Groupe de travail sur la coopération internationale en matière d'application de la loi

Sensibilisation au bourrage d'identifiants, v. 1, 30 mars 2022

Organismes membres du sous-groupe de travail sur le bourrage d'identifiants :

- Commissariat à la protection de la vie privée du Canada
- Autorité de réglementation de Gibraltar
- Commissariat à l'information de Jersey
- Préposé fédéral suisse à la protection des données et à la transparence
- Autorité de protection des données de Turquie
- Commissariat à l'information du Royaume-Uni

Table des matières

Sommaire

Le Groupe de travail sur la coopération internationale en matière d'application de la loi est un groupe de travail permanent de l'Assemblée mondiale pour la protection de la vie privée (AMVP), coprésidée par le Commissariat à la protection de la vie privée du Canada; le Commissariat à la protection des données personnelles de Hong Kong, Chine; la Surintendance de l'industrie et du commerce de Colombie et l'Autorité norvégienne de protection des données.

Les travaux du Groupe de travail font partie intégrante de l'Assemblée dans sa mission de promotion du respect de la vie privée à titre de chef de file mondial en la matière et de la coopération mondiale à cet effet à l'ère numérique. En particulier, le Groupe de travail a la responsabilité première de diriger la mise en œuvre des actions relevant du pilier de coopération en matière de réglementation et de mise en application du plan stratégique 2021-2023 de l'AMVP (en anglais seulement).

Le Groupe de travail a établi que la situation entourant le bourrage d'identifiants devenait préoccupante lors d'une séance d'étude à huis clos[1] en mars 2021. En conséquence, il a été déterminé qu'un suivi était nécessaire, et donc un sous-groupe de travail a été formé, celui-ci ayant comme mission de se pencher sur le dossier et de produire des documents visant à aider les autorités à faire face à la menace croissante du bourrage d'identifiants.

Le présent document décrit la menace que représente le bourrage d'identifiants pour les données personnelles et fournit des conseils au grand public sur les moyens de se protéger contre les risques associés.

C'est en même temps une reconnaissance de la menace mondiale que représente le bourrage d'identifiants pour les données personnelles. L'utilisation qu'en feront les autorités dépendra d'un cas à l'autre. Par exemple, les lignes directrices peuvent servir de point de référence pour les autorités dans une optique de diffusion des connaissances; aider les autorités lorsqu'elles cherchent à publier des lignes directrices, des avertissements ou des avis sur le bourrage d'identifiants et aider les autorités à informer le grand public de la façon dont il peut se protéger contre les risques de telles attaques.

[1] Lors de ses séances d'étude à huis clos, le Groupe de travail cerne et examine des enjeux ou des organisations d'importance qui ont des retombées mondiales en matière de protection des données et de droits à la vie privée des personnes. Ces séances constituent des plateformes pour favoriser une coopération concrète en matière d'application de la loi. En général, ces séances commencent par une présentation sur un sujet, suivie d'une discussion ouverte sur les motifs de préoccupation qui y sont associés, les stratégies de réglementation possibles et les options de coopération.

Remerciements

Beaucoup de publications d'une variété d'organisations ont servi à la rédaction du présent guide, qui les intègre lorsque la chose est pertinente. Nous dressons ci-dessous la liste des documents que nous avons utilisés et auxquels nous faisons référence. Des références sont également incluses dans le document.

Outre les documents mentionnés ci-dessous, les présentes lignes directrices intègrent également le fruit de consultations et de contributions d'experts dans le domaine de la cybersécurité[2], à savoir :

- Membres du groupe de référence de l'Assemblée mondiale pour la protection de la vie privée :
    - Bojana Bellamy, Centre for information Policy Leadership (avec la participation de Lisa Sotto, Hunton Andrews Kurth)
    - Clarisse Girot, Asian Business Law Institute (avec la participation de James McLeary, Kroll, et Rajesh Sreenivasan, Rajah & Tann LLP)
- Centre national de cybersécurité du Royaume-Uni
- Open Web Application Security Project – Shuman Ghosemajumder, F5

Agence de cybersécurité et d'infrastructures des États-Unis

« Security Tip (ST05-012) Supplementing passwords »
https://us-cert.cisa.gov/ncas/tips/ST05-012

Agence de l'Union européenne pour la cybersécurité

« Authentication Methods »
https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/authentication-methods

« How to Avoid SIM-Swapping – Leaflet »
https://www.enisa.europa.eu/publications/how-to-avoid-sim-swapping-leaflet

Akamai

Akamai, *[State of the Internet]/security credential stuffing: attacks and economies* (vol. 5 | 2019)

Akamai, *[State of the Internet]/security web attacks and gaming abuse* (vol. 5, nº 3 | 2019)

Akamai, *[State of the Internet] phishing for finance* (vol. 7, nº 2 | 2021)

[2] L'approche collaborative adoptée a permis au groupe de travail de bénéficier de l'expérience et du savoir-faire de spécialistes qui ont enrichi les travaux effectués. Les consultations et collaborations externes contribuent également à donner une voix et de l'influence à l'AMPV, conformément à sa priorité stratégique 2.

Autorité norvégienne de sécurité nationale

« Passordanbefalinger fra Nasjonal sikkerhetsmyndighet » [Password Recommendations]
https://nsm.no/aktuelt/passordanbefalinger-fra-nasjonal-sikkerhetsmyndighet

Centre canadien pour la cybersécurité

« Conseils de sécurité sur les gestionnaires de mots de passe (ITSAP.30.025) »
https://cyber.gc.ca/fr/orientation/conseils-de-securite-sur-les-gestionnaires-de-mots-de-passeitsap30025

« Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032) »
https://cyber.gc.ca/fr/orientation/pratiques-exemplaires-de-creation-de-phrases-de-passe-et-de-mots-de-passeitsap30032

« Repensez vos habitudes en regard de vos mots de passe de manière à protéger vos comptes des pirates informatiques (ITSAP.30.036) »
https://cyber.gc.ca/fr/orientation/repensez-vos-habitudes-en-regard-de-vos-mots-de-passe-de-maniere-proteger-vos-comptes

« Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030) »
https://cyber.gc.ca/fr/orientation/securisez-vos-comptes-et-vos-appareils-avec-une-authentification-multifacteur

Centre national pour la cybersécurité du Royaume-Uni

« Cyber Aware »
https://www.ncsc.gov.uk/cyberaware/home#action-1

« Most hacked passwords revealed »
https://www.ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security

« Paws-word change recommended on National Pet Day »
https://www.ncsc.gov.uk/news/national-pet-day-password-advice

« Recovering a hacked account »
https://www.ncsc.gov.uk/guidance/recovering-a-hacked-account

« Setting up two-factor authentication (2FA) »
https://www.ncsc.gov.uk/guidance/setting-two-factor-authentication-2fa

« Three random words or #thinkrandom »
https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0

« Top tips for staying secure online »
https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/activate-two-factor-authentication-on-your-email

« Top tips for staying secure online »
https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers

« Top tips for staying secure online »
https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/use-a-strong-and-separate-password-for-email

« Use of credential stuffing tools »
https://www.ncsc.gov.uk/news/use-credential-stuffing-tools

« Using passwords to protect your devices and data »
https://www.ncsc.gov.uk/information/infographics-ncs

Commissariat à l'information du Royaume-Uni

« Passwords in online services »
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/passwords-in-online-services/

F5

« 2021 Credential Stuffing Report »
https://www.f5.com/labs/articles/threat-intelligence/2021-credential-stuffing-report

Federal Bureau of Investigation (FBI) des États-Unis

« Scams and safety: Business email compromise »
https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise

Institut national des normes et des technologies des États-Unis

« Special Publication 800-63-3 Digital Identity Guidelines: 4.3.1 Authenticators »
https://pages.nist.gov/800-63-3/sp800-63-3.html#431-authenticators

International Business Machines Corporation

« IBM Survey : Pandemic-Induced Digital Reliance Creates Lingering Security Side Effects »
https://newsroom.ibm.com/2021-06-15-IBM-Survey-Pandemic-Induced-Digital-Reliance-Creates-Lingering-Security-Side-Effects

Microsoft

« Your Pa$$word doesn't matter »
https://techcommunity.microsoft.com/t5/azure-active-directory-identity/your-pa-word-doesn-t-matter/ba-p/731984

Open Web Security Project Foundation

« Credential stuffing »
https://owasp.org/www-community/attacks/Credential_stuffing

Ponemon Institute

Ponemon Institute, *The cost of credential stuffing* (oct. 2017)

Shape Security

Shape Security, *The 2018 credential spill report* (2018)

Shape Security, *Attacker economics* (2020)

Verizon

« 2021 data breach investigations report »
https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf

Résumé du guide

- Les attaques par bourrage d'identifiants profitent de la tendance d'une personne à réutiliser les mêmes justificatifs d'identité (c'est-à-dire le nom d'utilisateur et le mot de passe) pour plusieurs comptes.

- Les mots de passe ne doivent **pas être réutilisés** pour plusieurs comptes. Un mot de passe **unique** et fort doit être créé pour chaque compte, application et service en ligne.

- Il ne faut pas utiliser de mots de passe courts.

- Les **utilisateurs ne doivent pas utiliser de mots de passe prévisibles**, comme ceux basés sur des informations personnelles, par exemple un anniversaire ou le nom d'un animal de compagnie.

- Les utilisateurs devraient envisager d'utiliser la technique des **trois mots aléatoires** pour créer des mots de passe forts et faciles à retenir.

- Envisagez d'utiliser un **gestionnaire de mots de passe** pour vous aider à stocker et à utiliser des mots de passe distincts en toute sécurité.

- L'**authentification multifactorielle** doit être utilisée dans la mesure du possible.

- Si un compte en ligne a été compromis, le titulaire du compte doit changer **immédiatement** son mot de passe ainsi que celui de tout autre compte protégé par le même mot de passe ou un mot de passe similaire.

- Les **utilisateurs doivent vérifier régulièrement les informations relatives à leurs comptes** pour détecter toute activité inhabituelle ou toute transaction non autorisée, en particulier si un compte a été compromis ou est suspecté de l'avoir été.

- Il faut communiquer avec l'institution financière concernée si une carte ou d'autres informations financières liées à un compte ont été compromises ou sont soupçonnées de l'avoir été.

- Les **utilisateurs doivent communiquer avec l'organisation concernée** si un compte a été verrouillé par un pirate.

- Les **appareils doivent être mis à jour et rustinés régulièrement** de manière à ce que les plus récents logiciels de sécurité soient installés.

1. Introduction

Une attaque par bourrage d'identifiants est une méthode de cyberattaque qui exploite la tendance d'une personne à utiliser les mêmes justificatifs (une même combinaison de nom d'utilisateur ou de courriel et de mot de passe, par exemple) sur de multiples plateformes en ligne. Les attaques sont automatisées et souvent à grande échelle et font appel à des justificatifs volés (à la suite de fuites et de ventes sur le Web clandestin) pour accéder illégalement aux comptes des utilisateurs sur d'autres sites Web.

Les attaques par bourrage d'identifiants peuvent entraîner des pertes financières, car les pirates peuvent, par exemple, effectuer des achats en utilisant le compte compromis ou transférer des fonds sur leur propre compte. Les attaques peuvent également servir à causer des dégâts immatériels, notamment l'atteinte à la réputation par la diffusion de renseignements personnels sensibles ou de fausses informations ou de fausses déclarations sur une personne à partir du compte compromis.

La réutilisation des mots de passe peut augmenter l'efficacité des attaques par bourrage d'identifiants et représente une excellente porte d'entrée pour une attaque envers une organisation, même lorsque des niveaux élevés de cybersécurité ont été mis en œuvre.

La question de la sécurité des mots de passe a pris de l'ampleur après que la pandémie de COVID-19 a entraîné des changements soudains dans notre vie professionnelle et personnelle et un passage jamais vu vers les services en ligne. Rien qu'au Royaume-Uni, 27 % de la population ont créé au moins quatre nouveaux comptes protégés par un mot de passe et 6 % ont déclaré avoir ouvert plus de dix nouveaux comptes au cours des 12 mois précédents[3]. En outre, une enquête mondiale a également révélé que les gens ont créé 15 nouveaux comptes en moyenne pendant la pandémie de COVID-19 (ce qui équivaut à des milliards de nouveaux comptes créés dans le monde), et 44 % de ces personnes ont déclaré qu'ils ne prévoient pas supprimer ou désactiver ces nouveaux comptes[4]. En outre, il a été signalé que plus de la moitié des personnes de la génération Y interrogés préfèrent passer une commande sur une application ou un site Web plutôt que par téléphone ou en personne[5].

Notre dépendance envers les services numériques ne montre aucun signe de ralentissement, pas plus que les méthodes d'exploitation et les moyens utilisés par les cybercriminels pour mener des attaques sur ces services, semble-t-il. Selon des rapports émanant des secteurs public et privé, le bourrage d'identifiants gagne du terrain et menace les données personnelles à l'échelle mondiale[6].

Par les présentes lignes directrices, le Groupe de travail officialise la menace que représente le bourrage d'identifiants pour les données personnelles. Les autorités peuvent s'en servir pour informer les citoyens des risques que représente le bourrage d'identifiants et les conseiller sur la manière dont ils peuvent se protéger contre ces risques.

---

[3] Centre national de cybersécurité du Royaume-Uni, « Paws-word change recommended on National Pet Day », https://www.ncsc.gov.uk/news/national-pet-day-password-advice, consulté le 27 mai 2021.

[4] International Business Machines Corporation (IBM), « IBM Survey : Pandemic-Induced Digital Reliance Creates Lingering Security Side Effects », https://newsroom.ibm.com/2021-06-15-IBM-Survey-Pandemic-Induced-Digital-Reliance-Creates-Lingering-Security-Side-Effects, consulté le 29 juillet 2021.

[5] *Ibid.*

[6] Akamai, *[State of the Internet]/security credential stuffing: attacks and economies* (vol. 5 | 2019).

2. Qu'est-ce que le bourrage d'identifiants?

Une **attaque par bourrage d'identifiants** consiste à obtenir frauduleusement des justificatifs d'identité valides (combinaisons de nom d'utilisateur ou courriel et mot de passe, par exemple) en se basant sur les justificatifs de comptes compromis, qui sont saisis automatiquement en masse dans les pages d'ouverture de session de sites jusqu'à ce qu'une correspondance soit trouvée.

Voici les étapes typiques d'une attaque par bourrage d'identifiants, illustrée à la figure 1.

(a) Obtenir des justificatifs d'identité valides : Les justificatifs d'identité légitimes qui ont déjà fait l'objet de violations[7] sont rendus accessibles, par exemple sur le Web clandestin. Les cybercriminels achètent souvent de grandes quantités de ces justificatifs et tentent d'accéder illégalement à des comptes d'utilisateurs sur des sites Web non liés.

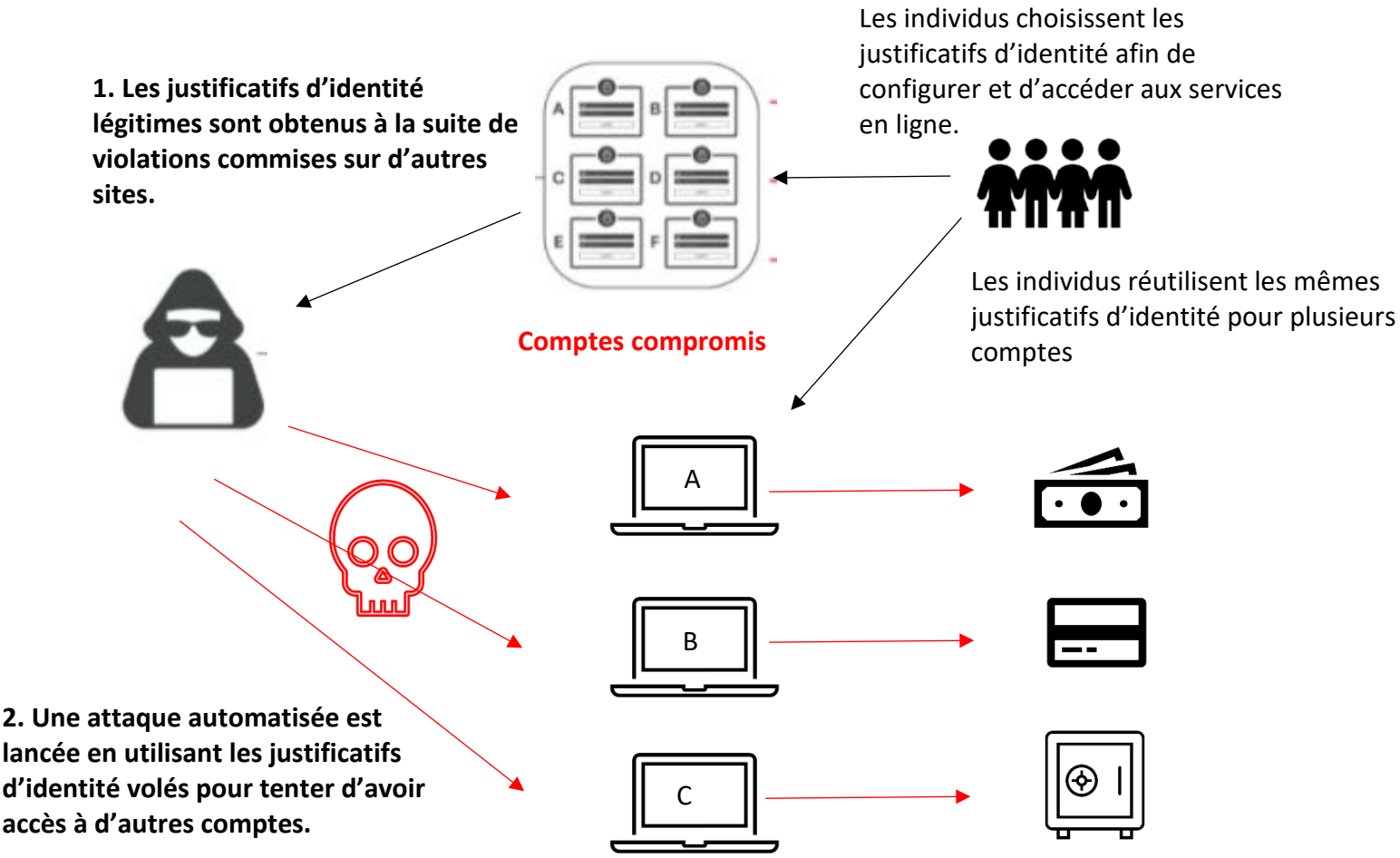
(b) Lancer l'attaque : Pour lancer une attaque par bourrage d'identifiants, des outils généralement automatisés, tels que les botnets (groupes de bots Internet codés avec des logiciels malveillants pour obéir aux commandes des pirates) et les outils de vérification de compte, sont utilisés pour entrer automatiquement les justificatifs dans les champs correspondants d'autres sites Web[8].

(c) Prendre le contrôle : L'outil de vérification de comptes testera tous les justificatifs d'identité disponibles et informera le pirate des correspondances trouvées. Le pirate pourra ainsi prendre le contrôle du compte et, par exemple, vider le compte de tout crédit stocké, effectuer des achats frauduleux, copier les informations du compte bancaire ou accéder à toute donnée personnelle ou autre disponible.

[7] Il y a violation de données lorsque des informations détenues par une organisation sont volées ou consultées sans autorisation.

[8] Centre canadien pour la cybersécurité, « Repensez vos habitudes en regard de vos mots de passe de manière à protéger vos comptes des pirates informatiques (ITSAP.30.036) », https://cyber.gc.ca/en/guidance/rethink-your-password-habits-protect-your-accounts-hackers-itsap30036, consulté le 27 mai 2021.

Figure 1 :


1. Les justificatifs d'identité légitimes sont obtenus à la suite de violations commises sur d'autres sites.
Les individus choisissent les justificatifs d'identité afin de configurer et d'accéder aux services en ligne.
Comptes compromis
Les individus réutilisent les mêmes justificatifs d'identité pour plusieurs comptes
A
B
C
2. Une attaque automatisée est lancée en utilisant les justificatifs d'identité volés pour tenter d'avoir accès à d'autres comptes.
3. Le pirate informatique prend le contrôle du compte afin de mener des activités illicites. Il peut notamment effectuer des achats frauduleux, vider le compte de tout crédit stocké et extraire tous les renseignements personnels figurant dans le compte.

3. Quels sont les risques du bourrage d'identifiants?

Après avoir réussi à accéder à un compte, un pirate peut utiliser les informations qu'il contient pour causer des préjudices **matériels** et **immatériels** à des personnes.

(a) Quelques exemples de préjudices matériels :

- Perte financière, car les pirates peuvent effectuer des achats en utilisant le compte compromis, voler les informations relatives à la carte de crédit/au compte bancaire associé ou transférer des fonds ou des points de fidélité accumulés sur leur propre compte[9].

- Les pirates peuvent également tenter de tirer profit de leurs gains en vendant ou en publiant en ligne les justificatifs d'identité validés ainsi que toutes les données personnelles recueillies sur le compte, les mettant à la disposition d'autres criminels qui peuvent ensuite commettre des fraudes, des vols d'identité ou mener d'autres activités malveillantes[10].

(b) Quelques exemples de préjudices immatériels :

- Détresse émotionnelle si le pirate, par exemple, fait de fausses déclarations ou diffuse de la désinformation à partir du compte compromis d'un utilisateur.

- Les pirates peuvent également divulguer des informations personnelles sensibles dans le domaine public, ce qui peut nuire à la réputation d'une personne ou affecter ses relations personnelles.

- Une attaque par bourrage d'identifiants donne au pirate un accès illimité à **toutes** les données personnelles de **chaque** compte compromis, qui peuvent comprendre des informations financières ou médicales ou d'autres types de données sensibles. Cette fuite massive d'informations peut donner le sentiment de perte de contrôle de ses données personnelles.

[9] Centre national de cybersécurité du Royaume-Uni, « Use of credential stuffing tools », https://www.ncsc.gov.uk/news/use-credential-stuffing-tools, consulté le 27 mai 2021.

[10] *Ibid.*

4. Pourquoi le bourrage d'identifiants est-il problématique?

En raison de la nécessité de créer un mot de passe pour chaque compte en ligne, les personnes choisissent par simple habitude un mot de passe facile à mémoriser, comme une date importante ou le nom d'un animal de compagnie[11], qu'elles réutilisent ensuite pour plusieurs comptes en ligne. Selon une enquête menée par le Centre national de cybersécurité du Royaume-Uni (NCSC) en 2019, les particuliers continuent d'utiliser des mots de passe prévisibles et faciles à deviner. Le rapport révèle que 23,2 millions de comptes pour lesquels l'utilisateur avait utilisé « 123456 » comme mot de passe avaient été piratés dans le monde[12].

En outre, étant donné que les justificatifs d'identité utilisés sont corrects, il peut être difficile pour les organisations de faire la différence entre un pirate et un utilisateur légitime, ce qui fait que les attaques par bourrage d'identifiants passent souvent inaperçues[13]. En 2018, il a été rapporté qu'il fallait en moyenne 15 mois à une organisation pour découvrir une atteinte à la sécurité découlant d'un bourrage d'identifiants et en informer ses utilisateurs[14]. Bien que la recherche laisse entendre qu'il y a eu des améliorations au cours des trois dernières années, le délai demeure bien présent[15]. Par conséquent, si un mot de passe compromis a été utilisé ailleurs, un pirate a tout le temps de mener d'autres attaques et de tenter d'accéder à d'autres comptes vulnérables.

Le potentiel de gain financier est souvent important par rapport au travail à accomplir pour y parvenir, ce qui rend ce type d'attaque attrayant. Des outils automatisés peu coûteux sont faciles à trouver et à utiliser, ce qui permet aux pirates de lancer des attaques à grande échelle et à grande vitesse[16]. Les attaques par bourrage d'identifiants auraient généralement un taux de réussite de 0,2 à 2 %[17]. Bien que le chiffre puisse sembler bas, la menace est élevée étant donné l'ampleur des attaques par bourrage d'identifiants. Par exemple, une recherche du secteur privé a mis au jour 55 milliards d'attaques par bourrage d'identifiants dans l'industrie du jeu en ligne de novembre 2017 à mars 2019[18], ce qui équivaut à plus de 3 000 millions d'attaques par mois et plus de 107 millions d'attaques par jour. D'autres recherches ont révélé 193 milliards d'attaques par bourrage d'identifiants dans le monde en 2020[19], ce qui équivaut à plus de 16 milliards d'attaques par mois et à plus de 500 millions d'attaques par jour.

---

[11] Les résultats d'une enquête du NCSC montrent que 15 % des personnes ont utilisé le nom d'un animal de compagnie et 13 %, une date importante comme mot de passe. Centre national de cybersécurité du Royaume-Uni, « Paws-word change recommended on National Pet Day », https://www.ncsc.gov.uk/news/national-pet-day-password-advice, consulté le 27 mai 2021.

[12] Centre national de cybersécurité du Royaume-Uni, « Most hacked passwords revealed », https://www.ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security, consulté le 27 mai 2021.

[13] Ponemon Institute, *The cost of credential stuffing* (oct. 2017), p. 2.

[14] Shape Security, *The 2018 credential spill report* (2018) | p. 6-7 et 14.

[15] F5, « 2021 Credential Stuffing Report », https://www.f5.com/labs/articles/threat-intelligence/2021-credential-stuffing-report, consulté le 8 février 2022.

[16] Centre national de cybersécurité du Royaume-Uni, « Use of credential stuffing tools », https://www.ncsc.gov.uk/news/use-credential-stuffing-tools, consulté le 27 mai 2021.

[17] Shape Security, *Attacker Economics* (2020).

[18] Akamai, *[State of the Internet]/security web attacks and gaming abuse* (vol. 5, nº 3 | 2019).

[19] Akamai, *[State of the Internet] phishing for finance* (vol. 7, nº 2 | 2021).

5. Recommandations au grand public pour réduire le risque d'une attaque par bourrage d'identifiants

Les paragraphes suivants donnent des conseils aux particuliers sur les mesures qu'ils peuvent prendre pour limiter le risque d'une attaque par bourrage d'identifiants.

MESURES DE PRÉVENTION

(a) Création de mots de passe

Lorsque vous créez un nouveau mot de passe, il est impératif de ne le divulguer à personne d'autre et de **ne pas le réutiliser**. La réutilisation de mots de passe, même ceux qui sont considérés comme forts, peut rendre un compte tout aussi vulnérable, car il suffit d'un seul mot de passe compromis pour accéder à plusieurs comptes[20]. C'est particulièrement important pour tous les comptes qui contiennent des informations financières, beaucoup de renseignements personnels ou des informations particulièrement sensibles, car les répercussions pourraient être bien pires si les comptes étaient compromis.

Les mots de passe restent une forme courante de protection des comptes et, afin de garantir leur efficacité, les utilisateurs doivent éviter de commettre des erreurs courantes. À cet égard, les utilisateurs devraient[21] :

- éviter d'utiliser des mots de passe prévisibles tels que « 12345 », « qwerty » ou « motdepasse », même s'ils comprennent des caractères spéciaux (« motdepasse1! » par exemple);
- éviter d'utiliser des détails personnels tels qu'un anniversaire, une équipe sportive ou le nom d'un animal de compagnie;
- éviter d'utiliser des mots qui se rapportent au service fourni, comme le nom de la banque concernée pour se connecter aux services bancaires en ligne.

N'utilisez pas des mots de passe courts[22]. Les mots de passe plus longs sont reconnus comme étant plus difficiles à compromettre pour les pirates[23]. Cependant, avec le développement de la technologie, les mots de passe plus longs ne sont pas nécessairement plus forts.

---

[20] Agence de l'Union européenne pour la cybersécurité, « Authentication Methods », https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/authentication-methods, consulté le 27 mai 2021.

[21] Centre canadien pour la cybersécurité, « Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032) », https://cyber.gc.ca/fr/orientation/pratiques-exemplaires-de-creation-de-phrases-de-passe-et-de-mots-de-passeitsap30032, consulté le 27 mai 2021.

[22] Commissariat à l'information du Royaume-Uni, « Passwords in online services », https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/passwords-in-online-services/, consulté le 27 mai 2021; Autorité norvégienne de sécurité nationale, « Passordanbefalinger fra Nasjonal sikkerhetsmyndighet », https://nsm.no/aktuelt/passordanbefalinger-fra-nasjonal-sikkerhetsmyndighet, consulté le 27 avril 2022.

[23] Agence de l'Union européenne pour la cybersécurité, « Authentication Methods », https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/authentication-methods, consulté le 27 mai 2021.

À cet égard, le NCSC recommande la technique des trois mots aléatoires. Cette technique est considérée comme un compromis entre sécurité et convivialité, car elle consiste à choisir trois mots aléatoires qui peuvent être mémorisables pour un utilisateur, mais difficiles à deviner pour un pirate[24]. Il est important que ces mots soient complètement aléatoires, comme « thémaisonpoisson », et non des expressions courantes, des citations célèbres, des paroles de chansons ou des successions prévisibles comme « undeuxtrois »[25].

L'ajout de caractères spéciaux, de chiffres ou de lettres majuscules peut rendre un mot de passe plus difficile à pirater et, par conséquent, prévenir certaines cyberattaques. Toutefois, le mot de passe peut ainsi devenir moins facile à mémoriser, ce qui peut être contre-productif dans la lutte contre les attaques par bourrage d'identifiants si les utilisateurs choisissent de réutiliser le même mot de passe sur plusieurs comptes afin de ne pas avoir à se souvenir de plus d'un mot de passe complexe.

L'utilisation d'un gestionnaire de mots de passe peut également faciliter la création, le stockage et la mémorisation de mots de passe forts et uniques, car il encourage la création de mots de passe complexes et décourage la réutilisation des mots de passe[26].

Les comptes de messagerie électronique, en particulier, doivent être protégés par un mot de passe fort et unique. En effet, après une compromission, un pirate peut abuser de la fonction « mot de passe oublié » et modifier les mots de passe de **tous** les autres comptes liés à ce courriel[27].

(b) Protection par mot de passe

S'il est important de créer un mot de passe fort pour chaque compte en ligne, il est tout aussi important de le faire de manière sécurisée lorsque les mots de passe sont stockés.

Écrire une liste de mots de passe n'est certainement pas l'option la plus sûre, mais c'est un moyen de gérer plusieurs mots de passe. Si les utilisateurs choisissent cette option, il est essentiel que la liste soit conservée dans un endroit sûr, idéalement dans un coffre-fort verrouillé, **loin** de l'ordinateur ou de l'appareil que le mot de passe est censé protéger[28]. L'ajout de trois lettres aléatoires au début et à la fin de chaque mot de passe est une autre précaution que les utilisateurs peuvent prendre pour protéger leurs mots de passe, au cas où la liste serait découverte par une personne mal intentionnée.

Il est aussi possible d'utiliser un gestionnaire de mots de passe, qui non seulement crée des mots de passe forts et uniques, mais fait également office de coffre-fort pour les mots de passe en stockant les

---

[24] Centre national de cybersécurité du Royaume-Uni, « Three random words or #thinkrandom », https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0, consulté le 27 mai 2021.

[25] *Ibid.*

[26] Centre canadien pour la cybersécurité, « Conseils de sécurité sur les gestionnaires de mots de passe », https://cyber.gc.ca/fr/orientation/conseils-de-securite-sur-les-gestionnaires-de-mots-de-passeitsap30025, consulté le 17 mars 2022.

[27] Centre national de cybersécurité du Royaume-Uni, « Top tips for staying secure online », https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/use-a-strong-and-separate-password-for-email, consulté le 26 janvier 2022.

[28] Centre national de cybersécurité du Royaume-Uni, « Using passwords to protect your devices and data », https://www.ncsc.gov.uk/information/infographics-ncsc, consulté le 27 mai 2021.

justificatifs d'identité pour plusieurs sites Web, applications et services[29]. Bien que les gestionnaires de mots de passe soient utiles pour composer avec l'excès de mots de passe, ils comportent également des risques. En effet, si un pirate parvient à accéder au gestionnaire de mots de passe, tous les mots de passe qui y sont stockés seront compromis. Par conséquent, l'authentification multifactorielle (expliquée au point c) ci-dessous) devrait **toujours** être activée, et les mots de passe requis pour les comptes sensibles, tels que les comptes bancaires en ligne ou les comptes assortis de privilèges administratifs tels que la messagerie électronique, ne doivent pas être stockés dans un gestionnaire de mots de passe[30].

Une autre solution consiste à stocker les mots de passe en ligne sur un navigateur Web en utilisant la fonction d'enregistrement de justificatifs d'identité[31]. L'utilisateur n'a donc plus à s'inquiéter, car il peut accéder à son compte en utilisant le mot de passe enregistré depuis n'importe quel appareil où il utilise le même navigateur Web[32]. Toutefois, un mot de passe ne doit jamais être enregistré sur un navigateur public (par exemple, dans une bibliothèque ou un café), car les justificatifs d'identité enregistrés pourraient être exposés à des personnes inconnues. Pour les ordinateurs partagés avec des membres de la famille ou des colocataires, il est également essentiel que chaque personne crée son propre compte et veille à fermer sa session à la fin[33].

(c) Activation d'une authentification multifactorielle

L'authentification multifactorielle est le fait d'exiger plus d'un facteur d'identification pour qu'une personne puisse accéder à son compte. L'ajout d'un second facteur présente en soi divers avantages et risques associés; **la mise en place de tout type d'authentification multifactorielle est en fait une mesure de protection très efficace, et un seul facteur supplémentaire vaut mieux que de ne pas en avoir du tout**[34]. Il est important de noter que lorsque l'authentification multifactorielle est utilisée, le deuxième facteur n'est généralement demandé qu'après la saisie du nom d'utilisateur et du mot de passe corrects, ce qui signifie qu'un pirate connaîtra dans ce cas les justificatifs d'identité du compte. À ce stade, le pirate pourrait alors chercher à compromettre le second facteur, par exemple en envoyant un message d'hameçonnage, et c'est un point à prendre en considération.

Voici des exemples de facteurs d'identification qui peuvent être utilisés, en plus de la saisie d'un mot de passe, d'une phrase de passe ou d'un NIP :

---

[29] Centre canadien pour la cybersécurité, « Conseils de sécurité sur les gestionnaires de mots de passe », https://cyber.gc.ca/fr/orientation/conseils-de-securite-sur-les-gestionnaires-de-mots-de-passeitsap30025, consulté le 27 mai 2021.

[30] Centre canadien pour la cybersécurité, « Conseils de sécurité sur les gestionnaires de mots de passe », https://cyber.gc.ca/fr/orientation/conseils-de-securite-sur-les-gestionnaires-de-mots-de-passeitsap30025, consulté le 27 mai 2021.

[31] *Ibid.*

[32] Centre national de cybersécurité du Royaume-Uni, « Cyber Aware », https://www.ncsc.gov.uk/cyberaware/home#action-1, consulté le 27 mai 2021.

[33] Centre national de cybersécurité du Royaume-Uni, « Top tips for staying secure online », https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers, consulté le 9 février 2022.

[34] Centre national de cybersécurité du Royaume-Uni, « Setting up two-factor authentication (2FA) », https://www.ncsc.gov.uk/guidance/setting-two-factor-authentication-2fa, consulté le 29 juillet 2021.

- recevoir un message SMS ou un NIP de vérification sur un appareil mobile. Ces codes ne peuvent généralement être utilisés qu'une seule fois[35]. Dans la mesure du possible, évitez d'utiliser les SMS pour recevoir des codes à usage unique et envisagez d'utiliser des outils tels que les applications d'authentification à deux facteurs, en raison des attaques connues contre les SMS, ou usurpations de carte SIM[36]. Ces attaques impliquent qu'un pirate redirige le numéro de téléphone utilisé pour recevoir le SMS afin d'accéder au code du second facteur sans avoir besoin du téléphone physique;

- demander un appel téléphonique vers un numéro de téléphone fixe ou mobile[37];

- installer une application d'authentification, telle que Google Authenticator ou Microsoft Authenticator, qui peut être utilisée sur les téléphones intelligents et les tablettes pour mettre en place une authentification à deux facteurs sur tous les comptes offrant cette option[38]. Ces types d'applications peuvent être plus avantageux que les messages texte dans la mesure où ils ne nécessitent pas de signal mobile ou de réception d'un SMS;

- utiliser un jeton d'authentification matériel tel qu'une clé de sécurité, qui est un petit dispositif qu'on peut acheter et qui est branché sur un ordinateur ou un portable pour authentifier un compte utilisateur[39];

- ajouter une caractéristique biométrique fournie par l'utilisateur, telle qu'une empreinte digitale, un balayage de la rétine ou une reconnaissance faciale ou vocale[40].

L'authentification multifactorielle est considérée comme la mesure la plus efficace pour protéger les comptes en ligne contre le bourrage d'identifiants, car le pirate doit entrer d'autres facteurs même s'il a le mot de passe entre les mains[41]. Selon une analyse de Microsoft, l'authentification multifactorielle mettrait fin à la quasi-totalité (99 %) des compromissions de comptes liées à des attaques par bourrage d'identifiants[42].

Certains services en ligne activeront automatiquement l'authentification multifactorielle, tandis que d'autres nécessiteront que l'utilisateur l'active manuellement. L'option permettant d'activer l'authentification multifactorielle se trouve généralement dans les paramètres de sécurité d'un compte.

---

[35] Agence de cybersécurité et de sécurité des infrastructures des États-Unis, « Security Tip (ST05-012) Supplementing passwords », https://us-cert.cisa.gov/ncas/tips/ST05-012, consulté le 27 mai 2021.

[36] Agence de l'Union européenne pour la cybersécurité, « How to Avoid SIM-Swapping - Leaflet », https://www.enisa.europa.eu/publications/how-to-avoid-sim-swapping-leaflet, consulté le 7 mars 2022.

[37] *Ibid.*

[38] Centre national de cybersécurité du Royaume-Uni, « Setting up two-factor authentication (2FA) », https://www.ncsc.gov.uk/guidance/setting-two-factor-authentication-2fa, consulté le 27 mai 2021.

[39] Centre canadien pour la cybersécurité, « Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030) », https://cyber.gc.ca/fr/orientation/securisez-vos-comptes-et-vos-appareils-avec-une-authentification-multifacteur, consulté le 27 mai 2021.

[40] Centre national de cybersécurité du Royaume-Uni, « Setting up two-factor authentication (2FA) », https://www.ncsc.gov.uk/guidance/setting-two-factor-authentication-2fa, consulté le 27 mai 2021.

[41] Centre national de cybersécurité du Royaume-Uni, « Top tips for staying secure online », https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/activate-two-factor-authentication-on-your-email, consulté le 25 mai 2021.

[42] Microsoft, « Your Pa$$word doesn't matter », https://techcommunity.microsoft.com/t5/azure-active-directory-identity/your-pa-word-doesn-t-matter/ba-p/731984, consulté le 25 mai 2021.

Notez que d'autres termes peuvent être utilisés pour désigner une authentification multifactorielle (ou authentification multifacteur), par exemple *authentification à deux facteurs* et *authentification à double facteur*[43], qui constituent un sous-ensemble d'authentification multifactorielle.

Certains services en ligne peuvent offrir d'autres solutions, par exemple en permettant aux utilisateurs d'accéder à un compte après avoir saisi un mot facile à mémoriser ou une série de questions de sécurité, par exemple « Quel est le nom de jeune fille de votre mère? ». Cependant, ces mesures **n'offrent pas** le même niveau de protection que l'authentification multifactorielle et ne sont plus considérées comme un moyen sûr de protection des comptes dans l'environnement actuel[44].

Il est recommandé aux utilisateurs d'activer l'authentification multifactorielle spécifiquement sur les comptes de messagerie et sur tous les comptes considérés comme importants[45]. Les comptes de messagerie sont particulièrement attrayants pour les pirates, car l'accès à la boîte de réception d'un utilisateur leur permet de réinitialiser les mots de passe d'autres comptes ou de transférer des courriels contenant des informations personnelles supplémentaires à leur propre compte[46]. L'accès à un compte de messagerie professionnelle peut permettre à un pirate de se faire passer pour le titulaire légitime du compte et d'envoyer des courriels frauduleux dans le but d'escroquer une organisation ou un particulier. C'est ce qu'on appelle l'escroquerie au faux ordre de virement. Par conséquent, à titre de mesure supplémentaire, toutes les demandes de paiement ou d'achat, ainsi que les modifications des détails ou des procédures de paiement, doivent être vérifiées en personne ou par téléphone pour s'assurer que la demande est authentique. Il convient également d'être prudent lorsqu'on traite des demandes marquées comme urgentes ou lorsque le demandeur semble être pressé[47].

(d) Mise à jour des appareils

Les logiciels, applications et systèmes obsolètes peuvent présenter des faiblesses logicielles qui les rendent plus vulnérables aux cyberattaques[48]. Bien que cette mesure ne soit pas spécifique aux attaques par bourrage d'identifiants, en règle générale, tous les appareils doivent être régulièrement mis à jour et rustinés pour que les derniers correctifs de sécurité soient installés.

SOLUTIONS POUR UN COMPTE QUI A ÉTÉ COMPROMIS

En plus des mesures que les utilisateurs peuvent mettre en œuvre pour protéger plus efficacement leurs comptes en ligne contre la menace d'une attaque par bourrage d'identifiants, il existe également des mesures qu'un utilisateur peut prendre si l'on soupçonne, ou si l'on confirme, que son compte a été compromis.

---

[43] Centre national de cybersécurité du Royaume-Uni, « Setting up two-factor authentication (2FA) », https://www.ncsc.gov.uk/guidance/setting-two-factor-authentication-2fa, consulté le 27 mai 2021.

[44] Institut national des normes et technologies des États-Unis, « Special Publication 800-63-3 Digital Identity Guidelines: 4.3.1 Authenticators », https://pages.nist.gov/800-63-3/sp800-63-3.html#431-authenticators, consulté le 9 février 2022.

[45] Centre national de cybersécurité du Royaume-Uni, « Setting up two-factor authentication (2FA) », https://www.ncsc.gov.uk/guidance/setting-two-factor-authentication-2fa, consulté le 27 mai 2021.

[46] Akamai, *[State of the Internet]/security web attacks and gaming abuse* (vol. 5, nº 3 | 2019), p. 18.

[47] Federal Bureau of Investigation (FBI), « Scams and safety: Business email compromise », https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise, consulté le 8 février 2022.

[48] Centre national de cybersécurité du Royaume-Uni, « Cyber Aware », https://www.ncsc.gov.uk/cyberaware/home#action-1, consulté le 8 février 2022.

(a) Changer immédiatement le mot de passe (ou la phrase de passe)[49]

Il faut le faire dès que possible, car les pirates changent souvent eux-mêmes le mot de passe pour empêcher l'utilisateur de reprendre le contrôle légitime et pour se donner un temps et un accès illimités au compte. Les mots de passe de tout autre compte protégé par le même mot de passe ou un mot de passe similaire **doivent également être modifiés** dès que possible afin d'éviter que d'autres comptes ne soient compromis.

(b) Vérifier les informations et les transactions du compte

De nombreux indices peuvent laisser penser qu'un pirate a accédé à un compte, notamment des transactions inhabituelles et non autorisées, ou des tentatives de connexion à partir d'endroits ou à des moments inhabituels, par exemple pendant la nuit[50]. À cet égard, il est important de vérifier l'historique du compte (et de mettre en place des alertes si possible) et de joindre la banque si une carte de crédit ou un compte bancaire est lié au compte, même si les fonds n'ont pas quitté le compte[51]. Les utilisateurs victimes d'une attaque par bourrage d'identifiants, ou de tout autre cybercrime, doivent également le signaler aux autorités compétentes.

Les modifications apportées aux paramètres de sécurité ou les messages inconnus envoyés depuis le compte sont d'autres signaux d'alarme à surveiller[52]. Lorsqu'elles sont utilisées[53], les questions et réponses de sécurité doivent également être modifiées. En outre, les amis, la famille et les abonnés doivent être informés du compte qui a été compromis et ouvrir les messages ou les notifications avec prudence[54], notamment pour éviter d'être eux-mêmes piratés.

(c) Vérifier si les comptes de messagerie sont compromis[55]

Vérifiez les filtres de messagerie et les règles de transfert pour vous assurer qu'un pirate n'a pas mis en place une « règle » pour recevoir une copie de tous les courriels reçus. Vous trouverez généralement des informations sur la façon de vérifier et d'éliminer ce problème sur la page d'assistance du fournisseur de messagerie.

(d) Communiquer avec le fournisseur du compte

---

[49] Centre canadien pour la cybersécurité, « Repensez vos habitudes en regard de vos mots de passe de manière à protéger vos comptes des pirates informatiques (ITSAP.30.036) », https://cyber.gc.ca/en/guidance/rethink-your-password-habits-protect-your-accounts-hackers-itsap30036, consulté le 27 mai 2021.

[50] Centre national de cybersécurité du Royaume-Uni, « Recovering a hacked account », https://www.ncsc.gov.uk/guidance/recovering-a-hacked-account, consulté le 27 mai 2021.

[51] Centre canadien pour la cybersécurité, « Repensez vos habitudes en regard de vos mots de passe de manière à protéger vos comptes des pirates informatiques (ITSAP.30.036) », https://cyber.gc.ca/en/guidance/rethink-your-password-habits-protect-your-accounts-hackers-itsap30036, consulté le 27 mai 2021.

[52] Centre national de cybersécurité du Royaume-Uni, « Recovering a hacked account », https://www.ncsc.gov.uk/guidance/recovering-a-hacked-account, consulté le 27 mai 2021.

[53] Comme il est indiqué précédemment, ces mesures n'offrent **pas** le même niveau de protection que l'authentification multifactorielle et ne sont plus considérées comme un moyen sûr de protection des comptes dans l'environnement actuel. Cependant, lorsqu'elles sont utilisées, elles doivent faire l'objet d'une surveillance.

[54] Centre national de cybersécurité du Royaume-Uni, « Recovering a hacked account », https://www.ncsc.gov.uk/guidance/recovering-a-hacked-account, consulté le 27 mai 2021.

[55] *Ibid.*

Si l'accès à un compte a été refusé parce qu'il a été verrouillé par un pirate, l'organisation concernée dispose souvent d'une page d'aide fournissant des informations sur la manière de récupérer le compte[56]. Si le compte est récupérable et que l'authentification multifactorielle n'a pas encore été activée, il est recommandé de le faire lorsque l'option est offerte.

Si le compte est irrécupérable, un nouveau compte devra être créé. Afin de récupérer les informations perdues ou volées, les utilisateurs doivent s'assurer qu'ils sauvegardent régulièrement les données enregistrées sur un autre appareil ou sur un site de stockage en ligne[57].

(e) Vérifier si les mots de passe sont compromis

Il existe également des sites Web accessibles au public qui fournissent des listes de mots de passe piratés[58], où les utilisateurs peuvent vérifier si leurs justificatifs d'identité ont été compromis lors d'une violation de données. Les utilisateurs peuvent également vérifier régulièrement si leurs mots de passe sont compromis, à titre de mesure préventive et de moyen de contrôler la sécurité de leurs comptes en ligne.

[56] *Ibid.*

[57] Centre national de cybersécurité du Royaume-Uni, « Cyber Aware », https://www.ncsc.gov.uk/cyberaware/home#action-1, consulté le 27 mai 2021.

[58] « Pwned Passwords », www.haveibeenpwned.com, consulté le 27 mai 2021.

Annexe 1 – Astuces pour se protéger contre le bourrage d'identifiants