

- Exposé 6.3 :  
Pourquoi les  
objets connectés  
sont des cibles de  
choix pour les  
hackers ?

*Alice et Emma*



# Introduction

Les objets connectés (montres, enceintes, caméras, voitures, etc.) facilitent notre quotidien grâce à leur connexion Internet.

Cependant, cette connexion les rend vulnérables aux hackers.

Pourquoi sont-ils des cibles ?





# La multiplication des objets connectés

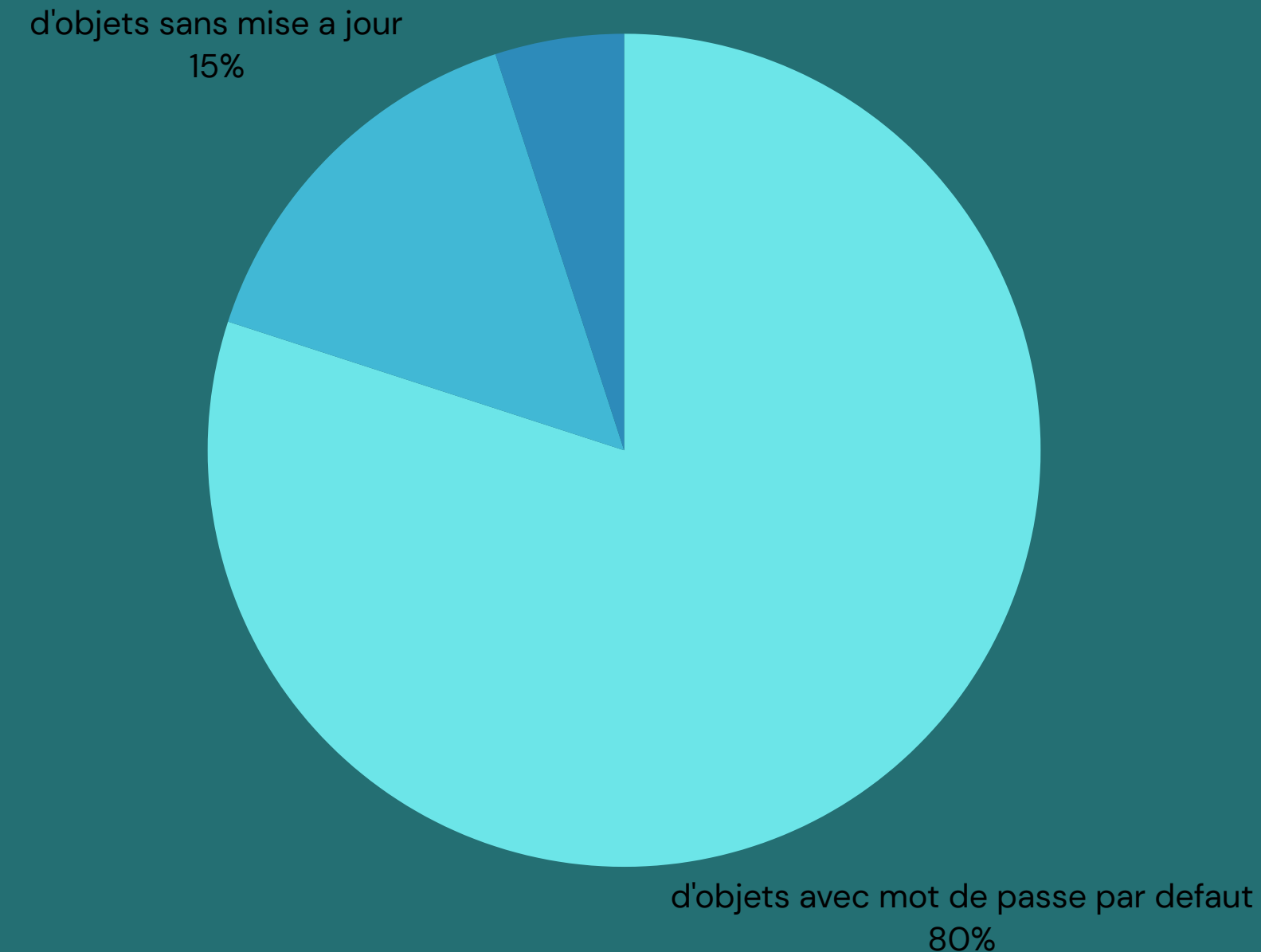


- Les objets connectés se multiplient partout : maison, santé, loisirs, villes.
- Chaque objet peut être une porte d'entrée pour les hackers.
- Certains appareils peu sécurisés sont des cibles faciles.
- Plus il y a d'objets connectés, plus les failles et les risques augmentent.

### 3. Une sécurité souvent insuffisante

- Les objets connectés sont peu protégés : conçus pour être rapides et peu coûteux, pas pour résister aux attaques.
- Mots de passe faibles : souvent “admin” ou “1234”, rarement changés.
- Manque de mises à jour : les failles restent ouvertes, les fabricants oublient certains appareils.
- Systèmes simples : sans antivirus ni firewall → faciles à pirater.

Résultat : les objets connectés sont une cible facile pour les hackers.





## 4. Des données personnelles sensibles

- Les objets connectés collectent des données personnelles très précises (santé, trajets, vie privée).
- Ces informations sont très sensibles et attirent les hackers.
- Elles peuvent être utilisées pour du chantage, de l'espionnage ou revendues à des entreprises.
- Les données personnelles sont une véritable mine d'or, souvent plus rentable que l'argent.





# Menaces courantes

- A** **Espionnage :**  
accès a une caméra  
pour surveiller une  
personne ou un lieu



- C** En 2016, des caméras connectées piratées ont servi à lancer des attaques massives, rendant inaccessibles des sites tels que Twitter, Spotify et Netflix



- B** **Contrôle à distance :**  
manipulation de serrures,  
d'alarmes ou d'une voiture  
connectée, avec des  
risques pour la sécurité



# Conclusion

- Les objets connectés sont très répandus et attirent les hackers car ils sont difficiles à sécuriser.
- Leur protection est souvent insuffisante : mots de passe faibles et mises à jour rares.
- Ils collectent des données personnelles sensibles, très prisées par les pirates.
- Les risques incluent l'espionnage, le contrôle à distance et les attaques massives.
- Pour limiter ces dangers : changer les mots de passe par défaut, accepter les mises à jour et choisir des appareils fiables.
- Les objets connectés améliorent le confort et la vie quotidienne, mais il faut rester vigilant pour en profiter en toute sécurité.

