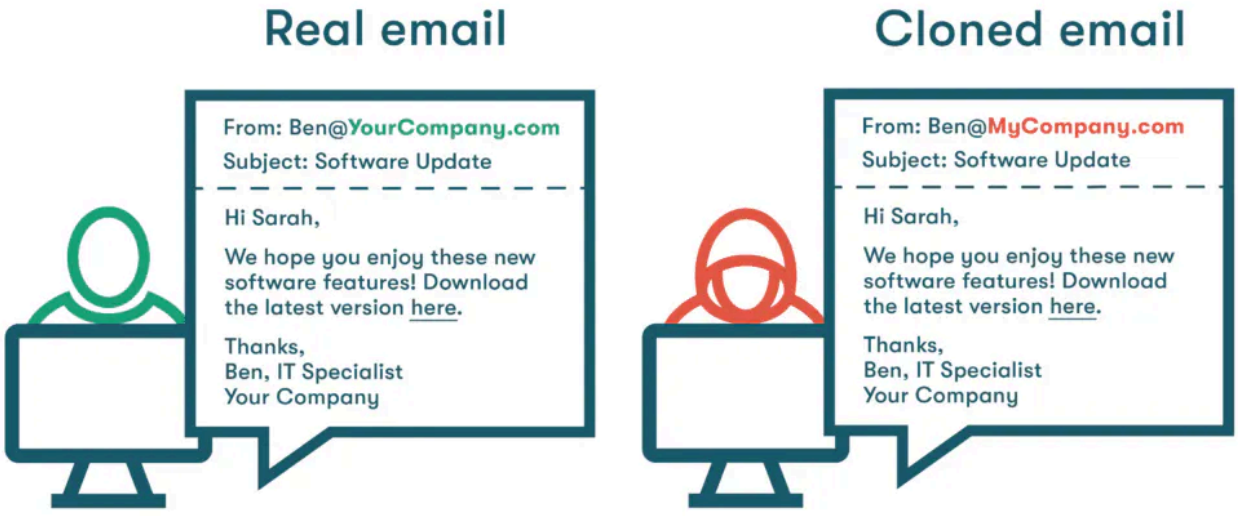
Qu’est-ce que le phishing par clone, voici des cas courants et conseils de sécurité

NDLR: le mot "phishing" signifie "hameçonnage"

Ils disent que l'imitation est la forme la plus sincère de la flatterie.
Le phishing par clone donne un nouveau sens à cet adage lorsque les cybercriminels répliquent de véritables courriels professionnels et personnels à des fins malveillantes.
Examinons de plus près quelques caractéristiques du phishing par clone et les stratégies de prévention.

Qu’est-ce que le phishing par clonage ?

Le phishing est une tactique d'ingénierie sociale courante qui utilise des courriels semblant provenir d'un expéditeur de confiance pour inciter les destinataires à fournir des informations personnelles ou à cliquer sur des liens dangereux.
Une **attaque de phishing par clonage** fait passer cette méthode au niveau supérieur en utilisant des répliques de courriels légitimes pour accroître la crédibilité.
Cette attention aux détails peut rendre les courriels de phishing clones difficiles à repérer.



Phishing par clone et phishing par harponnage

Le spear phishing est un type d’attaque de phishing qui profile des cibles spécifiques. Les pirates effectuent des recherches supplémentaires pour les aider à personnaliser le contenu des messages.
Les attaques baleinières vont encore plus loin en ciblant uniquement les cadres supérieurs.
Les tactiques de phishing par clonage peuvent être utilisées à la fois pour les attaques de spear phishing et de

chasse à la baleine, car la copie d'un format de courriel officiel aide à convaincre la cible que le courriel et l'expéditeur sont honnêtes.

Exemples de phishing par clone

Étant donné que le phishing par clonage permet de faire passer les courriels malveillants à travers nos défenses, les attaques sont de plus en plus courantes et diversifiées.
Voici quelques exemples dangereux de phishing par clone que vous avez peut-être déjà rencontré :

- **Courriels bancaires répliqués :** en utilisant un format de courriel bancaire réaliste et une signature comme modèle, les pirates informatiques envoient des courriels semblant provenir de votre banque pour accéder aux informations de votre compte financier ou à vos identifiants de connexion.
  Un faux courriel bancaire peut inclure un faux lien vers un remboursement ou une demande de mise à jour de vos informations d'identification.
  Gardez à l'esprit que votre banque ne vous demandera jamais de divulguer des informations personnelles ou des numéros de compte par courrier électronique.
- **Courriels en double provenant du service informatique :** les pirates se rendent compte que de nombreux destinataires de courriels sont susceptibles de faire confiance à n'importe quel message de leur service informatique et de suivre les instructions qu'ils incluent, comme l'installation ou la mise à jour d'un logiciel.
  Une attaque de phishing par clonage peut utiliser comme modèle d'un courriel informatique précédemment envoyé à quelqu'un d'autre, puis ajouter un lien vers un site Web malveillant ou un logiciel malveillant à la place du lien logiciel d'origine.
- **Courriels imités provenant de services de streaming :** les comptes tels que les services de streaming sont si courants qu'ils permettent aux attaquants de trouver facilement des exemples de messages électroniques légitimes, puis d'y ajouter leur propre version malveillante.
  Une tactique courante consiste à informer un destinataire de l'échec de son mode de paiement et à lui demander de saisir à nouveau les informations de sa carte ou de son compte bancaire.

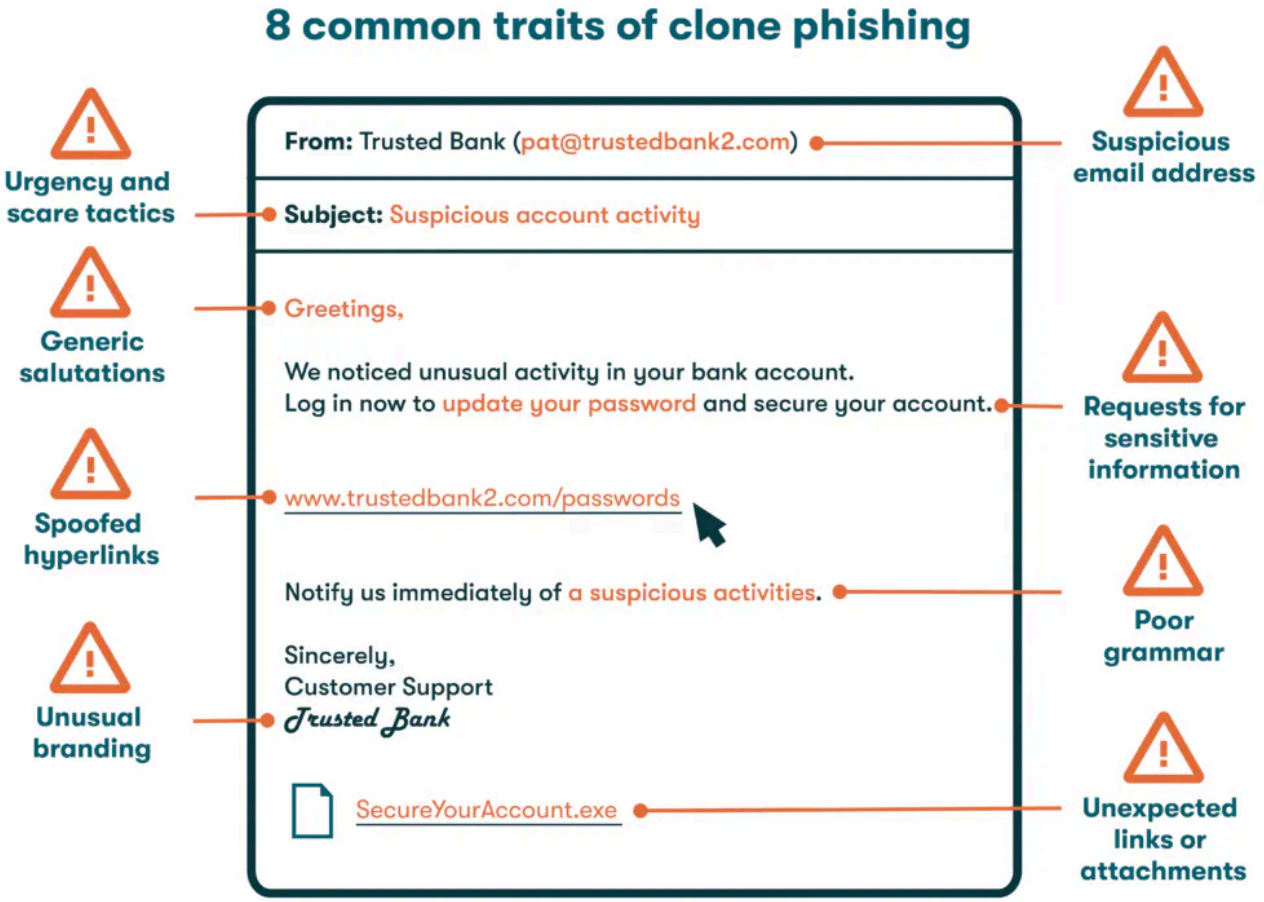
8 caractéristiques communes d'un courriel de phishing cloné

Les courriels de phishing par clonage sont dangereux car ils sont plus difficiles à identifier qu'une escroquerie de phishing traditionnelle.
Il existe néanmoins certains traits communs que vous pouvez rechercher pour renforcer votre sécurité et réduire l'impact du phishing par clonage :

1. **Adresse courriel suspecte.** Examinez attentivement l' adresse e-mail de l'expéditeur , car c'est une chose que les pirates ne peuvent pas cloner.
   La présence de caractères supplémentaires ou manquants peut être un signal d'alarme, alors recherchez toujours l'expéditeur ou supprimez simplement le message en cas de doute.
   Vous pouvez également contacter directement l'expéditeur ou comparer le site Web réel de l'entreprise avec le nom de domaine figurant dans le courriel de l'expéditeur pour voir s'il y a des divergences.
2. **Liens hypertextes usurpés.** Les pirates peuvent utiliser un formatage ou des boutons radio pour masquer l'adresse réelle du lien hypertexte.

Survolez donc toujours n'importe quel lien pour vérifier l'URL complète avant de cliquer dessus, même si vous pensez que le courriel est légitime.
Un lien hypertexte usurpé peut ressembler beaucoup à l'adresse réelle, avec seulement des changements subtils, comme des 0 à la place des O, qui sont faciles à manquer.

3. **Liens ou pièces jointes inattendus.** La plupart des courriels que vous recevez d'amis, de collègues ou d'entreprises ne contiennent que des pièces jointes en réponse à quelque chose que vous aviez demandé ou dont vous aviez connaissance à l'avance.
   Si vous recevez un courriel contenant un lien ou une pièce jointe dont vous n'avez pas besoin ou que vous n'attendiez pas, il est préférable de s'abstenir d'ouvrir ou de télécharger le fichier .
4. **Demandes d'informations sensibles.** Une demande d'informations sensibles ou personnelles est une caractéristique partagée par tous les types de courriels de phishing.
   La plupart des entreprises réputées ne vous demanderont jamais d'informations telles que des informations d'identification ou des numéros de compte dans un courriel.
   Ne répondez pas aux questions contenues dans un courriel avant d'avoir vérifié la légitimité de l'expéditeur.
5. **Urgence et tactiques alarmistes.** Les courriels de phishing captent notre attention en transmettant un sentiment d'urgence inhabituel, en menaçant de conséquences désastreuses si nous ne répondons pas ou en présentant des offres qui semblent trop belles pour être vraies (et le sont toujours).
   Tous les courriels de phishing utilisent ces stratégies, y compris les courriels de phishing clonés.
6. **Salutations génériques.** Quelqu'un tentant de vous joindre au sujet d'une question urgente commencerait-il son message en disant « Cher Monsieur ou Madame » ou simplement « Bonjour » ? Probablement pas.
   Ces salutations génériques se retrouvent souvent dans les spams ou les campagnes marketing ciblées.
   Si un expéditeur d'un courriel ne connaît pas votre nom, il ne devrait certainement pas être autorisé à savoir quoi que ce soit d'autre sur vous, alors ne répondez pas.
7. **Mauvaise grammaire.** Une mauvaise orthographe et une mauvaise grammaire ont toujours été la marque des courriels de phishing.
   Les courriels clonés sont moins sujets à ces erreurs, car ils sont copiés à partir de messages réels, mais les sections nouvellement ajoutées peuvent toujours présenter ces défauts.
   Les outils d'intelligence artificielle (IA) générative commencent à permettre aux cybercriminels de rédiger plus facilement des courriels de phishing sur un ton plus professionnel.
8. **Une marque inhabituelle.** En clonant un courriel, les pirates tentent de faire en sorte que le logo, l'arrière-plan, la police et le format ressemblent à l'objet réel, mais ils échouent parfois.
   Si des détails tels que la taille du logo ou la palette de couleurs semblent erronés, il se peut que l'entreprise ait mis à jour son image de marque, mais cela peut également indiquer un faux.
   Examinez attentivement l'URL et les autres informations si l'apparence de l'e-mail est incohérente.



7 conseils de sécurité pour prévenir les attaques de phishing par clonage

Les outils avancés de cybersécurité peuvent minimiser le risque de sécurité du clonage. Les tactiques d'ingénierie sociale comme le phishing qui reposent sur la nature humaine et l'erreur humaine peuvent également être évitées grâce à une formation et une sensibilisation continues.

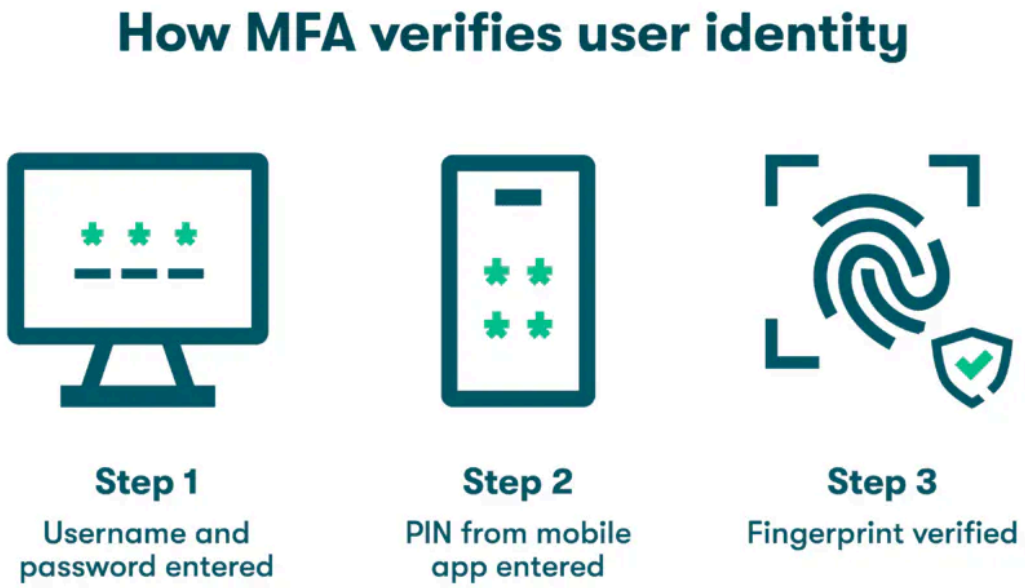
Pour les entreprises :

- **Favoriser une culture de sécurité :** les entreprises peuvent établir une culture de sécurité en partageant les objectifs et les statuts de haut en bas et en aidant chaque employé à comprendre l'impact de ses propres actions sur la posture de sécurité globale de l'entreprise.
  Une solide culture de sécurité peut prévenir les attaques de phishing par clonage en encourageant la communication bidirectionnelle avec les équipes informatiques et en signalant en temps opportun les courriels suspects.
- **Créez un programme de formation en cybersécurité :** la formation contribue à la culture de sécurité en apprenant aux employés ce qu'il faut rechercher et comment réagir aux signes d'avertissement.
  Des tactiques de piratage insaisissables telles que le phishing par clonage sont l'une des raisons pour lesquelles le marché mondial de la formation à la sensibilisation à la sécurité croît de 15 % chaque année
  .

- **Exécutez des campagnes de phishing simulées :** de nombreuses entreprises font appel à des pirates informatiques et à d'autres experts en phishing pour développer des campagnes de phishing simulées. Ces programmes à long terme utilisent des exemples réalistes de courriels de phishing envoyés aux employés pour tester leur jugement et leur sensibilisation.
  Si un employé répond par erreur à un courriel test de phishing, cela devient l'occasion de l'informer des signes de danger qu'il a manqués.
- **Déployez des outils de sécurité de messagerie :** les outils de sécurité de messagerie, notamment des pare-feu et des logiciels de sécurité de messagerie, analysent les messages entrants et le trafic en fonction de critères prédéfinis.
  De nombreux services de messagerie destinés aux entreprises incluent des filtres de messagerie configurables qui empêchent les courriels de phishing d'atteindre les utilisateurs.
  Les logiciels antivirus et anti-malware prennent en charge ces outils en identifiant et en éliminant les logiciels malveillants qui se propagent fréquemment via des attaques de phishing.

Pour tout le monde:

- **Utilisez un gestionnaire d'informations d'identification :** un gestionnaire d'informations d'identification réduit l'impact du phishing par clonage en créant des mots de passe forts et complexes qui ne sont jamais stockés ou partagés dans un format non chiffré.
  Si l'attaque de phishing inclut une URL usurpée, les meilleurs gestionnaires d'informations d'identification vous empêchent de remplir automatiquement vos informations d'identification sans le savoir lorsque l'URL ne correspond pas à l'adresse du site Web vérifiée.
- **Gardez les logiciels à jour :** la gestion des correctifs et les mises à jour logicielles permettent de garantir que les vulnérabilités du système sont corrigées rapidement afin de réduire l'efficacité du phishing et d'autres tactiques de piratage.
  Les navigateurs Web doivent également être tenus à jour afin que des fonctionnalités telles que la validation des certificats et les bloqueurs de pop-up puissent minimiser efficacement l'impact d'une attaque de phishing.
- **Activez l'authentification multifacteur :** l'authentification multifacteur (MFA) utilise des facteurs supplémentaires tels que les codes envoyés via une application, les analyses d'empreintes digitales ou les clés d'accès pour vérifier l'identité de l'utilisateur.
  Bien que la MFA n'empêche pas un courriel de phishing d'atteindre votre boîte de réception, les couches de sécurité supplémentaires rendent plus difficile l'accès aux comptes pour les pirates s'ils parviennent à voler les informations d'identification via une attaque de phishing par clonage.



Comment Dashlane contribue à atténuer le phishing par clonage

Pour lutter contre le phishing par clonage et autres menaces persistantes, Dashlane propose une génération simple de mots de passe, un stockage et un partage sécurisés, un cryptage AES-256 et une saisie automatique personnalisable qui vous empêche automatiquement de vous connecter à des sites Web non sécurisés.
Un score de santé des mots de passe suit vos mots de passe faibles, réutilisés et compromis pour vous protéger du piratage, tandis que notre surveillance du Dark Web analyse les profondeurs d'Internet à la recherche de vos informations d'identification et vous alerte si elles sont trouvées sur le Dark Web.
Notre architecture brevetée sans connaissance garantit que personne d'autre (pas même Dashlane) ne peut accéder à vos données non chiffrées.

Ne laissez pas le jargon de la cybersécurité entraver la protection de votre organisation. Nous décomposons les termes fondamentaux, le jargon et les acronymes dans notre Guide essentiel des termes courants en matière de cybersécurité .

Les références

1. Dashlane, « Qu'est-ce que le phishing ? » Mars 2020.
2. Mimecast, « Qu'est-ce qu'une attaque de phishing à la baleine ? » 2023.
3. Association des banquiers canadiens, « Ce courriel semble-t-il frauduleux? Découvrez des exemples des derniers e-mails frauduleux », juillet 2023.
4. Dashlane, « Qu'est-ce qu'un malware ? » Février 2020.
5. Dashlane, « Comment détecter une arnaque par phishing », novembre 2019.
6. Dashlane, « Meilleures pratiques de sécurité des e-mails pour protéger votre entreprise », août 2023.
7. Microsoft, « Protégez-vous du phishing », 2023.
8. Dashlane, « Pourquoi Dashlane ne vous demandera jamais d'informations d'identification dans un e-mail (car c'est ainsi que fonctionne le phishing) », novembre 2021.

9. Dashlane, « Strange Security : Que savoir sur l'IA générative et la cybersécurité », juin 2023.
10. Dashlane, « Comment créer une culture de sécurité », mars 2022.
11. Cybercrime Magazine, « Almanach de la cybersécurité 2023 : 100 faits, chiffres, prévisions et statistiques », mai 2023.
12. Dashlane, « Entretien avec un hacker : Rachel Tobac vous explique comment vous défendre contre… enfin, elle ! » Mars 2021.
13. NIST, « Phishing », 2023.
14. Dashlane, « Ces nouvelles alertes vous avertissent en cas d'hameçonnage », septembre 2023.
15. Dashlane, « Un guide complet de l'authentification multifacteur », octobre 2023.
16. Dashlane, « Qu'est-ce qu'un mot de passe et comment fonctionnent les mots de passe ? » Février 2024.
17. Dashlane, « Un aperçu des scores de santé des mots de passe dans le monde en 2022 », 2022.
18. Dashlane, « Surveillance du Dark Web : vos employés utilisent probablement des mots de passe compromis », juillet 2022.
19. Dashlane, « La sécurité avant tout : comment Dashlane protège vos données », octobre 2023.
20. Dashlane, « Guide essentiel des termes courants en matière de cybersécurité », 2023.

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20240430
"C'est ensemble qu'on avance"