Les attaques par phishing sont une menace sérieuse pour la sécurité en ligne aujourd'hui.

Devenues l'une des menaces les plus courantes pour la confidentialité et la sécurité individus et des entreprises (figure 1), les attaques par phishing sont des tentatives frauduleuses d'obtenir des informations sensibles, telles que les mots de passe, les informations de carte de crédit et d'autres informations personnelles.

Il existe plusieurs types d'attaques phishing

Généralement effectuées par des e-mails, des messages instantanés ou des sites web qui ressemblent à des sources fiables, chaque type a une gravité qui ne peut être sous-estimée, et des méthodes pour inciter les utilisateurs à fournir des informations sensibles.

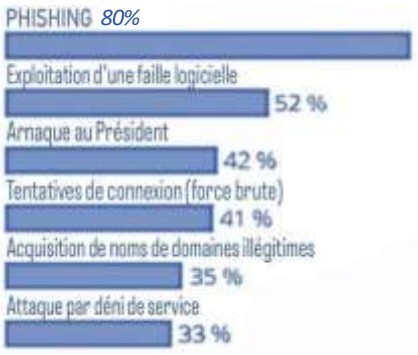

Figure 1. Les cyberattaques les plus communes, selon Statista.

Phishing par courriel: Un courriel est envoyé à un utilisateur, prétendant être une source de confiance et demandant des informations sensibles telles que les mots de passe, les informations de carte de crédit, etc. Effectivement, selon le portail des statistiques Statista, 54% des attaques de cybercriminalité en 2020 ont commencé par un e-mail.

Phishing par clonage de site web: Cette forme de phishing implique la création d'un site web qui ressemble à un site légitime réputé et qui demande aux utilisateurs de saisir leurs informations personnelles.

Phishing par SMS: Ce type implique l'envoi de SMS frauduleux qui demandent aux utilisateurs de saisir leurs informations personnelles en cliquant sur un lien.

Phishing de médias sociaux: Ce type d'attaque utilise les plateformes de médias sociaux pour diffuser des messages frauduleux, comme des liens menant à des sites web malveillants ou des demandes de renseignements personnels.

Phishing d'assistance technique: L'attaquant se fait passer pour un représentant de l'assistance technique d'une entreprise, et demande aux utilisateurs de fournir des informations sensibles ou d'installer des logiciels malveillants sur leur ordinateur, sous prétexte de résoudre un problème technique.

Ces tentatives d'intrusion ont un impact sur le monde industriel (figure 2)

Fuite de données sensibles : Les attaques de phishing compromettent la sécurité des informations sensibles et la vie privée des clients et des employés. Par exemple, en 2017, la société de télécommunications 'Equifax' a subi une attaque de phishing, exposant les informations financières de plus de 145 millions de consommateurs.

Réputation d'entreprise endommagée: Une fois les clients découvrent que leur information a été compromise, les entreprises subissent des dommages à leur réputation et chiffres d'affaires grâce à l'impact négatif sur la confiance des clients et la fidélité à l'entreprise. Notamment, après l'attaque de phishing de 'Equifax', la réputation de l'entreprise a été gravement endommagée et leur action ont chuté de près de 35%

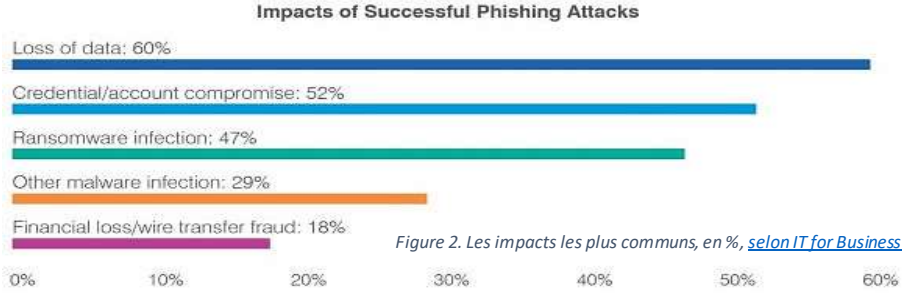

Figure 2. Les impacts les plus communs, en %, selon IT for Business

en bourse, ce qui a entraîné une perte de près de 6 milliards de dollars en capitalisation boursière.

Coûts supplémentaires : Après une attaque, les entreprises mettent en place des politiques de gestion des conséquences, notamment de restauration des systèmes de sécurité et de mise en place de mesures de protection supplémentaires. Le cas de l'attaque de phishing de 'Target' en 2013 est un exemple concret, ayant touché les données personnelles de près de 40 millions de clients aux États-Unis. Effectivement, Target a dû dépenser environ 18.5 millions de dollars en tant que frais de remboursement pour les clients touchés et plus de 200 millions de dollars pour engager des enquêteurs afin d'investiguer l'incident et éliminer les logiciels malveillants de leurs systèmes. De plus, la société a dû mettre en place des mesures de sécurité supplémentaires pour éviter tous futurs incidents.

Les attaques de phishing ont un impact significatif sur la vie des utilisateurs individuels

Perte financière : Les utilisateurs peuvent être incités à fournir leurs informations bancaires ou financières à des escrocs, ce qui peut entraîner une perte de fonds.

Vol de données sensibles et atteinte à la vie privée : Les informations personnelles et sensibles peuvent être volées par les criminels, compromettant la sécurité et la vie privée des utilisateurs.

Infection de malware : Les utilisateurs peuvent télécharger involontairement des logiciels malveillants qui peuvent endommager leur ordinateur et compromettre leur sécurité.

Spam : Les utilisateurs peuvent recevoir des courriels, des appels téléphoniques et des messages textes frauduleux.

Des pratiques de sécurité en ligne minimisent les risques de se faire escroquer lors d'une attaque de phishing :

Mettre en place **l'authentification à deux facteurs (2FA)** qui implique la vérification de l'identité de l'utilisateur à l'aide de deux éléments distincts, tels qu'un mot de passe et un code envoyé par SMS. Cela rend difficile pour les attaquants de se faire passer pour l'utilisateur légitime.

Ne **jamais fournir** des informations personnelles à des sources inconnues/réseaux **Wi-Fi publics,** vulnérables aux attaques de phishing.

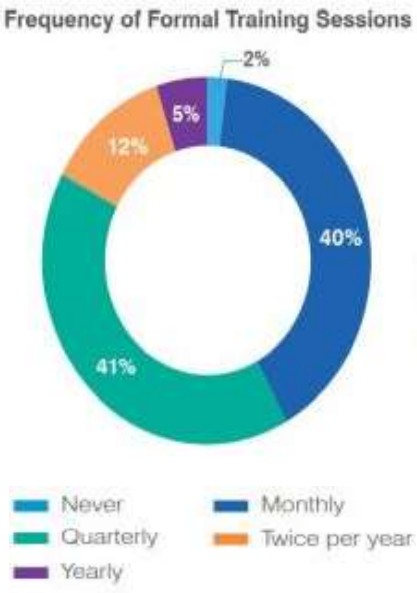

Figure 3. La fréquence des formations selon IT for business.

Suivre des **sessions de formation** à propos des méthodes courantes utilisées par les attaquants de phishing, afin de savoir les reconnaître et les éviter (figure 3).

Utiliser et mettre à jour des **logiciels antivirus** et **antimalware** qui protègent les ordinateurs contre les logiciels malveillants et les attaques.

Utiliser des **mots de passe forts et uniques.**

Vérifier les **URL** (https) et les **certificats de sécurité** des sites web et rester attentif envers les courriels/messages qui demandent de cliquer sur un **lien** ou de **télécharger** un fichier joint.

Des technologies de sécurité doivent être mises en place contre les attaques phishing pour les entreprises :

L'authentification à deux facteurs (2FA) pour les employés et leur formation sur les méthodes courantes utilisées par les attaquants de phishing.

La validation de domaines pour vérifier l'identité de l'expéditeur d'un e-mail et la validation de **certificats SSL** pour s'assurer que les informations transmises par le biais d'un site web sont sécurisées.

La mise en place de **politiques de sécurité** strictes pour protéger les informations sensibles de l'entreprise et la **surveillance régulière** des activités pour détecter toute activité suspecte.

L'implémentation des **algorithmes de filtrage** qui détectent les caractéristiques courantes des e-mails malveillants, telles que les liens malveillants et les mots clés spécifiques, pour bloquer les e-mails de phishing.

L'installation des **logiciels de sécurité**, tels que les programmes antivirus sur tous **les ordinateurs de l'entreprise**.

Dans cette recherche, nous avons développé un modèle de détection de phishing en utilisant les algorithmes de filtrage.

En mettant en œuvre ces algorithmes, nous pouvons aider les utilisateurs à se protéger contre les attaques de phishing et à éviter d'être victimes de fraude en ligne, ce qui peut contribuer à renforcer la sécurité en ligne. Notre modèle peut aider à détecter les liens malveillants avec une bonne précision en identifiant les caractéristiques importantes des liens frauduleux (figure 4), telles que la présence d'une adresse IP, la présence d'un caractère "@" dans l'URL, l'existence d'un préfixe ou suffixe dans l'URL, la présence d'un enregistrement DNS, la longueur de l'URL, la possibilité de cliquer avec le bouton droit de la souris et la capacité de redirection du site.

Les données utilisées ont été collectées à partir de deux jeux de données contenant 500 liens de phishing et 500 liens légitimes et les caractéristiques de ces liens ont été extraites et utilisées pour entraîner trois modèles : La régression logistique, la forêt aléatoire et le KNN. De plus, les caractéristiques les plus importantes pour la détection de liens de phishing ont été identifiées en comparant la distribution des caractéristiques entre les liens frauduleux et les liens légitimes. L'efficacité du modèle a été évaluée en utilisant le score AUC (Area Under the Receiver Operating Characteristic Curve) comme métrique de performance (figure 5). Les résultats de cette recherche peuvent être utilisés par les entreprises, les organisations et les utilisateurs finaux pour améliorer leur capacité à reconnaître et à éviter les attaques, ce qui contribue alors à protéger les données sensibles.

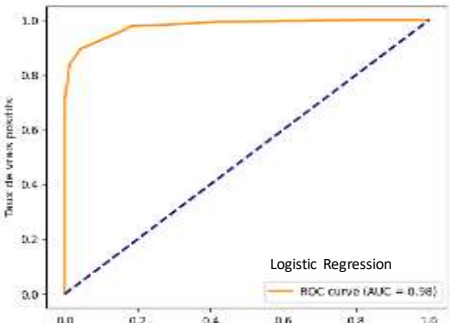

Figure 5. La courbe ROC, "receiver operating characteristic", de notre modèle de régression logistique, qui maximise notre score AUC.

Il est probable que les tendances suivantes continueront à influencer la sécurité des réseaux à long terme

Les perspectives à long terme pour la sécurité des réseaux dépendent de nombreux facteurs, tels que les avancées technologiques, les changements dans les méthodes d'attaque et la sensibilisation des utilisateurs et des entreprises à la sécurité en ligne.

L'intégration des **algorithmes de l'intelligence artificielle et de l'apprentissage machine** peuvent aider à détecter et à prévenir les attaques de sécurité plus rapidement et plus efficacement en s'adaptant aux nouvelles menaces.

La migration des systèmes d'entreprise vers le **cloud computing** peut offrir de nouvelles opportunités pour les attaquants, mais peut également permettre une meilleure protection des données grâce à la centralisation des ressources de sécurité.

La sécurité basée sur les comportements peut aider à identifier les activités anormales dans les réseaux et à prendre des mesures pour les empêcher, même lorsque les attaquants utilisent des techniques nouvelles et inconnues.

Les **réglementations** sur la protection des données, telles **que le RGPD en Europe**, et les sanctions imposées par la CNIL en cas de violation, encouragent les entreprises à adopter des pratiques de sécurité plus rigoureuses pour protéger les informations sensibles des utilisateurs.

Les attaques par phishing viole les obligations du RGPD et de plusieurs textes législatifs.

Le Règlement Général sur la Protection des Données (RGPD) exige que les entreprises prennent toutes les mesures nécessaires pour protéger les données personnelles de leurs utilisateurs et clients, souvent ciblées lors des attaques de phishing, se conformant ainsi

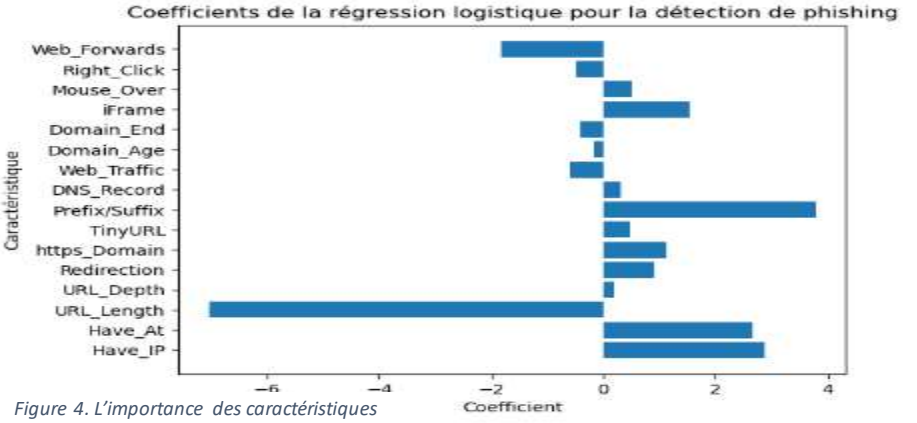

Figure 4. L'importance des caractéristiques

aux directives de la CNIL, Commission Nationale de l'Informatique et des Libertés. La collaboration avec la CNIL est essentielle pour s'assurer que les pratiques sont conformes aux réglementations en vigueur, notamment en ce qui concerne la prévention du phishing. En cas de violation de données, les entreprises sont tenues de signaler l'incident dans les 72 heures suivant sa découverte avec les sanctions pour non-conformité pouvant atteindre jusqu'à 4% du chiffre d'affaires annuel mondial.

Dans ces conditions, la CNIL recommande de signaler les spams, les tentatives de phishing et les escroqueries sur Internet en France. En outre, les articles 226-18, 313-1, 323-1, 226-4-1 du code pénal punissent respectivement la collecte frauduleuse de données personnelles, l'escroquerie, l'accès illégal à des données informatiques, et l'usurpation d'identité. De même, les articles L163-3 et L163-4 du code monétaire et financier sanctionnent la contrefaçon et l'usage frauduleux de moyens de paiement, tandis que les articles L.713-2 et L.713-3 du Code de la propriété intellectuelle répriment la contrefaçon de marques utilisées dans le cadre de l'hameçonnage, avec des peines d'emprisonnement allant jusqu'à sept ans et des amendes pouvant atteindre 750 000 €.

Le gouvernement recommande plusieurs mesures à prendre en cas de fraude en ligne

1- En cas de doute, contactez directement l'organisme concerné pour confirmer le message ou l'appel reçu.

2- Si vous avez communiqué des informations sur vos moyens de paiement ou si vous avez constaté des débits frauduleux sur votre compte, faites opposition immédiatement auprès de votre organisme bancaire/financier.

3- Conservez les preuves et le message d'hameçonnage reçu.

4- Déposez plainte au commissariat de police ou à la brigade de gendarmerie.

5- Si vous êtes un particulier, vous pouvez être accompagné gratuitement dans cette démarche par une association de France Victimes au 116 006.

6- Changez immédiatement vos mots de passe compromis.

7- Signalez tout message, site douteux ou tentatives d'escroquerie à Signal Spam, PHAROS ou au 33 700.

8- Signalez l'adresse à Phishing Initiative qui bloquera le site.

9- Contactez la plateforme Info Escroqueries du ministère de l'Intérieur pour être conseillé dans vos démarches.

Il existe plusieurs défis futurs pour la protection contre les attaques par phishing

Les attaquants continueront de développer de nouvelles techniques pour contourner les mesures de sécurité existantes, telles que des e-mails de phishing de plus en plus réalistes et les sites web de phishing plus convaincants.

Les attaquants utilisent la **messagerie instantanée** et les **réseaux sociaux** de plus en plus pour lancer des attaques de phishing, ce qui peut rendre plus difficile la détection et la prévention des attaques.

La connaissance insuffisante de la sécurité en ligne peut rendre les entreprises et les utilisateurs vulnérables aux attaques, malgré leur développement, puisqu'ils ne pourront pas utiliser les mesures de sécurité correctement.

La **prolifération des objets connectés**, tels que les appareils domestiques intelligents, peut offrir de nouvelles opportunités pour les attaquants de phishing.

En fin de compte, la sécurité des réseaux continuera d'être un défi en constante évolution à mesure que les technologies et les méthodes d'attaque évoluent. C'est pourquoi, les défis futurs pour la protection contre les attaques par phishing nécessiteront une approche proactive en matière de sécurité, y compris une éducation continue des utilisateurs et des entreprises sur les méthodes courantes d'attaque, ainsi que la mise en place de mesures de sécurité pour minimiser les risques.

Pour en savoir plus

- Notre projet sur Github, 24 Av 2023
-CNIL, *Mots de passe*, 17 Oct 2022
-CNIL, *Phishing : détecter un message malveillant*, 16 Oct 2017
-CNIL, Spam, phishing, arnaques : signaler pour agir, 06 juillet 2017
-CyberMalveillance, Que faire en cas de phishing, 10 Janv 2020
-Microsoft, Cyber Attacks
-DELATTRE Laurent, *Le Phishing en France et dans le monde*, 08 Février 2021
-FORTRA, *6 Phishing Attacks & How to Protect Against*, 16 Jan 2023
-Paul R. LA MONICA, *Equifax shares plunge again*, 14 Sép 2017
-CYBSAFE, *How can phishing affect a business?*, 19 Fév 2021
-IBM, Cyberattaques
-Altonéo, Comment se protéger?
-Red River, *Warnings of the 2013 Target Data Breach*, 26 Oct 2021
-Statista, Most Common Cause of Ransom Attacks, 6 Juillet 2021
-Statista, cyberattaques courantes contre les entreprises françaises, 6 Juillet 2021
-Numerama, régions, villes et départements impactés, 12 Déc 2022
-Luke Irwin, 5 Most Common Types of Phishing, 31 Janvier 2023