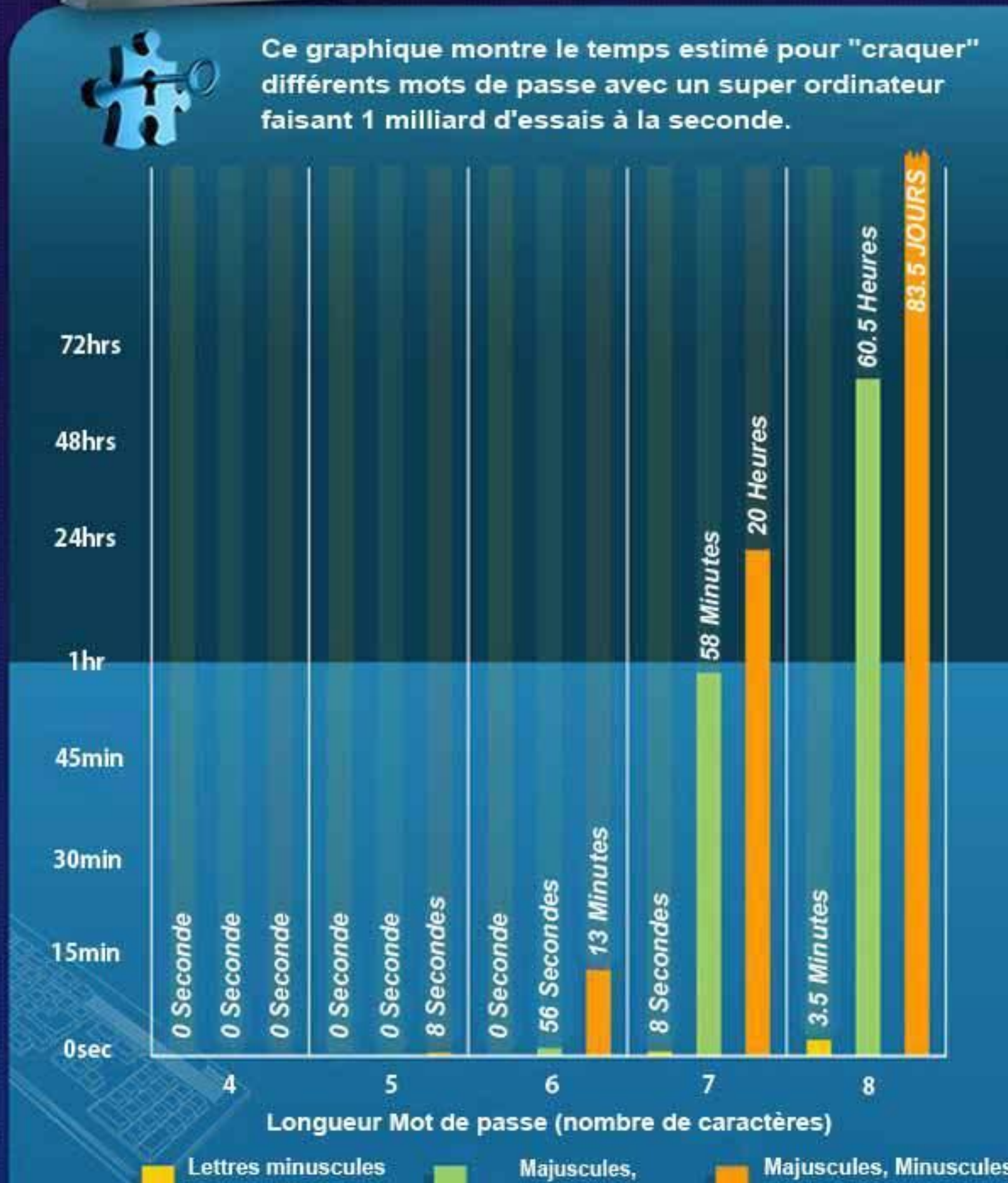
The Basics of Online Account Security

Étape 1 : Choisir un Bon Mot de Passe

Ce graphique montre le temps estimé pour "craquer" différents mots de passe avec un super ordinateur faisant 1 milliard d'essais à la seconde.



Les Essentiels d'un Bon Mot de Passe

	god	ther1v3r	Fk8!$skT%f
	love	poker159	rR7&jJ9(!f3
	password	5uck0u7	jkH*#lk6L[]2
	secret	d0nkey	pAsSw@Rd!
Force	faible	moyen	fort

Tuyau : Pour un ordinateur standard à double cœur (essayant 10 millions de mots de passe par seconde), il faudrait 23 ans pour craquer un password de 8 caractères utilisant une combinaison de majuscules, minuscules et symboles. Ex : P0k3r$tR

Étape 2 : Avoir Différents Mots de passe

Chaque compte en ligne que vous créez est lié à votre e-mail, faisant de votre password de compte mail le plus important à sécuriser. Si quelqu'un peut accéder à votre boîte mail, il peut accéder à tous vos mots de passe, ou les remettre à 0. C'est pourquoi vous devez avoir au moins 3 passwords:

1 - Password mail　2 - Password compte poker　3 - Password autres sites

Tuyau : Quand vous vous inscrivez sur un site vous devez fournir une adresse mail et un mot de passe. Si vous utilisez le même mot de passe que pour votre mail, vous donnez au propriétaire du site l'accès à toute votre vie en ligne.

Étape 3 : Soyez Vigilant

Ne vous connectez pas sur un ordinateur public

Lancez des scans réguliers contre virus et spywares

Ne laissez pas des inconnus installer des choses sur votre ordinateur

Ne donnez aucune information.
L'assistance d'un site ne vous demandera JAMAIS votre mot de passe.

Allez toujours sur le site via la même méthode (lancer le logiciel ou aller vous-même sur la page du site). N'allez jamais sur une page ni ne vous connectez via un lien dans un e-mail non-sollicité, aussi légitime qu'il puisse sembler.

Tuyau : Presque aucun ordinateur ou compte ne sont réellement "hackés". Un compte compromis est presque toujours le résultat :
- d'un espion (spyware)
- d'un mot de passe trop évident (nom de votre chien)
- d'hameçonnage (phishing), où le voleur vous fait donner votre mot de passe via un faux e-mail ou site web ressemblant à l'original.

Tuyau : Vous pouvez obtenir de bons programmes antivirus et anti-spywares gratuits tels que AVG.

Étape 4 : Encryptez

Le meilleur moyen de vous protéger encore plus est d'ajouter une couche de sécurité, une qui ne peut être volée sur Internet. Certains sites de poker proposent d'utiliser une clé RSA pour vous connecter. Cela demande que vous connaissiez :

1: Votre mot de passe
2: Votre PIN de votre clé RSA
3: Le nombre en cours affiché sur la clé RSA

Ce nombre change automatiquement à chaque minute. Sans cette clé RSA physiquement sous la main, il est impossible de se connecter.

Tuyau : RSA signifie Rivest, Shamir et Adleman, les trois hommes ayant conçu cet algorithme public de cryptage. Avant cette clé RSA, un vrai cryptage était une technologie top secrète réservée à l'armée.

Étape 5 : Ne vous laissez pas duper

Si vous suivez les 4 étapes précédentes, vous pouvez dormir tranquille : vos comptes en ligne sont sécurisés. Malheureusement tout le monde n'est pas aussi vigilant. S'agissant d'informations personnelles, accès de compte ou détails de vos fonds, on n'est jamais trop prudent. Certaines personnes pourtant intelligentes sont déjà tombées dans ce genre de piège :

Comment éviter ce scam : N'envoyer jamais d'argent à quiconque (même un meilleur ami) sans lui parler au téléphone avant. Vérifiez à deux fois.