



# Mise en place des bonnes pratiques **BYOD**

Ladrière Valentine

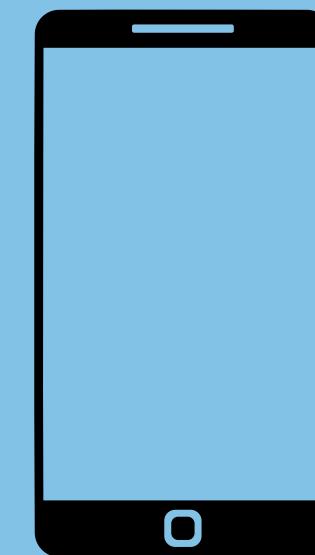
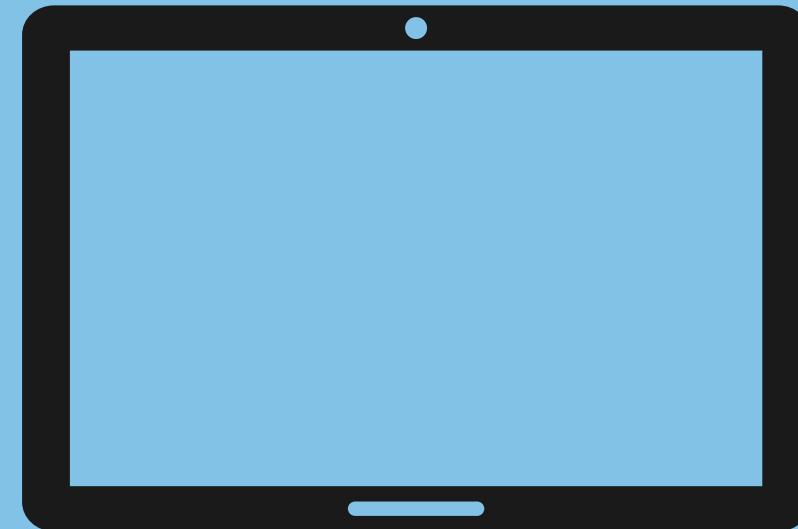


# **BYOD**



# BYOD (Bring Your Own Device):

désigne l'usage d'équipements informatiques personnels dans un contexte professionnel (employé qui utilise un équipement personnel comme son ordinateur, sa tablette ou son smartphone pour se connecter au réseau de l'entreprise).





# Outils de sécurisation des postes informatique



VPN (NordVPN, CyberGhost, Surfshark...)



Antivirus/Anti-Malware (Avast, Avira, Norton, McAfee, Bitdefender, Malwarebytes...)



Pare-feu (ZoneAlarm, Windows Defender Firewall...)



Gestionnaire de mots de passe (KeePass, ZenyPass...)



Logiciel de sauvegardes et de récupération de données (Acronis, Veeam, Carbonite)



Anti spam (Mailinblack, Altospam...)





# Logiciels interdits sur les postes informatique

-  Logiciels de piratage (Metasploit, Cain & Abel)
-  Logiciels de peer-to-peer (uTorrent, BitTorrent...)
-  Logiciels de contrôle à distance (TeamViewer, AnyDesk...)
-  Logiciels piratés (licences craquées)
-  Jeux vidéo
-  Messagerie instantanée non sécurisée
-  Cloud personnel non autorisé (Dropbox, Google Drive)
-  Streaming vidéo (Netflix, Amazon Prime, Twitch)



# ZED!

## FOR FILES IN TRANSIT



[Watch video on YouTube](#)  
Error 153  
Video player configuration error

## Quel outil de communication utiliser?

Zed! permet de protéger des fichiers au sein de conteneurs à des fins d'archivage, d'échange par courriel sur des réseaux publics (Internet) ou par support physique (clé USB).

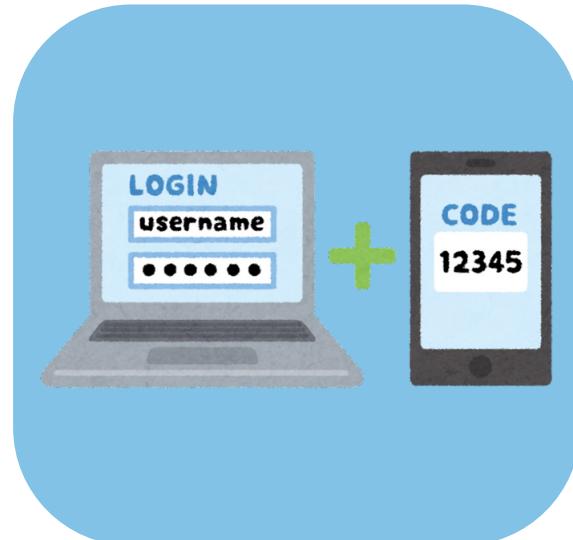
Zed! offre la possibilité de créer des .zed qui sont des conteneurs chiffrés (cryptés) dans lesquels on insère des documents, des images, des vidéos, etc. : tous fichiers que l'on souhaite garder confidentiels.



# Politique de sécurité de mots de passe mise en œuvre sur les postes informatique



Utiliser un mot de passe long et complexe<sup>1</sup>



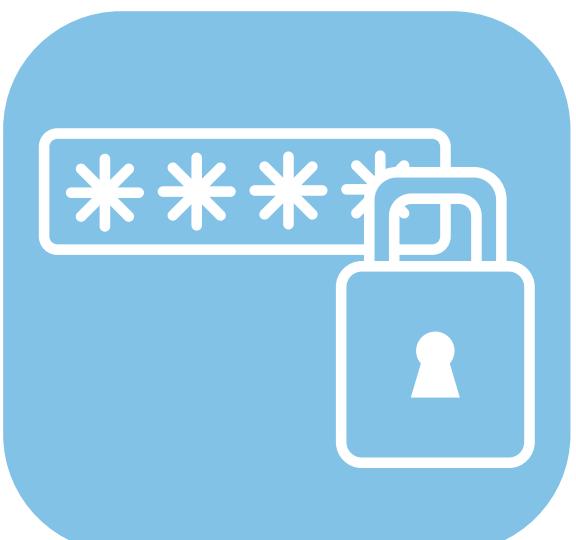
Identification à deux facteurs



Renouveler régulièrement le mot de passe



Utiliser un gestionnaire de mots de passe



Verrouiller ses comptes/son poste lorsqu'on quitte son poste

Garder en tête que si quelqu'un découvre un de vos mots de passe, il a accès à l'intégralité de vos informations. Imaginez qu'il s'agisse de votre application bancaire...

1/ les mots de passe doivent être composés d'au minimum 12 caractères comprenant des majuscules, des minuscules, des chiffres et des caractères spéciaux à choisir dans une liste d'au moins 37 caractères spéciaux possibles.



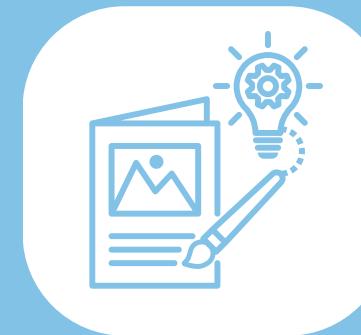
## Sensibiliser vos utilisateurs à l'usage du BYOD

Pourquoi est-ce important de sensibiliser et de communiquer ?

Avant de passer à l'action, tout acteur a besoin de connaître les enjeux et de comprendre le sens et l'impact de son action.

Les utilisateurs sont souvent négligents et manquent de connaissances sur le sujet, cela les rendant ainsi vulnérables aux attaques malveillantes.

Prévenir des erreurs récurrentes, Renforcer le niveau de sécurité de l'entreprise, Diminuer les coûts liés aux cyberattaques



## Distribution de flyers



## Ateliers de formation interactifs



## Quiz et certifications internes



## Témoignages d'employés ou de spécialistes

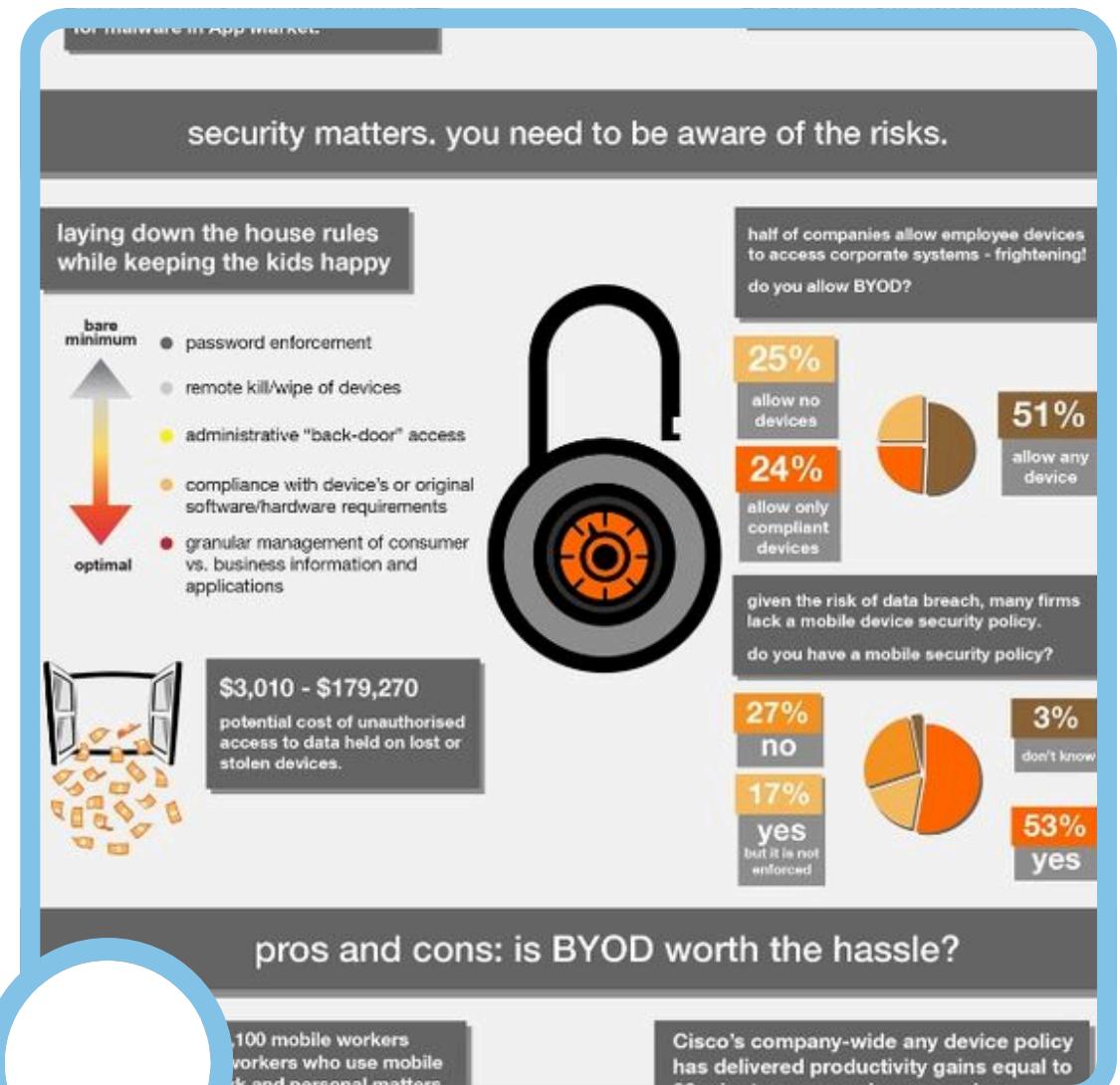


## Journée du numérique

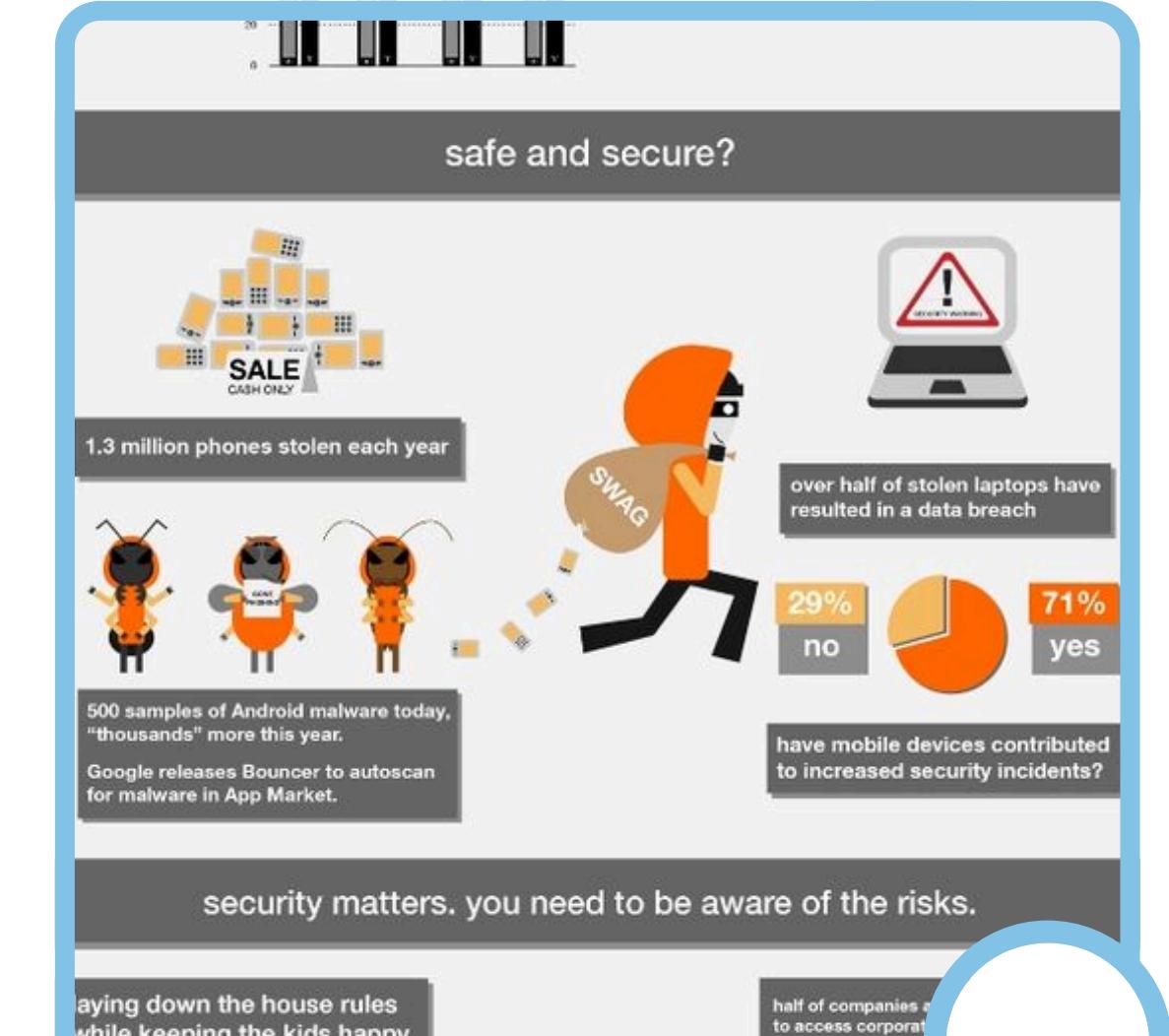


# Distribution de flyers

**Les flyers peuvent s'avérer d'une grande aide pour effectuer un processus de sensibilisation grâce à la condensation d'informations clés, de points "forts", le tout illustrer, rendant la sensibilisation plus "ludique".**



## Des pourcentages et des chiffres pour appuyer la sensibilisation



**Sur cette partie du flyer, quelques exemples forts répondant à la problématique “sûr et sécurisé?” Parfait pour une sensibilisation efficace.**

**Le flyer reste le meilleur outil pour attirer l'attention et délivrer rapidement votre message à la plus large cible possible en plus d'offrir une interaction physique avec les membres de votre entreprise.**



# Quiz et certifications internes

La certification est une preuve irréfutable, délivrée suite à un audit mené par un organisme certificateur impartial et objectif, qu'un produit, service ou une organisation, respecte les exigences d'un cahier des charges strict.



Il existe effectivement des certifications visant le BYOD qui peut effectuer une sensibilisation tout en formant les employés d'une entreprise. Ce processus deux en un peut également offrir un sentiment de satisfaction en recevant un certificat si la formation a été réussite, de quoi se motiver à s'intéresser un peu plus au BYOD !

On peut retrouver des entreprises fournissant des formations tel que PLB Consultant:  
<https://www.plb.fr/formation/TELECOM/formatio n-byod,25-1051.php>



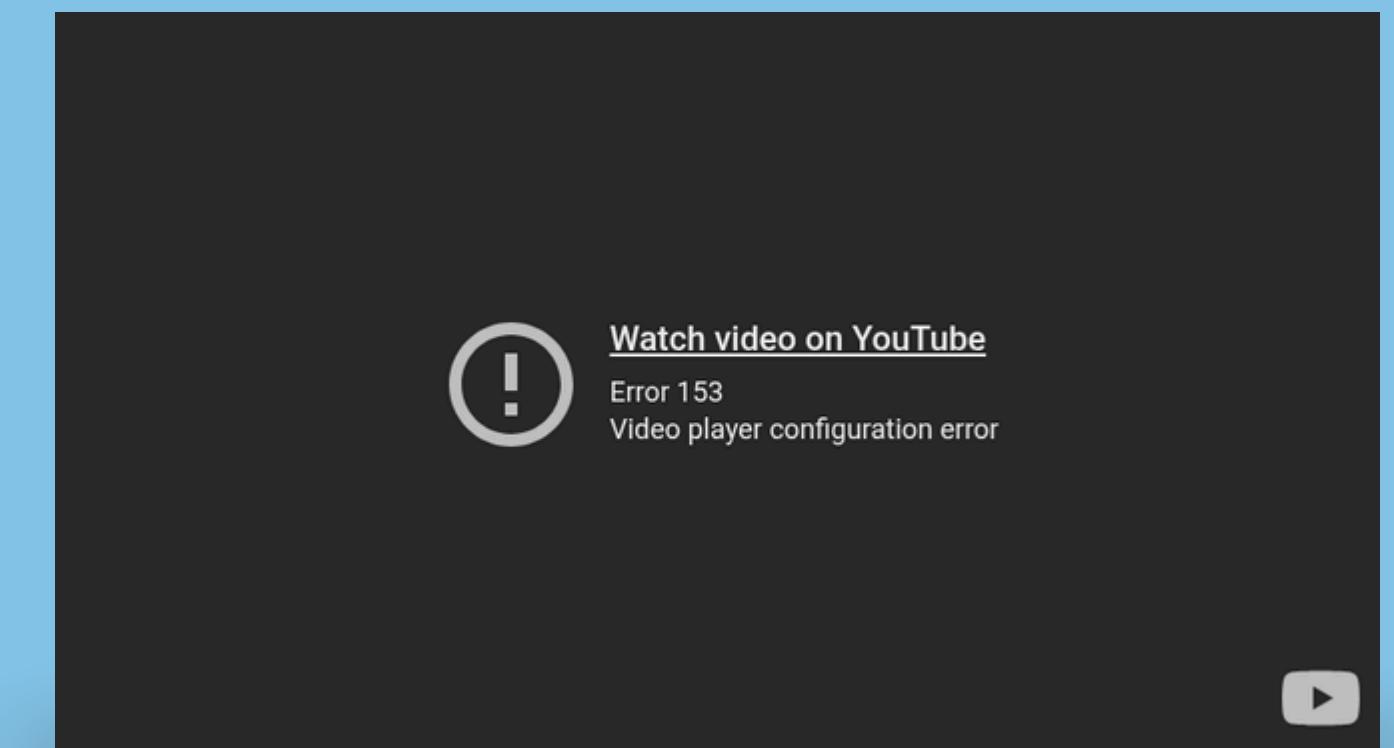


# Témoignages d'employés ou de spécialistes

Les témoignages seront toujours un moyen fiable de sensibiliser les êtres humains avec un minimum d'empathie.  
Pour cela, rien de mieux que de s'adresser directement aux personnes concernées pour nous offrir un discours au sein de l'entreprise



Pour ceux qui seraient moins réceptifs à ce type de sensibilisation, il existe également des courts-métrages animés par exemple, plus "sympathique" et "ludique" et qui pourraient également s'adresser à un public plus jeune... L'informatique prenant une place considérable dans la vie de chacun (et de plus en plus chez les jeunes), commencer une sensibilisation chez les plus jeunes pourraient être que bénéfique...

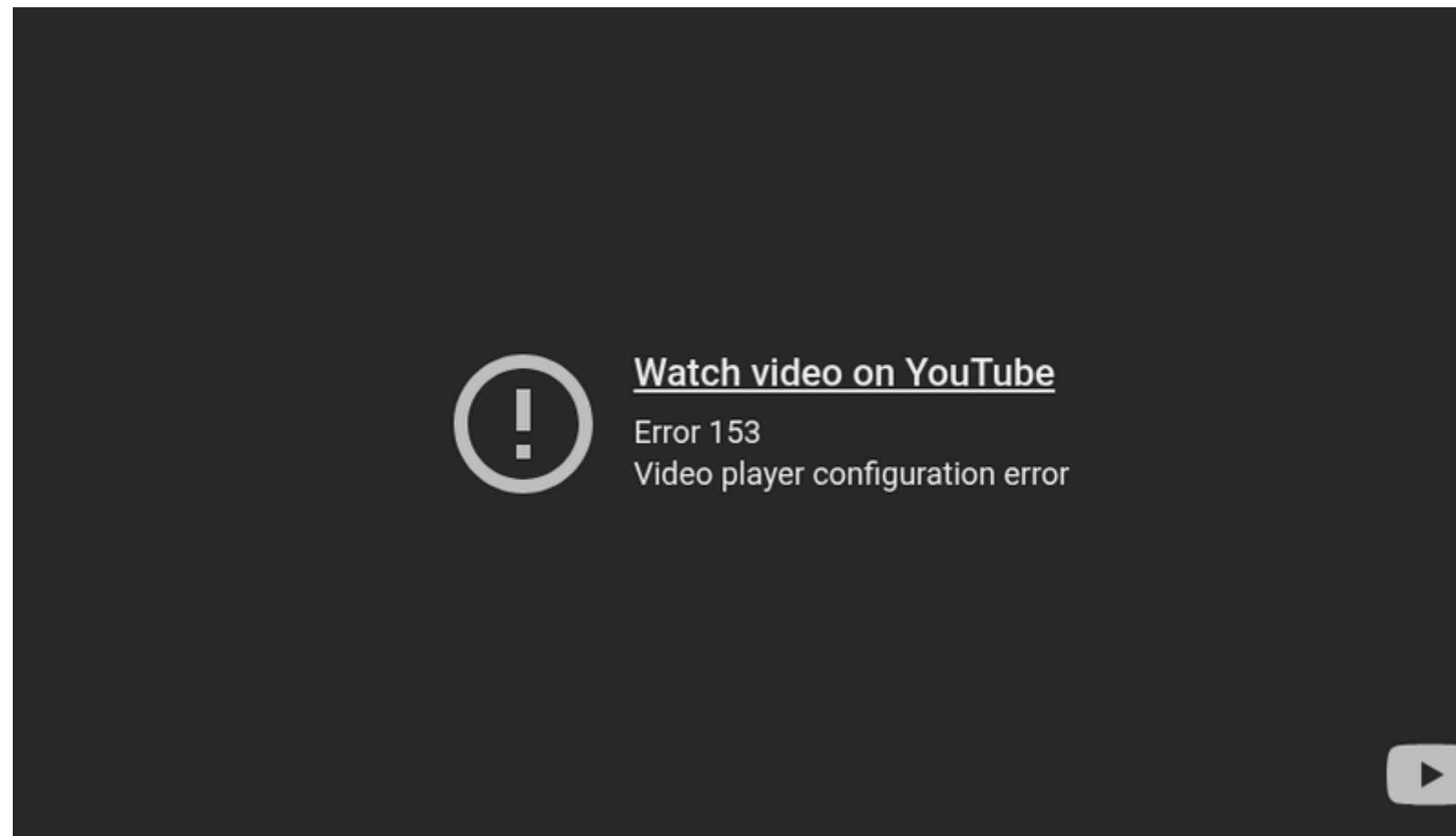




# Journée du numérique

Une journée dédiée à la cybersécurité nous permet d'être au plus proche de cette thématique, de rencontrer des professionnels le tout dans un cadre convivial.

C'est typiquement dans ce genre de journée que nous pouvons assister à des conférences, notamment sur le BYOD par exemple:



Lors d'une journée du numérique, énormément de sujets seront abordés. Bien que ce soit le BYOD qui nous intéresse, les autres sujets pourraient être tout autant bénéfiques pour l'apprentissage des risques liés au numérique. Voici quelques exemples:



Attaques de phishing.



Mots de passe et authentification.



Sécurité physique (répercussions mental, oculaire...)



Travail à distance (le télétravail étant de plus en plus présent)



Wi-Fi public.



Sécurité dans le Cloud.



# La séparation des bonnes pratiques personnel et professionnel

La première étape pour réussir cette séparation est de reconnaître l'importance de chacun de ces domaines.

La vie professionnelle demande des compétences spécifiques, un engagement envers les objectifs de l'entreprise et souvent une interaction constante avec les collègues. En revanche, la vie personnelle est un espace où l'on peut se ressourcer, s'adonner à ses passions et entretenir des relations interpersonnelles significatives.

## Définir des horaires clairs

Établir des heures de travail précises aide à éviter les débordements.

Par exemple, en respectant des horaires de début et de fin de journée, on favorise une meilleure gestion du temps.

## Créer des espaces distincts

Aménager un espace de travail séparé de l'espace de vie

Cela aide à marquer la différence entre ces deux sphères mais également de se concentrer sur le travail sans être distrait par les obligations personnelles...

## Établir des priorités

Savoir quelles sont les priorités dans chaque domaine permet de mieux gérer son temps et son énergie. Il est important d'évaluer régulièrement ses engagements pour éviter de se sentir submergé.

## Utiliser des outils de gestion

L'utilisation d'applications ou de techniques de gestion du temps peut aider à structurer les tâches et à garder une vision claire des obligations tant professionnelles que personnelles.