Document d'information, Boîte à outils de cybersécurité de la GCA : Éviter l'emploi de mots de passe simples

L'une des méthodes les plus courantes que les criminels utiliseront pour accéder à vos comptes, à votre réseau et à vos informations est de se connecter en utilisant votre identité. Il est très important que vous utilisiez des mots de passe (ou des phrases secrètes) uniques et forts pour chacun de vos comptes, que ces mots de passe restent privés, en sécurité, et que vous ne les réutilisiez jamais.

- La réutilisation du même mot de passe pour plusieurs comptes implique que si un criminel met la main sur l'un de vos mots de passe, il a facilement accès à tous vos comptes.
    - *Plusieurs tentatives de saisie du même nom d'utilisateur et du même mot de passe seront effectuées sur de nombreuses applications courantes.*

Les criminels utiliseront de nombreuses techniques pour accéder à vos mots de passe. Il existe également un marché très actif sur Internet (parfois appelé le « dark web ») où ces informations personnelles sont achetées et revendues dans le cas où l'une des sociétés dans laquelle vous détenez un compte subit une violation de ses données.

Les méthodes utilisées sont les suivantes :

- **Attaque par force brute** : utilisation de la puissance de calcul pour saisir automatiquement toutes les combinaisons possibles.
    - *Utilisez des mots de passe longs ou des phrases secrètes et des caractères spéciaux pour compliquer l'attaque.*

- **Attaque par dictionnaire** : forme d'attaque par force brute qui utilise des mots/phrases connus issus de dictionnaires ou des mots de passe fréquents.
    - *Utilisez des mots ou des mots de passe mémorisables sans qu'ils soient issus d'un dictionnaire, qu'il s'agisse de mots communs ou qui soient en relation avec vous.*

- **Credential stuffing** : dès que la sécurité du compte est compromise, le criminel tente d'utiliser le même nom d'utilisateur/mot de passe pour accéder à un autre compte.
    - *Utilisez un mot de passe différent pour chaque compte, ainsi qu'une protection supplémentaire (double authentification) pour les comptes qui disposent de cette fonction.*

- **E-mail d'hameçonnage :** vous recevez par exemple un e-mail dont l'objet est « Il est temps de réinitialiser votre mot de passe » contenant des liens vers un site web malveillant ou un enregistreur de frappe installé en ouvrant une pièce jointe malveillante (un enregistreur de frappe surveille ce que vous tapez sur votre clavier).
    - *Restez sur vos gardes lorsqu'il s'agit d'ouvrir une pièce jointe, de cliquer sur des liens ou de télécharger une pièce jointe à partir d'un e-mail, même si ce dernier semble avoir été envoyé par une personne ou une organisation que vous connaissez.*

- **Ingénierie sociale** : les professionnels savent très bien manipuler les conversations et utiliser diverses techniques (appel téléphonique, SMS ou réseaux sociaux) pour vous inciter à révéler vos mots de passe et autres informations personnelles en se faisant passer pour quelqu'un de légitime.
    - *Ne donnez jamais votre mot de passe, ou une partie de celui-ci, à personne. Une entreprise légitime ne vous le demandera pas.*

- **Supposition manuelle** : le criminel utilise vos informations personnelles pour savoir si votre nom ou votre date de naissance a été utilisé(e) dans votre mot de passe.
    - *N'utilisez pas d'informations personnelles dans vos mots de passe. Réfléchissez aux informations qui pourraient apparaître sur le web et les réseaux sociaux à votre sujet et évitez de les utiliser dans vos mots de passe.*

- **Shoulder surfing** : dans un lieu public ou même à votre bureau, il est possible que quelqu'un surveille votre activité par-dessus votre épaule.
    - *Lorsque vous saisissez des informations sensibles, vérifiez si quelqu'un se trouve derrière ou à côté de vous, ou si une caméra est présente.*

- **Interception** : étant donné qu'ils sont transmis via un réseau, les mots de passe peuvent être interceptés.
    - *Vérifiez que le symbole du cadenas https apparaît en regard de l'adresse du site web et méfiez-vous lorsque vous utilisez le Wi-Fi dans les lieux publics. Un site web peut ne pas être sécurisé ou avoir été « détourné » en utilisant des noms semblables, permettant aux criminels de « voir » ce que vous transmettez.*

La puissance de calcul a augmenté de façon exponentielle au fil du temps, tout comme notre utilisation d'Internet et des réseaux sociaux. Les criminels peuvent ainsi accéder plus rapidement et plus facilement à vos informations :

	PC Apple MacIntosh de 1984	iMac « Core i5 » de 2019 (standard)	Différence
Mémoire vive :	128 ko	8 Go	Augmentation de 64 500 000 %
Vitesse de traitement :	8 MHz	3 GHz	37 400 % plus rapide
Coût :	2 500 $	1 500 $	40 % moins cher

- Les progrès rapides de la technologie ont vraiment profité aux pirates : le piratage d'un mot de passe à l'aide d'un ordinateur portable moderne et d'un programme n'a jamais été aussi rapide.
    - *Cette avancée technologique ne fait qu'accroître la nécessité d'utiliser des mots de passe plus longs et plus complexes et des méthodes de protection supplémentaires.*

Double authentification (2FA) :

La double authentification offre un deuxième niveau de protection qui rend l'accès à vos comptes encore plus difficile. En effet, cette méthode dépend :

- De quelque chose que vous connaissez :
    - Un mot de passe

- Et/ou de quelque chose que vous détenez :
    - Un jeton (Google Authenticator, Okta, RSA)
    - Un code de vérification envoyé par SMS

- Ou de quelque chose qui vous appartient :
    - Une empreinte digitale ou votre visage (biométrie)

La double authentification exige ces facteurs pour accorder un accès, ce qui fournit une couche supplémentaire de défense.

Les conseils pour créer des mots de passe longs et forts ou des phrases secrètes sont nombreux. Quels que soient les conseils que vous décidez de suivre :

- Assurez-vous qu'une politique forte a été mise en place à l'échelle de l'entreprise et qu'un système interdit l'utilisation de mots de passe faibles.
- Évitez d'utiliser des noms d'animaux de compagnie ou des mots de passe qui pourraient être devinés par le biais des réseaux sociaux.
- Utilisez un mot de passe différent pour chaque compte.
- Envisagez d'utiliser un gestionnaire de mots de passe pour y stocker vos mots de passe.

De plus :

- Mettez à jour vos mots de passe sur tous les comptes dont la sécurité a été compromise (vous pouvez le vérifier via l'outil « Have I Been Pwned » de la boîte à outils).
- Supprimez les comptes et désinstallez les applications que vous n'utilisez plus.
- Assurez-vous d'utiliser des mots de passe forts et uniques sur tous vos comptes.
- Activez la double authentification sur tous vos comptes (lorsqu'elle est prise en charge).
- Vérifiez les paramètres d'administration par défaut de vos appareils accessibles à distance. Changez toujours les mots de passe par défaut qui peuvent être devinés avant leur première utilisation.

Utilisez les outils de la boîte Éviter l'emploi de mots de passe simples pour obtenir des conseils, vérifier si la sécurité de l'un de vos comptes a été compromise, et vous aider à mettre en place des améliorations.

https://gcatoolkit.org/fr/petites-entreprises/eviter-lemploi-de-mots-de-passe-simples/