LA SÉCURITÉ DU NUMÉRIQUE

À PORTÉE DE CLIC

TABLE DES MATIÈRES

INTRODUCTION

La cybersécurité consiste à protéger les systèmes, les réseaux et les programmes contre les attaques numériques.

L'IMPORTANCE DE LA CYBERSÉCURITÉ

La cybersécurité est importante car elle protège les données et l'intégrité des actifs numériques contre les menaces en constante évolution.

Avec la dépendance croissante à la technologie, la cybersécurité est devenue cruciale pour maintenir la confidentialité, l'intégrité et la disponibilité de l'information.

MÉTHODES DE PROTECTION DE LA CYBERSÉCURITÉ :

Voici quelques méthodes clés pour se protéger contre les cybermenaces :

Wi -Fi / Clé USB

Que ca soit sans contact ou avec contact ne laisser jamais rien vous pénétrer

Mots de passe / A2F

Adopter une politique de mot de passe robuste et moins deux formes de vérification

identité numérique

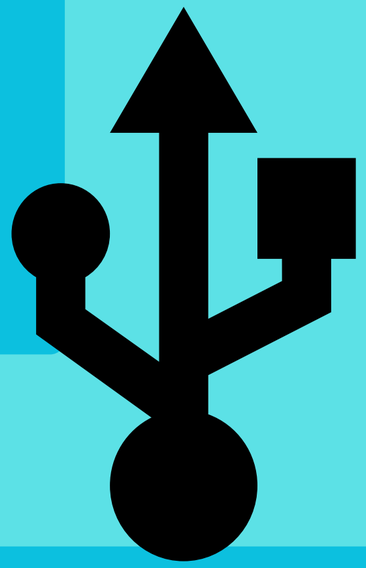
Sécuriser vos données c’est sécuriser votre vie

COMMENT SÉCURISER SON ACCÈS WIFI ?

- Utiliser des mots de passe fort
- Mise à jour des protocoles de sécurité
- Utiliser un VPN pour les wifi publics
- N’activer la Wi-Fi que lorsqu’elle celle-ci doit être utilisée

COMMENT SE PROTÉGER DES ATTAQUES VIA CLÉ USB ?

- Installez et mettez à jour des logiciels **antivirus** capables de scanner les périphériques USB pour détecter les malwares.
- Attention aux chargeurs USB : Évitez d'utiliser des chargeurs USB inconnus. Utilisez des câbles bloqueurs de transfert de données.
- Distinguez les clés USB **personnelles** et les clés USB **professionnelles**
- Si vous ne connaissez pas l'origine d'une clé USB, **ne l'utilisez pas !!**
- Changez vos clés de temps en temps
- **Nettoyez** régulièrement vos clés en les formatant (clic droit puis formater)
- **Désactivez** les fonctions d'exécution automatique



MOTS DE PASSE:
FAITES PREUVE D'IMAGINATIONS

Pour améliorer votre sécurité, suivez ces bonnes pratiques :

- 10 caractères minimum, favoriser les phrases ou une suite de caractères illogique
- Jeu de caractères variés, dispatché sur toute la longueur
- Eviter les rapports psychosociaux et professionnel
- Bannir tout mot issu du dictionnaire
- Double authentification
- Un mot de passe différent/site
- Coffre fort de mots de passe à privilégier

TESTEZ VOS MOTS DE PASSE SUR

BEE-SECURE.LU

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

HIVE SYSTEMS

› Learn how we made this table at hivesystems.io/password

LES RISQUES LIÉS AUX MOTS DE PASSE

- Divulgation par négligence
- Divulgation suite à un acte de malveillance (attaque directe ou indirecte):
  - Force Brute
  - Par dictionnaire/permutation
  - Via keylogger
  - Attaque distribuée
  - De proximité

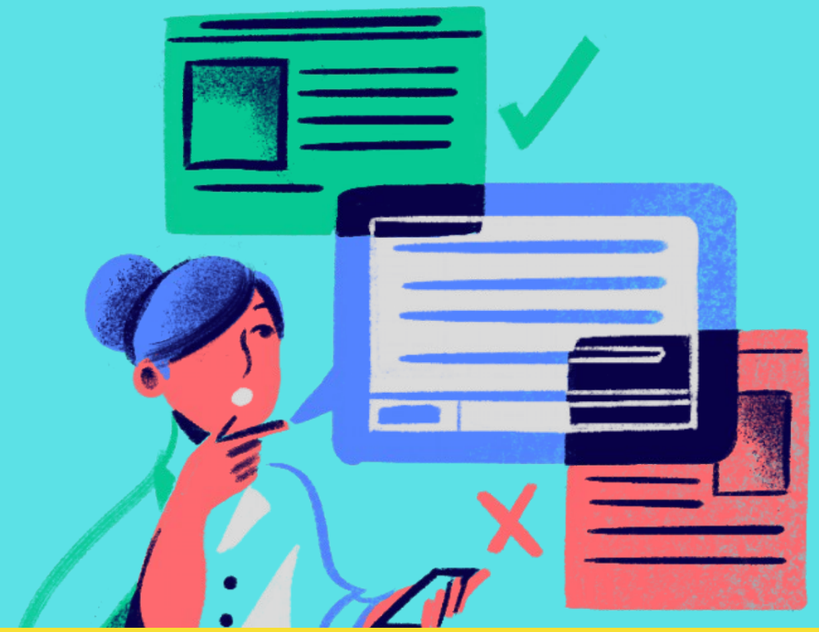
PROTÉGER SON IDENTITÉ NUMÉRIQUE ?

- Limiter les informations partagées
- Contrôler les paramètres de confidentialité / de visibilité
- Éviter de renseigner des données sensibles sur des sites non fiables (formulaires...)
- Eviter les réseaux publics et favoriser les réseaux Wi-Fi protégés
- Bloquer les cookies

MESSAGERIE : MÉFIEZ VOUS DES APPARENCES

QUELS SONT LES RISQUES LIÉS À LA MESSAGERIE

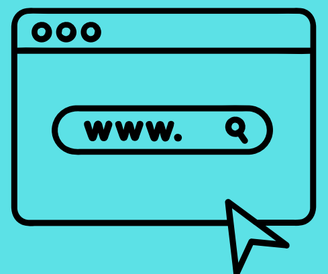
- Hameçonnage (phishing) : technique destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles.
- Virus
- Fraudes pour recueillir des informations



COMMENT DÉTECTER UN COURRIEL SUSPECT ?

- Les incohérences de fond : expéditeur inconnu, demandes d'informations sensibles
- Les incohérences de forme : fautes d’orthographe, mise en page étrange, liens suspects, adresses suspectes

DIFFERENTS TYPES DE PHISHING



Le smishing est un message texte envoyé à votre téléphone d'une manière qui vous met à l'aise pour partager des informations personnelles.

Aujourd'hui, la poste vous apporte un colis.

la poste <noreply@xyz542.be>
To YOU

4 septembre à 8 h 29

Bonjour,

BOLSY vous a envoyé un colis portant la référence 3232000179598199566320 40. La poste vous le livrera aujourd'hui entre 8 h et 17 h. Nous espérons que vous serez présent.

Vous pouvez consulter le statut de votre colis via notre application track & trace. Si vous ne parvenez pas à ouvrir le lien, veuillez télécharger notre outil pour suivre votre colis en direct.

Sincères salutations,
La poste.

Annexe à l'e-mail

Reply Reply to All Forward ••• More

Aujourd'hui, la poste vous apporte un colis.

la poste <noreply@xyz542.be>
To YOU

4 septembre à 8 h 29

la poste

Bonjour,

BOLSY vous a envoyé un colis portant la référence 3232000179598199566320 40. La poste vous le livrera aujourd'hui entre 8 h et 17 h. Nous espérons que vous serez présent.

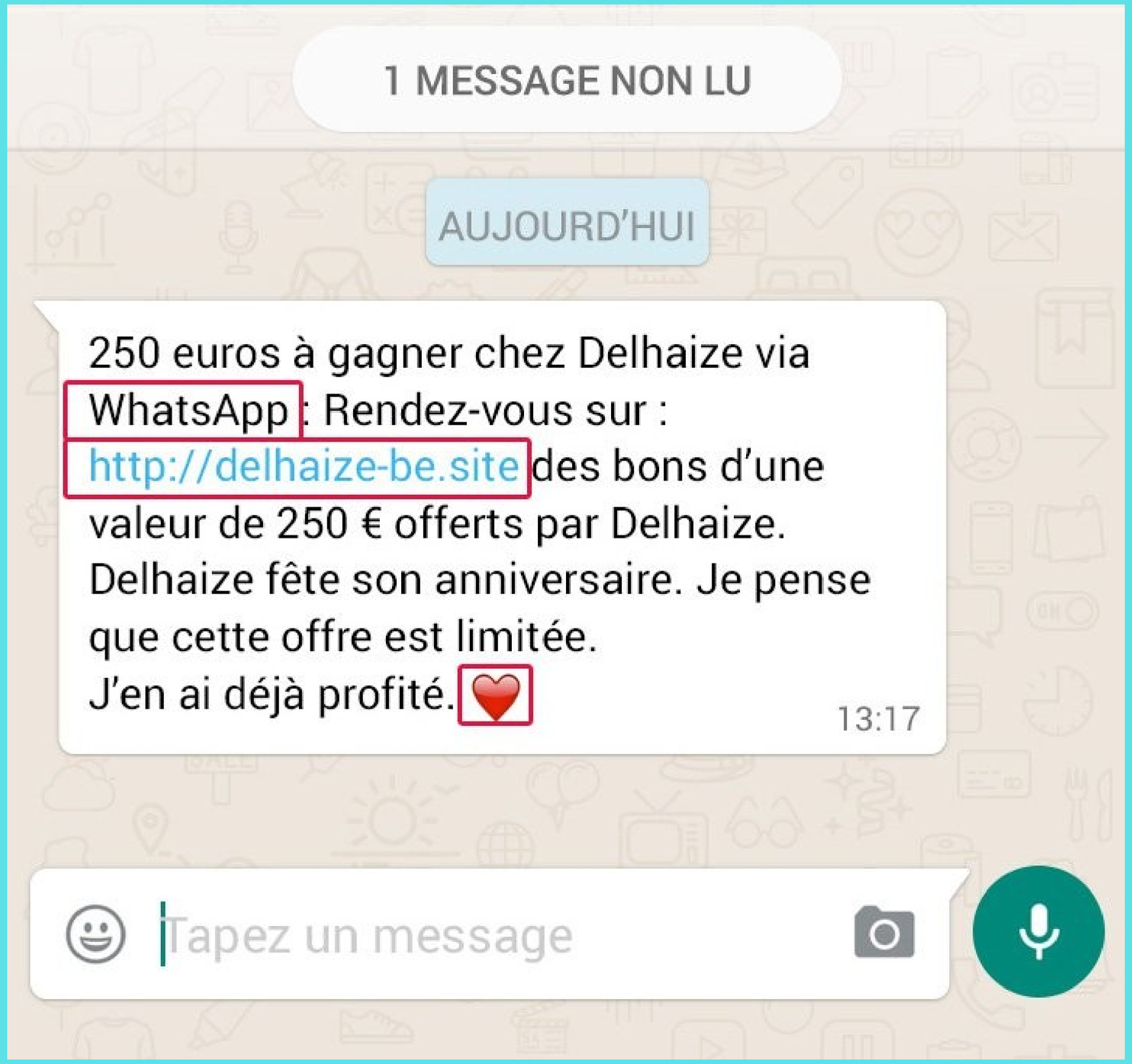
Vous pouvez consulter le statut de votre colis via notre application track & trace. Si vous ne parvenez pas à ouvrir le lien, veuillez télécharger notre outil pour suivre votre colis en direct.

Sincères salutations,
La poste.

Annexe à l'e-mail

Reply Reply to All Forward ••• More


1 MESSAGE NON LU
AUJOURD'HUI
250 euros à gagner chez Delhaize via WhatsApp : Rendez-vous sur : http://delhaize-be.site des bons d'une valeur de 250 € offerts par Delhaize. Delhaize fête son anniversaire. Je pense que cette offre est limitée.
J'en ai déjà profité. ❤️
13:17
Tapez un message


1 MESSAGE NON LU
AUJOURD'HUI
250 euros à gagner chez Delhaize via WhatsApp : Rendez-vous sur : http://delhaize-be.site des bons d'une valeur de 250 € offerts par Delhaize. Delhaize fête son anniversaire. Je pense que cette offre est limitée.
J'en ai déjà profité.
13:17
Tapez un message

TF1+

de: info@tf11.fr

Bonjour,

Votre mot de passe est erroné, veuillez modifier celui-ci en cliquant sur le lien ci dessous.

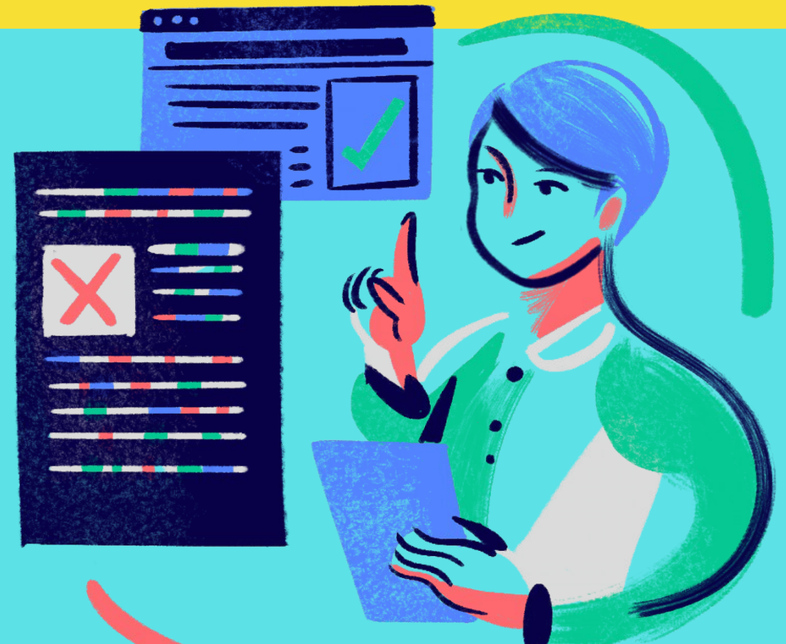
Vous pouvez le consulter ci-dessous :

CHANGER VOTRE MOT DE PASSE

Merci pour votre compréhension, pour tout aide contacter suppot@amazon.fr

COMMENT RÉAGIR FACE À UN COURRIEL SUSPECT ?

- Ne pas répondre ou cliquer sur les liens
- Signaler le courriel comme spam ou hameçonnage
- Supprimer le courriel suspect
- Informer ses contacts en cas de piratage



LES BONNES PRATIQUES A AVOIR !

- Utiliser des mots de passe forts et les changer régulièrement
- Utiliser des filtres anti-spams : les boites mails comme Gmail ou Outlook les appliquent déjà.
- Vérifier l’authenticité de l’expéditeur avant de répondre

ORDINATEURS, TÉLÉPHONES PORTABLES, TABLETTES : MÊME COMBAT !

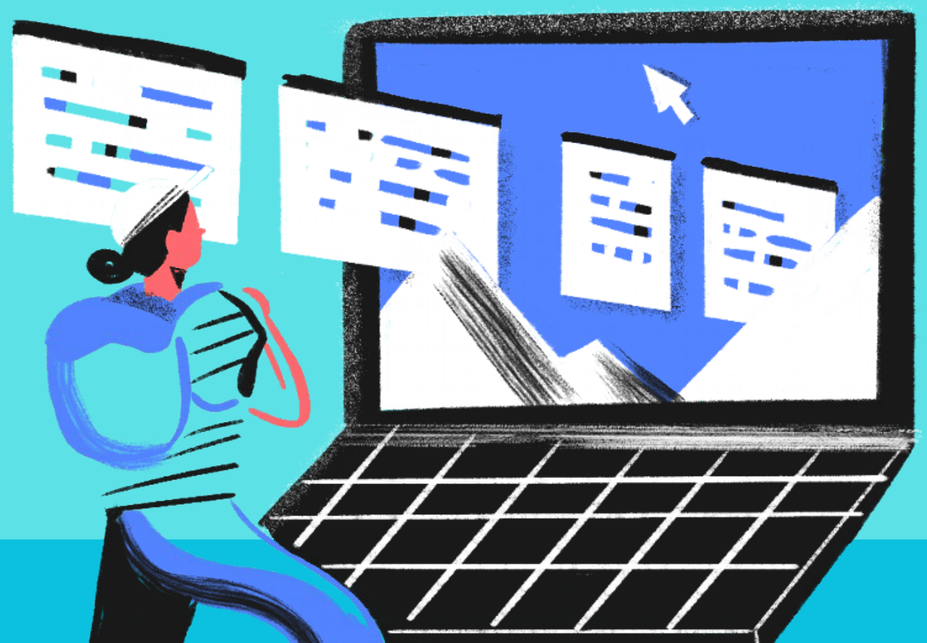
- Activer le verrouillage automatique et les codes d'accès
- Installer les mises à jour
- Activer son pare-feu
- Faire des sauvegardes
- Vérifiez les autorisations de ses applications
- Ne pas laisser son appareil sans surveillance
- Conserver le code IMEI de son appareil
- Ne pas stocker d'informations confidentielles sans protection
- Signaler la perte de son téléphone professionnel

LES ATTAQUES COURANTES

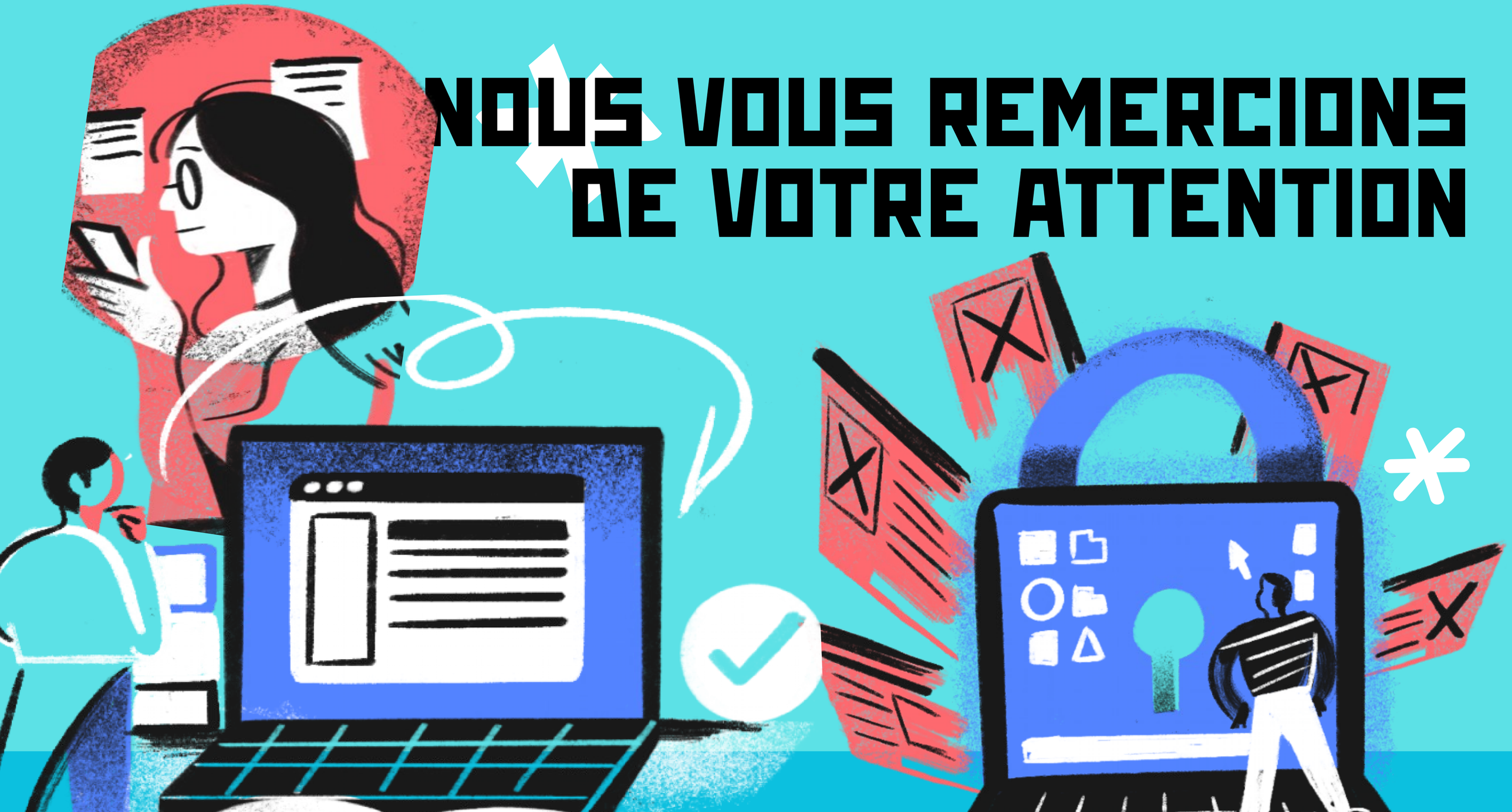
- Attaques par mot de passe
- Attaques par logiciels malveillants
- Ransomwares (logiciel de rançons)
- Attaques Zero Day
- Attaques par hameçonnage

CONCLUSION

Utilisez des mots de passes robustes et variés
- Gardez vos appareils/logiciels à jour
- Utilisez des méthodes de paiement sécurisées
- Ne jamais connecter un équipement inconnu à son ordinateur
- Ne dévoilez pas vos informations personnelles en ligne
- Faire aussi attention à ses téléphones et tablettes qu'à son ordinateur
- Ne pas se connecter au premier wifi qui passe



NOUS VOUS REMERCIONS DE VOTRE ATTENTION



A VOUS DE JOUER

Kahoot

CETTE FOIS CI A VOUS DE JOUER

Ouvrez ou téléchargez **KAHOOT** sur PlayStore ou AppStore