#IdOAuTravail pour les petites et moyennes entreprises

Comprendre l'**Internet des objets**

PENSEZCYBERSECURITE.CA

Canada

Ordre du jour

- Qu'est-ce que l'Internet des objets ?
- Comment l'IdO fonctionne-t-il ?
- Quels secteurs emploient l'IdO ?
- Bénéfices commerciaux découlant de l'IdO
- Risques pour la sécurité de l'information
- Risques pour la confidentialité
- Risques pour la sécurité
- Liste de vérification pour la mise en œuvre sécuritaire de l'IdO

Qu'est-ce que l'Internet des objets ?

L'Internet des objets (IdO) est un réseau créé à partir d'appareils « intelligents » qui sont connectés et qui communiquent entre eux via Internet.

Comment l'IdO fonctionne-t-il ?

Les appareils intelligents collectent et échangent de l'information entre eux (machine à machine) et avec nous :

- Ils peuvent être contrôlés et surveillés à distance
- Ils fonctionnent automatiquement grâce à des logiciels, caméras et capteurs

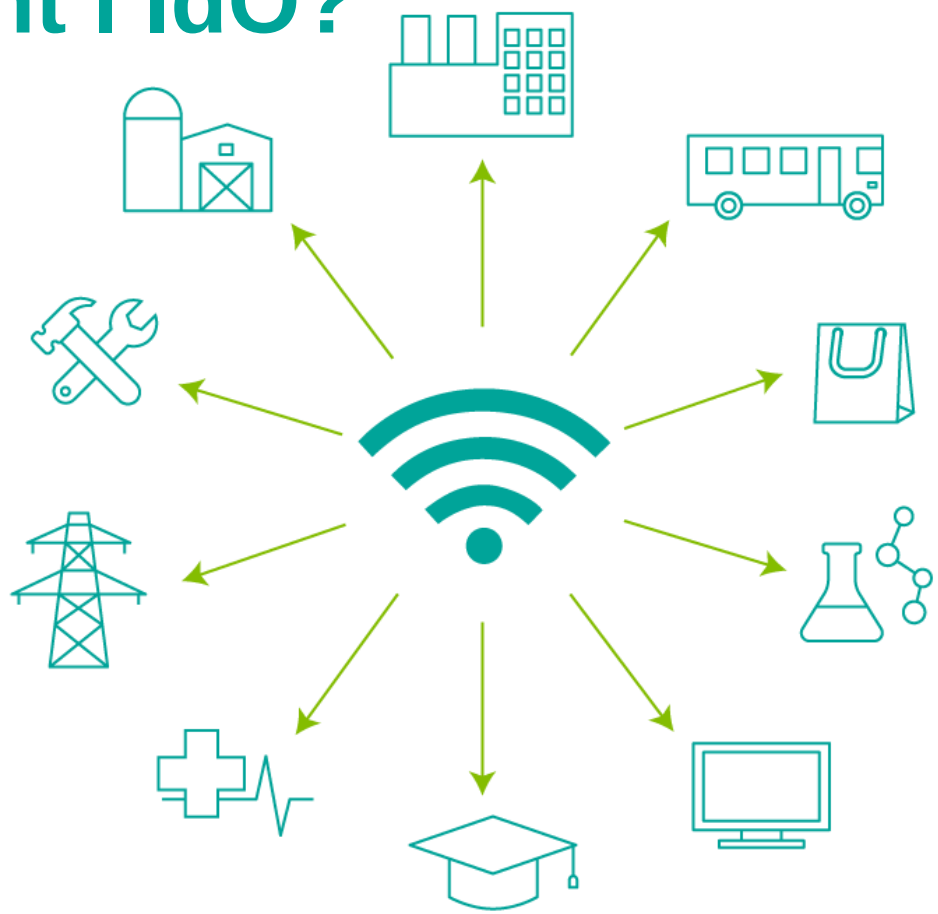
L'**IdO est utilisé** dans des secteurs d'activité variés, de **l'agriculture** aux **soins de santé** en passant par celui de la **fabrication**.

PENSEZCYBERSECURITE.CA

#IdOAuTravail

Quels secteurs emploient l'IdO?

1. Fabrication
2. Transports
3. Commerce de détail
4. Sciences et technologie
5. TI et communications
6. Éducation
7. Soins de santé
8. Énergie
9. Construction
10. Agriculture



Bénéfices commerciaux découlant de l'IdO

Commerce de détail

- Caisses automatisées
- Gestion des stocks et de l'entrepôt

Bénéfices commerciaux découlant de l'IdO

Fabrication

- Opérations plus performantes
- Gestion et entretien des biens

Bénéfices commerciaux découlant de l'IdO

Consommateurs

- Divertissement
- Santé et activité physique

Bénéfices commerciaux découlant de l'IdO

Bureaux et gouvernement

- Amélioration de la productivité et économie d'énergie
- Sécurité et surveillance

Bénéfices commerciaux découlant de l'IdO

Transports

- Automatisation et contrôle de la circulation
- Gestion des parcs de véhicules

Bénéfices commerciaux découlant de l'IdO

Soins de santé

- Suivi médical
- Administration automatisée des traitements

Le **plus grand obstacle** que représente la mise en œuvre de l'IdO dans une entreprise est la **sécurité**.

PENSEZCYBERSECURITE.CA

#IdOAuTravail

Risques pour la sécurité de l'information

Répercussions possibles d'une brèche dans la sécurité de l'information :

- Atteinte à la réputation ou à la crédibilité
- Perte de temps et d'argent
- Conséquences juridiques

Risques pour la sécurité de l'information

Cyberincidents directs :

- Dommages à plusieurs niveaux de l'entreprise
  - Du siège social aux consommateurs en passant par la chaîne d'approvisionnement

Cyberincidents indirects (menaces virales, logiciels malveillants) :

- Effets en aval sur l'infrastructure de sécurité des TI
  - Vos objets connectés pourraient être touchés par l'attaque d'un logiciel malveillant sur leur fabricant

Les **cyberincidents** liés à l'IdO augmentent les **risques de vol**, de **divulgation**, et **d'altération** de **l'information**.

PENSEZCYBERSECURITE.CA

#IdOAuTravail

Risques pour la confidentialité

L'information concernant l'entreprise, ses employés et ses clients pourrait être :

- Détruite
- Altérée
- Volé et publiée
- « Retenue en otage » jusqu'au versement d'une rançon

Risques pour la confidentialité

Il est important de connaître les politiques des objets connectés en matière de collecte d'information :

- Quelle information sera collectée ?
- Combien de temps sera-t-elle conservée ?
- À quoi servira-t-elle (recherches marketing, etc.) ?

L'utilisation non autorisée ou la prise de contrôle à distance **d'un objet connecté** pourraient causer des **dommages matériels** ou **physiques**.

PENSEZCYBERSECURITE.CA

#IdOAuTravail

Risques pour la sécurité

La défaillance ou le piratage d'un objet connecté pourrait :

- Endommager les données
- Occasionner des dommages matériels
- Causer des dommages physiques

Risques pour la sécurité

Répercussions possibles de la défaillance ou du piratage d'un objet connecté :

- Réparations coûteuses liées aux systèmes, biens et équipements
- Conséquences juridiques des dommages physiques causés aux employés, aux clients ou au grand public
- Perte de la réputation

Avant l'implantation :

- Informez-vous sur les objets connectés avant d'en faire l'achat; lisez les avis et obtenez des recommandations; renseignez-vous sur leur capacité de sécurité.
- Établissez un point de contact avec les fabricants en cas de problème dans le futur.
- Lisez la documentation des objets : guides de l'utilisateur, instructions, forums de soutien.
- Élaborez des politiques « Apportez votre équipement personnel de communication » (AVEC) et IdO à l'intention des employés.
- Évaluez les risques en fonction des politiques et normes actuelles de l'entreprise en matière de TI.

Durant l’implantation :

- ❑ Sécurisez votre réseau sans fil.
- ❑ Changez les noms d’utilisateur et mots de passe par défaut des objets connectés et utilisez des mots de passe forts.
- ❑ Isolez les réseaux sur lesquels circule de l’information sensible; envisagez l’utilisation d’un réseau distinct pour les objets connectés.
- ❑ Vérifiez que le système de l’objet connecté peut être réinitialisé pour supprimer définitivement l’information sensible servant à la configuration.
- ❑ Contrôlez l’accès au réseau pour déterminer qui peut l’utiliser et à partir de quel endroit.
- ❑ Chiffrez les données, commandes et communications, aussi bien celles qui sont inactives que celles qui circulent.
- ❑ Si possible, activez la mise à jour automatique des systèmes d’exploitation, logiciels et micrologiciels; effectuez périodiquement des mises à jour manuelles, au besoin.

Après l’implantation :

- Mettez en œuvre des processus reproductibles pour vérifier toutes les mesures de protection et contre-mesures de sécurité durant l’implantation.
- Effectuez régulièrement des tests simulant des « cyberincidents » et des vérifications pour confirmer l’intégrité du réseau.
- Sauvegardez régulièrement les données au moyen de solutions d’entreposage sûres et redondantes, comme des serveurs multiples ou le nuage; testez périodiquement le processus de récupération des données.

Liste de vérification

Respectez la politique « Apportez votre équipement personnel de communication »/IdO élaborée par votre entreprise.

- ❑ Avant d'acheter un appareil d'IdO ou de télécharger une application, comprenez bien quelle information sera recueillie par chacun d'eux et pour quelles raisons elle le sera.
- ❑ Utilisez un mot de passe pour verrouiller l'écran de vos appareils et choisissez des mots de passe forts.
- ❑ Sauvegardez régulièrement vos données dans plusieurs unités de stockage et dans le nuage.
- ❑ Établissez uniquement une connexion avec les réseaux Wi-Fi sécurisés.
- ❑ Utilisez des sites Web, des services de stockage infonuagiques et autres qui sont sûrs.

Téléchargez le Guide
Pensez cybersécurité pour les petites et moyennes entreprises
et obtenez d'autres ressources sur l' **#IdOAuTravail** à
PensezCybersecurite.ca

PENSEZCYBERSECURITE.CA

Canada