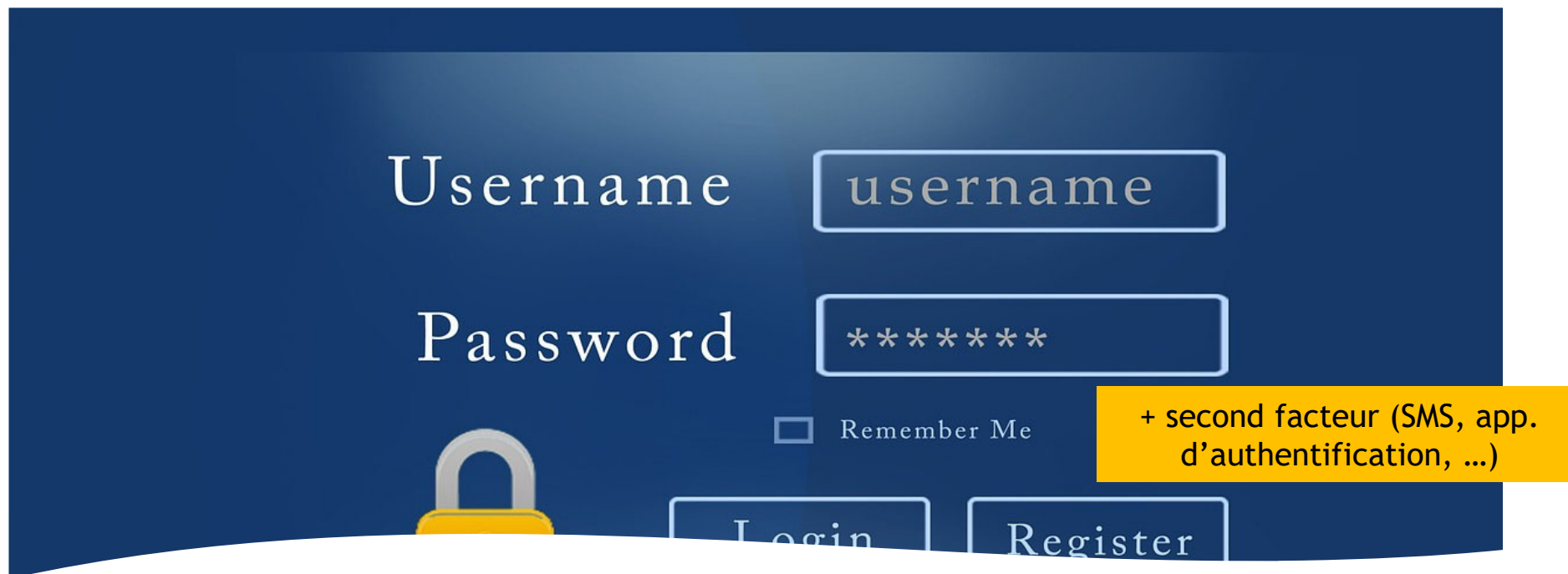




5 bonnes pratiques contre les ransomwares



Username

Password

Remember Me

+ second facteur (SMS, app. d'authentification, ...)

**L'AUTHENTIFICATION
FORTE EST AUJOURD'HUI
UNE OBLIGATION POUR
LES ACCÈS À DISTANCE**

**Les 5 principales protections
contre les cyberattaques**

Sécurisation des accès à distance:

Les accès à distance, comme le VPN ainsi que tous les autres accès aux ressources internes doivent **obligatoirement** être sécurisés avec un second facteur (authentification forte).

L'IMPORTANCE VITALE D'AVOIR DES SAUVEGARDES "DÉCONNECTÉES"

Les 5 principales protections contre les cyberattaques

Sauvegardes hors ligne:

Créez régulièrement des copies de secours de vos données.

Assurez-vous à chaque fois que le canal sur lequel vous effectuez les copies de secours soit physiquement séparé de l'ordinateur et du réseau, et protégé après l'opération de sauvegarde.





LES MISES À JOUR CORRIGENT DES FAILLES DE VULNÉRABILITÉS RECHERCHÉES PAR LES CYBERCRIMINELS

Les 5 principales protections contre les cyberattaques

Gestion des correctifs et des cycles de vie:

En matière de sécurité, tous les systèmes doivent être systématiquement et régulièrement mis à jour. Les logiciels ou les systèmes qui ne sont plus actualisés par le fabricant (fin de vie) doivent être désactivés ou transférés dans une zone du réseau séparée et isolée.

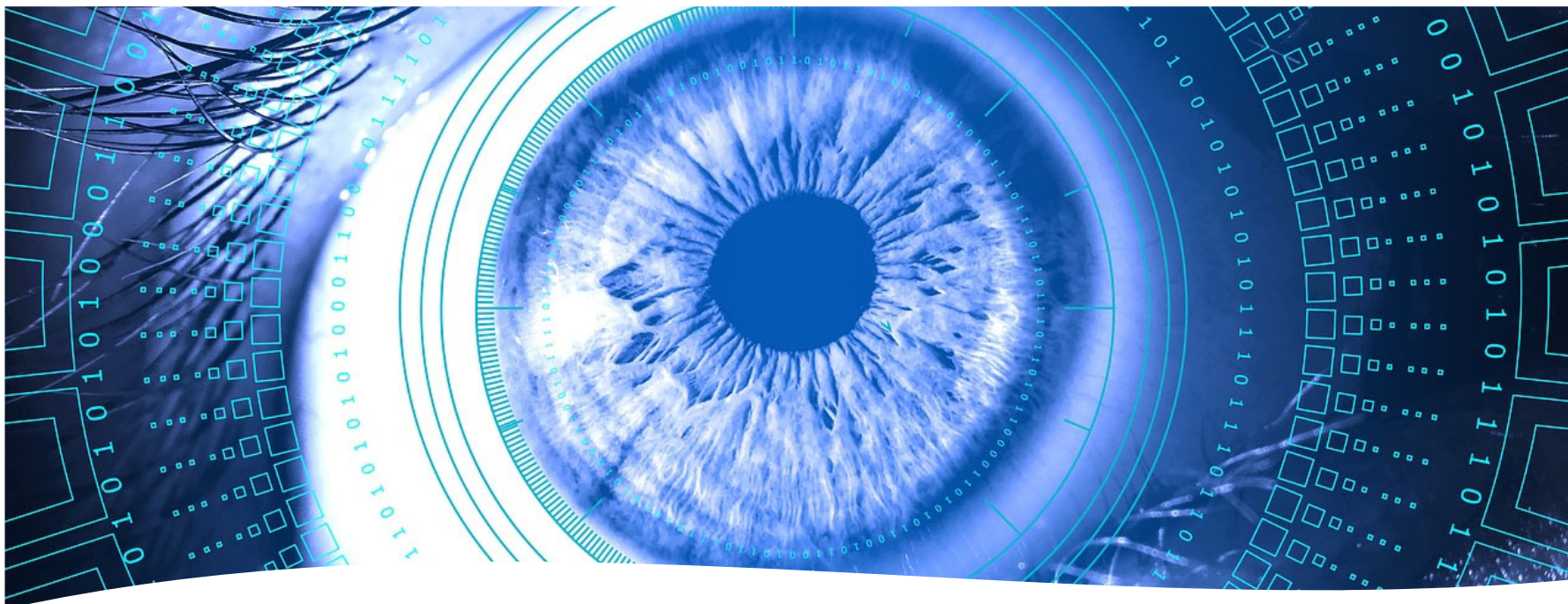


**LA MESSAGERIE EST UN
VECTEUR D'ATTAQUE TRÈS
UTILISÉ PAR LES
CYBERCRIMINELS**

**Les 5 principales protections
contre les cyberattaques**

**Blocage des pièces jointes et des liens à risque
dans les courriels:**

Bloquez la réception de pièces jointes dangereuses sur votre messagerie, y compris les **documents Office avec macros**. Sensibilisez et formez vos collaboratrices.teur.s à reconnaître les courriels suspects, par exemple avec des exercices de prévention du phishing



**UNE SURVEILLANCE
CONTINUE EST
NÉCESSAIRE POUR RÉAGIR
RAPIDEMENT ET RÉDUIRE
LES IMPACTS D'UNE
CYBERATTAQUE**

**Les 5 principales protections
contre les cyberattaques**

**Surveillance des fichiers journaux (logs), en
particulier de l'accès à distance:**

Une surveillance continue de l'environnement IT est nécessaire pour réagir rapidement et réduire les impacts d'une cyberattaque.