MODULE

MOT DE PASSE

LEÇON 1

Introduction

Le mot de passe, cette séquence de caractères alphanumériques (lettres, chiffres et caractères spéciaux) utilisée pour protéger l'accès aux ressources informatiques quelles qu'elles soient est un des piliers de la cybersécurité.

A, b, c, D, e, F, G, h, i, J, K,L, m,n, o, p, Q, r, s, T, u, v, w, x, Y, Z

1, 2, 3, 4, 5, 6, 7, 8, 9, 0

$? % ^ & * ( ) _ - + = @ ~#

Par ressources informatiques, nous entendons généralement:

- **les appareils** (les ordinateurs, les smartphones et les tablettes);
- **les zones d'accès restreint des sites Web;**
- **les applications et toute information sur support numérique**, où qu'elles se trouvent.

Code d'accès

Le mot de passe est donc le code d'accès à toutes ces ressources informatiques qui doivent rester sécurisées et confidentielles.

Nous saisissons des mots de passe à une fréquence qui aurait été inimaginable il y a quelques années car ce « mot magique » est justement la clé d'accès à de nombreuses applications qui concernent à la fois la sphère privée et professionnelle. Réseaux sociaux, comptes bancaires, programmes, applications professionnelles et même applications installées sur notre smartphone, tout est généralement protégé par un mot de passe.

Risques

Malheureusement, le mot de passe peut également **déclencher des scénarios catastrophes.**

Sa violation peut permettre à un pirate informatique d'agir en votre nom et donc d'obtenir des informations confidentielles et des ressources qui vous appartiennent ou d'échanger avec d'autres personnes en usurpant votre identité.

Ainsi, la récupération du mot de passe peut être la première étape d'un « vol d'identité » beaucoup plus grave, avec des conséquences facilement imaginables.

Cela peut entraîner des dommages sérieux pour vous et votre organisation, et c'est la raison pour laquelle il est nécessaire d'adopter un bon comportement lorsque vous utilisez des mots de passe.

Je suis certain que vous identifiez très bien les conséquences possibles d'une violation des codes d'accès à votre compte bancaire en ligne, votre messagerie ou vos réseaux sociaux.

Pourtant, vous pensez peut-être à l'heure actuelle que ce scénario est peu probable :

« Pourquoi cela devrait-il m'arriver ? »

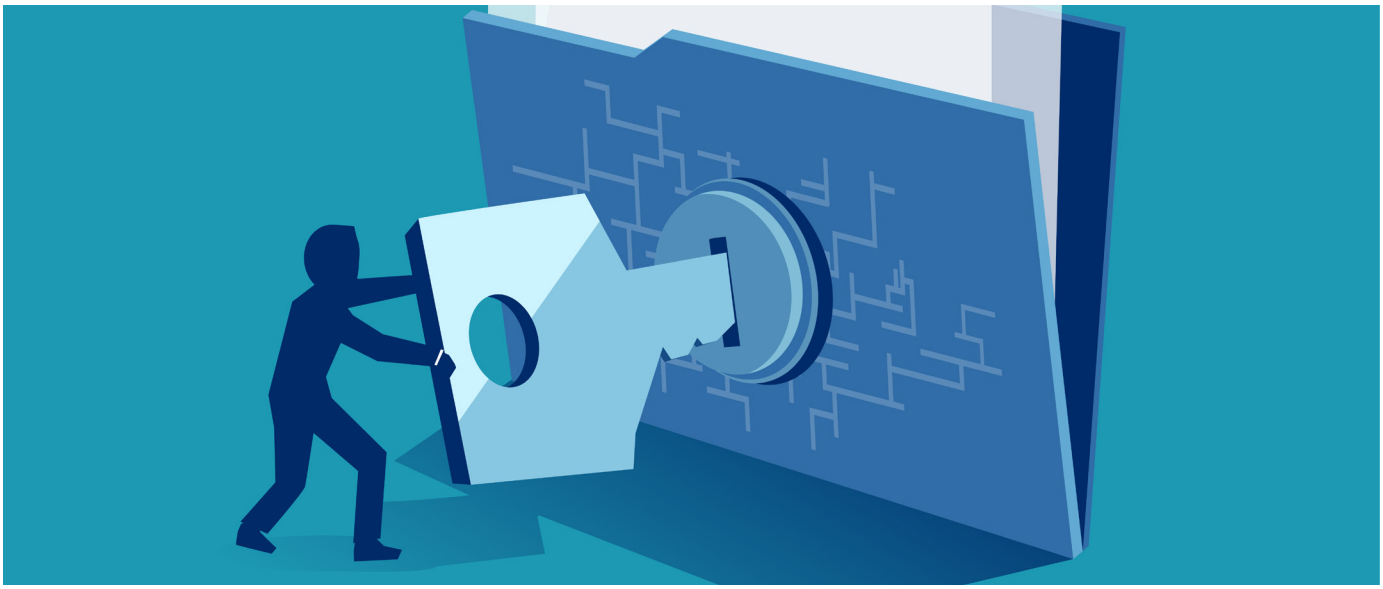
Ce manque de conviction pourrait vous amener à agir à la légère, et donc à faire de vous une proie facile pour des groupes de pirates informatiques.

Pensez-y :

«Donneriez-vous les clés de votre maison à des inconnus ?»

Eh bien, le mot de passe a maintenant la même valeur que les clés de votre maison et vous devez donc éviter de le traiter à la légère.

Pourtant, des milliards de mots de passe ont été diffusés en ligne, obtenus frauduleusement. Des millions d'utilisateurs ont vécu cette expérience amère. Pendant trop longtemps, nous avons sous-estimé le phénomène en élaborant des mots de passe sans trop réfléchir, facilitant ainsi la tâche des pirates informatiques. **Nous avons remis nos clés à des étrangers !**



Politiques de gestion des mots de

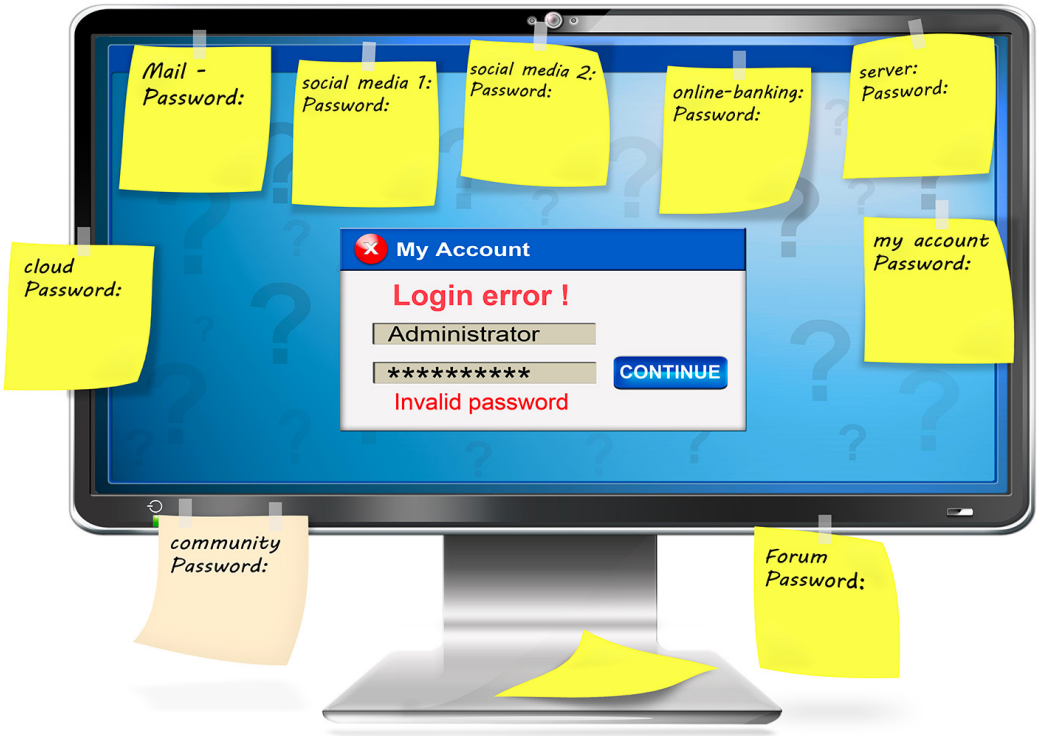
Chaque organisation définit elle-même ses politiques de sécurité et donc ses processus liés à la gestion des mots de passe. Prenons un exemple : pour autoriser l'accès à son portail interne, votre organisation vous demandera de choisir un mot de passe qui doit avoir une certaine longueur et complexité, et vous demandera de le modifier à une certaine fréquence.

Le mot de passe doit comporter au moins 8 caractères et doit contenir au moins une lettre majuscule, un chiffre et un caractère spécial.

Quelle que soit la politique de sécurité choisie, son point faible reste généralement le comportement humain et donc notamment le vôtre.

Par exemple, si, après avoir choisi un mot de passe très complexe, vous l'écrivez sur un post-it que vous collez sur le coin de votre ordinateur pour vous en souvenir, tous les efforts déployés par votre organisation risquent d'être anéantis par votre imprudence.

L'objectif de ce module de formation n'est donc pas de remettre en question les politiques de sécurité d'une organisation, mais de vous sensibiliser sur le sujet pour vous permettre de faire les meilleurs choix à chaque fois que vous devez saisir un nouveau mot de passe. Il vise également à s'assurer que vous adoptez les bonnes pratiques pour sécuriser les nombreux mots de passe que vous utiliserez.



Je dis « nombreux mots de passe » car dans votre sphère professionnelle comme dans votre sphère privée, vous serez amené à utiliser de nombreuses ressources informatiques, dont certaines sous le contrôle de votre organisation et d'autres non. Vous devrez donc saisir différents mots de passe et à vous adapter à différentes politiques et règles.

Maintenant que nous vous avons donné un aperçu général sur la question des mots de passe, nous allons l'approfondir dans la prochaine leçon.