagram pour vous authentifier à nouveau, cependant il est déjà trop tard.

1

Création d'un site web falsifié identique au site web légitime

2

Envoi d'un courriel redirigeant vers le site falsifié

Redirection vers le site falsifié
+
Saisie des informations d'identification

4

5

Récupération des informations dans une Base de donnée qui stocke l'identifiant et le mot de passe de la victime

3

La victime ouvre le mail et clique sur le lien malveillant

Vol des données d'identification Instagram

6

Exemple concret Phishing sur Instagram

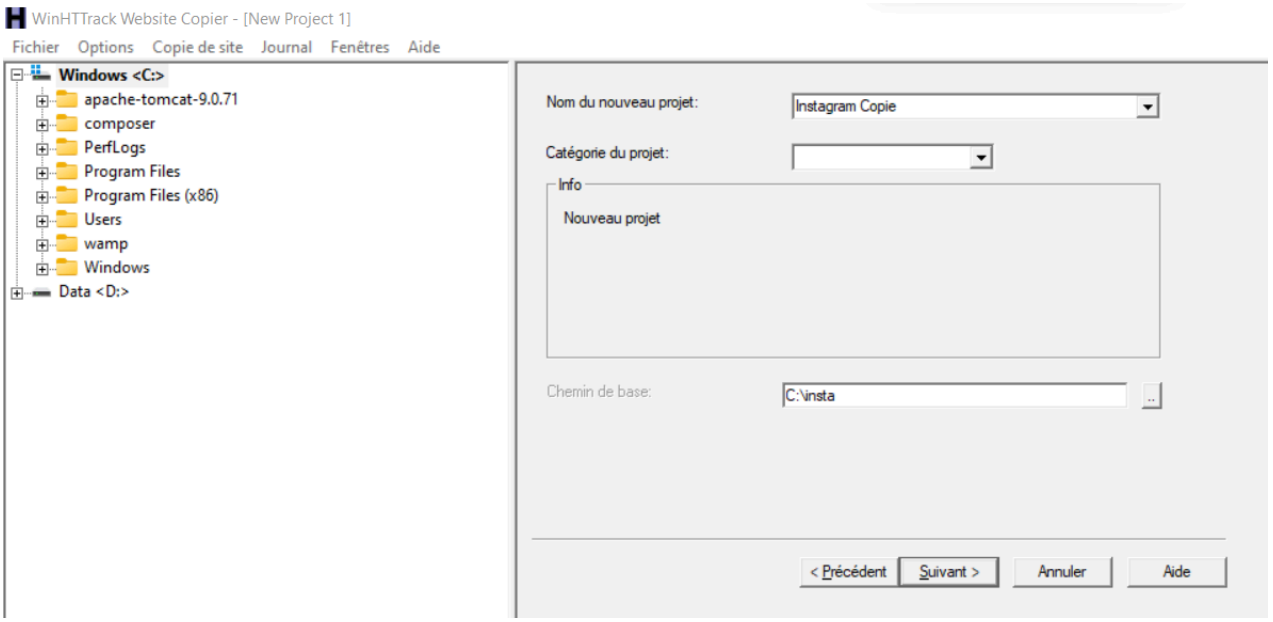
ÉTAPE 1 - Création d'un site web falsifié

Après avoir choisi la plateforme qu'il va utiliser pour réaliser ses attaques par hameçonnage, le pirate va donc faire en sorte de réaliser la création d'une page de connexion à Instagram falsifiée, afin de vous tromper, les pages falsifiées sont conçues à l'identique du vrai site.

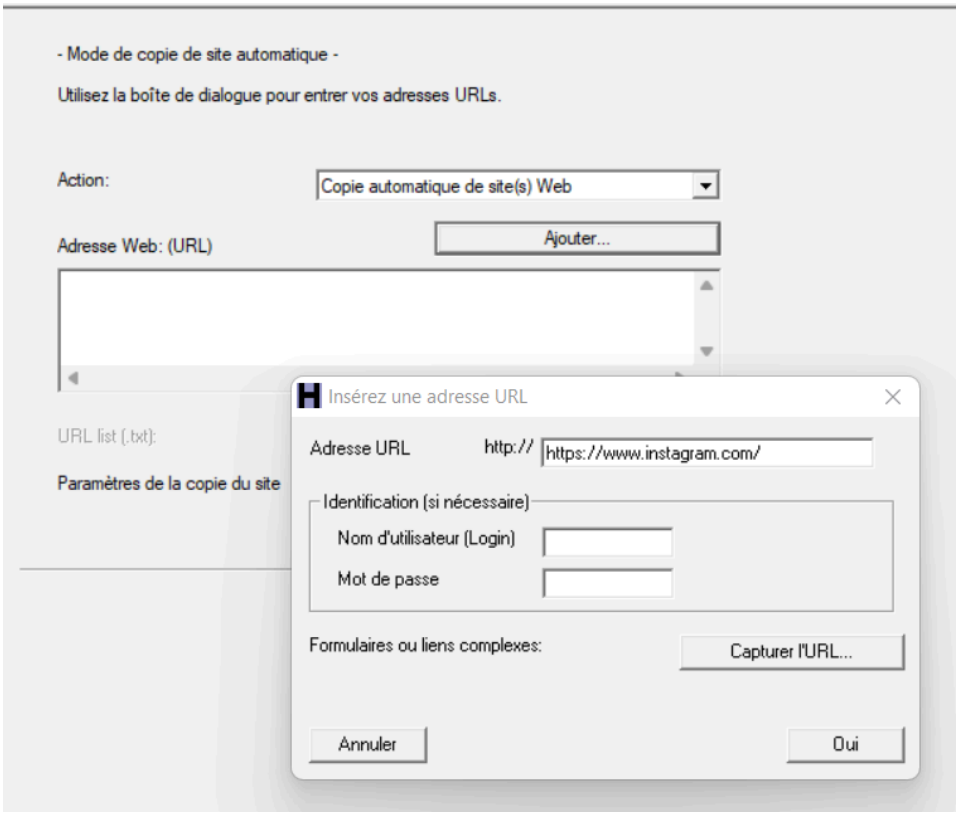
Pour cela le pirate va utiliser de nombreuses techniques et divers logiciels permettant d'aspirer un site à l'identique, par exemple certains attaquants vont utiliser le logiciel HTTrack qui est un logiciel permettant de copier un site web, également appelé "aspirateur de site Web" , c'est un logiciel libre d'accès et utilisable par tout le monde distribué sous la licence GPL.

Exemple d'utilisation du logiciel HTTrack :

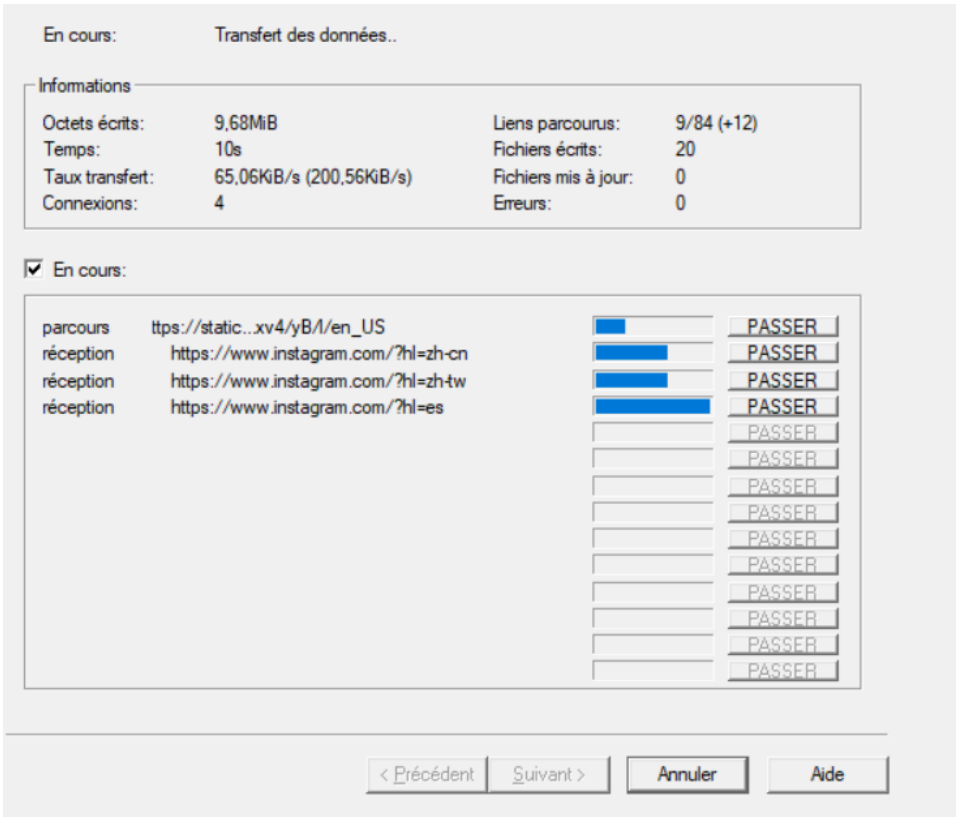
Le pirate crée un nouveau projet.



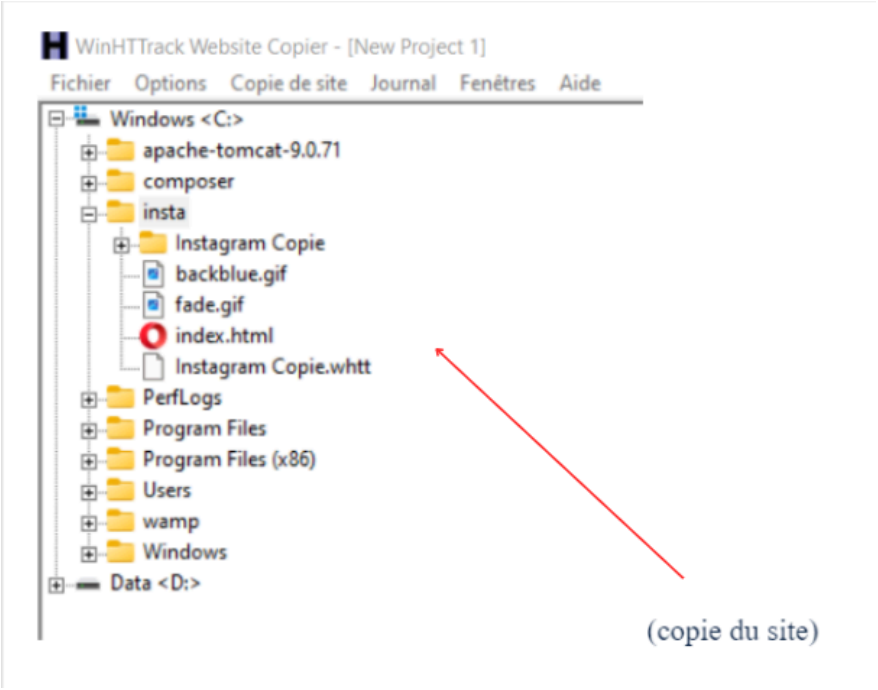
Puis il copie l'adresse URL du site original qu'il souhaite falsifié.



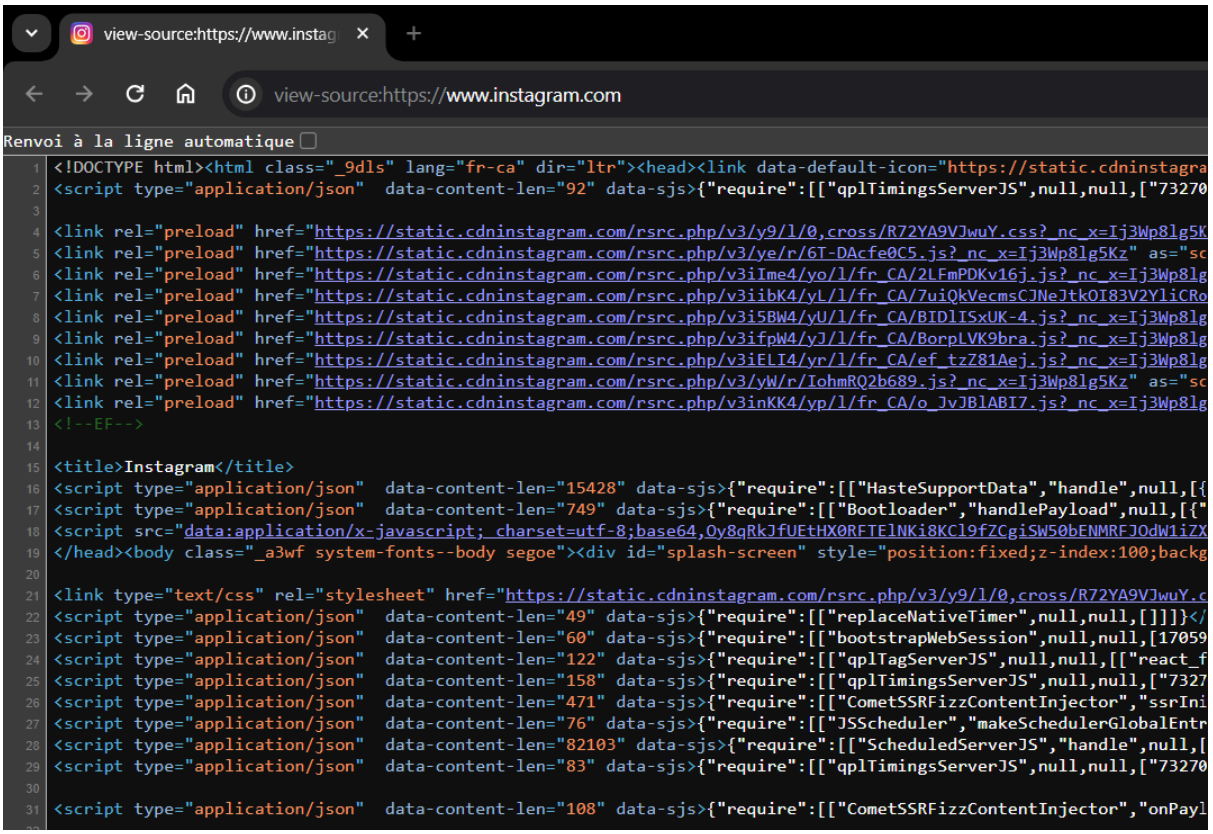
Puis lance l'aspiration et donc la copie du site web.



Il a plus qu'à adapter le site à sa convenance pour piéger les victimes.



Les pirates informatiques utilisent également de nombreuses autres techniques, ils peuvent copier le code source du site authentique en se rendant sur leur navigateur web comme Google par exemple, et en faisant un clique droit sur la page du site web qu'ils souhaitent falsifié, puis en sélectionnant "afficher le code source de la page".



Tous les codes sources des sites web étant accessibles aux utilisateurs, ils peuvent facilement être copiés, ce qui peut être dangereux, cependant la plupart des développeurs utilisent des méthodes permettant de rendre le code source illisible aux utilisateurs.

Néanmoins, les pirates expérimentés peuvent copier le site à la main, en réalisant la copie du code et du design à la main, en ajoutant les éléments tels que les photos et le texte correspondant eux-mêmes.

```
<!DOCTYPE html>
<html lang="fr">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
      <meta name="description" content="Instagram">
      <link rel="shortcut icon" href="img/icon.png" type="image/x-icon">
    <link rel="stylesheet" href="css/style.css">
    <title>Instagram Login</title>
</head>



<body onload="SwitchScreen()">
        <section class="container">
            <!-- SMARTPHONE SECTION -->
            <article class="smartphone">
                <div class="screens">
                    <img class="screen fade" src="img/screen1.png" alt="screen1">
                    <img class="screen fade" src="img/screen2.png" alt="screen2">
                    <img class="screen fade" src="img/screen3.png" alt="screen3">
                </div>
                <img src="img/smartphones.png" alt="smartphones">
            </article>
            <!-- SMARTPHONE SECTION END -->
            <!-- FORM SECTION -->
```

Pour cela les pirates informatiques vont utiliser des éditeurs de code tels que visual Studio Code qui est un logiciel utilisé par les développeurs de sites web pour créer et modifier du code source informatique, sur ces éditeurs de code on utilise les langage informatiques HTML et CSS pour la réalisation d'un site web simple.

C'est quoi HTML et CSS, en fait ?

Imaginons que tu veux créer une maison sur Internet, c'est-à-dire un site web. HTML (HyperText Markup Language) et CSS (Cascading Style Sheets) sont comme les architectes et les décorateurs de cette maison virtuelle.

HTML (L'architecture de la maison) :

HTML agit comme la structure fondamentale. C'est un peu comme les plans détaillés d'une maison qui indiquent où se situent chaque pièce, comme la cuisine, la chambre et la salle de bain. De la même manière, HTML décrit la disposition et la structure de ton site web.

Chaque élément de la page web, comme le titre, les paragraphes, les images et les liens, a son propre code HTML dédié. C'est ce code qui permet au navigateur web de comprendre comment organiser et afficher les différentes parties de ton site.

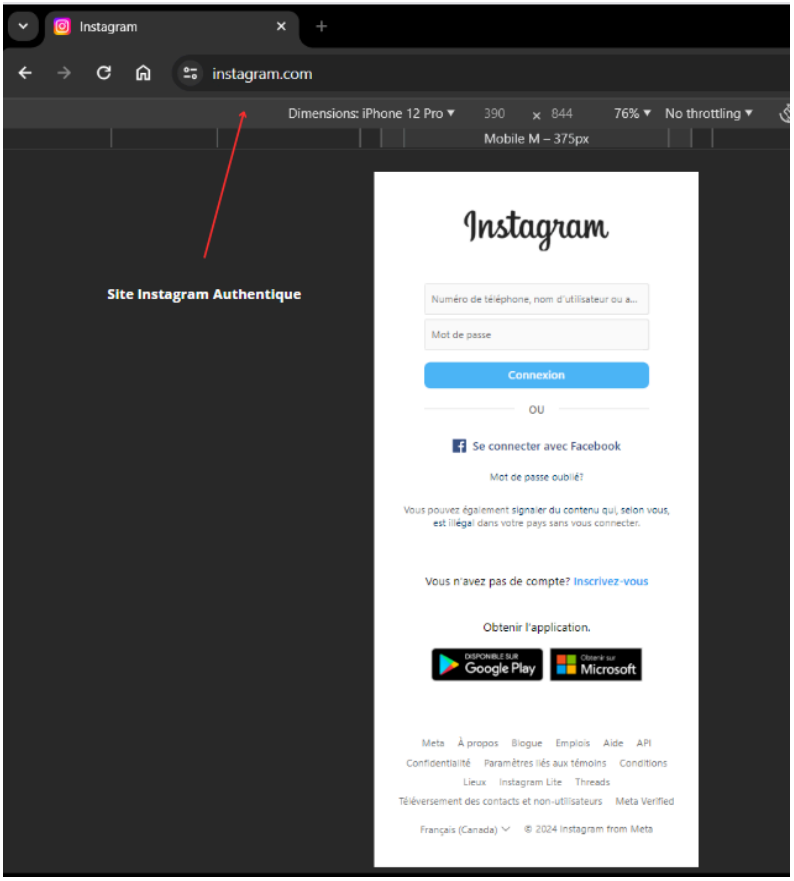
CSS (La décoration de la maison) :

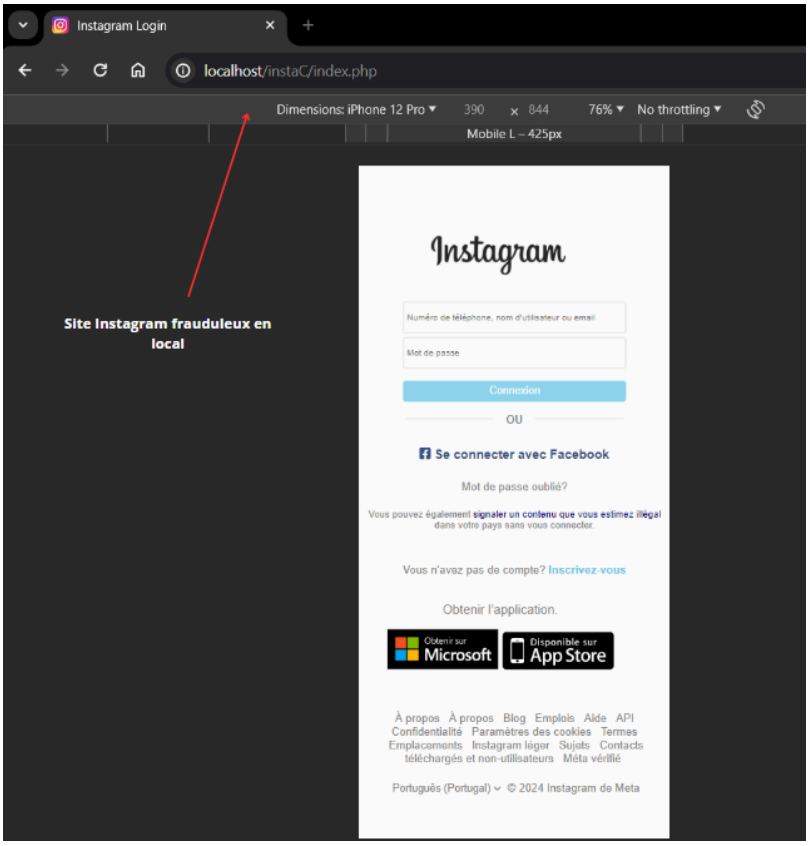
D'autre part, CSS est comparable à la décoration de la maison. Imagine que tu veux que les murs soient peints en bleu, les meubles soient en bois et les rideaux soient rouges. CSS te donne la possibilité de faire ces choix pour ton site web.

Avec CSS, tu as le pouvoir de définir l'apparence visuelle de chaque élément de ta page web. Tu peux spécifier la couleur, la taille, la police du texte, et bien d'autres aspects. Cela contribue à rendre ton site web attrayant et plaisant à regarder, un peu comme décider comment décorer et aménager une maison.

En résumé, HTML établit la structure de base de ton site web, à la manière des plans d'une maison, tandis que CSS ajoute la touche décorative, rendant tout esthétique et personnalisé, comme la décoration d'une maison.

Comparaison entre un site Instagram authentique et un site Instagram frauduleux





Nous pouvons voir que les différences entre un site Instagram authentique et un site Instagram frauduleux sont vraiment infimes.

Cependant, si nous examinons de plus près les subtiles différences, dans un premier temps, un site Instagram authentique, géré par la plateforme officielle, présente généralement un design professionnel et cohérent. Les logos, les icônes et la mise en page sont soigneusement élaborés pour offrir une expérience utilisateur claire et familière.

En revanche, un site Instagram frauduleux peut tenter de reproduire ces éléments visuels, mais les détails peuvent révéler des imperfections. Par exemple, les logos pourraient être légèrement déformés, la mise en page pourrait manquer de précision, ou il pourrait y avoir des erreurs de grammaire et d'orthographe dans le contenu.

Un autre indice subtil peut se trouver dans l'URL du site. Les sites officiels d'Instagram utilisent généralement des URL bien établies et sécurisées, commençant par "https://" pour indiquer une connexion sécurisée. Les sites frauduleux peuvent tenter de copier cela, mais une attention particulière révélera parfois des différences mineures dans l'adresse, telles que des fautes de frappe ou l'utilisation de sous-domaines suspects.

En fin de compte, bien que les sites frauduleux puissent sembler authentiques à première vue, une analyse minutieuse permet souvent de détecter ces subtiles différences. Il est donc crucial d'être vigilant et de vérifier attentivement l'authenticité des sites que nous visitons, surtout lorsqu'il s'agit de plateformes populaires comme Instagram.

ÉTAPE 2 - Envoi d'un courriel redirigeant vers le site frauduleux

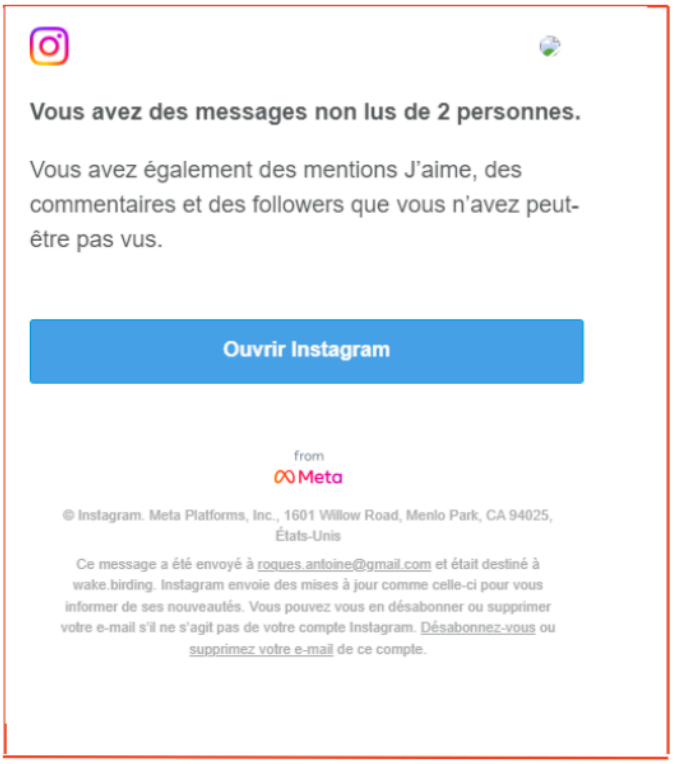
Généralement, afin de leurrer la victime, les attaquants envoient un e-mail prétendument légitime, souvent déguisé en provenance d'une source de confiance, avec un contenu trompeur.

Le courriel contient généralement un message alarmant ou indicatif pour inciter la victime à prendre des mesures immédiates, cela peut inclure des menaces de fermeture de compte, des alertes de sécurité ou de promotion attractives.

L'e-mail contient un lien qui semble légitime, mais en réalité, redirige la victime vers un site frauduleux conçu pour ressembler à celui d'une entité de confiance, ce site est souvent une imitation de la page de connexion d'un service populaire, ici dans notre exemple il s'agit de la page de connexion d'Instagram.

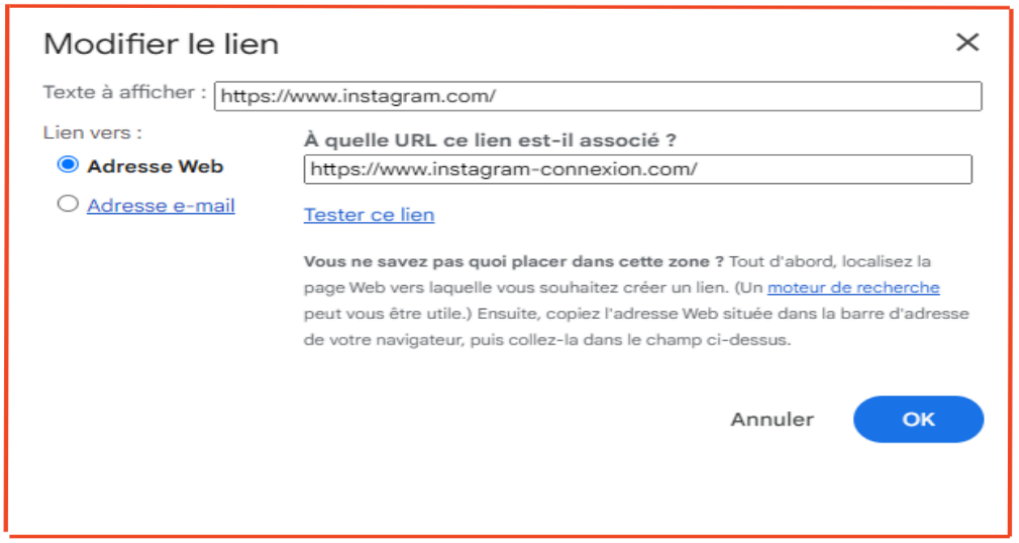
Une fois sur le site frauduleux, si la victime saisit ses informations d'identification, celles-ci sont capturées par les attaquants, ces informations peuvent par la suite être utilisées de manière frauduleuse.

Exemple de courriel redirigeant vers le site Instagram frauduleux par la falsification d'un lien:



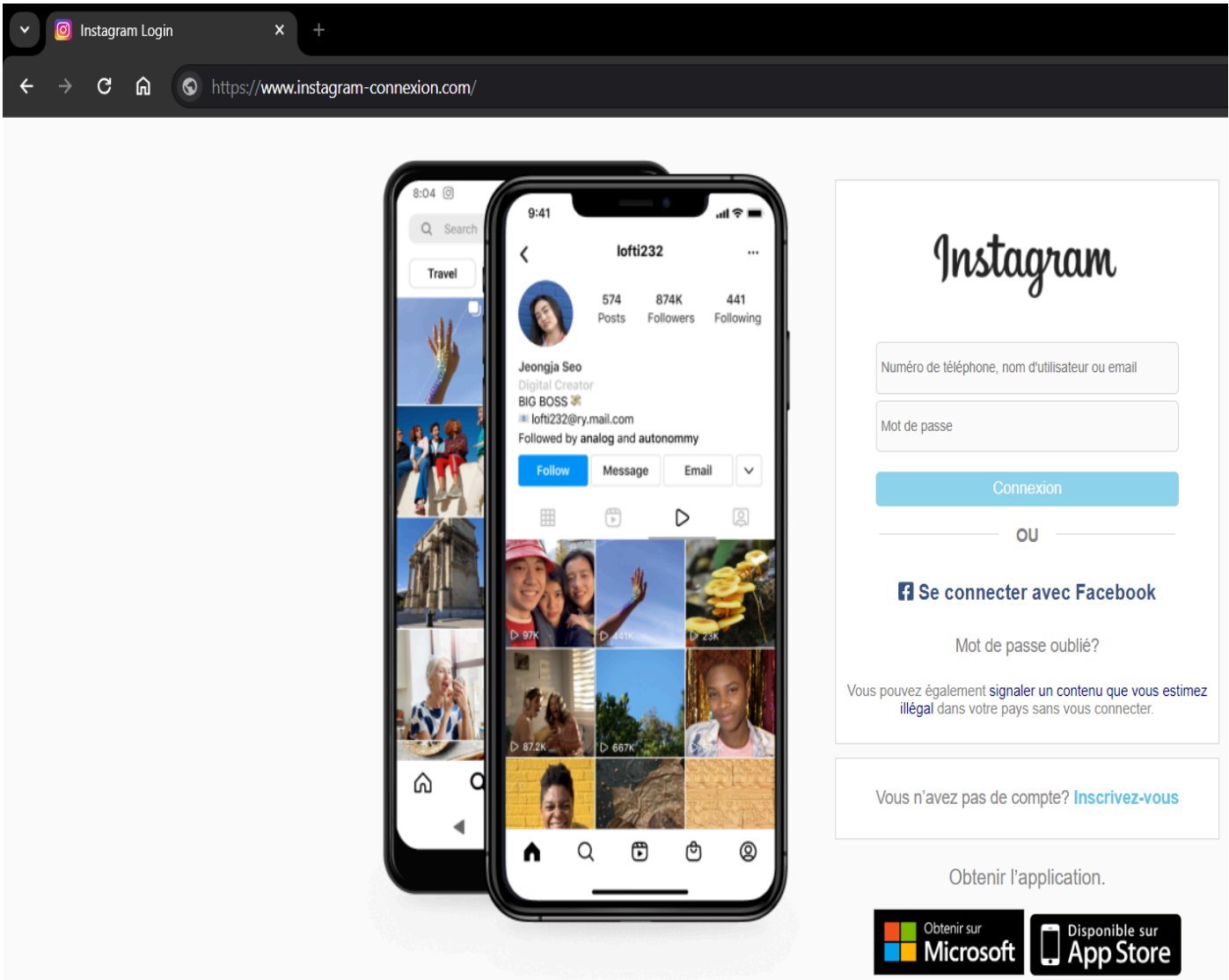
Exemple de courriel semblant provenir d'une source fiable redirigeant vers le site frauduleux

Exemple de falsification d'un lien



Lorsqu'on clique sur le lien "Ouvrir Instagram" on est redirigé vers la page de Connexion Instagram falsifiée.

ÉTAPE 3 - Le Piège de Redirection



Lorsque la victime saisit les champs du formulaire de connexion, tels que l'identifiant et le mot de passe, puis appuie sur le bouton de connexion, les données sont rassemblées dans une requête HTTP POST pour des raisons de sécurité. Cette requête est ensuite envoyée au serveur web associé au formulaire.

Le serveur, recevant la requête, procède au traitement des informations transmises. Normalement, ces informations seraient enregistrées dans la base de données du service légitime (comme Instagram) pour permettre l'authentification de la victime lors de

connexions ultérieures. Cependant, dans le scénario malveillant que nous décrivons, les données sont enregistrées dans la base de données du pirate informatique.

Si l'enregistrement dans la base de données du pirate est réussi, le serveur frauduleux renvoie une réponse au navigateur de la victime, confirmant l'enregistrement. À ce stade, la victime est généralement redirigée vers la page d'accueil d'Instagram pour dissimuler toute activité malveillante et maintenir l'apparence de la légitimité.

Le piège réside dans le fait que, même si la victime est redirigée vers la page d'accueil d'Instagram, les données de connexion (identifiant et mot de passe) ont déjà été capturées par le pirate. Même si la victime se rend compte de la redirection et tente de se reconnecter à son compte, le pirate dispose déjà des informations nécessaires pour accéder au compte de la victime.

En résumé, la victime est induite en erreur par la redirection vers la page d'accueil légitime d'Instagram après avoir saisi ses informations de connexion, mais en réalité, ces informations ont été discrètement enregistrées par le pirate informatique.

Exemple concret de code pour l'enregistrement dans une base de données.

```
<form action="bd.php" method="post">
                    <input type="email" name="username" id="username" placeholder="Numéro de téléphone,
nom d'utilisateur ou email">
                    <input type="password" name="password" id="password" placeholder="Mot de passe">
                    <input type="submit" name="submit" value="Connexion">
</form>
```

Ce formulaire HTML est conçu pour recueillir un nom d'utilisateur (qui peut être un numéro de téléphone, un nom d'utilisateur ou une adresse e-mail) et un mot de passe. Lorsque l'utilisateur appuie sur le bouton "Connexion", ces informations sont envoyées à un fichier PHP appelé "bd.php" pour traitement. Ce fichier PHP peut vérifier les informations et permettre ou refuser l'accès en fonction des données fournies.

```php
<?php
// Connexion à la base de données (à adapter selon vos paramètres)
$servername = "localhost";
$username = "nomUtilisateur";
$password = "password";
$dbname = "insta";

$bdd = new PDO("mysql:host=$servername;dbname=$dbname", $username, $password);

// Vérification de la connexion
if (!$bdd) {
    die("La connexion a échoué.");
}

// Vérification si le formulaire a été soumis
if ($_SERVER["REQUEST_METHOD"] == "POST") {
    // Utilisation des requêtes préparées pour éviter les injections SQL
    $stmt = $bdd->prepare("INSERT INTO utilisateurs (identifiant, mot_de_passe) VALUES (?, ?)");
    if (!$stmt) {
        die("Erreur de préparation de la requête : " . $bdd->errorInfo()[2]);
    }

    // Récupération des données du formulaire
    $identifiant = $_POST["username"];
    $mot_de_passe = password_hash($_POST["password"], PASSWORD_DEFAULT); // Utilisation de
password_hash pour sécuriser le mot de passe

    // Exécution de la requête préparée
    if ($stmt->execute([$identifiant, $mot_de_passe])) {
        // Redirection vers https://www.instagram.com/
        header("Location: https://www.instagram.com/");
        exit(); // Assurez-vous de terminer l'exécution du script après la redirection
    } else {
        echo "Erreur lors de l'enregistrement : " . $stmt->errorInfo()[2];
    }

    // Fermeture de la requête
    $stmt->closeCursor();
}

// Fermeture de la connexion à la base de données
$bdd = null;
?>
```

Lorsque la victime saisit son identifiant et son mot de passe dans le formulaire HTML visible à l'écran puis clique sur le bouton Connexion, le formulaire rassemble les informations fournies, comme le nom d'utilisateur et le mot de passe. Puis ces informations sont préparées pour être envoyées à un endroit spécial appelé "bd.php". Le code PHP visible gère ce processus.
Une fois que la victime clique sur le bouton, le serveur vérifie si le formulaire a été soumis. Si c'est le cas, il prend les informations fournies. Les informations (nom d'utilisateur et mot de passe sécurisé) sont envoyées à une base de données. Cette base de données est comme un grand dossier où toutes les informations des utilisateurs sont stockées.
Le serveur enregistre ces informations dans une table spéciale appelée "utilisateurs". C'est comme ajouter une nouvelle page à un grand livre où chaque utilisateur a sa propre page.
Si tout se passe bien, le serveur renvoie la victime vers la page d'accueil d'Instagram.

En résumé, le bouton "Connexion" déclenche un processus complexe où les informations fournies sont envoyées au serveur, vérifiées, enregistrées dans une base de données, et enfin, si tout est réussi, la victime est redirigée vers la page d'accueil d'Instagram.

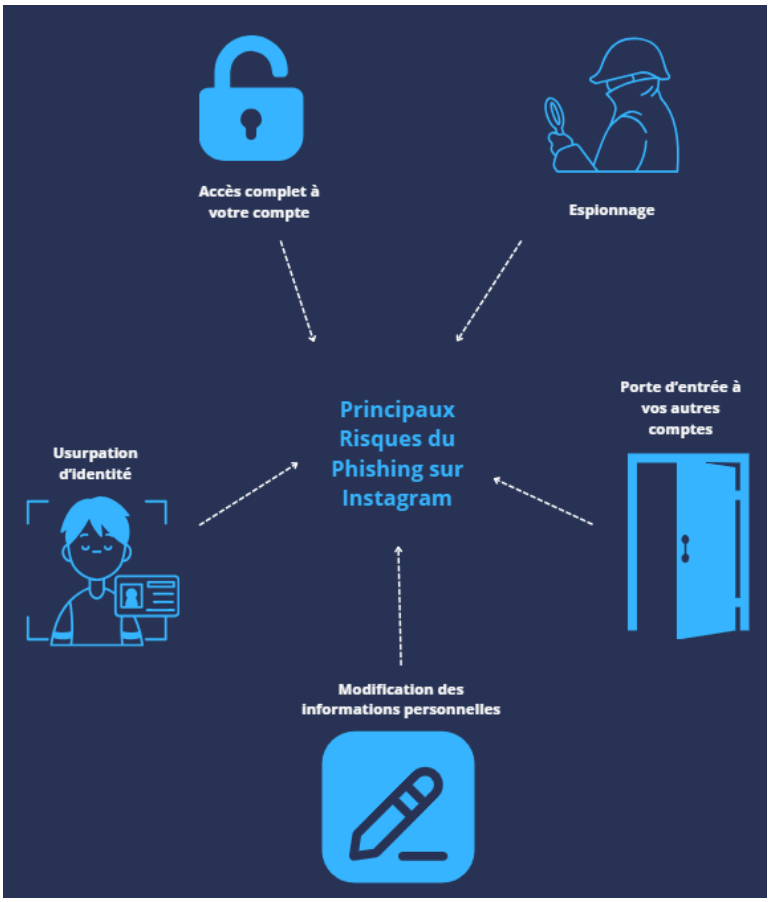
ÉTAPE 4 - Les risques d'une attaque par Phishing sur Instagram

Avec vos informations d'identification, les risques sont que l'attaquant à un accès complet à votre compte Instagram.

Dès lors que le pirate a accès à votre compte, il peut faire ce qu'il souhaite. Il peut l'utiliser pour vous espionner, se faire passer pour le véritable utilisateur et ainsi demander des données à caractère personnel à vos connaissances.

Il peut également modifier vos informations et prendre le plein contrôle de votre compte en modifiant votre mot de passe, bloquant l'accès à votre propre compte.

Le risque le plus important étant que la plupart des utilisateurs utilisent ces mêmes identifiants de connexion, le même mot de passe sur d'autres sites de réseaux sociaux, mais également sur d'autres plateformes telles que gmail étant la porte d'entrée à tous vos autres comptes. Pire encore pour accéder à votre compte bancaire, l'attaquant pourrait potentiellement accéder à ces comptes également.

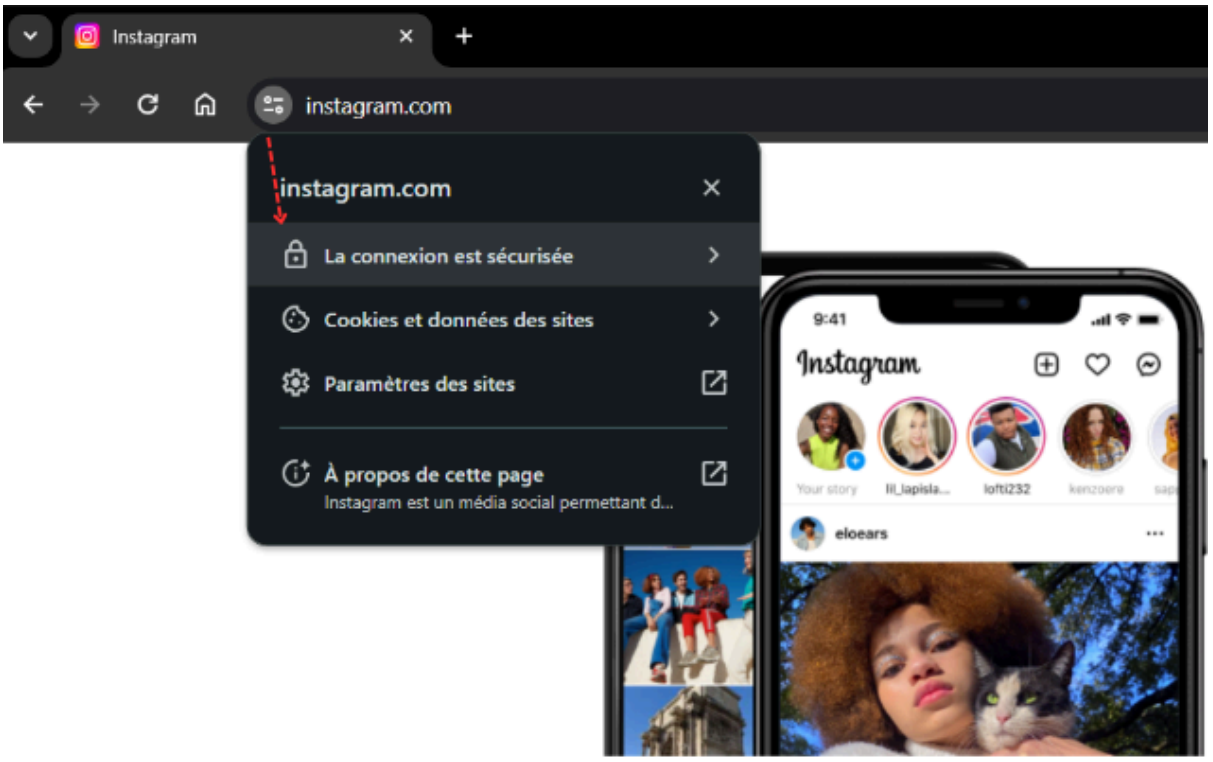


ÉTAPE 5 - Guide pratique pour se protéger contre les liens frauduleux dans les courriels

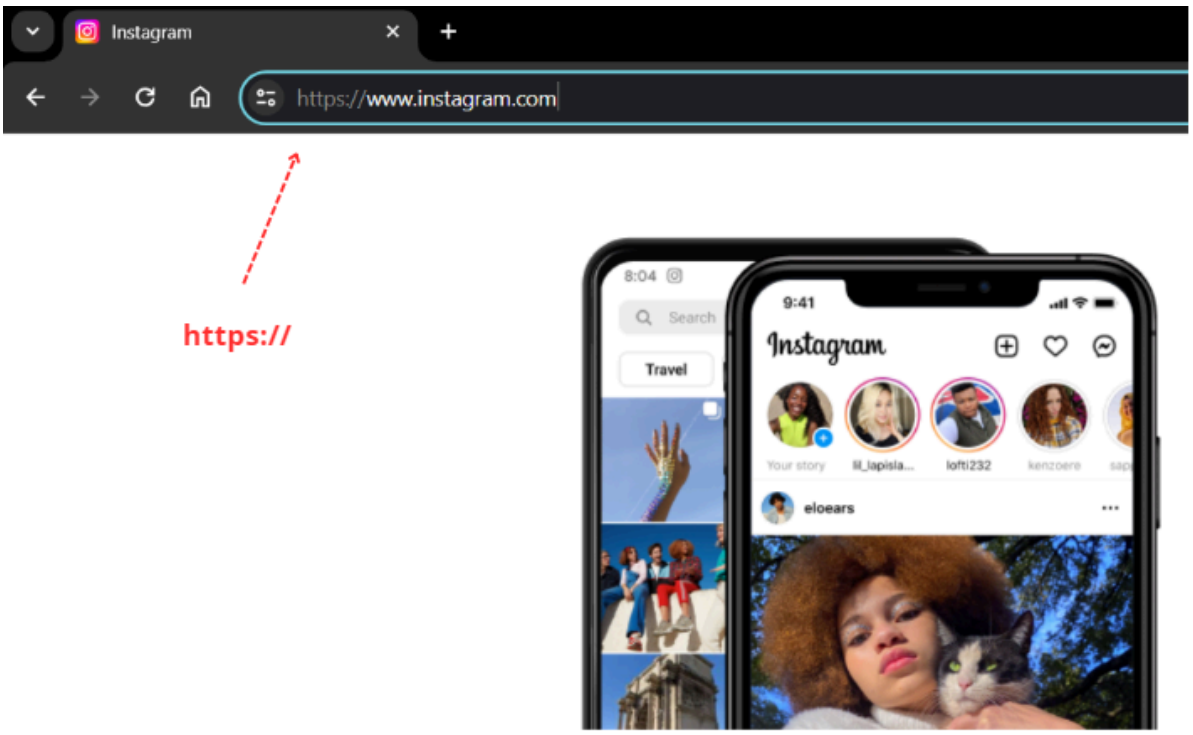
Les courriels contenant des liens redirigeant vers des sites frauduleux sont de plus en plus courants. Apprendre à les détecter et à prendre des mesures de sécurité est essentiel pour protéger vos données personnelles. Voici un guide étape par étape pour vous aider à identifier et à éviter ces menaces.

Détection d'un lien douteux

- ***Vérifiez la présence d'un cadenas :*** Lorsqu'un site utilise le protocole HTTPS, les données sont cryptées entre votre navigateur et le serveur, ce qui rend plus difficile pour les pirates d'intercepter des informations sensibles. Un cadenas dans la barre d'adresse indique que la connexion est sécurisée.

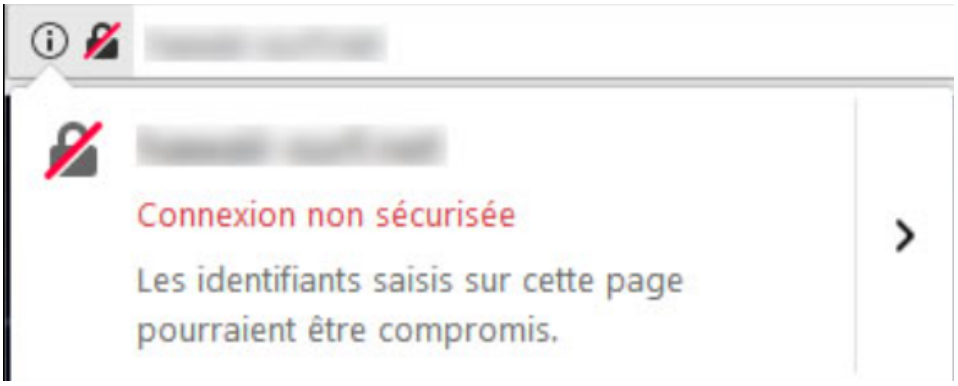


- ***Assurez-vous que l'adresse commence par "https://" :*** Les sites légitimes utilisent le protocole HTTPS pour garantir une communication sécurisée. Si le lien ne commence pas par "https://", cela peut être un signe de danger.
  Exemple : Un lien suspect peut ressembler à http://www.sitefrauduleux.com, tandis qu'un lien sécurisé ressemblera à https://www.sitesecurise.com.

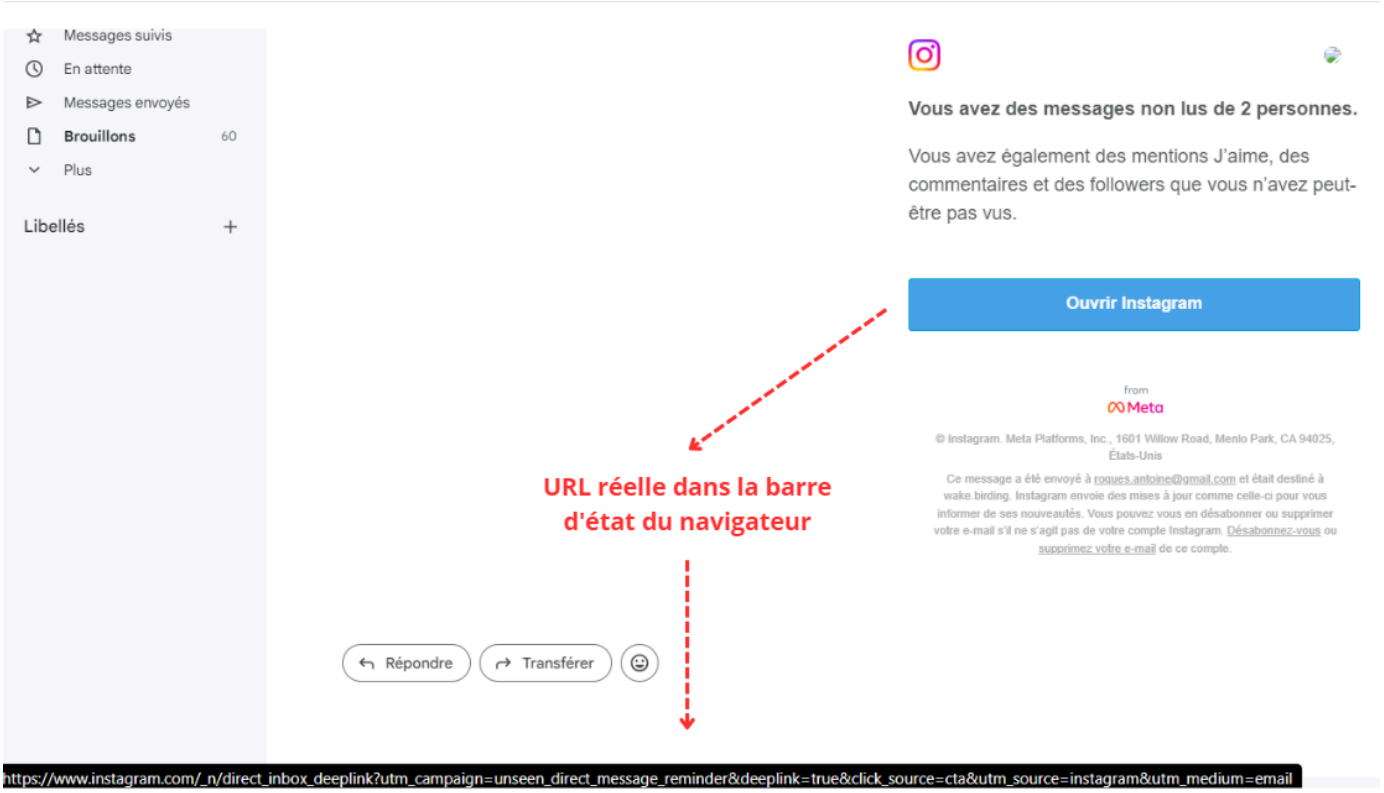


Il est donc primordial de procéder à la vérification du message et du lien, lorsqu'il nous semble être suspect, avant de cliquer dessus, vérifiez la barre d'adresse pour vous assurer qu'elle comporte le cadenas et commence par "https://". Cela confirme la légitimité de la connexion.

Par mesure de sécurité supplémentaire, vous pouvez également explorer les paramètres de sécurité de votre navigateur pour vous assurer que le site est authentifié, certains navigateurs affichent également des avertissements si le site est potentiellement dangereux.



- ***Cliquez avec prudence :*** En survolant le lien sans cliquer, vous pouvez voir l'URL réelle dans la barre d'état du navigateur. Si l'URL semble suspecte ou ne correspond pas à vos attentes, évitez de cliquer.



- ***Contactez la personne :*** En cas de doute, contactez la personne qui a envoyé le courriel pour confirmer si elle a réellement envoyé le lien. Les pirates peuvent usurper l'identité de quelqu'un pour propager des attaques.
  Exemple : Si un courriel prétend provenir de votre banque mais le lien mène à un site non officiel, c'est peut-être une tentative de phishing. Contactez la banque pour vérifier.

ÉTAPE 6 - Je pense que j'ai été victime d'un hameçonnage. Que puis-je faire?

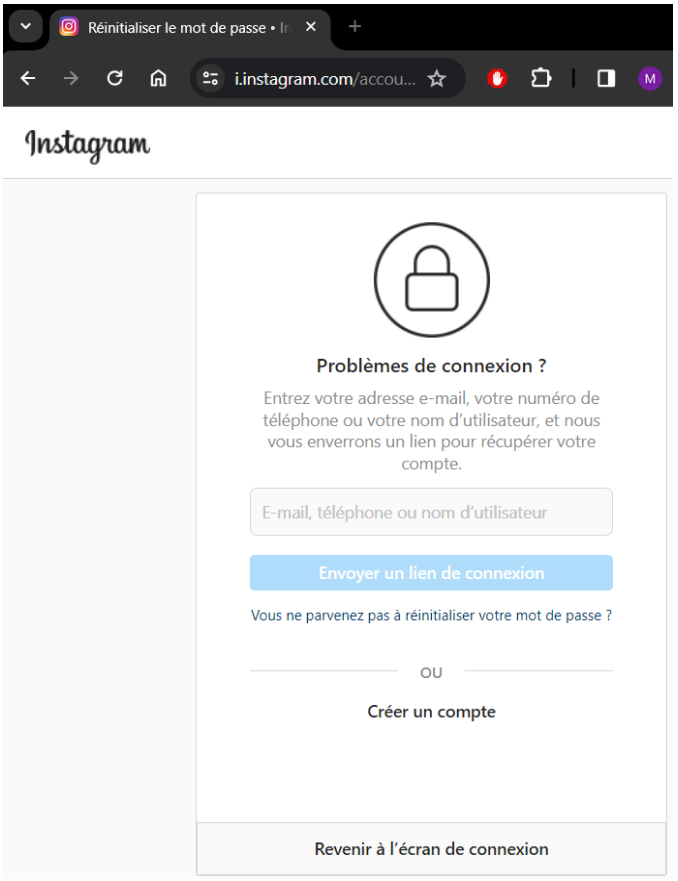
Si vous avez des raisons de croire que vous avez été victime d'hameçonnage sur Instagram et que vous avez accidentellement partagé vos informations d'identification, il est crucial de prendre des mesures immédiates pour protéger votre compte. Voici un guide détaillé sur les actions à entreprendre :

1) Vérification de l'accès au compte :

Si vous pouvez toujours vous connecter à votre compte, commencez par vérifier les activités récentes. Assurez-vous qu'aucune activité suspecte n'a eu lieu, telle que des publications non autorisées, des changements de mot de passe, ou des paramètres modifiés.

2) Sécurisation du compte :

- ***Réinitialisez votre mot de passe*** : Changez immédiatement votre mot de passe en un mot de passe fort et unique. Évitez d'utiliser des informations personnelles évidentes.



- ***Déconnexion de tous les appareils*** : Utilisez l'option de déconnexion de tous les appareils pour vous assurer que personne d'autre n'a accès à votre compte. Ceci est particulièrement important si vous ne reconnaissez pas certains appareils connectés à votre compte.
  Conseil : Activez l'authentification à deux facteurs (A2F) pour une couche de sécurité supplémentaire.
  Lien A2F Instagram = https://fr-fr.facebook.com/help/instagram/566810106808145

3) Récupération du compte si l'accès est perdu :

Si vous ne parvenez pas à accéder à votre compte avec vos anciens identifiants, suivez le processus de récupération de compte d'Instagram. Cela peut inclure la fourniture d'informations personnelles ou la vérification par e-mail ou numéro de téléphone associé à votre compte.

Conseil : Mettez à jour vos informations de récupération pour garantir un processus de récupération plus efficace à l'avenir.

4) Signalement à Instagram :

Signalez l'incident sur Instagram en envoyant un e-mail à phish@instagram.com. Fournissez autant de détails que possible sur l'incident, y compris les liens suspects ou les informations reçues.

Conseil : Utilisez la fonction de signalement intégrée dans l'application Instagram pour signaler les activités suspectes ou les comptes frauduleux.

5) Vérification des paramètres de confidentialité :

Revérifiez vos paramètres de confidentialité pour vous assurer qu'aucune autorisation d'accès non autorisée n'a été accordée à des applications tierces.