Classement Phishers' Favorites

Bilan 2022

www.vadesecure.com

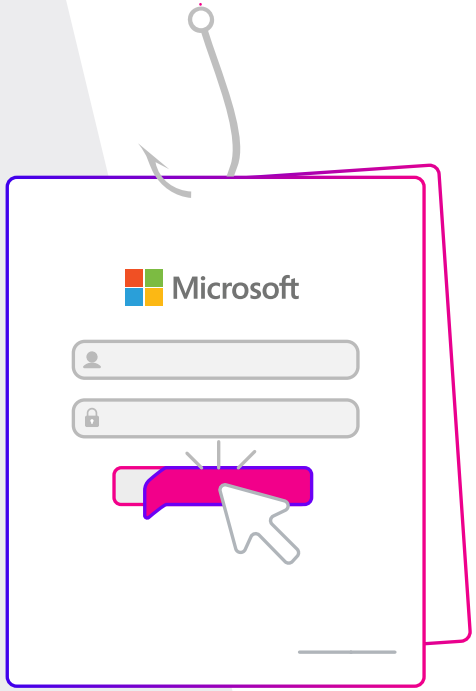
CONTENTS

Classement Phishers' Favorites : bilan de l'année

LES 20 MARQUES DONT L'IDENTITÉ EST LA PLUS SOUVENT USURPÉE LORS D'ATTAQUES DE PHISHING

Chaque année, Vade publie son bilan Phishers' Favorites, qui met en lumière les 20 marques les plus utilisées lors des attaques de phishing et se penche sur les tendances marquantes de l'année.

Chaque trimestre, le moteur de filtrage de Vade détecte et analyse des millions d'emails de phishing et des centaines de milliers de pages malveillantes. Pour classer les principales marques victimes de ces fraudes, nous nous basons sur le nombre de sites de phishing uniques les prenant pour cible. En effet, les cybercriminels envoient bien souvent des dizaines, voire des centaines ou des milliers d'emails de phishing contenant le même lien, et un même domaine peut héberger des milliers d'URL de phishing.



LES 20 MARQUES DONT L'IDENTITÉ EST LA PLUS SOUVENT USURPÉE LORS D'ATTAQUES DE PHISHING

En 2022, le nombre d'attaques de phishing a augmenté de 48 % par rapport à l'année précédente sur l'ensemble des marques de notre classement. Celles-ci ont ainsi représenté plus de 274 600 sites de phishing uniques, contre seulement 185 000 en 2021.

Pour la deuxième année consécutive, Facebook est la marque la plus usurpée, devant Microsoft. Avec plus de 25 000 sites de phishing uniques, Facebook représente 9 % du nombre total de sites de phishing comptabilisés dans notre classement 2022. Microsoft occupe la deuxième position pour la deuxième année consécutive, avec presque 2 000 sites de moins (une différence néanmoins insuffisante pour varier en pourcentage). Comme en 2021, la firme de Redmond reste la marque professionnelle la plus usurpée.

Google décroche la 3e place, avec une croissance de 1 560 % sur un an du nombre de pages de phishing le concernant, soit la deuxième plus forte hausse parmi les marques de notre top 20. Le leader du cloud a ainsi inspiré presque 20 000 pages de phishing uniques, soit 7 % du total. PayPal accède à la 4e place, avec 6 % du total, alors que le site de paiement n'était que 10e en 2021. Enfin, MTB vient fermer notre top 5, alors que la marque était 18e en 2021. Elle représente aujourd'hui 5 % des pages de phishing.

9%
des sites de phishing uniques

facebook

9%
des sites de phishing uniques

Microsoft

Classement Phishers' Favorites 2022

LES 20 MARQUES DONT L'IDENTITÉ EST LA PLUS SOUVENT USURPÉE LORS DES ATTAQUES DE PHISHING

Nombre	Evolution	Marque	Catégorie	URLs de Phishing Uniques
1	0	Facebook	Réseaux sociaux	25551
2	0	Microsoft	Cloud	22531
3	↑ 25	Google	Cloud	19695
4	↑ 6	PayPal	Services financiers	15863
5	↑ 13	MTB	Services financiers	13330
6	0	Orange	Internet/Télécom	12839
7	↓ -4	Crédit Agricole	Services financiers	11998
8	↓ -4	WhatsApp	Réseaux sociaux	10388
9	↓ -4	La Banque Postale	Services financiers	10242
10	N/A	au	Internet/Télécom	9542
11	↑ 1	Netflix	Cloud	9018
12	↑ 7	Apple	Commerce électronique/Logistique	7634
13	↓ -6	Amazon	Commerce électronique/Logistique	7364
14	↓ -1	Wells Fargo	Services financiers	6885
15	↓ -7	Chase	Services financiers	6788
16	↑ 6	Instagram	Réseaux sociaux	6403
17	↓ -8	Comcast	Internet/Télécom	6327
18	↓ -4	Rakuten	Commerce électronique/Logistique	4850
19	↑ 52	Credit Saison	Services financiers	4593
20	↓ -5	Adobe	Cloud	4503
				216344

Ajoutés :
Google, au, Instagram, Credit Saison

Supprimés :
OVH, LinkedIn, Yahoo, DHL

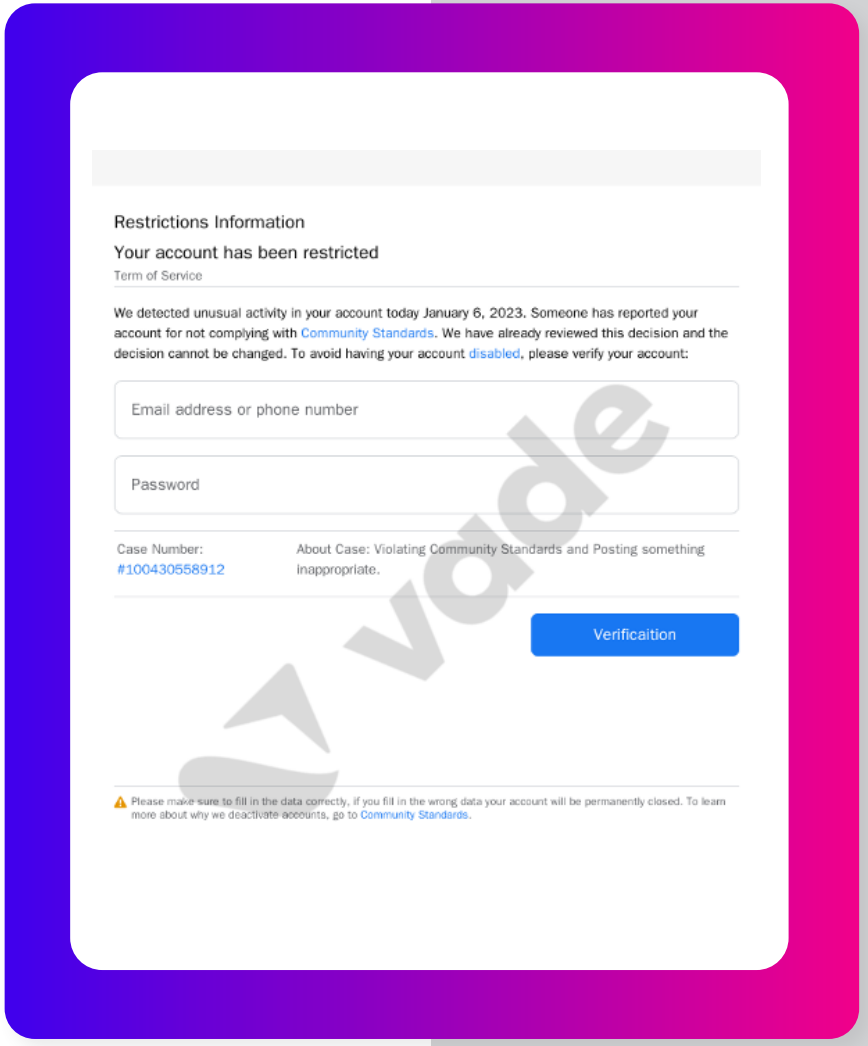
UNE ANNÉE RICHE EN INCERTITUDES POUR FACEBOOK, QUI RESTE LA MARQUE LA PLUS USURPÉE

Le géant des médias sociaux a encore une fois été confronté à un tsunami de phishing en 2022. Si la marque s'est classée en 4e position au premier semestre, ses « performances » du 2e semestre ont changé la donne et l'ont propulsée en tête du classement annuel.

L'explosion des sites de phishing se faisant passer pour Facebook a coïncidé avec une période tumultueuse pour l'entreprise. La publication de rapports suggérant une baisse du nombre de ses utilisateurs actifs et de ses revenus publicitaires a entraîné une chute de l'action de l'entreprise et une importante vague de licenciements.[1]

Les difficultés du réseau social semblent avoir motivé les hackers. La marque est en effet restée leur cible privilégiée dans la galaxie Meta, qui détient également WhatsApp et Instagram, deux plateformes également classées dans notre top 20 2022. Ensemble, les trois marques de Meta ont ainsi représenté 42 342 pages de phishing uniques, un chiffre impressionnant, quoiqu'en léger retrait par rapport à 2021 (43 169).

Les attaques de phishing utilisant Facebook prennent des formes variables, de la fausse notification de limitation du compte à la demande de contrôle de sécurité. Toutes ont néanmoins un point commun, rediriger les utilisateurs vers des pages malveillantes pour récupérer leurs identifiants.



Usurpation de Facebook

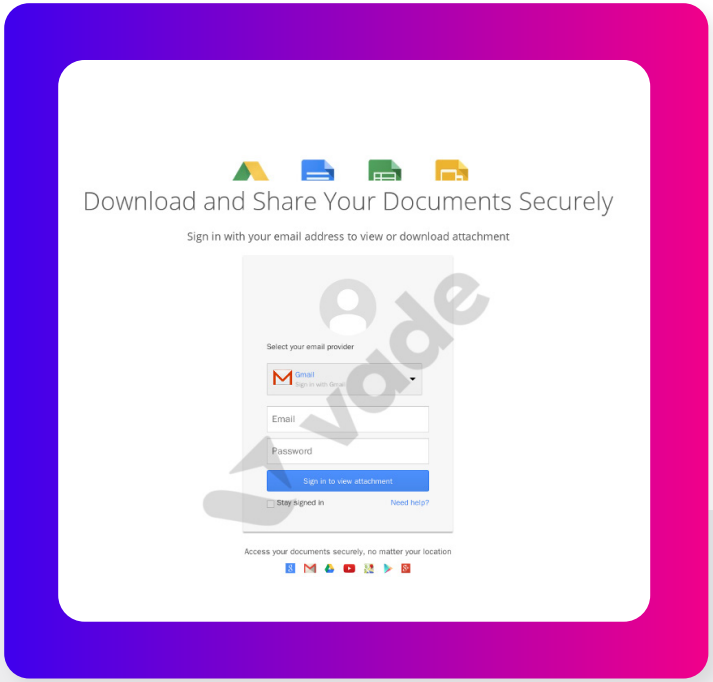
[1]Forbes. "Meta Layoffs – Facebook Continues to Cust Costs by Cutting Headcount." https://www.forbes.com/sites/qai/2022/12/07/meta-layoffsfacebook-continues-to-cut-costs-by-cutting-headcount/?sh=137a64328456

MICROSOFT ET GOOGLE PROUVENT QUE LES LOGICIELS DE PRODUCTIVITÉ SONT LA PRIORITÉ DES HACKERS

Microsoft figure depuis longtemps parmi les marques fétiches des hackers : elle s'est classée en 2e position de notre classement en 2021 et 2022. A contrario, la montée en flèche de Google à la 3e place en 2022 est une vraie nouveauté. Microsoft a terminé l'année avec 22 531 pages de phishing à son actif, contre 19 695 pour Google. Les deux marques dominent le cloud, en dépassant à elles seules toutes les autres marques du secteur (42 226 contre 38 893).

Leur popularité peut s'expliquer par l'intérêt toujours plus vif suscité par leurs suites de productivité. Microsoft 365 reste en effet la suite de productivité la plus populaire au monde, avec 345 millions d'utilisateurs professionnels en 2022[2], contre seulement 200 millions 2 ans plus tôt.[3] De son côté, Google Workspace continue de gagner des parts de marché et est désormais la deuxième suite de productivité la plus utilisée en entreprise.[4]

Les suites de productivité constituent des cibles de choix pour les hackers. En effet, elles réunissent plusieurs applications intégrées et leur offrent ainsi davantage d'opportunités d'exploiter les utilisateurs avant et après l'attaque initiale. Au sein d'un tel écosystème, les hackers peuvent par exemple détourner une solution de partage de fichiers lors de leur attaque initiale, puis utiliser des comptes compromis pour distribuer leurs liens et fichiers malveillants sur d'autres canaux, comme des outils de messagerie instantanée..



Usurpation de Google

[2]Microsoft. "Earnings Release Q3 2022." https://www.microsoft.com/en-us/investor/earnings/fy-2022-q3/press-release-webcast

[3]Microsoft. "Microsoft FY20 First Quarter Earnings Conference Call." https://www.microsoft.com/en-us/Investor/events/FY-2020/earnings-fy-2020-q1.aspx

[4]https://www.gartner.com/en/documents/4004066

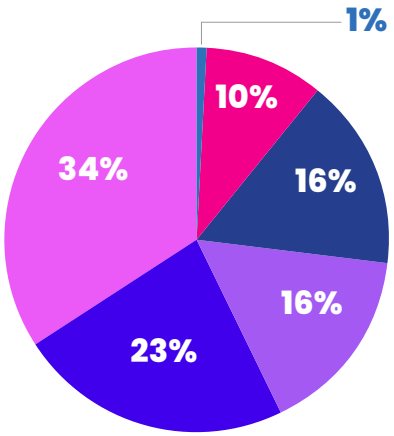
Tant que les suites de productivité resteront appréciées des utilisateurs professionnels, les hackers continueront de les prendre pour cible. Par conséquent, nous pensons que Microsoft et Google ont toutes les chances d'occuper les premières places de notre classement Phishers' Favorites l'année prochaine.

Usurpation de Microsoft

LE SECTEUR DES SERVICES FINANCIERS RESTE LE PLUS TOUCHÉ PAR LE PHISHING

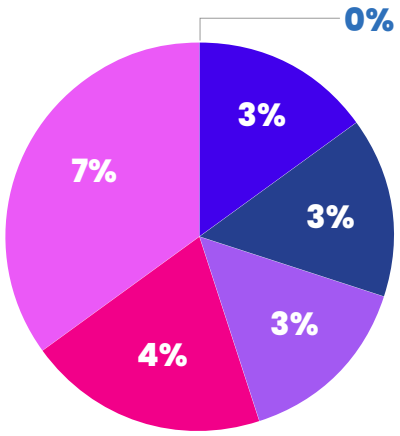
Si les secteurs des médias sociaux et du cloud sortent du lot en raison des leaders de leur catégorie, celui des services financiers attire l'attention de part sa dominance globale sur les autres secteurs. En effet, il reste en tête du classement en représentant plus de 34 % des pages de phishing uniques. Il est suivi par le secteur du cloud (23 %), des médias sociaux (16 %), d'Internet/télécommunications (16 %) et de l'e-commerce/logistique (10 %). Le secteur gouvernemental ferme la marche en représentant seulement 1 % des sites de phishing.percent).

Phishing par secteur écononmique : 2022



Répartition en pourcentage des attaques de phishing par secteur

Marques dans le top 20 : 2022



Nombre de marques classées dans le top 20 Phishers' Favorites par secteur

Services financiers
Internet/Télécom
Commerce électronique/Logistique
Cloud
Réseaux sociaux
Gouvernement

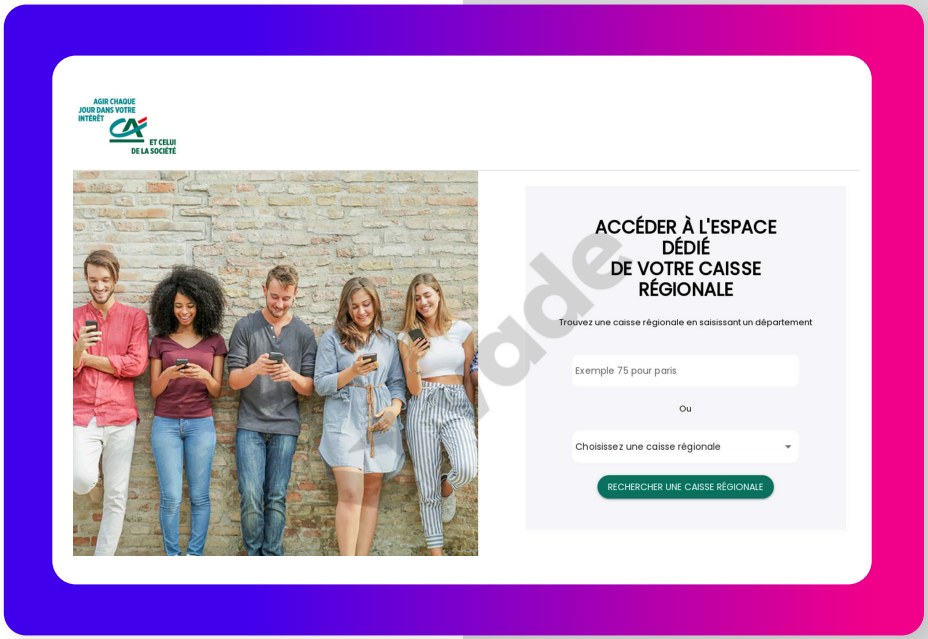
Les services financiers regroupent aussi le plus de marques classées dans le top 20 (7). Ils sont suivis du cloud (4), de l'e-commerce/logistique, d'Internet/télécommunications et des médias sociaux (3). Là encore, le secteur gouvernemental ferme la marche (0). PayPal a pris la tête du secteur financier et est suivi par MTB, le Crédit Agricole (7e place), La Banque postale (9e place), Wells Fargo (14e place), Chase (15e place) et Credit Saison (19e place).

Les services financiers restent populaires chez les hackers en raison de la récompense potentielle associée à chaque attaque, qui peut leur donner accès aux comptes bancaires et autres comptes financiers de leur victime. Cette année, le secteur a par ailleurs lui aussi connu une période tumultueuse, les médias ne cessant d'évoquer les craintes suscitées par l'inflation et la récession. Ces conditions difficiles sont idéales pour les hackers, qui ont l'habitude de recourir à des technologies d'ingénierie sociale pour jouer sur les peurs et inquiétudes du grand public.

LE NOMBRE D'ATTAQUES DE PHISHING A EXPLOSÉ DANS TOUS LES SECTEURS

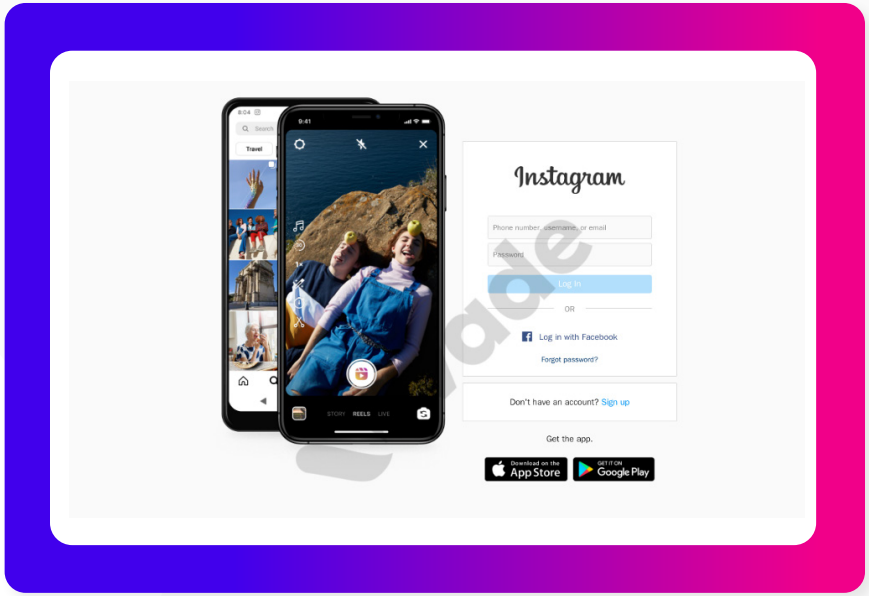
À l'exclusion des médias sociaux, chaque secteur a connu une hausse considérable du nombre de pages de phishing sur un an. C'est le secteur Internet/Télécommunication qui a subi la hausse la plus marquée (111 %). Il est suivi du cloud (77 %), de l'e-commerce/logistique (59 %), des services financiers (46 %) et du secteur gouvernemental (26 %).

Dans le secteur du cloud, Netflix (11e place) et Adobe (20e place) ont rejoint Microsoft et Google dans le top 20. En ce qui concerne les médias sociaux, WhatsApp reste derrière Facebook, à la 8e place, et est suivi par Instagram (16e). LinkedIn, 17e en 2021, quitte cette année le top 20 et dégringole à la 30e place.

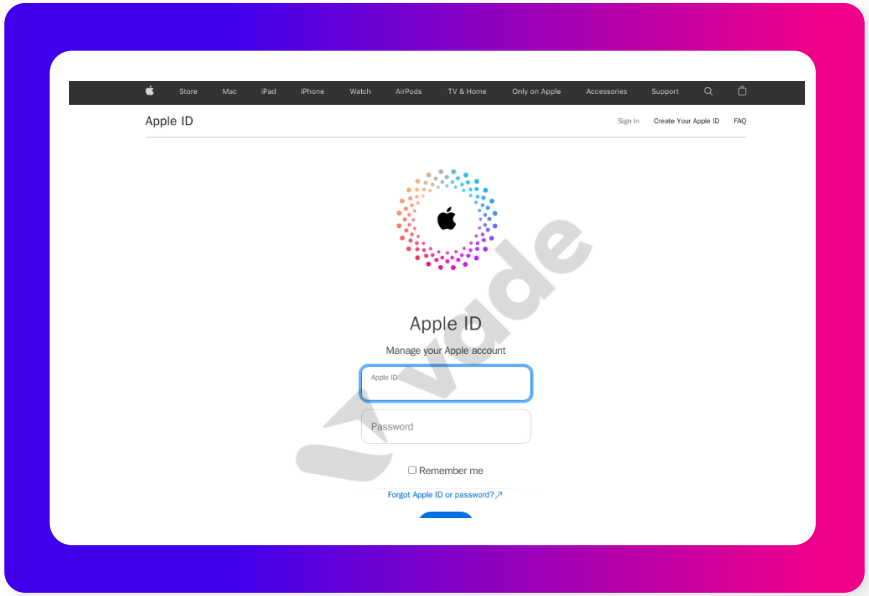


Usurpation du Crédit Agricole

Orange, au et Comcast sont les seules marques du secteur Internet/ Télécommunications présentes dans le top 20. Elles occupent respectivement la 6e, la 10e et la 17e place. Apple domine le secteur E-commerce/logistique en atteignant la 12e place. La firme de Cupertino est suivie par Amazon et Rakuten, respectivement à la 13e et la 18e place.



Usurpation d'Instagram

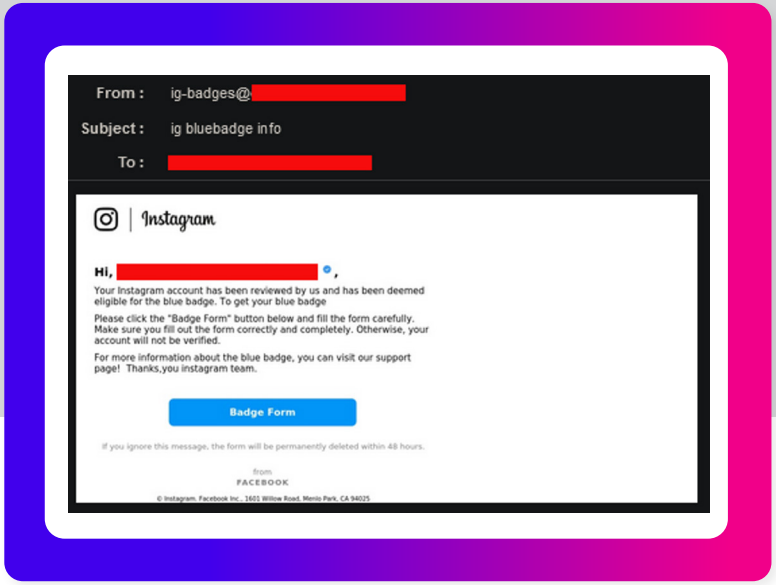


Usurpation d'Apple

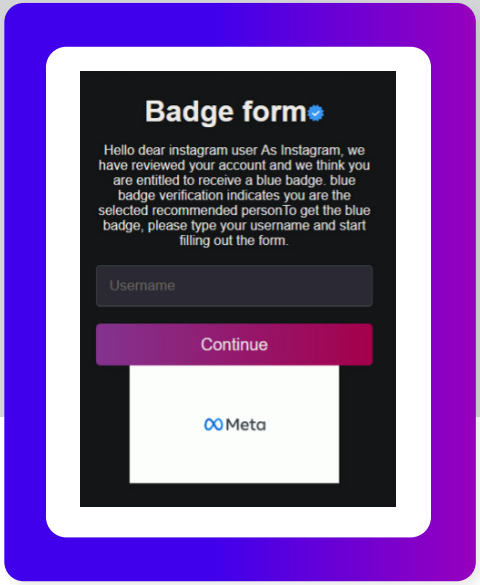
LES HACKERS PRIVILÉGIENT LES ATTAQUES CIBLÉES

Nous avons l'habitude des campagnes de phishing généralistes. Pourtant, confrontés à un grand public de plus en plus sensibilisé à leurs techniques, les hackers semblent choisir leurs victimes et leurs stratégies plus finement.

Une campagne de phishing menée sur Instagram témoigne de cette nouvelle approche. À la différence des autres, elle cible ses victimes en mentionnant leur véritable nom d'utilisateur sur la plateforme. Grâce à d'autres techniques, comme l'usurpation du logo et l'utilisation d'images de bonne qualité, cette attaque paraît plus vraie que les autres.



Email de phishing Instagram



Formulaire de phishing d'Instagram

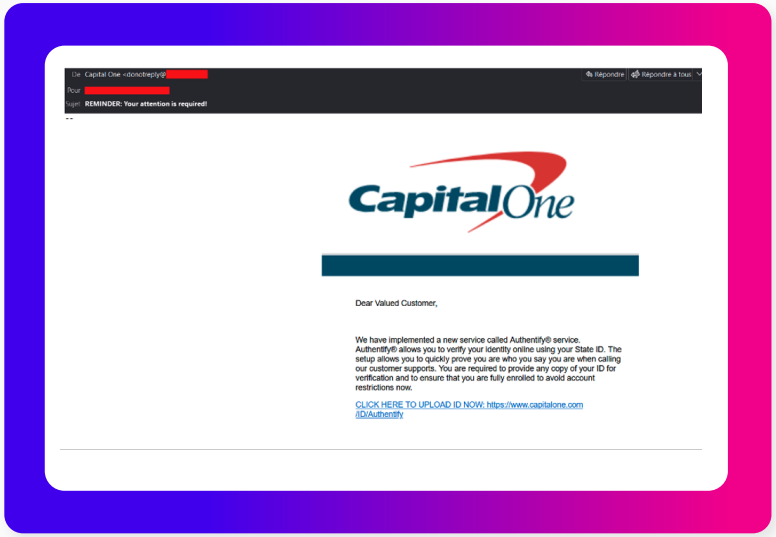
Les hackers ont de moins en moins de difficultés à lancer des attaques de phishing ciblées. En effet, ils peuvent très facilement mettre la main sur des informations personnelles leur permettant d'élaborer des scams sur mesure, que ce soit via des fuites de données ou les habitudes de partage des utilisateurs sur les médias sociaux. Ce phénomène montre qu'il est nécessaire de renforcer la sensibilisation au phishing et de déployer des solutions de sécurité de l'email de pointe.

LES HACKERS TIRENT PROFIT DE L'ACTUALITÉ

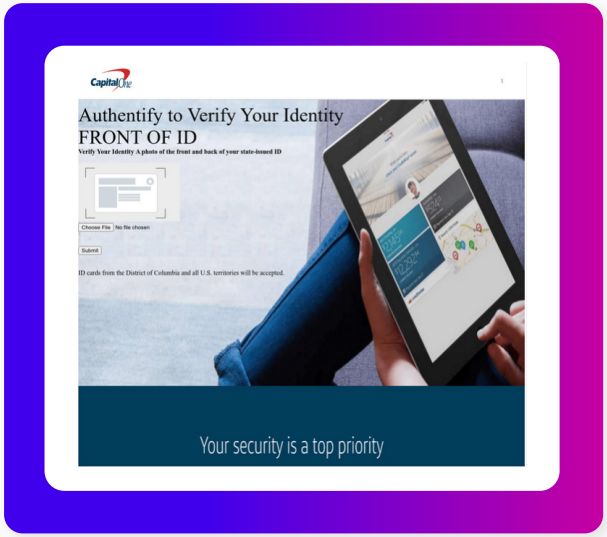
Les hackers gardent l'œil sur les événements en cours pour imaginer de nouveaux moyens d'exploiter leurs victimes. Nouveaux produits ou nouveaux partenariats, l'actualité pousse souvent le consommateur à baisser sa garde, ce qui permet aux hackers de faire preuve de davantage de créativité dans leurs attaques.

Par exemple, une campagne de phishing détectée par Vade au 2e trimestre 2022 a tenté d'exploiter le nouveau partenariat conclu entre l'établissement financier Capital One (48e dans notre classement 2022) et Authentify, un service de vérification en ligne utilisé par le secteur pour contrôler l'identité de ses clients. Des acteurs malveillants ont ainsi envoyé des emails de phishing aux clients de Capital One pour leur présenter le service Authentify et les inviter à valider leur identité afin d'éviter que leur compte Capital One ne soit restreint.

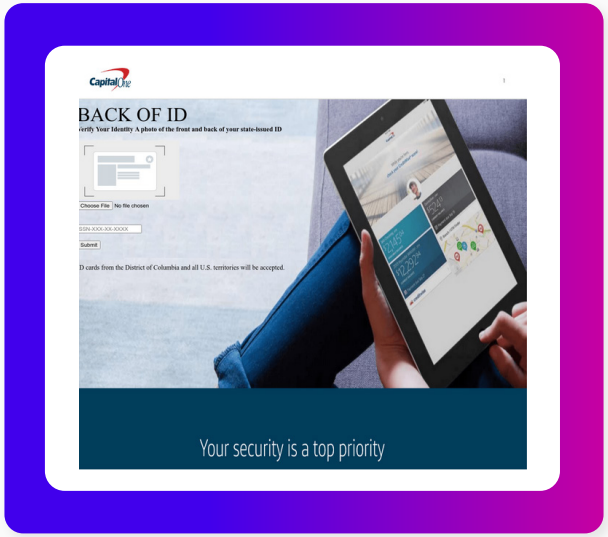
Cet email contient un lien malveillant dirigeant les utilisateurs vers un site Web compromis semblant édité par Capital One. Ils y sont alors invités à s'authentifier en scannant et envoyant les deux côtés de leur pièce d'identité. À la différence des autres campagnes de phishing, celle-ci tente d'usurper l'identité des victimes plutôt que de dérober leurs identifiants. attempts to steal the victim's identity rather than their account credentials.



Email de phishing Capital One / Authentify



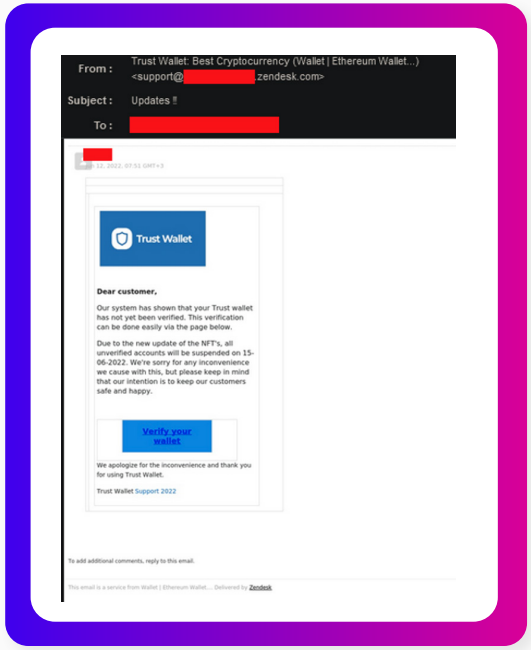
Première page de phishing Capital One



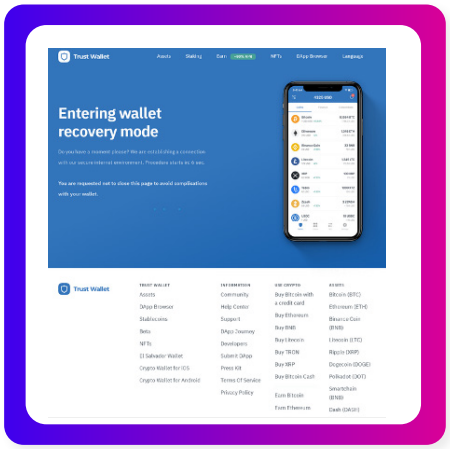
Deuxième page de phishing Capital One

Lors d'une autre campagne, les hackers se sont servis de l'actualité pour lancer une attaque en s'appuyant sur l'identité de TrustWallet, un portefeuille Ethereum et de stockage de cryptomonnaie très utilisé pour la conservation de jetons non fongibles (NFT). Ils ont tiré parti de la chute des cryptomonnaies au premier semestre pour jouer sur les angoisses des investisseurs et pousser les utilisateurs de TrustWallet à divulguer leurs phrases de récupération de mot de passe.

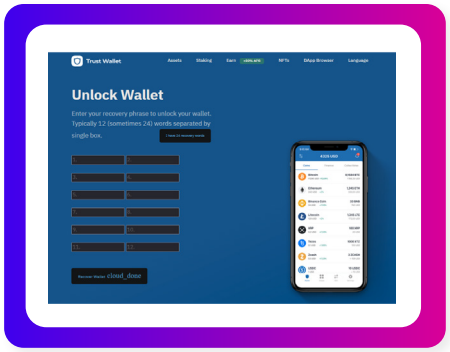
Dans ce scam, l'email de phishing informe l'utilisateur que son portefeuille doit être vérifié en raison d'une mise à jour d'un NFT. L'email prévient l'utilisateur que s'il ne le fait pas, son compte sera restreint. Il contient un lien de phishing raccourci qui masque la véritable destination de l'URL et redirige les utilisateurs vers un site malveillant reprenant l'apparence et les sections du site original de TrustWallet.



Email de phishing se faisant passer pour TrustWallet



Site de phishing TrustWallet



TrustWallet phishing page for recovery phrases

Une fois que les utilisateurs sont arrivés sur le site, ils sont confrontés à différentes manœuvres destinées à instiller un faux sentiment de sécurité. La page de phishing affiche un compte à rebours de 10 secondes le temps « d'ouvrir un environnement Internet sécurisé ». À la fin du compte à rebours, la page malveillante s'affiche.

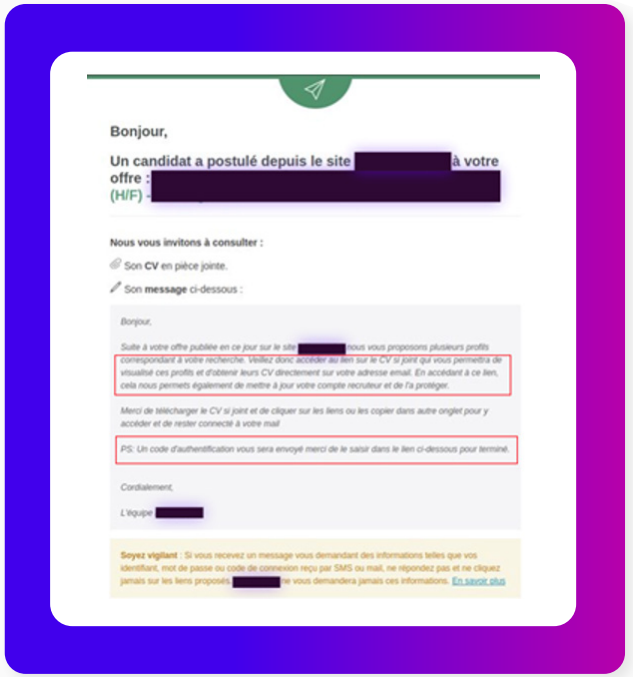
L'utilisateur est invité à saisir sa phrase de récupération pour débloquer son portefeuille. Pour tenir compte des différents portefeuilles de cryptomonnaies, la page accepte les phrases de 12 et 24 mots, permettant aux utilisateurs de choisir l'option qui leur convient. Cette fonction améliore la légitimité perçue de la page, mais augmente aussi le nombre de victimes potentielles.

LES HACKERS DÉTOURNENT DES SERVICES LÉGITIMES

En plus de réaliser des attaques plus ciblées, les hackers tirent aussi parti de services légitimes pour contourner la détection des solutions de sécurité. Un service d'offres d'emploi français en a par exemple été victime plus tôt dans l'année : les hackers ont répondu à des offres en envoyant des CV qui contenaient des liens de phishing.

Pour chacune de ces candidatures, la plateforme générait automatiquement un email remettant le CV vérolé aux recruteurs.

Lorsqu'elles ouvrent la pièce jointe PDF, les victimes sont invitées à cliquer sur les liens malveillants pointant vers un site de phishing, où les hackers peuvent récupérer leurs identifiants.



Email de réponse automatique de la plateforme

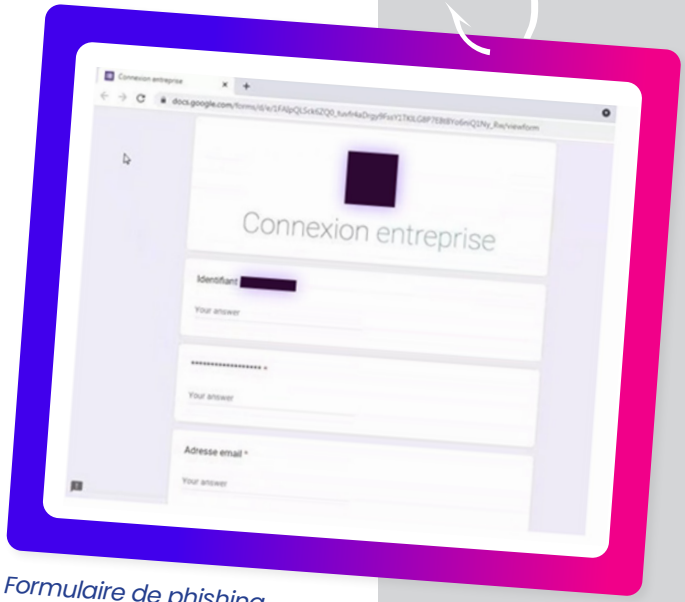
Pièce jointe malveillante au format PDF

L'attaque utilise les serveurs, adresses IP et noms de domaine légitimes du site, ce qui rend difficile sa détection par les filtres de messagerie des victimes.

Pour les hackers, le détournement de services légitimes présente un double intérêt. Tout d'abord, il dope leur productivité en éliminant certaines tâches techniques. Ensuite, il renforce l'efficacité d'une campagne en améliorant la légitimité perçue, ce qui rend l'attaque plus difficile à repérer.

LES ATTAQUES DE PHISHING SOPHISTIQUÉES NÉCESSITENT DES DÉFENSES QUI LE SONT TOUT AUTANT

Des attaques de phishing surviennent tous les jours, à une fréquence et une échelle impressionnantes. Il s'agit de l'une des cybermenaces les plus prisées des hackers, et elle ne risque donc pas de disparaître. Au contraire, elle va gagner en sophistication pour tromper les filtres plus pointus et les utilisateurs mieux sensibilisés. Pour protéger votre entreprise et vos clients des attaques de phishing dynamiques, associez formation, technologie et vigilance :



Formulaire de phishing Google

- **Formation des utilisateurs :** investissez dans une formation de sensibilisation au phishing qui va au-delà d'une simple session annuelle. En proposant une formation contextuelle lorsque l'utilisateur clique sur un lien de phishing, vous pouvez lier l'événement à la formation et favoriser ainsi sa mémorisation.
- **Technologie anti-phishing basée sur l'IA :** une technologie anti-phishing basée sur l'IA est plus performante que les défenses basées sur la réputation et la signature. Les algorithmes d'apprentissage non supervisé savent généraliser des situations en s'appuyant sur des jeux de données et peuvent ainsi reconnaître des variantes d'attaques connues. Les algorithmes d'apprentissage profond avec Computer Vision sont entraînés à reconnaître les images des marques et détectent même les altérations les plus légères destinées à tromper les filtres.
- **Réponse automatisée aux incidents :** les emails de phishing qui parviennent à tromper les filtres sont rapidement ouverts par leurs destinataires. La réponse automatisée aux incidents de phishing supprime les menaces après qu'elles ont été remises et réduit ainsi les recherches et mesures manuelles.
- **Protection contre les attaques en plusieurs phases :** les emails de spear phishing sans liens et les malwares inconnus nécessitent des technologies et capacités supplémentaires, réunies au sein d'une même solution. Les algorithmes d'apprentissage non supervisé détectent les événements rares et les anomalies, tandis que le natural language processing repère les comportements malveillants, comme des mots et expressions souvent utilisés dans le cadre du spear phishing.

À propos de Vade

Vade est une entreprise internationale de cybersécurité spécialisée dans le développement de technologies de détection et de réponse aux menaces grâce à l'intelligence artificielle. Les produits et solutions de Vade protègent les consommateurs, les entreprises et les organisations contre les attaques véhiculées par email, y compris les malwares/ransomwares, le spear phishing, les attaques Business Email Compromise et le phishing.

Fondée en 2009, Vade protège 1,4 milliard de messageries professionnelles et personnelles et propose aux marchés des FAI, PME et MSP des solutions et produits acclamés qui permettent de renforcer la cybersécurité et d'accroître l'efficacité informatique. increase cybersecurity and maximize IT efficiency.

vade

Abonnez-vous à notre blog :
www.vadesecure.com/fr/blog

Suivez-nous sur :

@vadesecure