Newsletter N°1/2013

RESTENA
Réseau Téléinformatique de l'Education Nationale et de la Recherche

Cette campagne a pour but de sensibiliser les utilisateurs d'internet de se munir de mots de passe forts.

CHOISIR SON MOT DE PASSE AVEC SOIN

A propos des mots de passe

Le mot de passe est un des éléments de base de la sécurité informatique et demeure encore aujourd'hui le moyen d'authentification le plus utilisé.

Le mot de passe, combiné avec le nom d'utilisateur, vous permet de vous identifier et d'accéder à votre messagerie électronique, à votre compte informatique ou à un service/ ressource réservé et protégé. Il sert à protéger l'accès à vos messages, vos documents et vos données personnelles.

Il est donc essentiel de choisir un bon mot de passe et de le garder secret afin que personne ne puisse usurper votre identité et ne puisse accéder à vos informations personnelles et/ou confidentielles.

info: Préservez la sécurité et la confidentialité de vos données personnelles en choisissant des bons mots de passe

Qu'est-ce qu'un bon mot de passe

! Un bon mot de passe doit être difficile à deviner par une personne tierce et difficile à trouver à l'aide d'outils automatisés. Mais il doit rester facile à retenir !

Par conséquent un **bon mot de passe** doit être :

- Une combinaison inhabituelle de **lettres** , de **chiffres** et de **symboles** ;
- Assez long, au moins 10 caractères, idéalement **12 à 16** caractères ;
- Sans signification précise (mélange quelconque de lettres, de chiffres et de symboles) ;

Fondation RESTENA
6, rue Richard Coudenhove-Kalergi
L-1359 Luxembourg
Tél: +352 42 44 09 -1
Fax: +352 42 24 73

Il faut donc éviter :

- Toutes les suites logiques possibles telles que « azerty », « qwertz » ou « asdfgh » et tout comme « abcdefg », « aaaaaa », « 1234567 », ... ;
- Les mots du dictionnaire (quelle que soit la langue), des noms propres, des lieux, etc.;
- Des mots de passe en rapport avec votre vie privée ou professionnelle (mot de passe composé de votre nom, prénom, date de naissance ou de ceux d'un proche, de votre matricule, numéro de téléphone, numéro d'immatriculation, etc.). Evitez également de reprendre des parties d'informations personnelles pour créer votre mot de passe ;
- Des mots de passe considérés à priori faible tels que les traditionnels « sesame », « password », « motdepasse »,…

Les mots de passe suivants sont absolument à proscrire :

NON! : **« Administrator », « Administrateur », « admin », « password », « 123456 », « qwertz » , « asdfgh » , …**

Comment créer un mot de passe sûr et facile à retenir ?

Il existe quelques astuces pratiques pour créer des mots de passe complexes/ forts mais faciles à retenir.

Une première méthode consiste à choisir une **phrase** ou un **vers** facile à retenir et de ne conserver que les initiales de chaque mot pour ensuite remplacer certaines lettres par des chiffres ou des symboles afin d'augmenter la complexité.

OUI! :

Phrase 1:

« Faire son jogging c'est agréable et bon pour la santé ! »

Mot de passe possible :

Fsjcaebpls! ou **Fsjcabpls!52** (rajouter un chiffre supplémentaire)

Phrase 2:

« Brrrr, il fait vraiment froid ce matin, -9 degrés! »

Mot de passe possible :

B,ifvfcm-9d! ou **Bifvfcm-9d!**

Recommandations de sécurité relatives aux mots de passe

- Tenez votre mot de passe absolument secret, ne donnez votre mot de passe à personne, sous aucun prétexte ;
- Ne transmettez jamais votre code d'accès (nom d'utilisateur et/ou mot de passe) par téléphone, par messagerie directe, par e-mail même si on vous le demande! ;
- Protégez vos mots de passe, ne les inscrivez pas en clair dans des documents ou sur des morceaux de papier facilement accessibles ;
- N'utilisez pas le même mot de passe pour tous vos comptes et vos accès. Sinon en cas de vol, le malveillant aura accès à tout. Le mot de passe utilisé pour votre compte professionnel/ messagerie professionnelle doit être impérativement différent du mot de passe que vous utilisez pour d'autres services en ligne ;

Comment les pirates attaquent–ils les mots de passe?

Parmi les attaques sur les mots de passe on peut citer les méthodes les plus importantes :

Attaque par force brute

Une attaque par force brute, ou attaque par recherche exhaustive, est une méthode technique utilisée par les pirates pour trouver un mot de passe en générant exhaustivement toutes les combinaisons de caractères possibles.

♦ Attaque par dictionnaire

L'attaque par dictionnaire est une méthode technique qui consiste à tester une série de mots de passe issus d'un dictionnaire (mots, noms, prénoms, mot de passe communs, films, etc.). Cette attaque est souvent utilisée en complément de l'attaque par force brute pour trouver le code secret plus rapidement.

La méthode n'est pas fructueuse (ne donnera aucun résultat) si le mot de passe est suffisamment aléatoire et s'il n'est pas composé d'un mot propre et/ou nom commun.

Pour augmenter les chances de trouver (casser) un mot de passe les logiciels automatisés appliquent aussi des transformations aux mots telles que :

- Le changement de la casse de certaines lettres (aViOn);
- L'ajout d'un chiffre ou symbole au début ou à la fin d'un mot (9marc, maison!);
- Le remplacement de certains caractères par des chiffres ou des symboles (mai5on, mai!on).

Les mots de passe tels que 'aVion12', 'marc123', … auront de grandes chances d'être trouvés.

info : Plus votre mot de passe est varié dans le type de caractères, plus il résistera aux attaques par force brute ou dictionnaire.

Attaque par ingénierie sociale/ hameçonnage/ phishing

Le phishing (hameçonnage ou filoutage) est une escroquerie très répandue sur Internet qui consiste à amener les internautes à révéler des informations personnelles ou sensibles (mot de passe, code PIN, informations bancaires) via un message électronique ou un site web frauduleux.

Le hameçonnage repose sur l'ingénierie sociale et exploite la « faille humaine », la confiance, la crédulité ou l'ignorance de l'internaute.

Pour éviter de se faire arnaquer, le respect de quelques règles élémentaires s'impose:

- Soyez vigilant par rapport au phishing ;
- Ne divulguez jamais des informations confidentielles (mot de passe, ...) si elles vous sont demandées par e-mail, téléphone ou par tout autre manière suspecte ;
- Ne saisissez pas directement des informations personnelles dans les formulaires reçus par courrier électronique.

Attaque par enregistreur de frappe (keylogger)

L'attaque par enregistreur de frappe (keylogger) vise à récupérer les mots de passe et autres données sensibles directement sur le clavier, en clair.

L'enregistreur de frappe (keylogger), est un programme espion (spyware) qui tourne sur l'ordinateur, à l'insu de l'utilisateur, et qui enregistre toutes les entrées clavier et envoie les données collectées aux réseaux des pirates.

La meilleure façon de se protéger contre ce type d'attaque est la vigilance :

- N'installez pas des logiciels sur votre ordinateur dont vous ne connaissez pas l'origine ;
- Installez et gardez à jour vos logiciels anti-virus/ anti-spyware ainsi que le pare-feu (firewall) pour protéger votre ordinateur contre les virus, chevaux de Troie et programmes espions ;
- Soyez extrêmement prudent lorsque vous vous connectez sur un ordinateur qui n'est pas sous votre contrôle (cybercafé, hotel, ...). Vous ne savez pas quels types de logiciels sont installés et s'il n'y a pas de programmes espion sur la machine.

Responsabilité

Vous êtes responsable de votre compte informatique, et devez en assurer la sécurité, notamment en choisissant un bon mot de passe et en le gardant secret.

Si un pirate parvient à trouver votre mot de passe, il pourra non seulement accéder à votre messagerie électronique et votre compte informatique, mais il pourra également utiliser le compte usurpé pour envoyer du spam ou des emails de hameçonnage et exploiter les ressources disponibles à toute fin qu'il jugera utile (avec des implications et conséquences pour vous-même, mais aussi pour d'autres utilisateurs).

! Les collaborateurs (-trices) de la Fondation RESTENA ne vous demanderont jamais votre mot de passe ni par téléphone, ni par courrier électronique !

Comment changer mon mot de passe RESTENA

Un mot de passe doit être changé régulièrement et au moindre doute sur son caractère personnel et confidentiel.

Vous pouvez à tout moment changer votre mot de passe en vous connectant à l'outil de « Gestion de compte en ligne », accessible depuis le site web de RESTENA.

info:

Traitez votre mot de passe de la même manière qu'une brosse à dents*:

Ne la partagez pas et changez la régulièrement!

Pour toute information supplémentaire sur les mots de passe, veuillez nous contacter ou visiter le site web de BEE-SECURE*.

Cette lettre d'information vous a été proposée dans le cadre du **SID2013**.

La RESTENA Newsletter est un nouveau service semestriel proposé par la Fondation RESTENA. Pour vous abonner à ce service veuillez envoyer un email à :

newsletter-subscribe@restena.lu

* BEE SECURE https://www.bee-secure.lu