Focus

La gestion des mots de passe sous Windows

Nature du problème

L'application des bonnes pratiques en matière de mot de passe impose notamment de respecter certaines règles comme :

- Définir d'un mot de passe long et complexe mixant caractères majuscules et minuscules, chiffres et caractères spéciaux ;
- Utiliser un mot passe différent pour chaque site ou service.
- Ne pas noter ses mots de passe sur des post-it ou tout autre support.

Malheureusement la mémorisation de tous ces mots de passe s'avère difficile et souvent même si la première règle est respectée, car imposée par la politique des mots de passe du service que l'on utilise, l'être humain est tenté de mettre le même mot de passe pour les autres services ou de noter quand même ces mots de passe sur des supports écrits.

La conséquence de ces pratiques est que si votre mot de passe est découvert, la personne mal intentionnée s'empressera d'essayer le couple d'identifiants (souvent votre adresse email) et le mot de passe découvert pour tenter d'accéder à d'autres services sur Internet. Vous pouvez en savoir plus ici :

https://cyberguerre.numerama.com/11278-pourquoi-est-ce-vraiment-grave-de-reutiliser-votre-mot-de-passe-sur-plusieurs-comptes.html

La solution

La solution, la plupart du temps gratuite, réside dans l'utilisation d'un gestionnaire de mot de passe. L'ensemble des identifiants est stocké soit sur le poste soit dans le cloud dans un fichier chiffré (wallet). Il existe trois familles de gestionnaire de mot de passe :

- la fonction est intégrée à votre navigateur
- le module est intégré à l'anti-virus
- c'est un logiciel spécifique.

Ces solutions proposent très souvent :

- un générateur de mot de passe complexe qui peut être utile dans le renforcement de la robustesse du mot de passe ;
- la possibilité de copier/coller manuellement les identifiants en cas de non fonctionnement du remplissage automatique des champs par l'outil dans le navigateur ;

- de capacités d'exportation et d'importation sous forme de fichiers des identifiants et mot de passe de ces outils afin de faciliter les changements de PC.
- Des capacités de synchronisation entre plusieurs appareils comme par exemple votre PC et votre smartphone.

Dans tous les cas, il convient de regarder comment sont gérées ces différentes fonctionnalités, avant de faire son choix. Par ailleurs, la perte ou vol du PC peut avoir aussi des conséquences graves si le fichier chiffré (Wallet) est stocké localement. Mais il peut aussi être sauvegardé dans le Cloud ou synchroniser avec un autre appareil.

Ces outils proposent aussi d'enregistrer vos données de cartes bancaires afin de faciliter le remplissage des champs lors d'un paiement en ligne. Il est prudent de ne pas utiliser cette fonction.

1. Gestionnaire de mot de passe intégré au navigateur.

Il est gratuit mais nécessite l'activation de la fonction dans le navigateur. Des vulnérabilités sont découvertes régulièrement sur les navigateurs et certaines pourraient remettre en cause la sécurité de vos mots de passe. Il convient donc de paramétrer impérativement la mise à jour de son navigateur en automatique si vous utilisez cette fonction.

Google Chrome

L'utilisation dans l'écosystème de Google permet d'avoir une transparence dans cet environnement qui inclut les smartphones Android.

https://support.google.com/chrome/answer/95606?hl=fr

Mozilla Firefox

https://support.mozilla.org/fr/kb/gerer-mots-de-passe-firefox-ordinateur-firefox-lockwise

Microsoft Edge

https://support.microsoft.com/fr-fr/microsoft-edge/enregistrer-ou-oublier-des-mots-de-passe-dans-microsoft-edge-b4beecb0-f2a8-1ca0-f26f-9ec247a3f336

2. Gestionnaire de mot de passe intégré à l'antivirus

La plupart des anti-virus proposent dans leur version la plus complète, un gestionnaire de mot de passe intégré. Ce n'est pas forcément vrai dans les versions gratuites ou standards. Voici, par exemple, à quoi cela ressemble dans l'antivirus Bitdefender :

https://www.bitdefender.fr/consumer/support/answer/10919/

Nous citons d'autre antivirus ayant cette fonction, la liste n'est pas exhaustive :

Norton password manager : https://fr.norton.com/feature/password-manager

McAfee Truekey : https://www.truekey.com/fr

ESET password manager : https://help.eset.com/password_manager/1/fr-FR/index.html

3. Gestionnaire de mot de passe spécifique

Keepass est un logiciel libre certifié par l'ANSSI :
https://www.ssi.gouv.fr/entreprise/certification_cspn/keepass-version-2-10-portable/

Considéré comme le plus sûr, il nécessite néanmoins des compétences informatiques pour sa mise en œuvre. Il est téléchargeable ici > https://keepass.fr/. Sa mise en œuvre n'est pas très ergonomique.

Des logiciels spécifiques existent mais sont en général payant dans la version premium la plus complète. Nous vous communiquons une liste non exhaustive :

Lastpass : https://www.lastpass.com/fr/

Dashlane : https://www.dashlane.com/fr

1password : https://1password.com/fr/

Keeper Individual : https://www.keepersecurity.com/fr_FR/personal.html

Conclusion

L'utilisation d'un gestionnaire de mot de passe s'avère aujourd'hui nécessaire si l'on souhaite respecter les bonnes pratiques en matière de sécurité.

Nous vous rappelons que vous pouvez retrouver les fiches pratiques dans la rubrique « Anticiper » de notre site www.c2rcsud.org.

En cas d'incident vous pouvez adresser le mail litigieux à csirt@c2rcsud.org .

Retrouvez aussi dans notre rubrique « Remédier », la possibilité de déclarer votre incident ou tentative d'escroquerie.

Rappel : En aucun le C2RC ne vous demandera de transmettre des informations confidentielles de l'entreprise. En cas de doute adresser un mail à csirt@c2rcsud.org.