BUREAU PROPRE

PLACE NETTE AVANT DE LEVER L'ANCRE

En quittant mon espace de travail, je mets en sécurité mes documents et je ne laisse rien traîner sur mon bureau !

Gare à la fuite de données si vous laissez traîner un dossier patient imprimé ou une facture fournisseur sur votre bureau. Prenez également garde aux informations que vous notez sur des post-it ! Avec tous les efforts que vous faites pour sécuriser vos postes de travail et vos données numériques, il serait dommage de laisser trainer ces mêmes informations au format papier sur votre bureau ou en sortie d'imprimante.

CAPSI

Cellule d'Appui à la Protection des Systèmes d'Information

CARTES CPS

PRÊTERIEZ-VOUS VOTRE CARTE BANCAIRE ?

Accordons la même protection à nos cartes professionnelles de santé (CPS, CPE et CPA) qu'à notre carte bancaire !

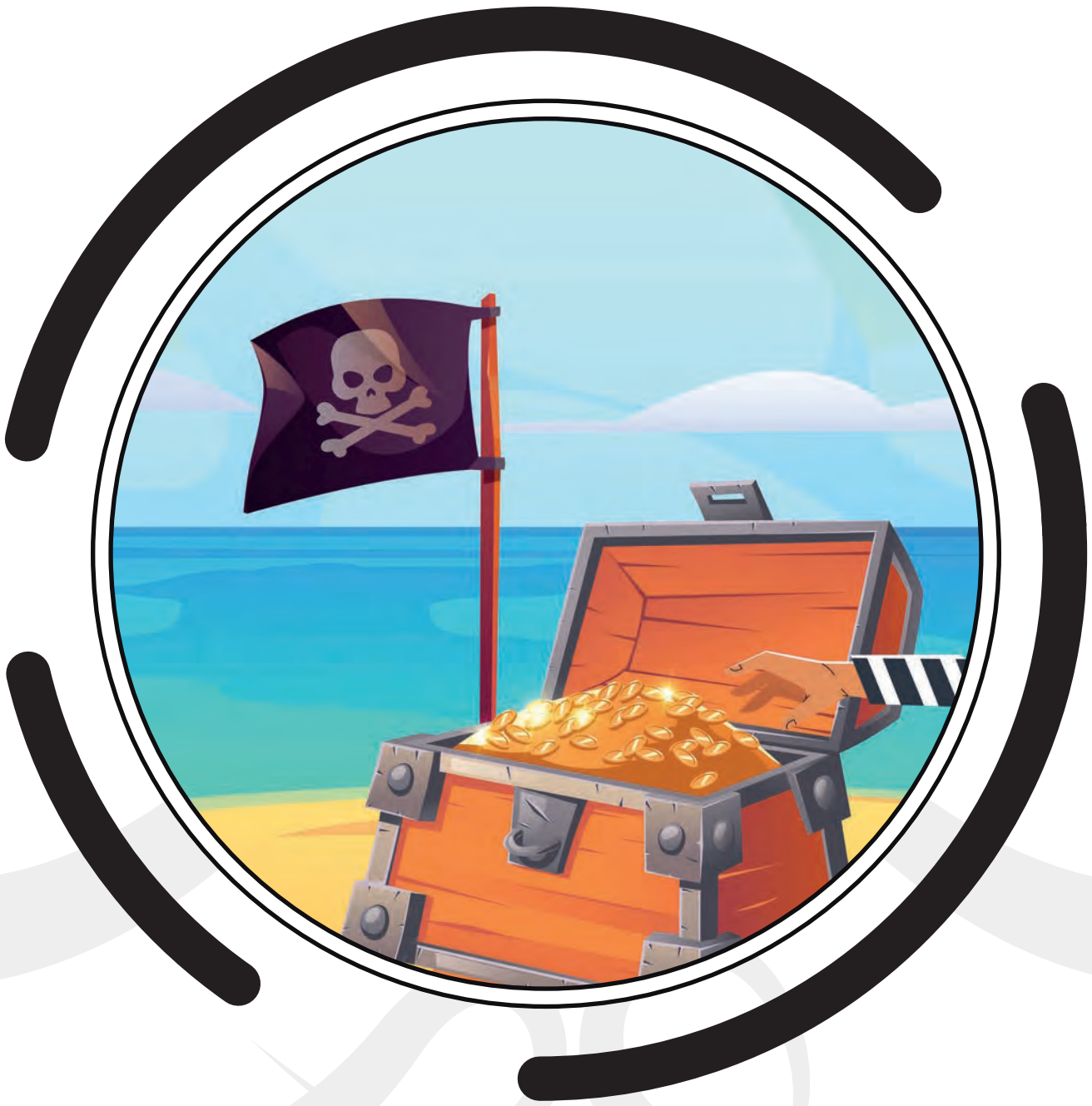
Les cartes professionnelles de santé donnent accès à des données sensibles. Elles sont nominatives et engagent notre responsabilité. Ne laissez pas votre code PIN traîner vers votre poste de travail et ne le confiez à personne !

CAPSI

Cellule d'Appui à la Protection des Systèmes d'Information

VEROUILLER SA SESSION

Laisseriez-vous votre coffre à trésors ouvert et sans surveillance ?



Vos comptes utilisateurs permettent l'accès à des données sensibles.
Ne laissez pas votre session déverrouillée sans surveillance !

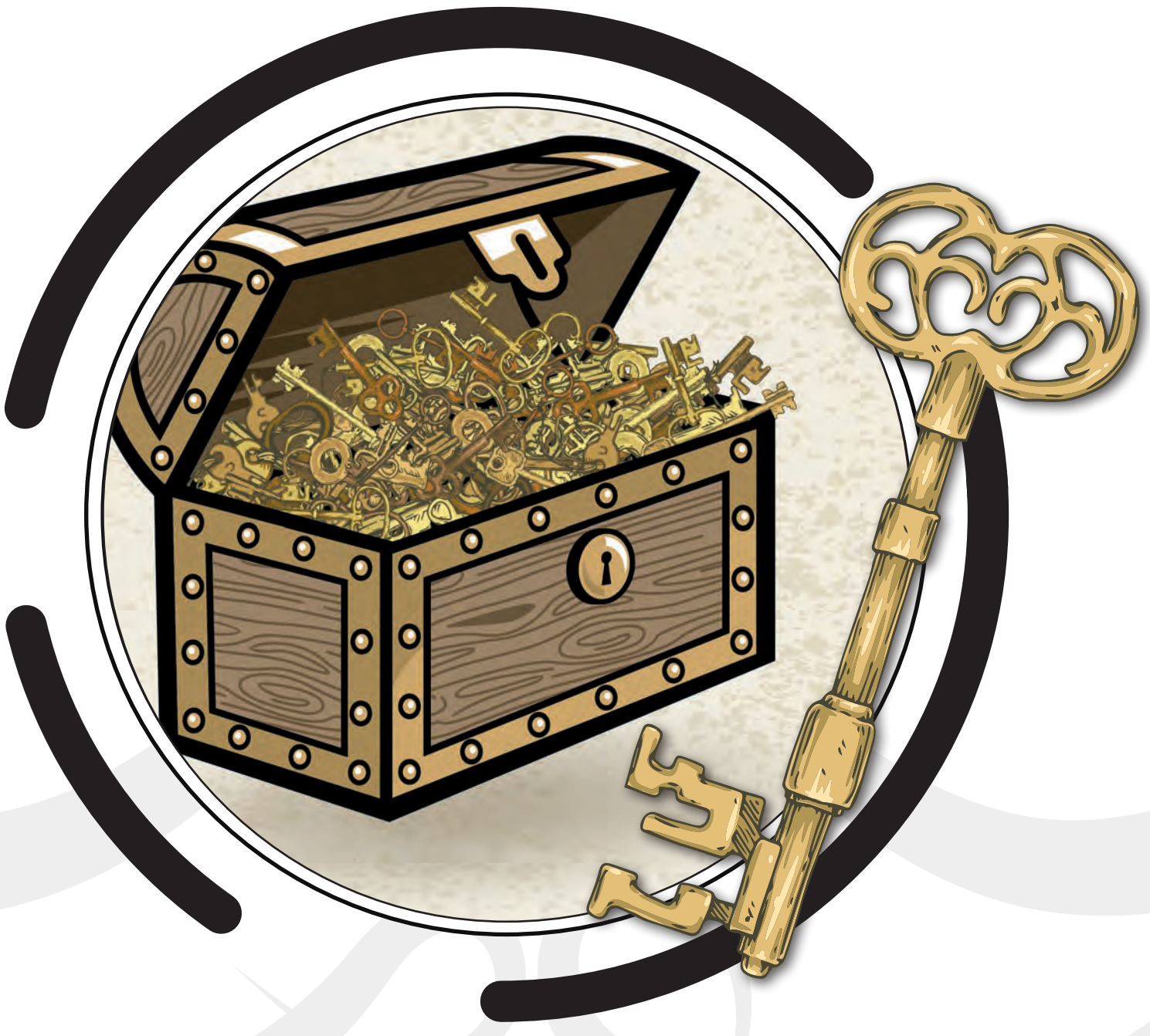
Laisser votre session déverouillée lorsque vous quittez votre poste de travail revient à rendre inutile toutes les mesures techniques visant à sécuriser l'accès à vos données. Même si vous pensez être dans un environnement de confiance, le vol et la détérioration de données peuvent arriver très vite. Ce serait dommage que cela arrive uniquement parce que vous n'avez pas verrouillé votre session.

CAPSI

Cellule d'Appui à la Protection des Systèmes d'Information

GESTIONNAIRE DE MOTS DE PASSE

UNE SEULE CLÉ À NE PAS OUBLIER



Tous vos mots de passe compliqués dans un coffre fort sécurisé, pour protéger vos accès !

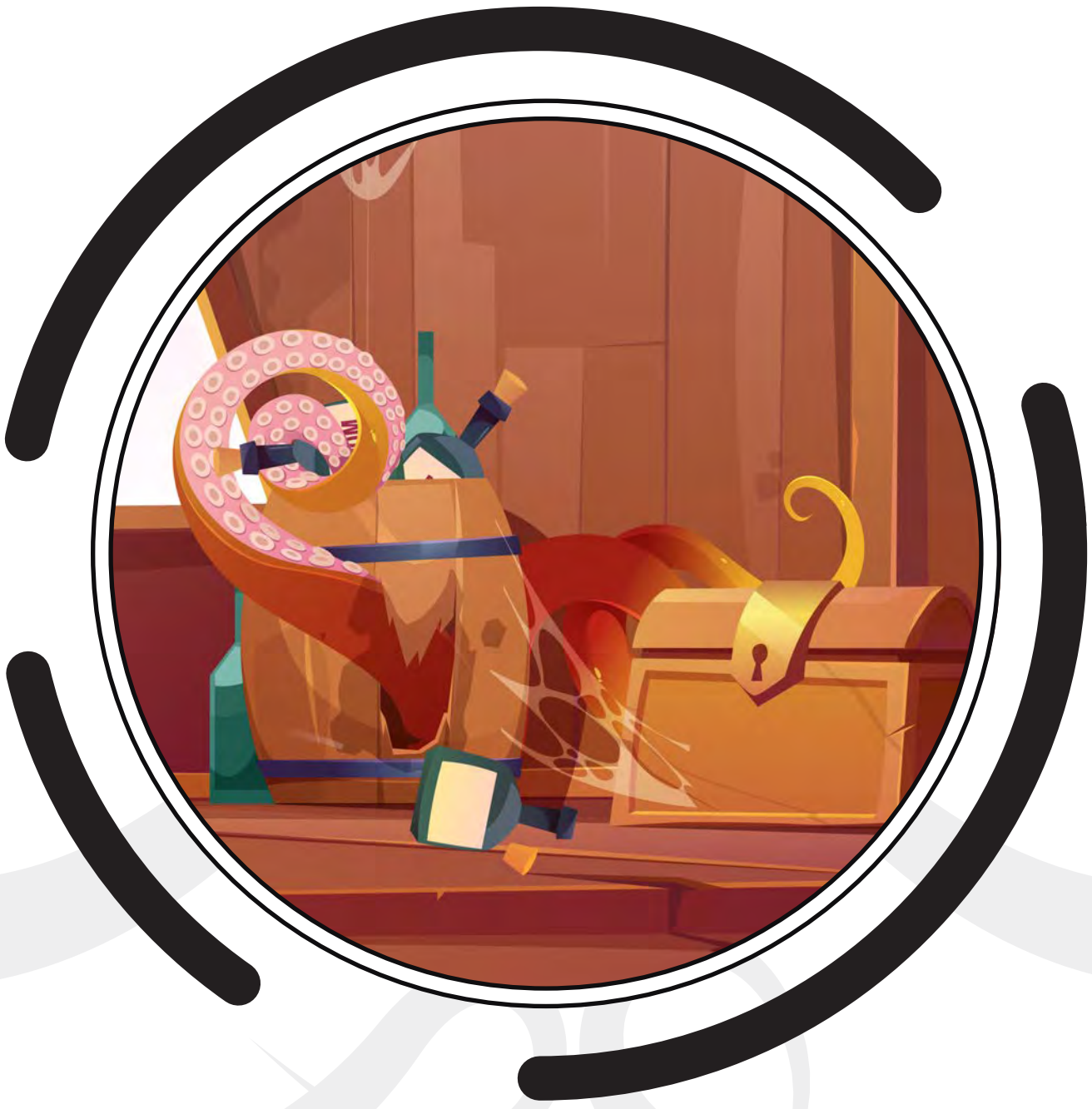
Un gestionnaire de mots de passe est un coffre fort numérique à l'aide duquel vous pouvez générer et mémoriser tous vos mots de passe. L'avantage : vous n'avez qu'un seul mot de passe robuste à protéger et à retenir. Par exemple, Keepass est un gestionnaire de mot de passe gratuit.

CAPSI

Cellule d'Appui à la Protection des Systèmes d'Information

MALWARE

ÉVITEZ TOUT PASSAGER INDÉSIRABLE À BORD



Gardez le contrôle et ne cliquez que sur des pièces jointes ou des liens dont vous êtes sûrs

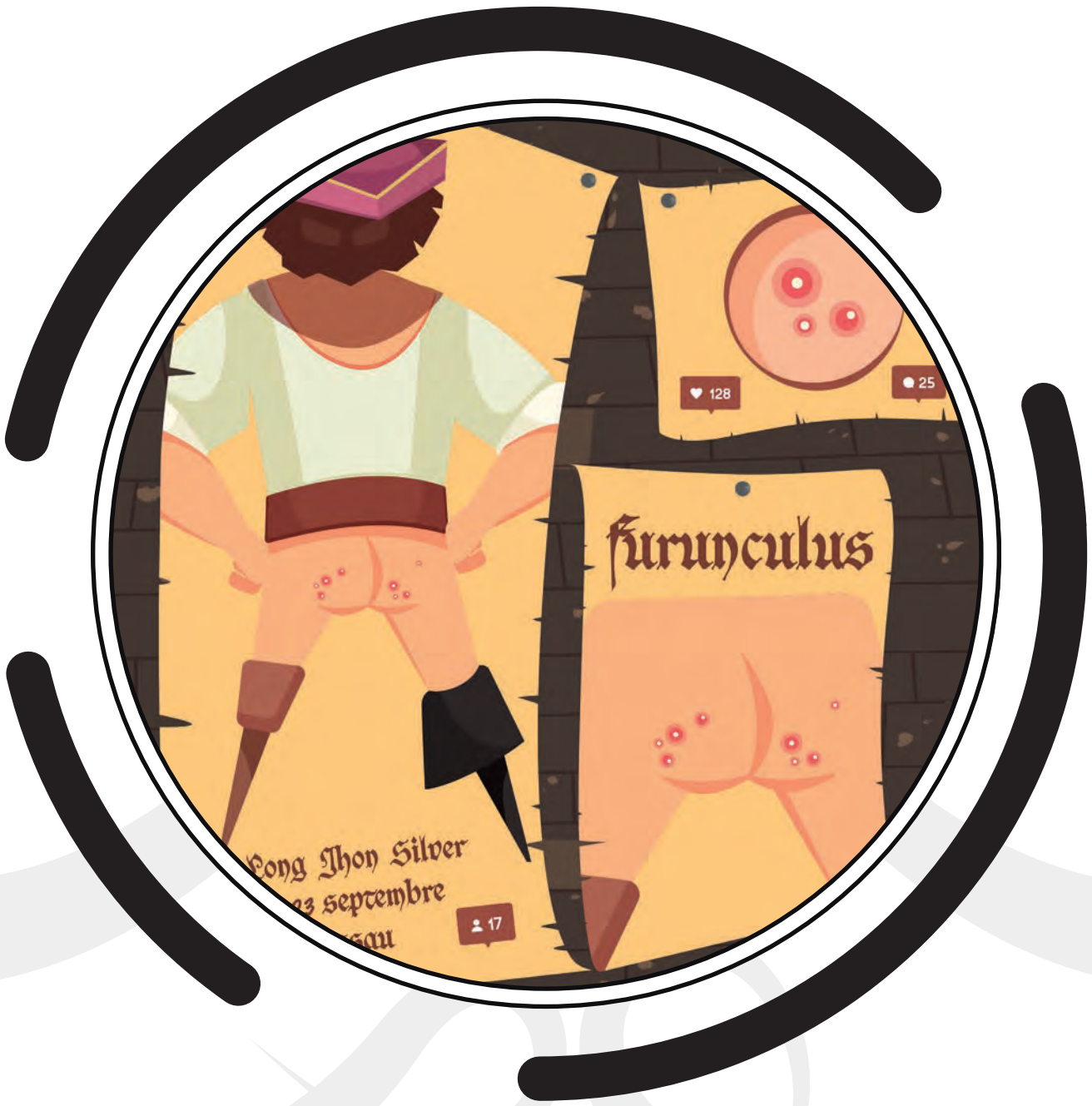
Plus de 300 000 nouveaux virus sont diffusés chaque jour sur internet, votre antivirus ne vous protégera pas à tous les coups ! C'est à vous d'être vigilant et ne pas télécharger ou ouvrir des pièces-jointes suspectes afin d'éviter d'être compromis par un virus ou un logiciel malveillant cherchant à prendre le contrôle de votre machine et de vos données.
De façon générale, n'ouvrez pas une pièce-jointe d'un expéditeur qui vous est inconnu. Et quand bien même la pièce-jointe semble être envoyée par l'un de vos contacts, il peut également s'agir d'un piège, ne vous faites pas avoir !

CAPSI

Cellule d'Appui à la Protection des Systèmes d'Information

RÉSEAUX SOCIAUX

NE DIVULGUEZ PAS TOUS VOS SECRETS À VOTRE ÉQUIPAGE



Partager vos données patients sur les réseaux sociaux, c'est comme les afficher dans la rue !

Les réseaux sociaux ne sont pas des espaces sécurisés sur lesquels vous pouvez stocker des informations professionnelles. Restez prudent et ne divulguez pas des données sensibles ou professionnelles sur les réseaux sociaux.

CAPSI

Cellule d'Appui à la Protection des Systèmes d'Information

URL

Vérifiez vos sources avant de partir à la chasse au trésor

Avant de cliquer sur un lien, vérifiez sa légitimité. Il s'agit peut-être d'une arnaque !

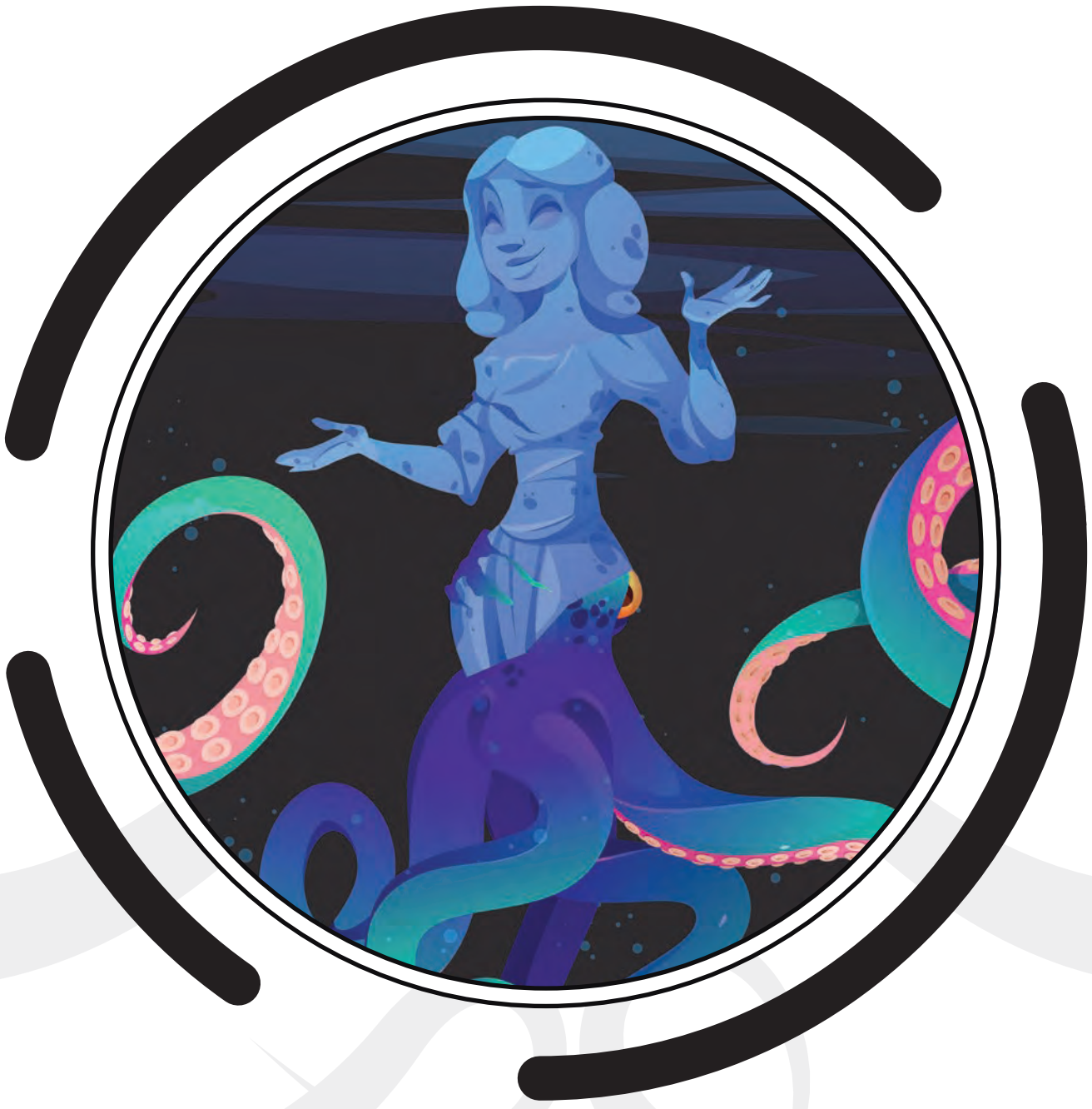
Avant de cliquer sur un lien, votre premier réflexe doit être de survoler ce lien afin de vérifier la destination réelle. En effet, les arnaques sur internet passent souvent par l'envoi d'un lien frauduleux et si vous n'êtes pas vigilant avant de cliquer, vous pourriez mettre en danger vos données et celles de votre entreprise.

CAPSI

Cellule d'Appui à la Protection des Systèmes d'Information

USURPATION D'IDENTITÉ

ASSUREZ-VOUS DE L'IDENTITÉ DE VOTRE INTERLOCUTEUR.



L'habit ne fait pas le moine : restez vigilant aux risques d'usurpation d'identité aussi bien dans votre vie professionnelle que personnelle

Des individus malveillants peuvent vous mettre dans une situation de stress ou d'urgence et vous demander des actions inhabituelles comme par exemple le fait d'effectuer un virement d'argent important en se faisant passer pour votre directeur ou président. Dans cette arnaque, l'arnaqueur utilise un rapport d'autorité pour vous inciter à réaliser l'action sans vous laisser le temps de faire les vérifications habituelles. Gardez votre sang froid, calmez le jeu et éliminez les doutes en vérifiant l'information auprès d'une autre personne et référez-vous à vos procédures avant toute action.

CAPSI

Cellule d'Appui à la Protection des Systèmes d'Information

CLÉ USB

Un petit objet qui peut vous faire très mal

Une clé USB trouvée ou reçue en cadeau ?
Ne la branchez surtout pas à votre ordinateur professionnel, vous pourriez mettre en danger vos données et celles de votre entreprise.

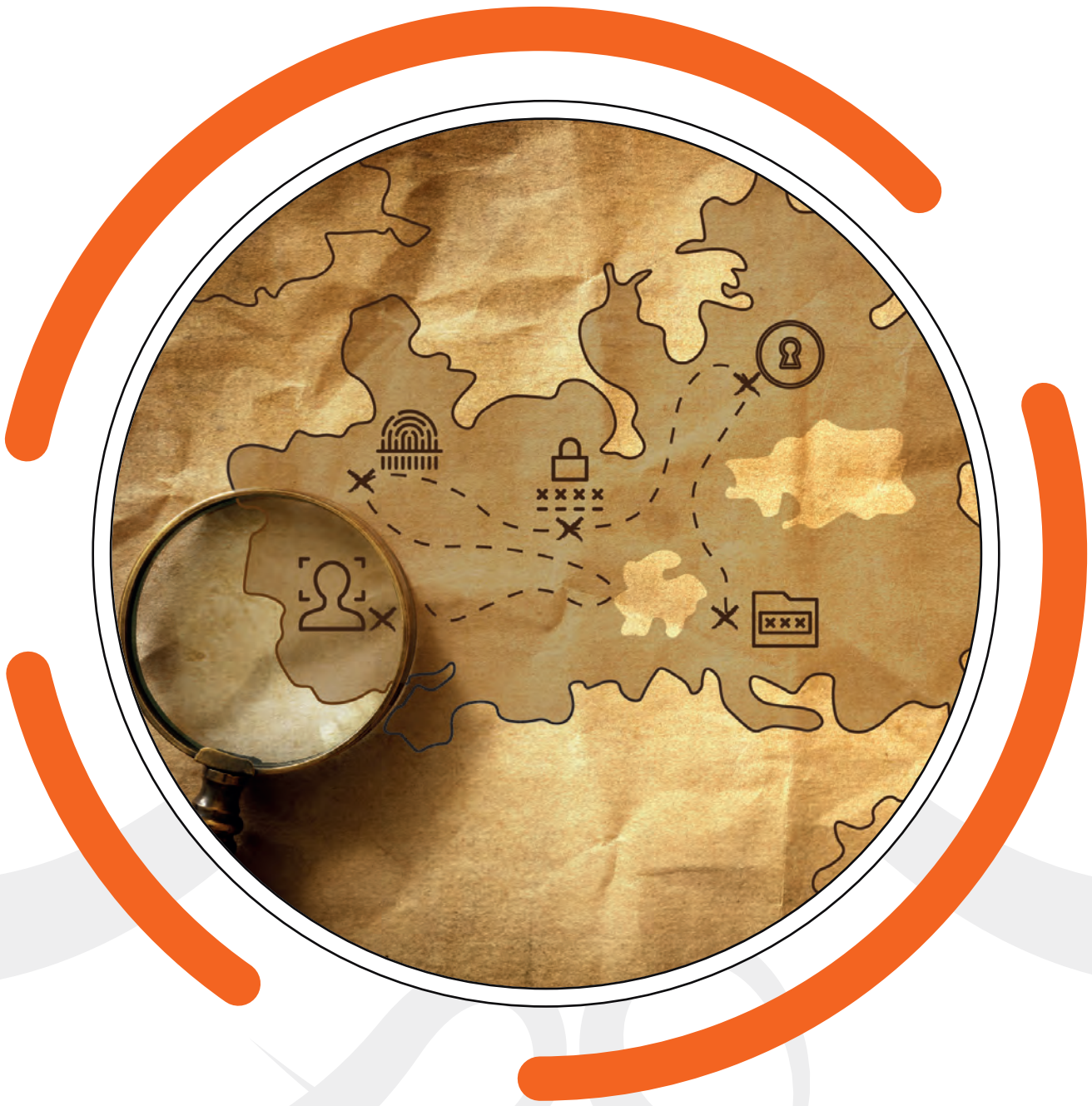
Ne branchez aucun support de stockage USB qui n'a pas été fourni par votre entreprise sur votre ordinateur professionnel. Une clé USB trouvée ou que l'on vous aurait offerte peut contenir un virus ou être une clé dédiée à l'attaque, ce qui mettrait en danger vos données (destruction, corruption ou vol). Votre clé ou disque USB personnel peut également être un vecteur de diffusion d'un virus au sein de votre entreprise. Ne prenez pas ce risque !

CAPSI

Cellule d'Appui à la Protection des Systèmes d'Information

DONNÉES À CARACTERE PERSONNEL

LE MYSTÈRE DES DONNÉES À CARACTÈRE PERSONNEL



Une "donnée personnelle" est "toute information se rapportant à une personne physique identifiée ou identifiable".

Une personne peut être identifiée :

- directement (exemple : nom, prénom) ;
- ou indirectement (exemple : par un identifiant (n° client), un numéro (de téléphone), une donnée biométrique, plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi la voix ou l'image).

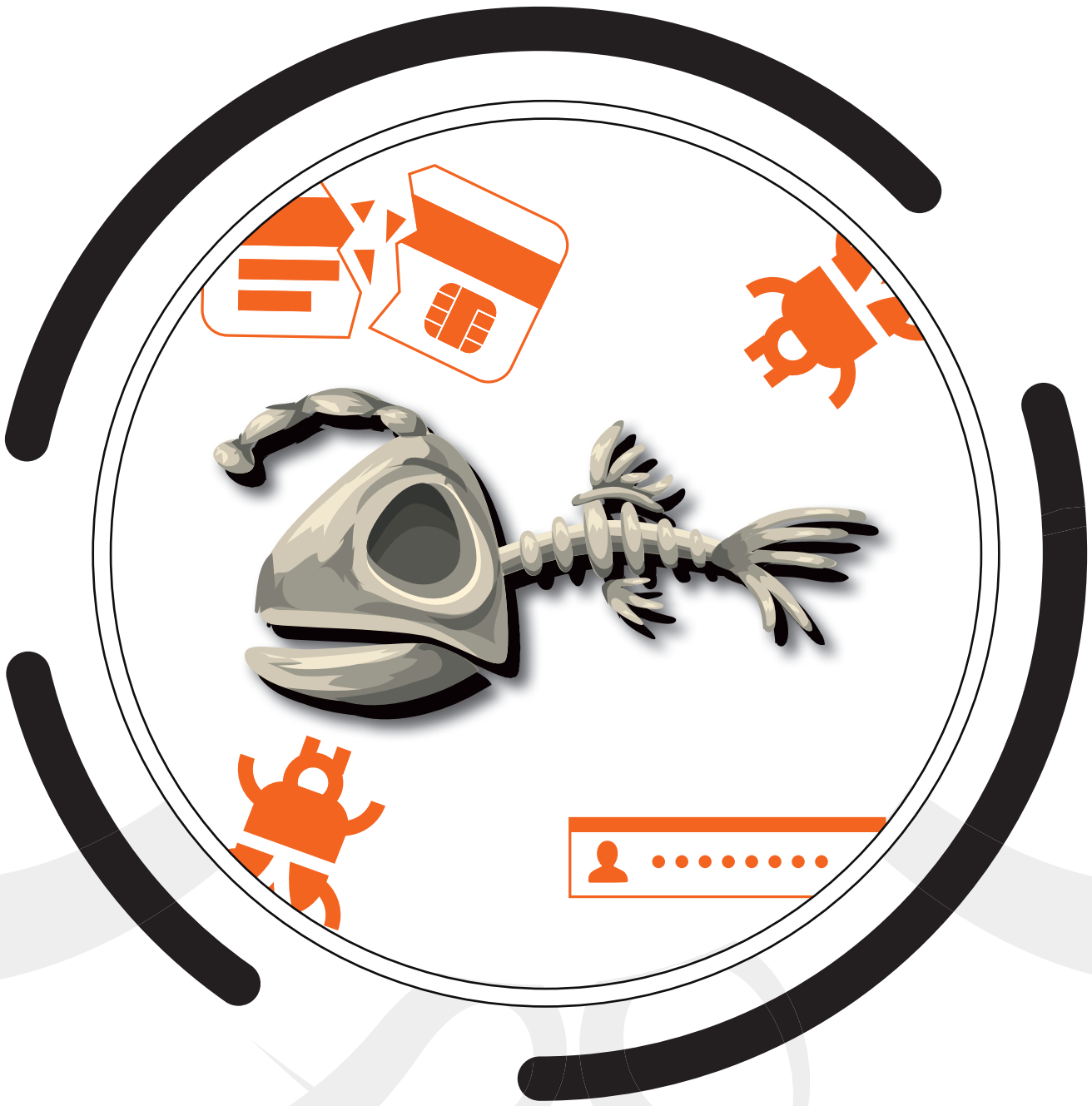
L'identification d'une personne physique peut être réalisée :

- à partir d'une seule donnée (exemple : numéro de sécurité sociale, ADN) ;
- à partir du croisement d'un ensemble de données (exemple : une femme vivant à telle adresse, née tel jour, abonnée à tel magazine et militant dans telle association).

CAPSI
Cellule d'Appui à la Protection des Systèmes d'Information

HAMEÇONNAGE

ÂME SENSIBLE S'ABSTENIR. VOICI UNE VICTIME DE L'HAMEÇONNAGE



L'hameçonnage est une technique par laquelle un attaquant va essayer d'obtenir illégalement des infomations ou de vous faire réaliser des actions contre vous ou votre entreprise.

L'objectif du hameçonnage *(phishing)* est généralement de vous dérober des données (identifiants de connexion, mots de passe, données bancaires...) ou de vous faire réaliser des actions comme l'installation d'un logiciel malveillant. La forme la plus connue pour ces attaques est l'e-mail mais vous pouvez également être ciblés via d'autres supports : SMS, appel téléphonique, fausse publicité, messagerie instantannée...
Soyez toujours attentifs aux détails et ne réagissez jamais dans l'urgence : êtes-vous certain de l'identité de la personne vous contactant ? Le style d'écriture correspond-il à l'émetteur ? Le message est-il suspect ? La demande est-elle inhabituelle ? Le lien est-il correct ?
En cas de doute, ne cliquez pas, ne donnez aucune information et contactez votre support informatique.

CAPSI

Cellule d'Appui à la Protection des Systèmes d'Information

TRAITEMENT DES DONNÉES PERSONNELLES

LE TRAITEMENT DES DONNÉES PERSONNELLES

Un "traitement de données personnelles" est une opération, ou ensemble d'opérations, portant sur des données personnelles, quelle que soit l'action réalisée (collecte, enregistrement, organisation, structuration, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission, diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, limitation, effacement ou destruction).

Un traitement de données doit avoir un objectif (une finalité) bien identifié, c'est-à-dire que vous ne pouvez pas collecter ou traiter des données personnelles simplement au cas où cela vous serait utile un jour. L'objectif poursuivi, doit, bien évidemment, être fondé sur une base juridique en lien avec votre activité professionnelle.

Un traitement de données personnelles n'est pas nécessairement informatisé : les fichiers papier sont également concernés et doivent être protégés dans les mêmes conditions.

CAPSI
Cellule d'Appui à la Protection des Systèmes d'Information

WI-FI PUBLIC

ATTENTION ! VOUS ENTREZ DANS UNE ZONE DANGEREUSE

En vous connectant à un point d'accès Wi-Fi public (hôtel, restaurant, train, aéroport...), vous prenez le risque de vous faire dérober très facilement vos informations de connexion et vos données personnelles ou professionnelles. Utilisez plutôt le partage de connexion de votre téléphone lorsque c'est possible.

Il est très facile pour un pirate de créer un faux point d'accès Wi-Fi public ressemblant en tout point à un véritable point d'accès. Vous n'avez aucun moyen de vous assurer que l'accès est bien légitime et même si c'est le cas, vous n'avez aucune garantie qu'un pirate n'est pas déjà à l'écoute sur le point d'accès. Lorsque c'est possible, un partage de connexion via votre téléphone vous permettra de vous affranchir de devoir vous connecter à un point d'accès public. Si ce n'est pas possible, d'autres solutions techniques sont à envisager : mise à disposition d'un modem 4G par votre entreprise lors de vos déplacements ou installation d'un tunnel VPN vers votre entreprise afin de sécuriser les échanges lorsque vous vous connectez sur un accès public.

CAPSI

Cellule d'Appui à la Protection des Systèmes d'Information

COMPTES UTILISATEURS GÉNÉRIQUES

QUI A MODIFIÉ LE DOSSIER DU PATIENT ?

Utiliser un compte générique ne permet pas d'assurer la traçabilité de l'information de santé ou de toute information sensible. Évitons autant que possible leur utilisation !

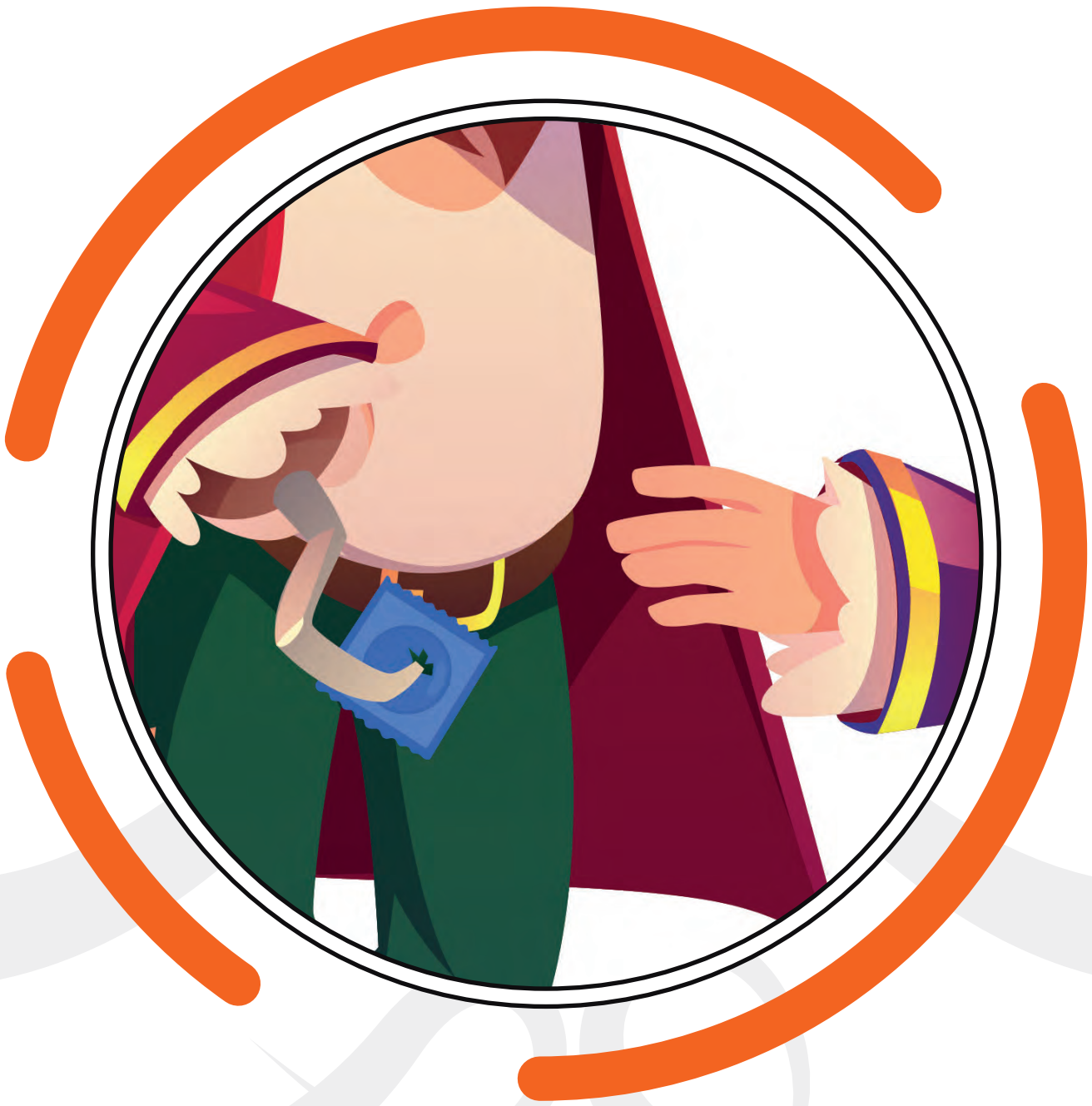
L'usage de comptes génériques n'est jamais une bonne solution. En effet, seuls les comptes nominatifs et individuels sont en mesure de garantir une traçabilité suffisante dans nos applications. Alors essayons autant que possible de limiter leur utilisation à des cas très spécifiques.

CAPSI

Cellule d'Appui à la Protection des Systèmes d'Information

MOTS DE PASSE

Est-ce que vous réutiliseriez un préservatif usagé ?



Un mot de passe, c'est comme un préservatif : vous ne pouvez l'utiliser qu'une seule fois, il doit être robuste et vous ne devez pas le prêter !

Lorsque vous choisissez un nouveau mot de passe, quelques règles simples doivent être respectées afin de ne pas mettre vos données en danger :

- Utilisez un mot de passe différent pour chaque accès en ligne ;
- Choisissez des mots de passe suffisamment longs et complexes (impossibles à deviner) ;
- Ne communiquez jamais votre mot de passe à un tiers ;
- Au moindre doute, changez votre mot de passe ;
- Activez systématiquement la double authentification lorsque cela est possible ;
- Et utilisez un gestionnaire de mots de passe pour être tranquille !

CAPSI

Cellule d'Appui à la Protection des Systèmes d'Information