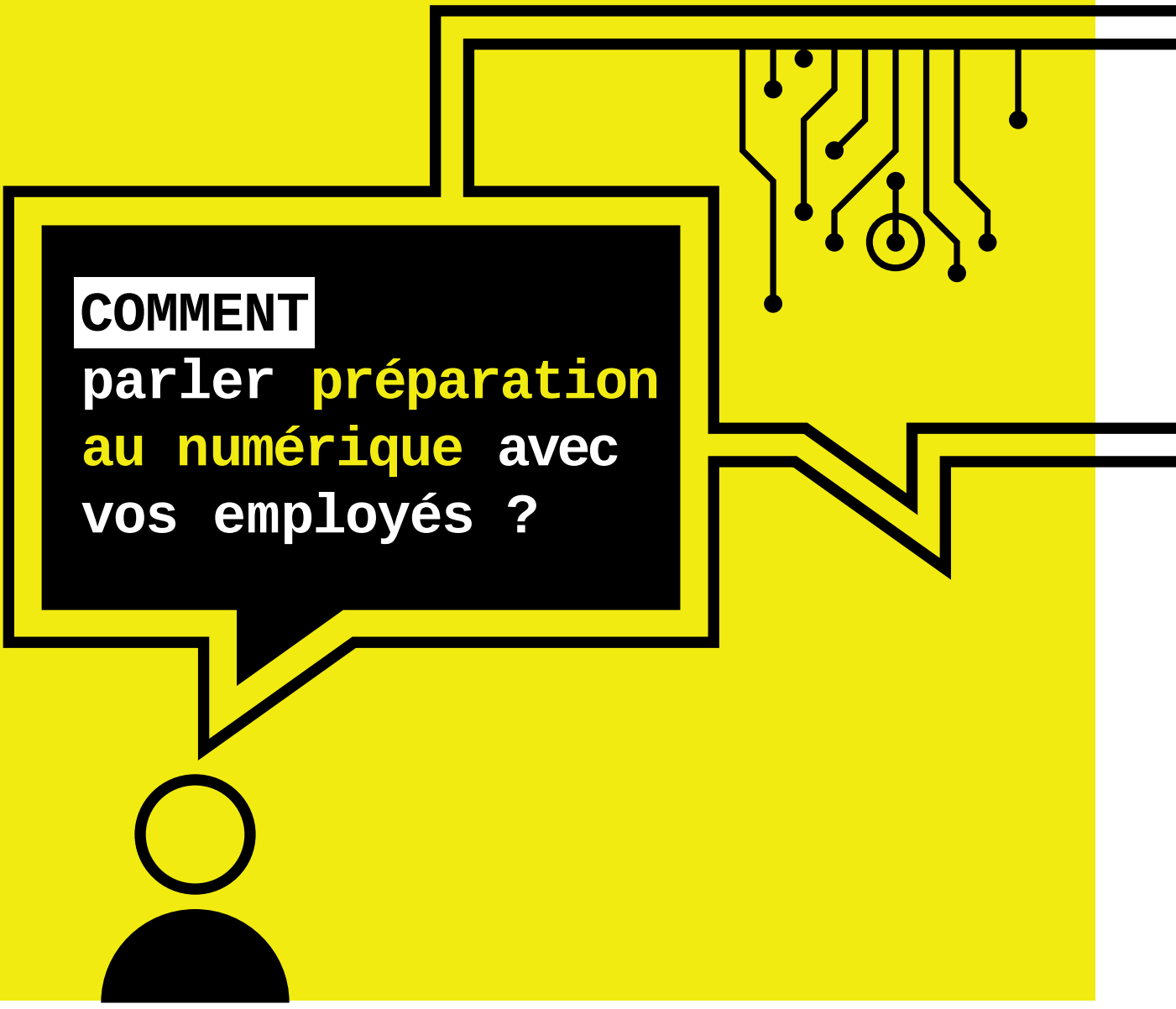
CYBER READINESS
INSTITUTE

# Discussion



## Prendre au SÉRIEUX la préparation au numérique est important.

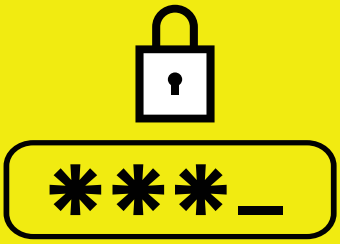
**La réputation de votre entreprise en dépend.**

### MAIS COMMENT DÉBUTER UNE CONVERSATION SI NOUS NE SOMMES PAS EXPERTS DU NUMÉRIQUE ?

Cela n'a pas besoin d'être compliqué ou intimidant. Référez-vous aux questions-réponses de ce document pour discuter avec vos employés des cyber-risques, des moyens pour se protéger et des bonnes pratiques en matière de préparation au numérique.

— 1 —

# les mots de passe

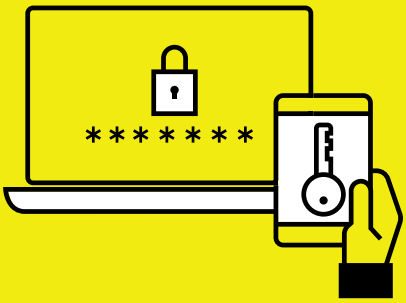



## Quel type de mot de passe est le plus efficace ?

Les mots de passe les plus efficaces sont composés de : phrases plutôt que de mots seuls, de pensées aléatoires qui forment une phrase, de chiffres et de symboles, de minuscules et de majuscules.

## Puis-je utiliser le même mot de passe pour le professionnel et le privé ?

Non, n'utilisez pas le même mot de passe plus d'une fois quand c'est possible.

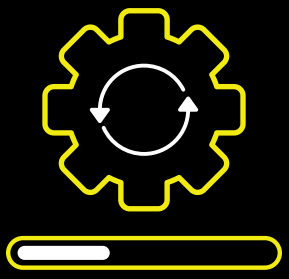




## Qu'est-ce que l'authentification à deux facteurs ?

L'authentification à deux facteurs consiste à confirmer votre identité à l'aide de votre mot de passe ainsi que d'une autre méthode comme un SMS ou un e-mail. L'authentification à deux facteurs est facile à mettre en place et réduit drastiquement les chances de se faire pirater.

- 2 -

# Mises à jour



## Qu'est ce qu'une mise à jour ?

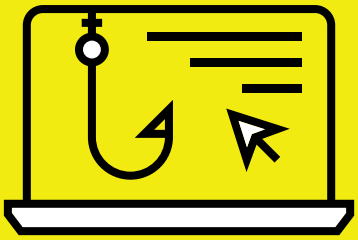
Pour faire simple, les "mises à jour" sont de nouvelles versions des logiciels et applications présents sur votre ordinateur et téléphone. Ces mises à jour corrigent certains problèmes et améliorent la sécurité. Installer les mises à jour est l'une des mesures les plus simples et les plus importantes à mettre en place pour vous préparer au numérique.

## Comment s'assurer que mes appareils sont à jour ?

Activez les notifications de mise à jour automatique et ne les ignorez pas. Pensez aussi à vérifier les mises à jour pour les applications tiers.

— 3 —

# Phishing



## Qu'est-ce que le phishing ?

Le phishing est une cyberattaque transmise grâce à un e-mail frauduleux. Le phishing a pour but d'utiliser votre compte de messagerie afin de dérober des données personnelles ou de prendre le contrôle de votre ordinateur. Ces attaques sont souvent difficiles à détecter.

## Quels sont les signes d'une tentative de phishing ?

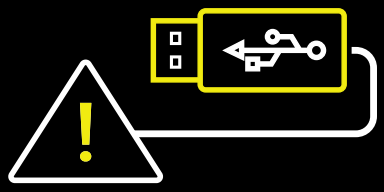
- Adresse e-mail suspecte
- E-mails de destinataires inconnus contenant des pièces jointes ou des liens
- Des fautes d'orthographe ou des phrases coupées
- E-mails suspects demandant des informations personnelles

## Pourquoi faut-il être conscient des risques liés au phishing ?

91 % des cyberattaques commencent avec un e-mail de phishing.
81 % des entreprises victimes de phishing ont perdu des clients.

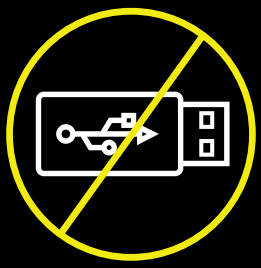
— 4 —

# Clés USB



## Pourquoi les clés USB sont-elles dangereuses ?

Plus d'un quart des infections par un malware proviennent d'une clé USB corrompue. En outre, plus de 87 % des employés déclarent avoir perdu un support amovible sans le signaler à leur employeur.



## Comment limiter les attaques via clé USB ?

**N'utilisez pas**

une clé USB qui n'a pas été approuvée par votre Cyber Leader

**N'utilisez jamais**

et n'acceptez pas de clé USB d'une personne externe ou d'une autre entreprise

**En cas d'usage**

analysez régulièrement si les clés USB contiennent des malwares

CYBER READINESS
INSTITUTE