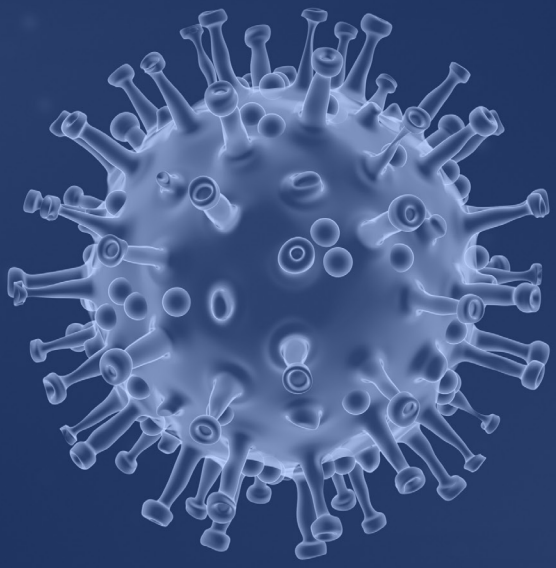
Rapport mondial sur la vulnérabilité à l'hameçonnage

rapport de PHISHED

Table des matières

1. Apprentissages clés

Sans formation préalable approfondie, **1 employé sur 2** est susceptible d'être victime d'hameçonnage.



La communication liée à la **COVID-19** est le sujet le plus connu d'une campagne d'hameçonnage réussie.

23%

des employés hameçonnés saisissent **ensuite des données** dans des pages de destination usurpées.

7% de tous les employés ouvrent **des pièces jointes** potentiellement dangereuses.

2. Introduction : Observations générales pour 2021

La crise sanitaire de 2020, à savoir **la pandémie de coronavirus**, a marqué le point de départ d'une hausse significative de la popularité – ou de la notoriété – des attaques par hameçonnage.
En tant que phénomène, la pandémie a continué à influencer chaque partie de notre vie quotidienne tout au long de l'année 2021. Pendant ce temps, les pirates informatiques et autres agents malveillants ont **efficacement adapté** leur mode de fonctionnement pour qu'il soit mieux adapté à nos nouveaux **modes de vie et de travail**, auparavant peu courants.

Ces modifications ont été, entre autres, motivées par :

- Une **augmentation de l'anxiété, des craintes et des émotions** à cause de la COVID-19.
- Un **manque d'expérience** en matière de travail à domicile, tant du point de vue des employés que des employeurs.
  - Comprend la nécessité de mettre en œuvre et de former rapidement les utilisateurs à de nouveaux outils et protocoles logiciels.
- Une forte augmentation dans :
  - Les achats en ligne
  - Les services en ligne (administrations, banques, fournisseurs…)
  - Les fausses nouvelles (mesures contre la COVID, informations sur la vaccination…)

Le public ayant été confronté à des changements soudains dans son environnement personnel et professionnel, il est devenu beaucoup plus facile pour les agents malveillants d'entrer dans le domaine de la cybercriminalité :

- **Les trousses d'hameçonnage** sont disponibles à des prix toujours plus bas. Ils sont faciles à utiliser et abaissent le seuil de difficulté pour quiconque est prêt à prendre le risque.
- **Les bases de données** sont de plus en plus accessibles, en partie à cause de la protection insuffisante des collecteurs de données, comme les plate-formes de médias sociaux. Rien qu'en 2021, les médias ont rapporté que **plus d'un milliard de données d'utilisateurs ont été extraites** sur deux des plus grandes plate-formes du monde.
- **Diversification des canaux :** il est de plus en plus facile de diversifier les attaques d'hameçonnage. Le coût par SMS (hameçonnage par texto) diminue chaque année, tandis que le logiciel pour l'exploiter devient moins cher et plus facile à utiliser également. L'hameçonnage vocal devient plus difficile à reconnaître en raison de **l'approche plus localisée** des acteurs de la menace.

Le saviez-vous ?

« Les gens ne pensent pas, ils cliquent », surtout quand :

- Le message d'hameçonnage est **court** et direct.
- Le message contient une **demande d'aide**.
- L'expéditeur semble être connu du destinataire (les chances de clic augmentent de **30 %** !).
- Le message d'hameçonnage fait référence à un **sujet d'actualité**.

La pandémie de coronavirus a ouvert la porte de manière décisive et permanente à une augmentation continue des menaces d'hameçonnage. Comme elles constituent la base de la grande majorité de toutes les cyber-violations, il est important que les gens prennent conscience des dangers, de la manière de les reconnaître et d'y faire face.

C'est pourquoi Phished présente son rapport **« Hameçonnage en 2021 »**.

Bonne lecture,
Arnout Van de Meulebroucke
PDF de Phished

3. Des précisions sur l'hameçonnage et la base de données

3.1. Qu'est-ce que Phished ?

Phished se concentre sur **l'aspect humain de la cybersécurité**. Le logiciel de formation basé sur l'IA combine des simulations d'hameçonnage personnalisées et réalistes avec le programme éducatif de la Phished Academy. Ainsi, vos employés sont qualifiés pour faire face correctement et en toute sécurité aux menaces en ligne. Comme les employés sont mieux préparés et plus sûrs, les données, la réputation et les actifs des organisations sont également plus sûrs.

3.2. Le logiciel et la base de données hameçonnés

90 % de toutes les violations de données commencent par une erreur humaine. Des erreurs qui peuvent conduire à des virus, des logiciels rançonneurs, le vol d'argent et de données, et la perte de réputation. Phished forme vos collaborateurs à gérer les cybermenaces de manière efficace et dans un environnement sûr et contrôlé.

Les données contenues dans ce rapport ont été accumulées en envoyant des millions de simulations d'hameçonnage à des **centaines de milliers de destinataires dans le monde entier**.

Nous construisons le human firewall chez PHISHED

4. L'hameçonnage à l'échelle mondiale

Tout le monde, aux quatre coins du monde, dans chaque industrie ou secteur, dans n'importe quel emploi, est vulnérable à l'hameçonnage. C'est ce que prouvent une fois de plus les statistiques mondiales sur l'hameçonnage pour 2021. Aperçu des principales statistiques sur les bénéficiaires de Phished à l'échelle mondiale.

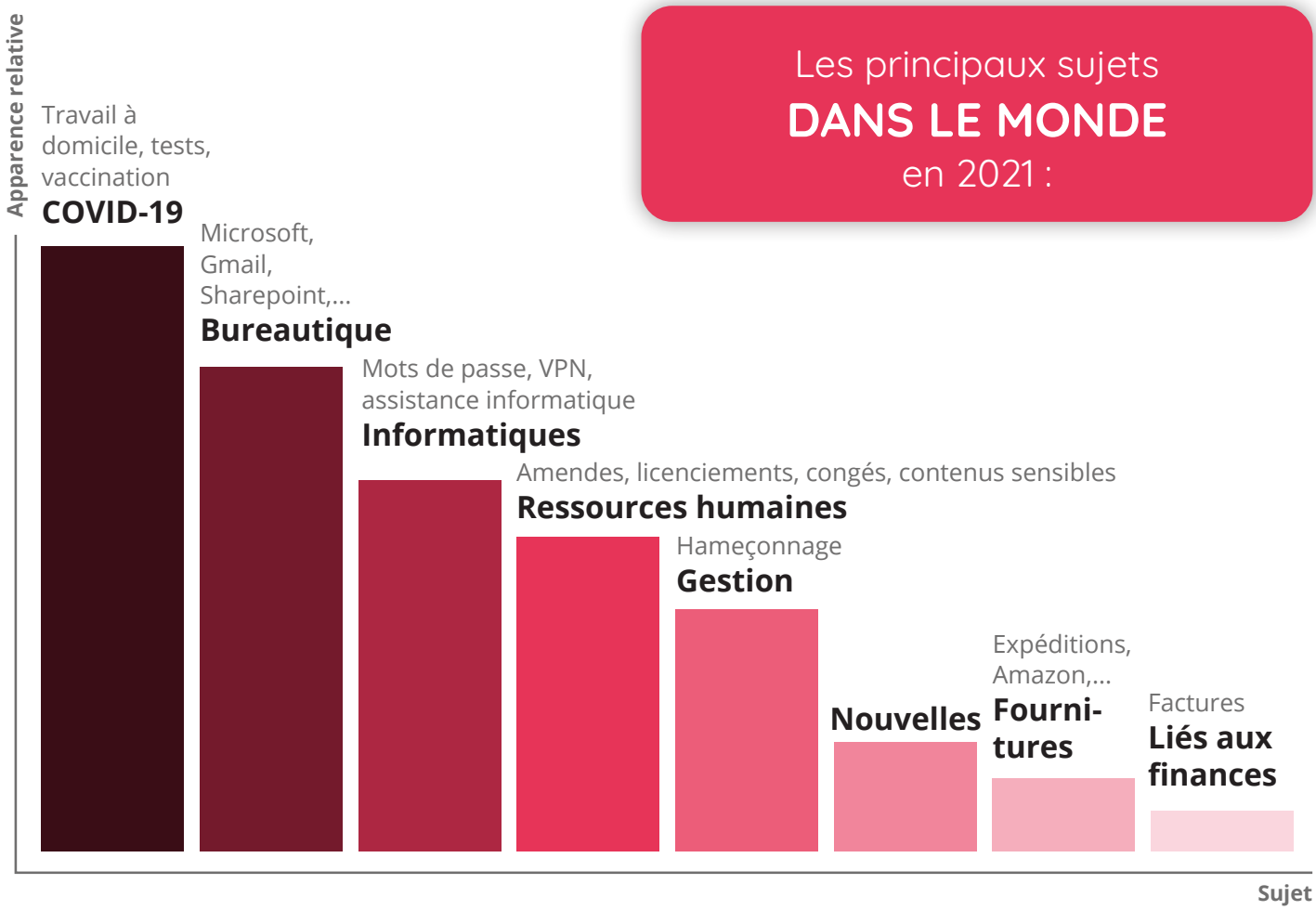
4.1. Sujets les plus populaires

Suivant la tendance de l'année dernière, la **COVID-19** arrive une fois de plus en tête du classement mondial. Rien de surprenant à cela, étant donné la vaste campagne d'information et de vaccination qui a touché la plupart des citoyens dans la plupart des pays. Les nombreuses campagnes de fausses nouvelles et de désinformation ont incité les acteurs malveillants à exploiter l'anxiété générale concernant les risques des vaccins et leurs effets secondaires.

Viennent ensuite les e-mails liés à la **bureautique**, qu'il s'agisse de problèmes avec les outils de Microsoft Office, d'invites de connexion à Gmail ou de messages d'hameçonnage plus généraux liés à l'informatique (demandes de mots de passe, **assistance informatique**, VPN, etc.

Les messages liés aux **ressources humaines** constituent une catégorie notable, car ils ont réussi à attirer de nombreuses personnes dans le piège du hameçonnage. Beaucoup de ces messages font référence aux vacances des employés, tandis que les messages « pas prudent pour le travail » entrent également dans cette catégorie : ils concernent des amendes, des licenciements ou mentionnent des aspects pornographiques.

Une mention spéciale pour les messages **financiers** (concernant des factures impayées, par exemple) : ils constituent une part importante de tous les messages d'hameçonnage réussis, **mais moins que ce que l'on croit généralement**.



4.2. Quel est le degré de vulnérabilité de l'employé moyen ?

Phished envoie des millions de simulations d'hameçonnage chaque année. Les organisations peuvent choisir les intervalles, mais en moyenne, un destinataire recevra une simulation tous les 10 jours.

Au niveau mondial, **22%** de toutes les simulations sont réussies. Si l'on ne tient compte que des messages d'hameçonnage ouverts, ce chiffre grimpe à **53%**.

Si une simulation offre la possibilité de saisir des données (par exemple, sur une page de connexion usurpée), **23%** des victimes saisissent leurs données.

Si un message contient une pièce jointe, **7%** de tous les destinataires la téléchargeront et l'ouvriront.

Les messages d'hameçonnage ne font pas l'objet d'une réponse fréquente : seuls **0,55%** des destinataires ont répondu à une simulation.

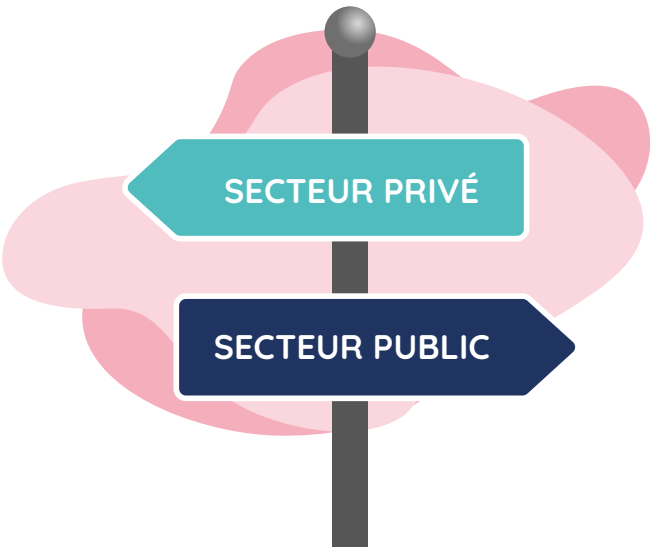
7% ont signalé avec succès la simulation.

Hameçonnage (des e-mails envoyés)	Hameçonnage (des e-mails ouverts)	Saisie des données (des e-mails ouverts)	Saisie des données (après avoir été hameçonné)	Répondus	Pièces jointes	Signalés
21,63 %	52,90 %	5,11 %	23,33 %	0,55 %	7,15 %	**6,85 %**

4.3. Secteurs public et privé

La façon dont le secteur public (doit) gérer la cybersécurité est très différente de celle du secteur privé. Les institutions publiques étant souvent financées par des fonds publics, elles sont, par exemple, tenues de respecter des critères de sélection stricts et rigoureux lorsqu'elles choisissent leurs programmes de sensibilisation à la cybersécurité.

S'il est difficile de déterminer s'il s'agit d'un facteur de différenciation dans la comparaison des deux domaines, il n'en reste pas moins que les employés du secteur public tombent dans le piège d'hameçonnage **3 %** plus souvent que ceux des organisations du secteur privé.



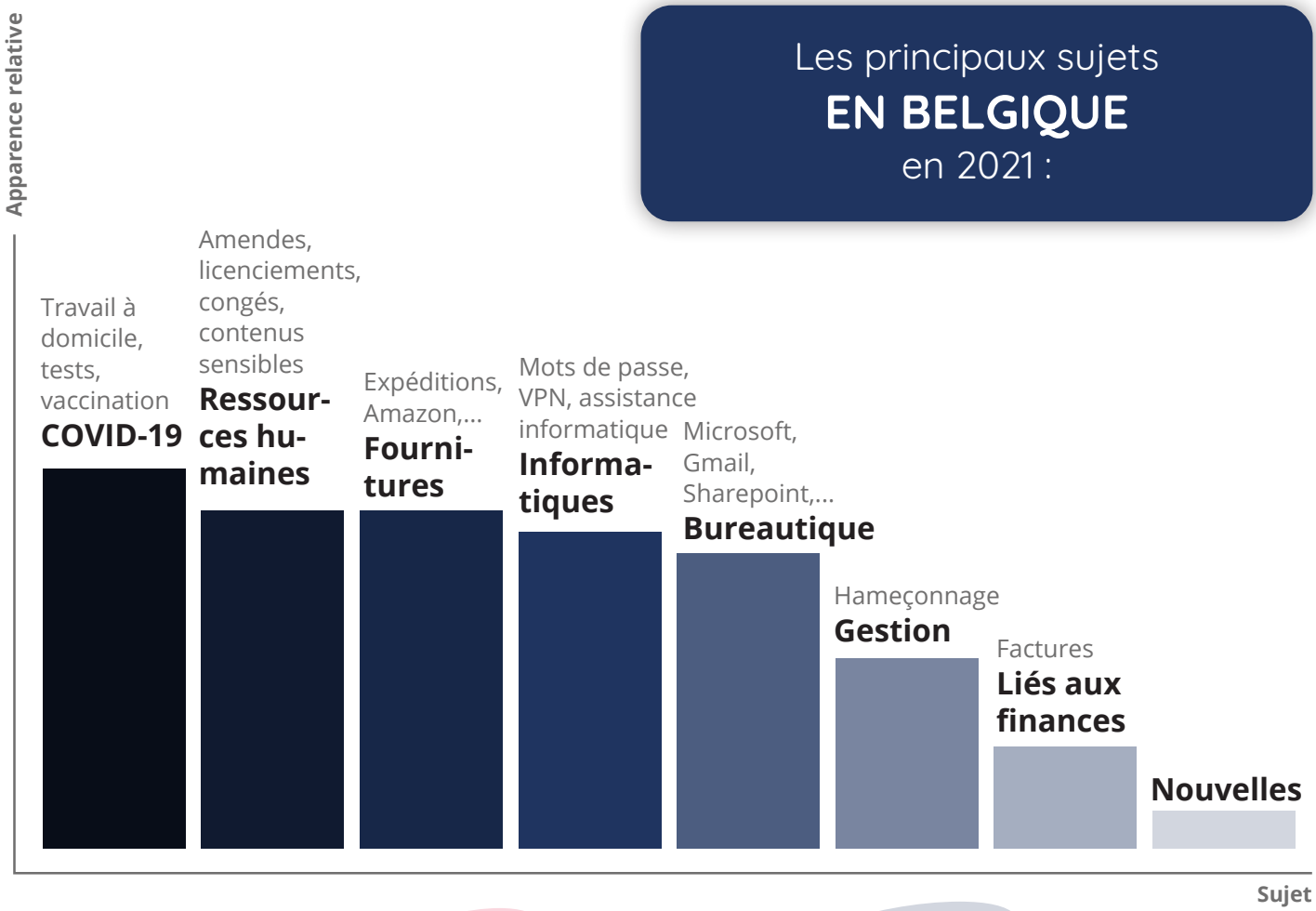
5. L'hameçonnage en Belgique

5.1. Sujets les plus populaires

La Belgique suit la tendance mondiale et montre une susceptibilité aux messages d'hameçonnage liés à la COVID-19. Cependant, derrière ces chiffres, les places deux à cinq sont presque équivalentes, avec une égalité pour la deuxième place : les messages liés aux **ressources humaines** et à **l'approvisionnement** sont (à peu près) aussi attrayants pour les employés belges.

En ce qui concerne la chaîne d'approvisionnement, les simulations les plus « populaires » ont une **saveur locale** notable. Alors que les simulations d'Amazon sont l'un des expéditeurs d'usurpation les plus perfides au monde, elles sont remplacées par des simulations de bol.com et de Coolblue en Belgique.

Les messages à caractère **financier** occupent la septième place car ils font **beaucoup plus de victimes** en Belgique que la moyenne mondiale. Les messages liés à l'actualité complètent la liste belge, mais avec un taux nettement inférieur à la moyenne mondiale.



5.2. Quel est le degré de vulnérabilité des employés belges ?

Par rapport aux résultats globaux, les employés belges se situent généralement au même niveau que leurs homologues.

Les employés belges obtiennent des résultats nettement supérieurs à la moyenne si l'on tient compte des simulations d'hameçonnage ouvertes : **47%** des messages ouverts conduisent à un hameçonnage, contre **53%** au niveau mondial.

Les différences sont moins explicites lorsqu'on examine les autres données : si une simulation contient la possibilité de saisir des données (par exemple, sur une page de connexion usurpée), **23%** de toutes les victimes saisissent leurs données.
Si un message contient une pièce jointe, près de **7%** des destinataires la téléchargent et l'ouvrent.

Les messages d'hameçonnage ne font pas l'objet d'une réponse fréquente : seuls **0,42 %** de l'ensemble des destinataires ont répondu à une simulation.

7% ont signalé avec succès la simulation, soit un peu moins que la moyenne mondiale.

Hameçonnage (des e-mails envoyés)	Hameçonnage (des e-mails ouverts)	Saisie des données (des e-mails ouverts)	Saisie des données (après avoir été hameçonné)	Répondus	Pièces jointes	**Signalés**
22,67 %	46,63 %	4,96 %	22,99 %	0,42 %	6,58 %	**6,82 %**

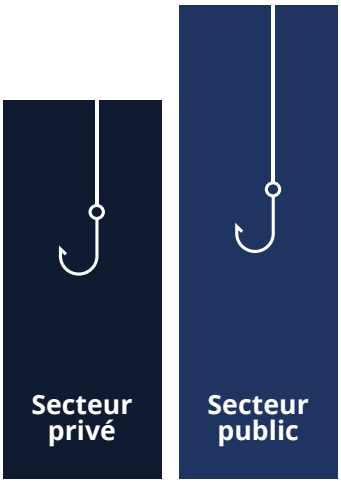
5.3. Secteurs public et privé

Poursuivant la tendance observée à l'échelle mondiale et au Royaume-Uni, les institutions publiques belges obtiennent des résultats légèrement inférieurs à ceux des organisations du secteur privé, mais la différence est ici beaucoup plus importante :

l'Ecart entre les deux secteurs s'élève à **5 %**.

Ce résultat est identique à celui de l'année précédente, à savoir 2020.

5% plus vulnérable que le secteur privé



6. Performance avec Phished

Lorsque de nouveaux clients commencent à utiliser la plate-forme Phished pour former leurs employés, la première simulation pour atteindre les destinataires sera le plus souvent un test général, souvent appelé « test de mesure de base ». Au cours de l'année dernière, Phished a conclu qu'en moyenne, **45%** de tous les destinataires ont été hameçonnés pendant le test de base initial. Si le test comprenait une partie de saisie de données, **27%** ont saisi des informations personnelles (données de connexion, identifiants uniques...).

Dans un cas, Phished a obtenu un taux de réussite de **100%** : il s'agissait d'une mesure de base où le client avait fourni des informations internes qui étaient, à l'époque, un sujet de conversation récurrent. Ce résultat souligne le danger des menaces internes. Le piratage de la boîte aux lettres d'un employé peut conduire à un résultat comparable.

7. Tendances pour 2022

Bien que de nouvelles tendances apparaissent régulièrement, la plupart des attaques d'hameçonnage réussies sont des variantes d'anciennes campagnes ou des campagnes réadaptées qui ont fait leurs preuves dans le passé. C'est pourquoi il est primordial que les entreprises commencent par former leur personnel aux principes de base :

Les problèmes fondamentaux de l'hameçonnage et la manière de les reconnaître.

La formation à l'hameçonnage consiste à apprendre les principes généraux qui permettent de protéger les personnes contre des menaces plus spécifiques.

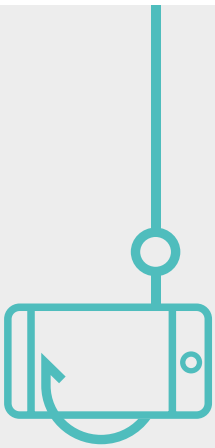
L'année 2022 marquera la poursuite de la tendance la plus populaire aujourd'hui : la communication liée à la **COVID-19**. Néanmoins, certaines **stratégies d'hameçonnage nouvelles ou réinventées** se profilent également à l'horizon.

Infox vidéo

Les infox vidéo deviennent relativement **faciles à créer en quelques secondes**, sur n'importe quel appareil intelligent. Il s'agit d'outils pratiques permettant d'imiter la voix et le visage d'une personne, à condition de disposer de suffisamment de données. En 2022, cependant, nous les verrons apparaître beaucoup plus souvent sur nos petits écrans, en combinaison avec des attaques d'hameçonnage.

Hameçonnage par texto

La COVID-19 a facilité la percée définitive de l'hameçonnage par SMS (hameçonnage par texto, prenant également en compte les services de textos basés sur le Web). Étant donné que de nombreuses communications liées au gouvernement utilisent les SMS, par exemple pour informer les gens de leur code de vaccination, les pirates ont commencé à copier ces messages et leur contenu. Ils les ont reliés à des **pages Web usurpées** convaincantes, ce qui a conduit à de nombreux cas de fraude. En 2022, l'hameçonnage invente des possibilités nouvelles et inattendues pour un outil de communication qui n'a rien de nouveau.



Hameçonnage vocal

Lorsque les gens sont confrontés à l'hameçonnage vocal, ils s'attendent à ce qu'il s'agisse d'un centre d'appels travaillant pour Microsoft, qui leur annonce un problème avec leur ordinateur. Cependant, l'hameçonnage vocal moderne fait appel à des **personnes locales, à des sujets locaux et à des sensibilités locales**. Il est de plus en plus difficile de distinguer les vrais appelants des escrocs qui vous demandent vos coordonnées bancaires.

Fraude par code QR

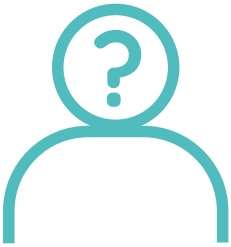
Les codes QR ont été inventés pour élargir les possibilités du code-barres traditionnel. Ils sont devenus un moyen populaire de réaliser des transactions en ligne, mais la prudence est primordiale. Un code QR ne montre pas immédiatement ses intentions, ce qui signifie que le fait de le scanner ouvre la porte à d'éventuelles menaces. Par exemple, les pirates peuvent ajouter des possibilités supplémentaires lors de la vérification des paiements afin d'accéder à un compte bancaire. Un autre danger se présente lors d'attaques par interception, où un pirate peut essayer de **remplacer un code QR légitime** par son propre code frauduleux.

Fraude aux invitations de calendrier

Ce type d'escroquerie existe en deux versions : dans la première, une entité piratée de source sûre envoie des invitations à des calendriers qui contournent les filtres anti-spam et qui, pour être ouvertes, nécessitent des informations de connexion à des comptes « e-mail » professionnels. Les données saisies sont ensuite envoyées aux pirates.

Dans une deuxième version, les invitations de calendrier commencent à remplir votre agenda après avoir cliqué sur un lien malveillant, une fenêtre contextuelle ou une bannière Web. Les pirates vous contacteront ensuite pour vous aider à « supprimer le virus », en se faisant passer pour une entreprise de cybersécurité professionnelle. Dans les deux cas, faites très attention aux invitations de calendrier étranges.

Anonymisation



Il est de plus en plus facile pour les attaquants de rester anonymes en ligne. Ce phénomène est dû, en partie, à l'essor et à la popularisation des crypto-monnaies. En tant que méthode décentralisée de règlement des comptes, il est de plus en plus difficile de suivre les flux de financement d'un point « A » à un point « B ». Les criminels prennent le train en marche et placent ainsi de nouvelles barrières entre eux et les forces de l'ordre.

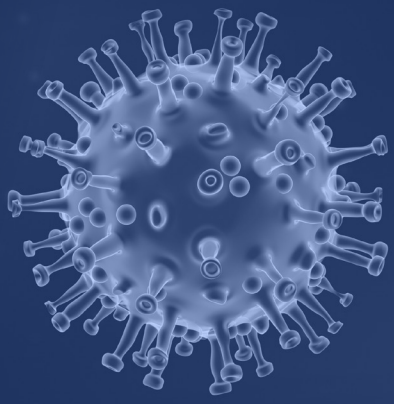
L'une des manifestations de ce phénomène est la percée des **« mules à bitcoins »** : des personnes qui croient travailler pour des agences de crypto-monnaies légitimes, chargées de créer, désigner et régler des comptes, alors qu'en réalité elles blanchissent de l'argent provenant d'activités criminelles.

8. Conclusions

Plus d'un employé sur cinq risque d'être victime d'hameçonnage.
Lorsqu'une simulation d'hameçonnage contient des possibilités de saisie de données, 23 % de toutes les victimes continueront à renoncer à leurs informations personnelles. 7 % de tous les destinataires ouvriront des pièces jointes éventuellement malveillantes. Cependant, lorsque Phished commence à former de nouveaux clients, nous remarquons souvent que jusqu'à la moitié des employés d'une organisation donnée tomberont dans le piège de l'hameçonnage. En moyenne, 45 % d'entre eux se feront hameçonner.

La crise du **coronavirus** arrive en tête de liste des sujets les plus populaires et il est clair que ce sera également le cas en 2022.

La variante **Omikron**, les campagnes de vaccination en cours et la suspicion des experts de la santé que la crise actuelle pourrait durer au moins jusqu'en 2025, entraînent une grande responsabilité pour les employeurs : former les personnes à reconnaître l'hameçonnage et les aider à le gérer en toute sécurité.



Bien entendu, il ne faut pas non plus oublier les autres sujets. Les sujets liés à la livraison de colis, aux ressources humaines et à l'informatique continuent d'influencer les employés, tout comme les messages liés au bureau :
l'influence **des outils de travail à domicile** joue clairement un rôle.

L'année **2022** devrait voir se poursuivre la tendance observée ces dernières années : l'hameçonnage continuera de gagner en popularité de manière exponentielle auprès des criminels, ce qui signifie que les prestataires de services de sensibilisation à la cybersécurité doivent rester vigilants. Pour ce faire, Phished aide les entreprises à sensibiliser leurs employés.

PHISHED

phished.io
hello@phished.io
+ 32 53 31 97 55