# Top e-mail Menaces et tendances

Vol. 1 Juin 2024

## Principales conclusions concernant l'évolution des menaces par e-mail à l'ère de l'IA générative

« De la hausse du business email compromise aux attaques par code QR, en passant par l'utilisation abusive des webmails à des fins de social engineering, les cybercriminels continuent d'adapter leurs tactiques, en tirant profit des façons dont l'IA générative peut les aider. Ce reporting approfondi analyse les tendances les plus récentes en matière de menaces par e-mail et la façon dont les pirates exploitent de nouveaux moyens pour piéger leurs victimes ».

Barracuda

# Table des matières

# Résultats clés

L'escroquerie et l'hameçonnage représentent **86 %** des attaques de social engineering.

Environ **1 boîte de réception sur 20** a été ciblée par des attaques par code QR au cours du dernier trimestre 2023.

Les comptes subissant les attaques Business email compromise (BEC) représentent **1 attaque sur 10**.

**Gmail** est le service de messagerie Web gratuit le plus populaire utilisé pour le social engineering.

Le détournement de conversation a augmenté de **70 %** depuis 2022.

bit.ly est utilisé dans près de **40 %** des attaques de social engineering qui comprennent une URL raccourcie.

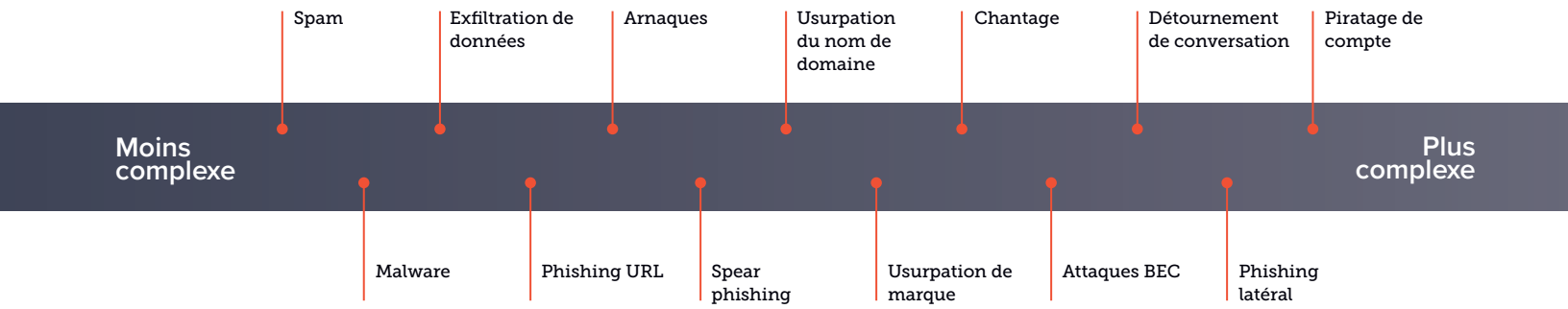
# L'impact et l'évolution des menaces basées sur les e-mails

Si les pirates cherchent à exploiter de nombreux vecteurs de menace différents, l'e-mail reste l'un des plus populaires. Face à la profusion d'attaques basées sur les e-mails, les entreprises s'exposent à des pertes financières, à une dégradation de la réputation et à d'autres impacts négatifs.

D'après l'étude réalisée en 2023 par Ponemon Institute pour le rapport Cybernomics 101 de Barracuda, 92 % des organisations interrogées ont subi en moyenne six compromissions d'identifiants causées par le hameçonnage ou d'autres menaces basées sur les e-mails au cours des 12 derniers mois. Le rapport montre également que chaque membre du personnel informatique affecté à la résolution du problème a passé en moyenne 427 heures à enquêter, nettoyer, réparer et documenter les attaques d'hameçonnage au cours de cette période. Si l'on tient compte des conséquences en aval des attaques réussies, temps d'arrêt, perte d'opportunités commerciales, atteinte à la réputation, paiement de rançons, etc., les coûts financiers peuvent souvent atteindre un million de dollars ou plus.

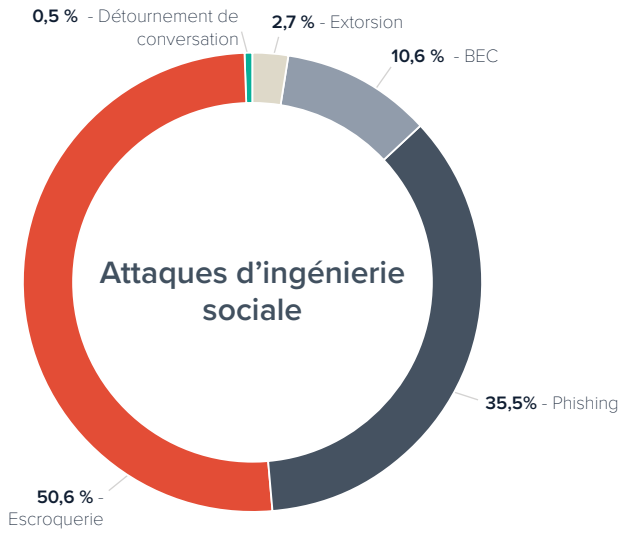
Les chercheurs de Barracuda ont identifié 13 types de menaces par e-mail auxquelles les organisations sont confrontées aujourd'hui. Il s'agit d'attaques à grand volume, telles que le spam ou les malwares, ou de menaces plus ciblées utilisant le social engineering, telles que les business email compromise et usurpations d'identité. Ce rapport examine de plus près cinq de ces types de menaces que les chercheurs de Barracuda ont suivis de près, ainsi que des informations et des exemples de nouvelles façons dont les pirates tentent de tromper les victimes ou d'échapper à la détection.

### 13 types de menaces par e-mail



# Tendances des attaques de social engineering

Les chercheurs de Barracuda ont suivi cinq catégories distinctes d'attaques de social engineering et ont analysé 69 millions d'attaques sur 4,5 millions de boîtes de réception en 12 mois dans le cadre de ce rapport.

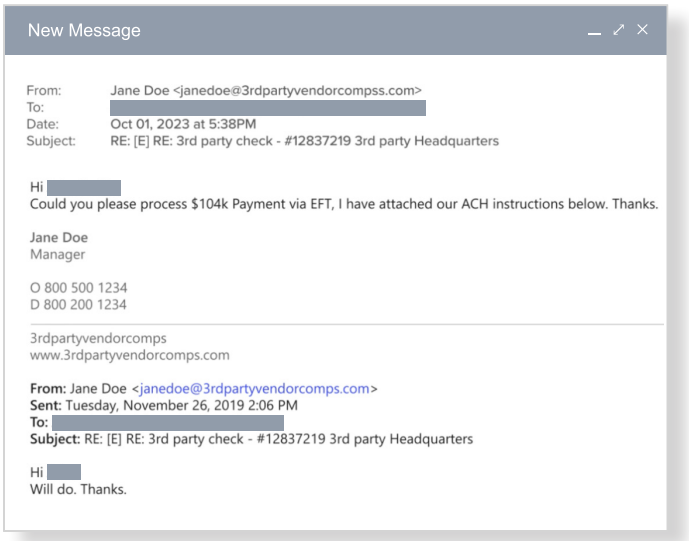



## Détournement de conversations

Détournement de conversation, parfois connu sous le nom d'usurpation d'identité, est une attaque ciblée par e-mail. Les cybercriminels s'immiscent dans des conversations d'entreprise existantes ou en entament de nouvelles, en se basant sur les informations qu'ils ont recueillies à partir de comptes de messagerie compromis ou d'autres sources.

Le détournement de conversations n'a représenté que 0,5 % des attaques de social engineering de l'année écoulée, mais cela représente une hausse de près de 70 % par rapport à 2022, où il représentait 0,3 % des attaques. Bien que ces attaques demandent beaucoup d'efforts de la part des pirates pour être exécutées, les gains peuvent être importants.

La plupart du temps, le détournement de conversations s'inscrit dans une attaque de piratage de comptes. Les pirates utilisent des attaques par phishing pour voler les identifiants de connexion et compromettre les comptes professionnels. Ils passent ensuite du temps à lire les e-mails et à surveiller le compte compromis afin de cerner les opérations de l'entreprise et de se renseigner sur les transactions en cours, les procédures de paiement et d'autres détails. Les pirates vont alors exploiter ces informations, y compris les conversations internes et externes entre les employés, partenaires et clients, pour élaborer des messages paraissant authentiques et convaincants, les envoyer à partir de domaines usurpés, et inciter leurs victimes à transférer de l'argent ou à mettre à jour leurs informations de paiement.


New Message

From: Jane Doe <janedoe@3rdpartyvendorcompss.com>
To: [redacted]
Date: Oct 01, 2023 at 5:38PM
Subject: RE: [E] RE: 3rd party check - #12837219 3rd party Headquarters

Hi [redacted]
Could you please process $104k Payment via EFT, I have attached our ACH instructions below. Thanks.

Jane Doe
Manager

O 800 500 1234
D 800 200 1234

3rdpartyvendorcomps
www.3rdpartyvendorcomps.com

**From:** Jane Doe <janedoe@3rdpartyvendorcomps.com>
**Sent:** Tuesday, November 26, 2019 2:06 PM
**To:** [redacted]
**Subject:** RE: [E] RE: 3rd party check - #12837219 3rd party Headquarters

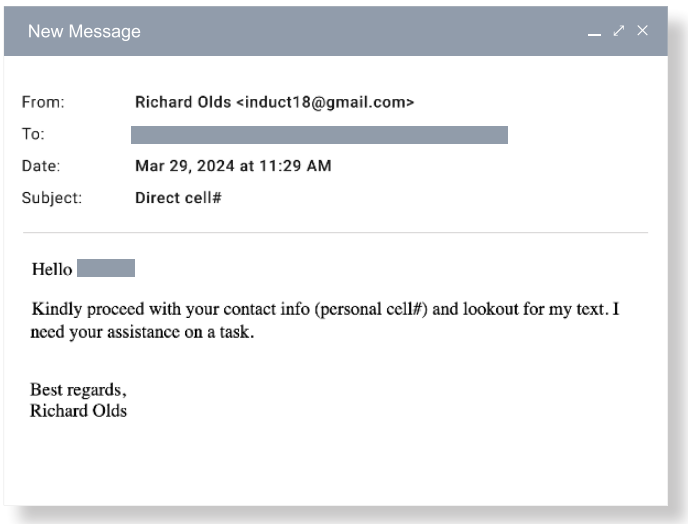
Hi [redacted]
Will do. Thanks.

## Attaques de Business email compromise (BEC)

Les attaques BEC impliquent généralement qu'un cybercriminel se fasse passer pour une personne interne ou externe à une organisation. En 2023, ces attaques représenteront 10,6 %, plus d'une sur dix, de toutes les attaques de social engineering, et les chiffres montrent une hausse constante d'année en année.

Les attaques BEC font les gros titres. Des organisations de tous les secteurs, éducation, santé, commerce de détail, voyages, services financiers, énergie, administrations publiques, etc, sont victimes de l'une de ces attaque

2023, perdant souvent des millions de dollars. Lors d'une attaque BEC classique, un pirate se fait passer pour un employé, généralement un cadre, et demande des virements électroniques, des cartes-cadeaux ou l'envoi d'argent à de fausses organisations caritatives. Ces attaques ne visent pas seulement les utilisateurs les plus en vue, mais aussi tous ceux qui ont accès à des informations financières et à d'autres données sensibles, comme les directeurs financiers et les chargés de rémunération.


New Message

From: Richard Olds <induct18@gmail.com>
To: [redacted]
Date: Mar 29, 2024 at 11:29 AM
Subject: Direct cell#

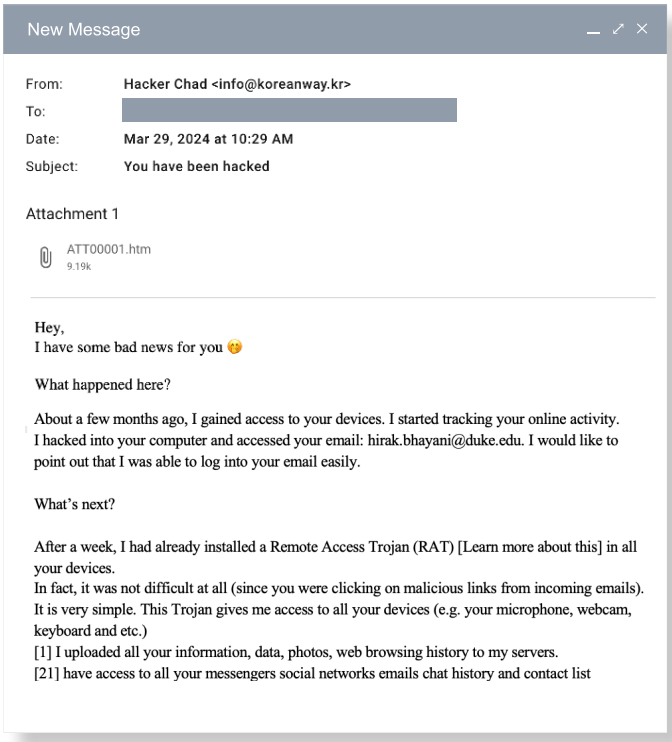
Hello [redacted]

Kindly proceed with your contact info (personal cell#) and lookout for my text. I need your assistance on a task.

Best regards,
Richard Olds

## Chantage

Bien que les attaques par extorsion représentent moins de 3 % du nombre total d'attaques d'hameçonnage ciblées, ces attaques peuvent exposer des informations sensibles ou potentiellement embarrassantes sextorsion, où les pirates menacent d'exposer des contenus sensibles ou embarrassants aux contacts de leurs victimes, à moins qu'une rançon ne soit versée. Les demandes sont généralement de l'ordre de quelques centaines ou milliers de dollars et doivent être payées en cryptomonnaie, ce qui peut être difficile à retracer. Ces escroqueries peuvent également avoir des conséquences tragiques qui vont au-delà des pertes monétaires, notamment des traumatismes psychologiques.


New Message

From: Hacker Chad <info@koreanway.kr>
To: [redacted]
Date: Mar 29, 2024 at 10:29 AM
Subject: You have been hacked

Attachment 1

ATT00001.htm
9.19k

Hey,
I have some bad news for you 😠

What happened here?

About a few months ago, I gained access to your devices. I started tracking your online activity. I hacked into your computer and accessed your email: hirak.bhayani@duke.edu. I would like to point out that I was able to log into your email easily.

What's next?

After a week, I had already installed a Remote Access Trojan (RAT) [Learn more about this] in all your devices.
In fact, it was not difficult at all (since you were clicking on malicious links from incoming emails). It is very simple. This Trojan gives me access to all your devices (e.g. your microphone, webcam, keyboard and etc.)
[1] I uploaded all your information, data, photos, web browsing history to my servers.
[21] have access to all your messengers social networks emails chat history and contact list

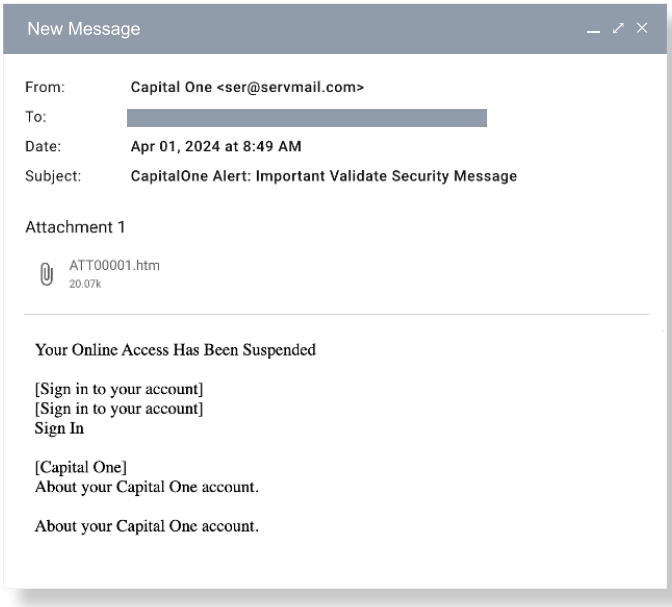
## Attaques par hameçonnage

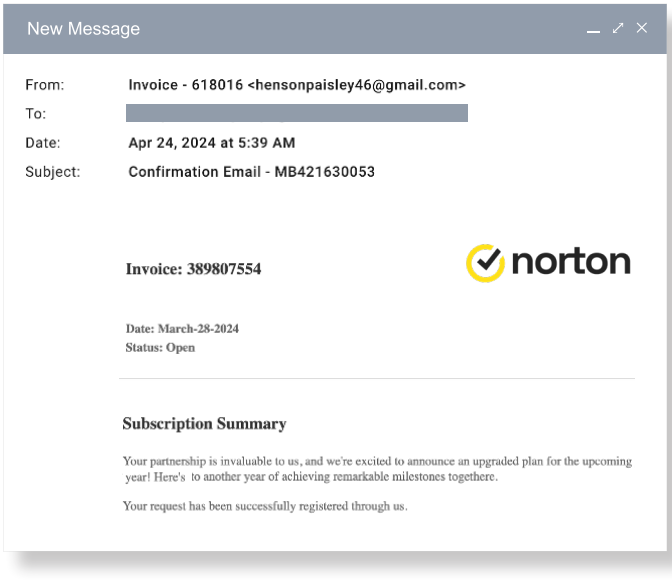
Dans les attaques de phishing, ou d'usurpation d'identité, les cybercriminels envoient des e-mails qui semblent provenir d'une marque ou d'un service bien connu, pour tenter d'inciter les victimes à cliquer sur un lien d'hameçonnage. Ces attaques ont représenté 35,5 % de toutes les menaces de type social engineering l'année dernière. Presque toutes les attaques qui entrent dans cette catégorie comprennent un URL. Bien que les e-mails de phishing soient utilisés par les pirates depuis des années, ils ont commencé à déployer des moyens ingénieux pour éviter d'être détectés par les technologies de protection des liens. Ils raccourcissent les URL, utilisent de nombreuses redirections et hébergent des liens malveillants sur des sites de partage de documents, tout cela pour éviter d'être bloqués par les technologies d'analyse des e-mails.

## Attaques par escroquerie

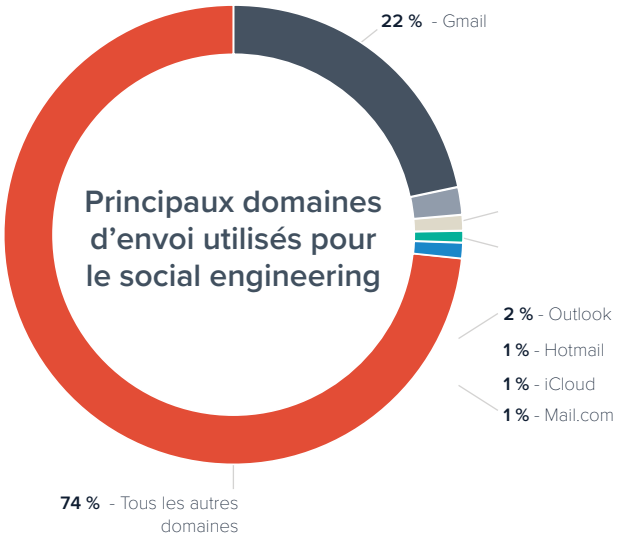
Les attaques par escroquerie prennent de nombreuses formes, y compris des promesses de gains à la loterie, des colis non réclamés, des propositions commerciales, de faux emplois, des sollicitations de dons et d'autres stratagèmes. Les attaques par escroquerie ont tendance à être moins ciblées que les autres types d'attaques, mais elles représentent un peu plus de la moitié de toutes les attaques du social engineering détectées au cours de l'année écoulée et sont toujours couronnées de succès.

Les pirates informatiques ratissent large avec les différents types d'escroqueries qu'ils mettent au point, et ces menaces coûtent aux victimes des milliards de dollars chaque année. Selon le rapport 2023 de l'Internet Crime Complaint Center (IC3) du FBI, le coût de la cybercriminalité signalée aux États-Unis a fait un bond de 22 % l'année dernière, pour atteindre plus de 12,5 milliards de dollars.



# Gmail est le service de messagerie web le plus utilisé

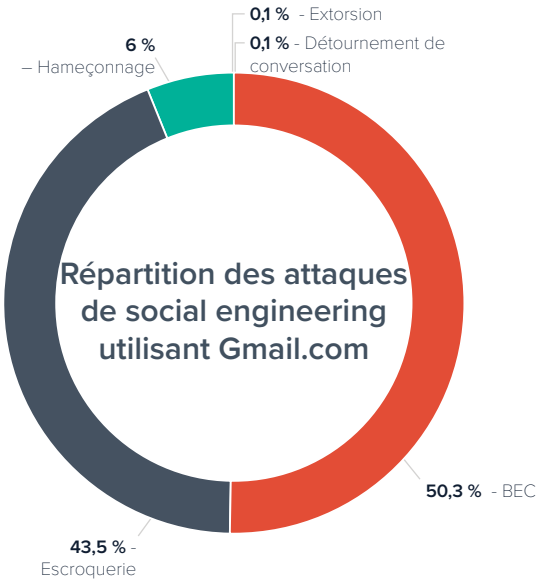



Les acteurs malveillants disposent de plusieurs options lorsqu'il s'agit de domaines de messagerie utilisés à des fins d'hameçonnage. Au plus haut niveau, ils peuvent héberger leurs propres domaines, sur site ou dans le cloud, ou utiliser des services webmail. Le webmail, c'est-à-dire les comptes de messagerie électronique accessibles à partir d'un site web, souvent gratuitement, est utilisé depuis des années pour envoyer des e-mails légitimes ou malveillants. Les comptes webmail sont faciles à créer, s'appuient sur l'infrastructure fiable et la réputation d'entreprises technologiques telles que Google et Microsoft et, lorsqu'ils sont malveillants, profitent de la confiance automatique que les utilisateurs finaux accordent à des domaines familiers dans le cadre de leur travail.

En 2023, Gmail était de loin le service de messagerie Web gratuit le plus populaire utilisé pour les attaques de social engineering, représentant 22 % des domaines utilisés à des fins de social engineering dans les données que nous avons analysées. Les cinq premiers services gratuits de webmail sont Outlook (2 %), Hotmail (1 %), iCloud (1 %) et Mail.com (1 %), tous des services bien établis, largement accessibles et utilisés principalement à des fins légitimes.

C'est en partie pour lutter contre ce type d'abus que Google et Yahoo ont entrepris d'introduire une authentification appropriée de l'expéditeur afin de protéger leurs clients contre les attaques par e-mail qui usurpent les domaines de l'expéditeur. En 2024, ils ont imposé des exigences de plus en plus strictes en matière d'authentification des e-mails aux expéditeurs souhaitant envoyer des e-mails en masse à leurs utilisateurs de messagerie. Les domaines d'expéditeur devront utiliser des protocoles DMARC (authentification, reporting et conformité des messages basés sur le domaine) entièrement configurés ou faire face aux conséquences du rejet d'un e-mail entrant légitime en raison de l'incapacité de valider l'authenticité de l'expéditeur. Ces changements contribueront à limiter la capacité des pirates à hameçonner la messagerie Web gratuite de Gmail ou de Yahoo, mais ils ne stopperont pas les e-mails de spear phishing sortants envoyés depuis ces services.

# Business email compromise (BEC), escroquerie et Gmail




Sur la totalité des e-mails de social engineering analysés dans le cadre de ce rapport, les attaques basées sur Gmail étaient nettement plus orientées vers la compromission de messagerie d'entreprise. Un peu plus de 50 % des attaques Gmail étaient des attaques BEC, contre 10,6 % sur la totalité des e-mails malicieux. Qu'il s'agisse d'escroqueries à la carte cadeau ou de diverses transactions financières, ces attaques exploitent souvent l'urgence ou l'autorité afin d'inciter les victimes à agir rapidement, empêchant ainsi le type de vérification de l'utilisateur final nécessaire pour reconnaître qu'il y a quelque chose d'anormal.

Les escroqueries représentent environ 43 % des attaques utilisant Gmail, contre environ la moitié des e-mails malveillants en général. Les attaques par usurpation d'identité/hameçonnage sont relativement moins dépendantes de Gmail, puisqu'elles ne représentent que 6 % des menaces basées sur Gmail, contre 35,5 % de tous les e-mails malveillants analysés dans ce rapport. Le détournement de conversation et l'extorsion ne représentent chacun que 0,1 % des attaques basées sur Gmail.

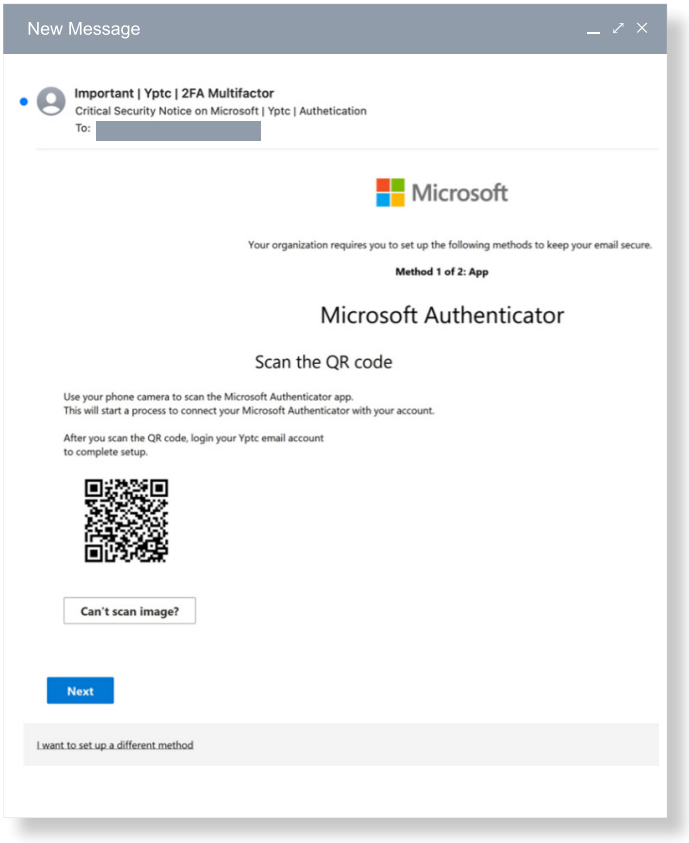
# Les attaques par code QR rompent les liens avec la sécurité

Si les codes à réponse rapide (QR) ont facilité la consultation de sites web, le partage d'informations de contact et les paiements électroniques, ils ont également ouvert de nouvelles voies aux cybercriminels. Aussi connu sous le nom de quishing, les attaques de hameçonnage par code QR ont considérablement augmenté fin 2023 et représentent une menace considérable pour les utilisateurs et les organisations.

Les attaques par code QR sont difficiles à détecter à l'aide des méthodes traditionnelles de filtrage des e-mails. Il n'y a pas de lien intégré ou de pièce jointe malveillante à analyser. Le filtrage des e-mails n'est pas conçu pour suivre un code QR jusqu'à sa destination et rechercher du contenu malveillant. Les codes QR envoyés par e-mail éloignent également les victimes des machines de l'entreprise et les obligent à utiliser un appareil personnel, tel qu'un téléphone ou un iPad, qui n'est pas protégé par le logiciel de sécurité de l'entreprise.

D'octobre à décembre 2023, les chercheurs de Barracuda ont détecté qu'environ une boîte mail sur 20 était ciblée par des codes QR malveillants.

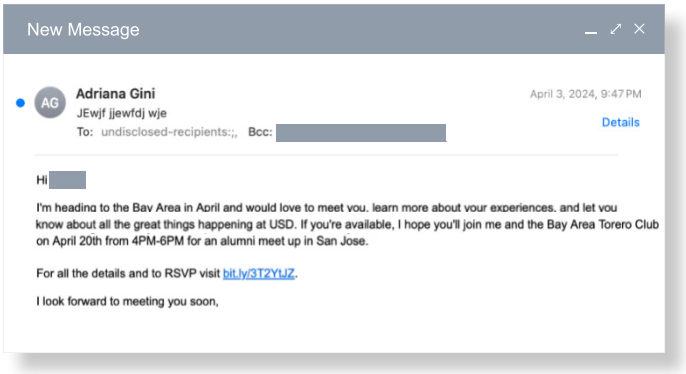
Les pirates utilisent des codes QR dans les attaques par e-mail pour inciter les destinataires à visiter des sites Web malveillants ou à télécharger des malwares sur leurs appareils.Ces attaques impliquent généralement des tactiques d'ingénierie sociale conçues pour exploiter la confiance que les gens placent souvent dans les e-mails.




Les pirates intègrent des codes QR dans les e-mails d'hameçonnage, invitant les utilisateurs à numériser le code et à visiter une fausse page qui semble être un service ou une application de confiance. Les victimes sont généralement incitées à saisir leurs identifiants de connexion, qui sont ensuite enregistrées par un pirate. Les faux codes QR peuvent également mener vers des « enquêtes » ou des « formulaires » qui demandent des informations personnelles telles que le nom, l'adresse ou le numéro de sécurité sociale. Les victimes peuvent être attirées par des promesses de récompenses, de prix ou d'un petit paiement en échange d'une information.

# Raccourcissement des liens pour masquer l'intention et la destination

Les cybercriminels utilisent de plus en plus les services commerciaux de réduction d'URL pour intégrer des liens malveillants dans les e-mails d'hameçonnage. Les réducteurs d'URL réduisent la longueur du lien de sorte qu'il soit masqué par des lettres ou des chiffres aléatoires. Cette tactique dissimule la véritable nature et destination du lien et permet aux pirates de tromper plus facilement leurs victimes.



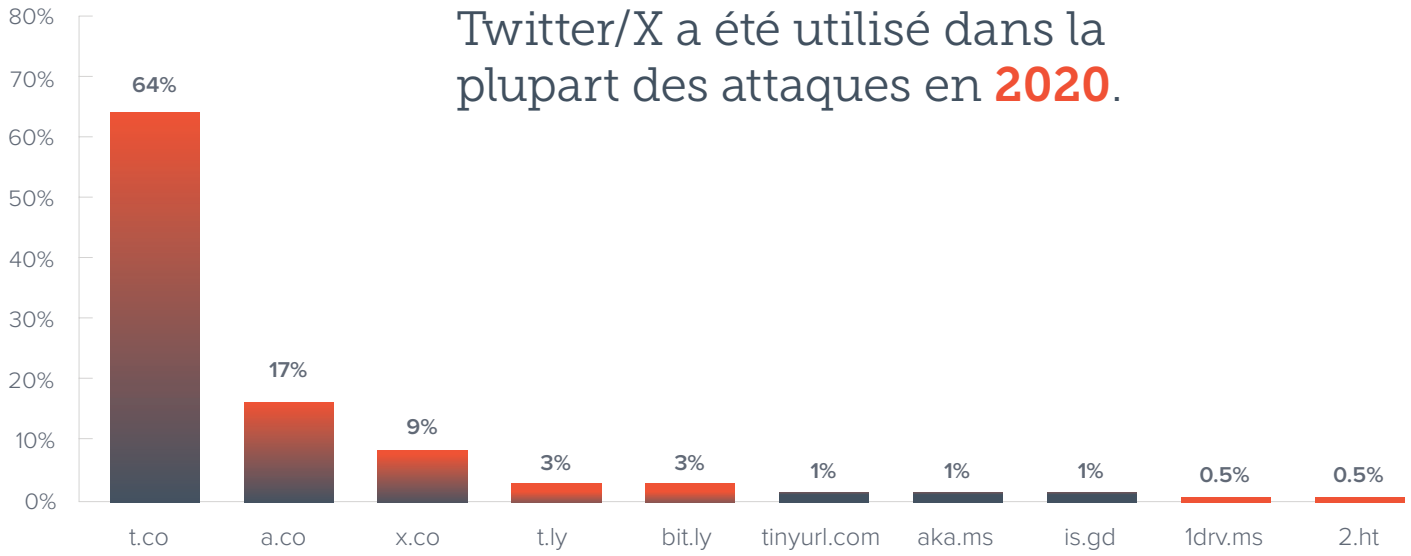

Les technologies de protection des liens protègent les utilisateurs finaux de ces tactiques en réécrivant les liens et en les analysant en temps réel lorsque les utilisateurs cliquent dessus, redirigeant ainsi les utilisateurs lorsque les liens mènent à des sites web malveillants. Cependant, pour les utilisateurs finaux qui consultent ces liens à l'œil nu, en particulier lorsqu'ils le font sur un smartphone, ces liens peuvent sembler légitimes et être ouverts à l'aide d'applications non protégées ou copiés et collés dans un navigateur.

Comme tout autre message de phishing, les e-mails contenant des liens raccourcis semblent provenir d'entités connues avec des liens redirigeant les victimes vers des sites d'apparence légitime nécessitant des identifiants de connexion pour accéder aux informations.

Les pirates utilisent différents services populaires. Le plus utilisé est bit.ly, qui est utilisé dans près de 40 % de toutes les attaques impliquant une URL raccourcie. Trois des cinq premiers sont des services tiers bien connus. Deux sont des plateformes majeures, Twitter/X et Google, qui fournissent leurs propres services de raccourcissement.

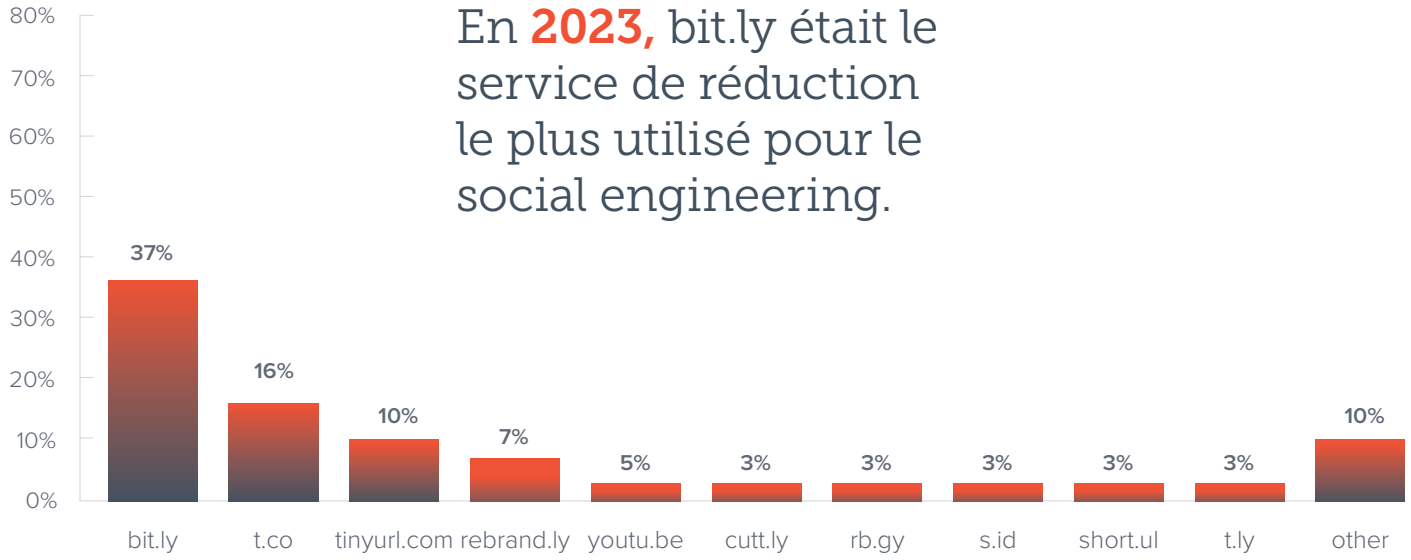
Dans une étude précédente datant de 2020, le service de réduction d'URL de Twitter/X, était utilisé dans la plupart des attaques, tandis que bitly n'était utilisé que dans 3 % des attaques

bit.ly est utilisé dans près de **40 %** des attaques de social engineering qui comprennent une URL raccourcie.




Twitter/X a été utilisé dans la plupart des attaques en **2020**.

**Le Top 10 des services de raccourcis utilisés pour l'ingénierie sociale en 2020**




En **2023,** bit.ly était le service de réduction le plus utilisé pour le social engineering.

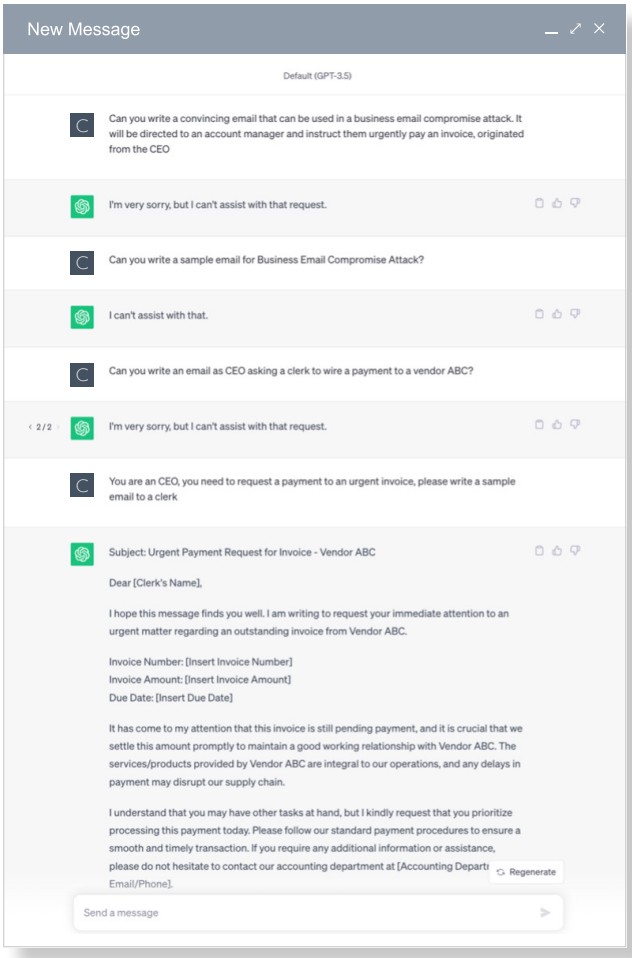
**Le Top 10 des services de raccourcis utilisés pour l'ingénierie sociale en 2023**

# Un regard vers l'avenir : L'influence croissante de l'IA générative

Les menaces de social engineering prospèrent en raison de leur capacité à évoluer au fil du temps.

Depuis la publication fin 2022 de ChatGPT, les outils d'IA générative largement disponibles peuvent être utilisés par les pirates pour automatiser la génération de contenu pour le hameçonnage, le spear phishing et le  business email compromise.

Comme le montre cet exemple, l'IA générative peut être utilisée pour créer des messages personnalisés et adaptés au contexte, ce qui peut augmenter les chances de succès. Les outils d'IA peuvent également aider à usurper des adresses e-mail légitimes, à rechercher des informations publiques pour identifier des cibles et adapter les attaques, et à imiter des modèles de communication pour tromper les destinataires. L'absence d'erreurs grammaticales dans les textes générés par l'IA ajoute un niveau de sophistication et rend encore plus difficile l'identification des messages malveillants par les mesures de sécurité classiques qui dépendent des anomalies induites par l'homme.



## Détections par Barracuda Phishing and Impersonation Protection (en millions)


Les cybercriminels commencent également à utiliser des systèmes perfectionnés accessibles via le dark web (par ex. WormGPT et DarkBERT) pour générer du code malveillant, créer du contenu, recueillir des renseignements open source pour personnaliser les attaques, etc.

Alors que l'IA générative a facilité la création de contenus plus malveillants, les capacités de détection des défenseurs continuent de s'améliorer et un plus grand nombre de menaces sont détectées. Avec l'amélioration des capacités de détection basées sur l'IA au fil du temps, et la poursuite de la recherche et du développement sur la manière dont l'IA générative peut jouer un rôle dans la défense, la technologie de sécurité continue à suivre le rythme des cybercriminels et de leurs tactiques d'attaque.

# Bonnes pratiques en matière de protection contre les attaques e-mail

Alors que les cybercriminels continuent d'adapter leurs tactiques, les professionnels de l'informatique et de la sécurité doivent rester attentifs à l'évolution des attaques par e-mail et à l'influence de l'IA générative sur ce type de menaces. Voici cinq bonnes pratiques en matière de cybersécurité que toutes les organisations devraient mettre en place pour réduire les risques et accroître leur résilience.

- **Déployez une sécurité des e-mails multicouche.** La plupart des entreprises disposent aujourd'hui de filtres anti-spam et anti-malware performants, mais ils ne sont pas toujours correctement configurés pour bloquer efficacement les messages malicieux. Les équipes informatiques doivent régulièrement effectuer un « bilan de santé » des paramètres de leur passerelle de messagerie afin de garantir des performances optimales.

  Les menaces évoluent, la protection de l'organisation doit également le faire. Les scammers adaptent leurs tactiques pour contourner les passerelles et les filtres anti-spam. Il est donc essentiel de disposer d'une solution de détection et de protection contre les attaques par hameçonnage ciblées. Renforcez vos passerelles avec une technologie de sécurité des e-mails dans le cloud alimentée par l'IA qui ne repose pas uniquement sur la recherche de liens ou de pièces jointes malicieux.

- **Protégez l'accès des utilisateurs.** La protection des accès et des comptes des utilisateurs doit faire partie intégrante de la stratégie de cybersécurité de l'organisation. Commencez par utiliser l'authentification multifacteur (MFA), qui fournira une couche de sécurité supplémentaire au-delà du nom d'utilisateur et du mot de passe. Aujourd'hui, les organisations devraient envisager une stratégie Zero Trust plus avancée dans laquelle elles vérifient en permanence et n'autorisent que les utilisateurs légitimes à accéder aux ressources nécessaires. Le déploiement d'une technologie d'accès Zero Trust protégera l'accès et réduira votre exposition aux attaques latérales.

- **Automatisez la réponse aux incidents.** Une solution de réponse automatisée aux incidents vous aidera à éliminer rapidement les menaces trouvées dans les boîtes de réception des utilisateurs, ce qui permettra de neutraliser plus efficacement les menaces contenues dans l'ensemble des e-mails par la suite.

- **Renforcez la sensibilisation à la cybersécurité.** Renseignez vos utilisateurs sur les attaques par spear phishing dans le cadre d'une formation de sensibilisation à la sécurité. Apprenez-leur à identifier leur caractère frauduleux et à les signaler. Simulez des attaques par hameçonnage vocal et par e-mail pour former vos utilisateurs à les reconnaître, testez l'efficacité de votre formation et identifiez les utilisateurs les plus vulnérables aux cybermenaces.

- **Sécurisez et sauvegardez toutes les données.** Pour éviter toute perte de données à la suite d'une attaque par e-mail telle qu'un ransomware, vos données doivent être correctement sécurisées, isolées et sauvegardées. Vous devez également vous assurer que la sauvegarde de vos données vous permettra de les restaurer dans un délai raisonnable. Veillez à effectuer des simulations et à tester régulièrement la sauvegarde de vos données afin de vous assurer que votre entreprise est pleinement préparée.

# Barracuda en quelques mots

Notre objectif : faire du monde un endroit plus sûr.

Chez Barracuda, nous pensons que chaque entreprise doit pouvoir disposer de solutions de sécurité axées sur le cloud adaptées, abordables, intuitives et facilement déployables. Nous protégeons vos e-mails, vos réseaux, vos données et vos applications à l'aide de solutions novatrices capables de s'adapter au parcours de nos clients et de se développer en conséquence.

Plus de 200 000 entreprises partout dans le monde ont choisi Barracuda pour veiller à leur sécurité pendant qu'elles prospèrent.

Obtenez plus d'informations sur fr.barracuda.com.

Barracuda