# Maintenez vos applications et logiciels à jour.

Les correctifs sont importants car ils corrigent les failles connues des produits que les attaquants peuvent exploiter pour compromettre vos appareils.

**Restez vigilants. Restez conscients des risques cybernétiques.**

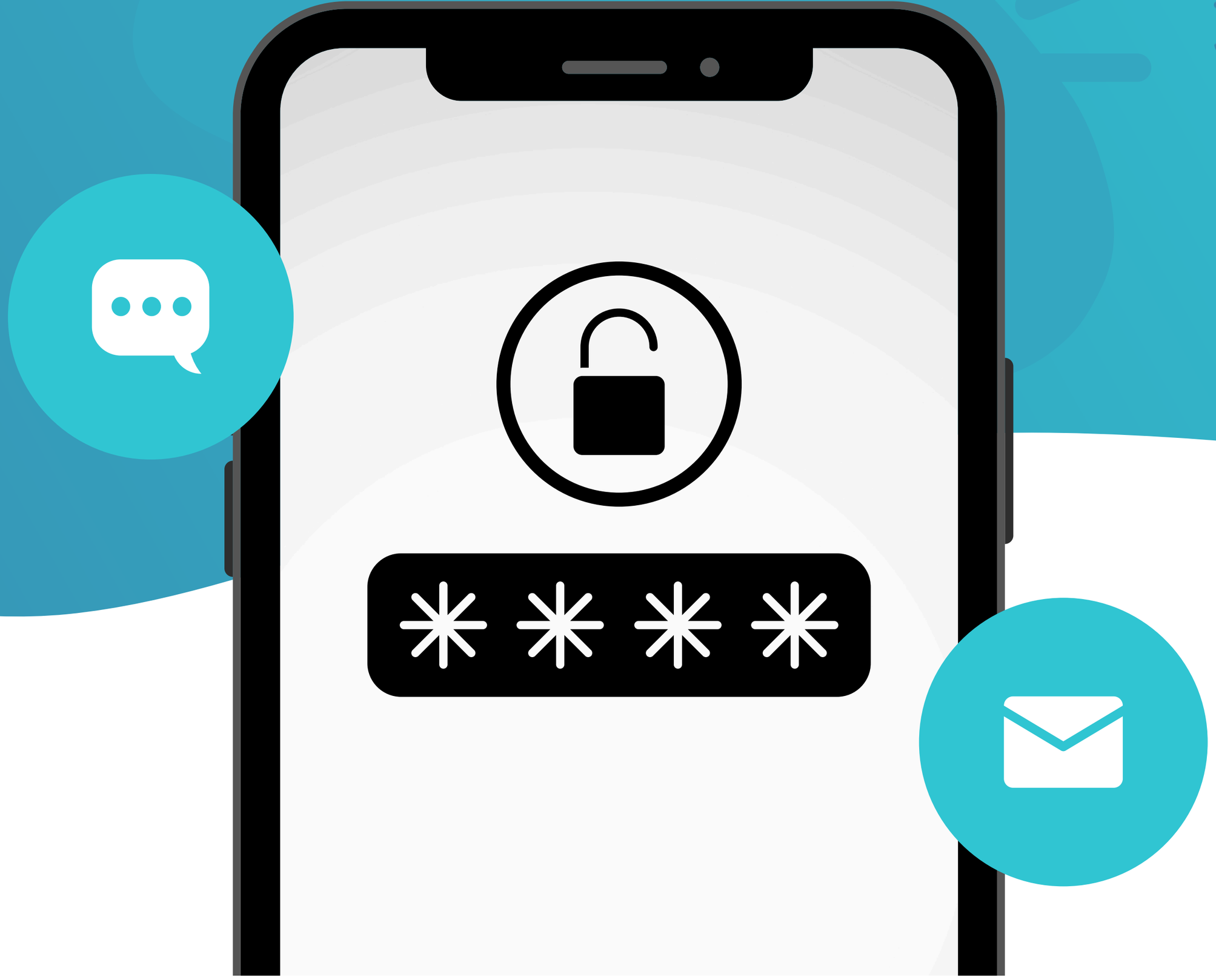
# Activer l'authentification multifacteurs (MFA)

**L'authentification multifacteur (MFA) contribue à sécuriser vos comptes et appareils en vous obligeant à prouver votre identité à plusieurs reprises.**

**Restez vigilants. Restez conscients des risques cybernétiques.**

# Activer l'authentification à deux facteurs (2FA)

L'authentification à deux facteurs (2FA) contribue à sécuriser vos comptes et appareils en vous obligeant à prouver votre identité à plusieurs reprises.



**Restez vigilants. Restez conscients des risques cybernétiques.**

# Assurez-vous que votre réseau domestique est sécurisé.

Changer le mot de passe par défaut de votre routeur et s'assurer que son micrologiciel est à jour contribuera à réduire le risque de piratage.

**Restez vigilants. Restez conscients des risques cybernétiques.**

# Pourquoi utiliser un VPN pour une sécurité renforcée ?

**Une connexion à un réseau privé virtuel (VPN) masque votre trafic de données en ligne et le protège des accès externes.**

**Restez vigilants. Restez conscients des risques cybernétiques.**

# N'oubliez pas la sécurité physique

Veillez à verrouiller votre ordinateur lorsque vous quittez votre bureau et à mettre sous clé tous les documents papier contenant des informations sensibles.

**Restez vigilants. Restez conscients des risques cybernétiques.**

# Partagez-vous des informations sensibles sur les réseaux sociaux ?

**Les cybercriminels peuvent utiliser les informations que vous publiez sur les réseaux sociaux pour obtenir des informations personnelles vous concernant (PII) qui peuvent être utilisées contre vous.**

**Restez vigilants. Restez conscients des risques cybernétiques.**

# Respectez toujours les politiques et procédures de l'entreprise.

Les politiques et procédures de sécurité fournissent des indications essentielles qui nous aident à protéger notre entreprise, nos collègues et nos clients contre les cyberattaques et les pertes de données.

**Restez vigilants. Restez conscients des risques cybernétiques.**

# Méfiez-vous de l'ingénierie sociale

L'ingénierie sociale est un vecteur d'attaque qui repose sur l'interaction humaine, impliquant souvent la manipulation de personnes pour qu'elles enfreignent les procédures de sécurité afin d'accéder à des systèmes, des réseaux ou des emplacements physiques.

**Restez vigilants. Restez conscients des risques cybernétiques.**

# 5 signes révélateurs d'une attaque d'ingénierie sociale

## Le message arrive de manière inattendue

Il s'agit là d'une caractéristique essentielle de l'ingénierie sociale, même si les attaquants peuvent également utiliser des comptes de messagerie compromis pour détourner des conversations.

## L'action demandée semble inhabituelle

Soyez méfiant si l'on vous demande de faire quelque chose que vous ne feriez généralement pas (par exemple, envoyer de l'argent, installer quelque chose, partager des informations client, etc.).

## L'action demandée semble risquée.

Si cette action est entreprise, pourrait-elle nuire au destinataire ou à l'entreprise ? Si oui, réfléchissez-y à deux fois.

## Une pièce jointe ou une URL inhabituelle

De nombreuses arnaques par ingénierie sociale incluent un lien frauduleux sur lequel l'utilisateur est invité à cliquer ou un document/programme à télécharger.

## Il y a un sentiment d'urgence.

De nombreuses arnaques jouent sur un sentiment d'urgence accru, l'escroc cherchant à communiquer une menace de préjudice.

**Restez vigilants. Restez conscients des risques cybernétiques.**

# Ne tombez pas dans le piège de l'hameçonnage !

**Les courriels d'hameçonnage ressemblent à des demandes légitimes provenant d'entités connues, vous incitant souvent à cliquer sur des liens, à télécharger des pièces jointes ou à fournir des informations sensibles.**

## Réfléchissez avant de cliquer


**Restez vigilants. Restez conscients des risques cybernétiques.**

# Conseils de sensibilisation au phishing

## Liens suspects dans l'e-mail

Soyez prudent si l'adresse web qui s'affiche lorsque vous survolez le lien ne semble pas correspondre à l'expéditeur ou si le courriel vous redirige vers une page vous demandant de vous connecter.

## Orthographe et grammaire médiocres

Les courriels et SMS d'hameçonnage peuvent parfois être truffés de fautes d'orthographe et de grammaire, alors soyez attentif à ces signes.

## Demande d'informations sensibles

Si l'on vous demande de partager des informations sensibles que vous ne partageriez généralement pas par courriel, appelez un numéro connu pour vérifier la demande.

## Urgence sous-jacente ou menaces

Les agresseurs s'appuient souvent sur un sentiment d'urgence pour vous inciter à agir rapidement sans vous laisser le temps de vous arrêter et de réfléchir.

## Domaines suspects

De nombreux courriels malveillants utilisent un domaine qui ressemble aux domaines légitimes, mais avec de légères différences.

**Restez vigilants. Restez conscients des risques cybernétiques.**

# Utilisez toujours des mots de passe forts, uniques et confidentiels.

**Vos mots de passe doivent être uniques, privés et faciles à retenir pour vous, sans pour autant être faciles à deviner pour un pirate.**



**Restez vigilants. Restez conscients des risques cybernétiques.**

# Conseils de sécurité pour les mots de passe

## Ne réutilisez pas vos mots de passe.

Si une fuite de données compromet l'un de vos comptes, l'attaquant pourrait accéder à d'autres comptes en utilisant vos mots de passe réutilisés.

## Ne laissez pas vos mots de passe à la vue de tous.

Ne laissez pas vos mots de passe dans un endroit non sécurisé comme un post-it, un journal intime ou un fichier texte non chiffré.

## Ne partagez pas vos mots de passe.

Ne partagez jamais vos mots de passe ou vos comptes avec qui que ce soit, pas même vos collègues.

## Créez des mots de passe longs et simples

Utilisez une série de mots sans lien apparent pour créer des mots de passe longs et simples plutôt que courts et complexes.

## Utilisez des méthodes d'authentification multifacteurs

Utilisez la méthode d'authentification multifacteurs la plus sécurisée à votre disposition, comme une application d'authentification.

**Restez vigilants. Restez conscients des risques cybernétiques.**