
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

a. Cyberattaques

Qu'est-ce qu'un rançongiciel ?

Un rançongiciel (Ransomware en anglais) est un **logiciel malveillant** qui bloque l'accès à l'ordinateur ou aux fichiers des victimes et qui leur réclame le paiement d'une rançon pour en obtenir à nouveau l'accès.

Fréquemment, ils chiffrent les fichiers se trouvant sur l'ordinateur de la victime, voire sur des serveurs qui hébergent leurs fichiers. Les victimes sont généralement infectées suite à l'ouverture d'une pièce-jointe infectée, ou après avoir cliqué sur un **lien malveillant** reçus dans des courriels, et parfois simplement en naviguant sur des sites Internet compromis par les cybercriminels. Dans la majorité des cas, les cybercriminels exploitent des vulnérabilités connues dans les logiciels, mais dont les correctifs n'ont pas été mis à jour par les victimes.

Le phishing, c'est quoi ?

L'hameçonnage ou phishing est une forme d'escroquerie sur internet.

Le fraudeur se fait passer pour un organisme que vous connaissez (banque, service des impôts, CAF, etc.), en utilisant le logo et le nom de cet organisme. Il vous envoie un mail vous demandant généralement de "mettre à jour" ou de "confirmer vos informations suite à un incident technique", notamment vos coordonnées bancaires (numéro de compte, codes personnels, etc.).

Qu'est-ce qu'un malware ?

Un malware, ou « logiciel malveillant » est un terme générique qui décrit tous les programmes ou codes malveillants qui peuvent être nocifs pour les systèmes.

Hostiles, intrusifs et intentionnellement méchants, les malwares cherchent à envahir, endommager ou mettre hors service les ordinateurs, les systèmes informatiques, les tablettes ou les appareils mobiles, généralement en prenant le contrôle partiel de leurs opérations. Comme la grippe, ils interfèrent avec le fonctionnement normal.

LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

a. Cyberattaques

ET SUR LE SECTEUR DE LA SANTÉ

- Les incidents de sécurité dans **le secteur de la santé ont doublé en un an**
- Des **centres hospitaliers victimes de cyberattaques** avec demande de rançon: Arles, Dax, Villefranche-sur-Saône et Corbeil-Essonnes
- Découverte d'une cyberattaque massive aux couleurs d'entreprises françaises, dont **l'Assurance Maladie**
- Aux Etats-Unis, une **violation de données concernant les informations de santé** de plus de 69 000 personnes a affecté l'un des principaux régimes et prestataire de soins de santé à but non lucratif

LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

b. Les mots de passes

LES DIX RÈGLES

Utilisez un mot de passe unique pour chaque service	**Choisissez un mot de passe qui n'a pas de lien avec vous**	Ne demandez jamais à un tiers de générer pour vous un mot de passe	Modifiez systématiquement et au plus tôt les mots de passe par défaut
Renouvelez vos mots de passe avec une fréquence raisonnable. Tous les 90-120 jours est un bon compromis pour les systèmes contenant des données sensibles	**Ne stockez pas les mots de passe dans un endroit facilement accessible (fichier, post it, …)**	**Ne vous envoyez pas vos propres mots de passe sur votre messagerie personnelle**	Configurez les logiciels, y compris votre navigateur web, pour qu'ils ne se « souviennent » pas des mots de passe choisis

La robustesse d'un mot de passe dépend en général d'abord de sa complexité, mais également de divers autres paramètres.
Une règle simple : choisissez des mots de passe **d'au moins 12 caractères de types différents** (majuscules, minuscules, chiffres, caractères spéciaux).

Deux méthodes pour choisir vos mots de passe :
La méthode phonétique : « J'ai acheté huit cd pour cent euros cet après-midi » deviendra **ght8CD%E7am** ;
La méthode des premières lettres : la citation « un tien vaut mieux que deux tu l'auras » donnera **1tvmQ2tl'A**.

LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

b. Les mots de passes

NOMBRE DE CARACTÈRES	UNIQUEMENT DES CHIFFRES	LETTRES MINUSCULES	LETTRES MINUSCULES ET MAJUSCULES	LETTRES MINUSCULES ET MAJUSCULES + CHIFFRES	LETTRES MINUSCULES ET MAJUSCULES + CHIFFRES + CARACTÈRES SPECIAUX
4	IMMÉDIATEMENT	IMMÉDIATEMENT	IMMÉDIATEMENT	IMMÉDIATEMENT	IMMÉDIATEMENT
6	IMMÉDIATEMENT	IMMÉDIATEMENT	IMMÉDIATEMENT	1 sec	5 sec
8	IMMÉDIATEMENT	5 sec	22 min	1 heure	9 heures
10	IMMÉDIATEMENT	58 min	1 mois	7 mois	5 ans
12	45 sec	3 semaines	300 ans	2000 ans	34 000 ans
14	41 min	51 ans	800 000 ans	9 millions d'années	200 millions d'années

*source : SCSP Community (Seasoned Cyber Security Professionnals)

LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

b. Les mots de passes

LA GESTION DES MOTS DE PASSE ET DES ACCÈS

Un mot de passe est personnel, je ne le communique jamais

Choisir des mots de passe complexes

Changer régulièrement mes mots de passe

Privilégier la double authentification (MFA) quand c'est possible

Mot de passe oublié ?
Mot de passe à changer ?
Configurer le Self-Service

Ordre National des Médecins
Conseil National de l'Ordre