Question

Après avoir brièvement présenté et résumé le(s) document(s), vous répondrez à la question : Comment les objets connectés peuvent aider des entreprises ou des personnes mal intentionnées à violer la vie privée des utilisateur·ice·s ?

Questions préparatoires

Ces questions ne sont là que pour vous aider à comprendre le document. Leurs réponses n'apparaitront pas forcément dans la réponse à la question principale.

1. Décrire le fonctionnement normal de la poupée et de la caméra connectée, telle qu'aurait pu les présenter le constructeur.
2. Dans chacun des deux cas, décrire quelles informations ont pu ou pourraient obtenir des personnes malveillantes en utilisant les défauts des objets.
3. Donner les avantages et inconvénients d'avoir chez soi des objets connectés, comme ceux décrits dans les deux articles.

Barème

⚠️ **Avertissements** ⚠️ Votre note ne pourra pas être supérieure à la moyenne :
- si votre podcast n'est que la liste des réponses aux questions préparatoires ;
- si votre texte de présentation est la transcription de votre podcast.

Texte de présentation	**(… / 4)**
Titre Vous avez proposé un titre, court, clair, et percutant.	
Forme Vous avez rendu une courte présentation, en français correct, sans (trop) de fautes d'orthographe.	
Fond Elle présente correctement le podcast, pour donner envie de l'écouter.	
Bibliographie Elle est présente, et les références sont assez précises pour pouvoir retrouver le document d'origine.	

Prestation	**(… / 6)**
Pertinence Le contenu est pertinent et intéressant. Il n'y a pas hors sujet, et la question a sa réponse.	
Vulgarisation Le contenu est suffisamment vulgarisé pour que les auditeurs et auditrices ne connaissant ni le sujet ni le document le comprenne.	
Plan Le contenu est structuré.	
Bibliographie Vous citez le ou les documents présentés.	
Crédits Vous citez tous les membres du groupes (même celles et ceux que ne parlent pas), en respectant le nom ou pseudonyme choisi.	

SNT > INFORMATIQUE EMBARQUÉE > ENJEUX JOUETS

Question

Après avoir brièvement présenté et résumé le(s) document(s), vous répondrez à la question : Comment les objets connectés peuvent aider des entreprises ou des personnes mal intentionnées à violer la vie privée des utilisateur·ice·s ?

Questions préparatoires

Ces questions ne sont là que pour vous aider à comprendre le document. Leurs réponses n'apparaitront pas forcément dans la réponse à la question principale.

1. Décrire le fonctionnement normal de la poupée et de la caméra connectée, telle qu'aurait pu les présenter le constructeur.
2. Dans chacun des deux cas, décrire quelles informations ont pu ou pourraient obtenir des personnes malveillantes en utilisant les défauts des objets.
3. Donner les avantages et inconvénients d'avoir chez soi des objets connectés, comme ceux décrits dans les deux articles.

Barème

⚠️ **Avertissements** ⚠️ Votre note ne pourra pas être supérieure à la moyenne :
- si votre podcast n'est que la liste des réponses aux questions préparatoires ;
- si votre texte de présentation est la transcription de votre podcast.

Texte de présentation	**(… / 4)**
Titre Vous avez proposé un titre, court, clair, et percutant.	
Forme Vous avez rendu une courte présentation, en français correct, sans (trop) de fautes d'orthographe.	
Fond Elle présente correctement le podcast, pour donner envie de l'écouter.	
Bibliographie Elle est présente, et les références sont assez précises pour pouvoir retrouver le document d'origine.	

Prestation	**(… / 6)**
Pertinence Le contenu est pertinent et intéressant. Il n'y a pas hors sujet, et la question a sa réponse.	
Vulgarisation Le contenu est suffisamment vulgarisé pour que les auditeurs et auditrices ne connaissant ni le sujet ni le document le comprenne.	
Plan Le contenu est structuré.	
Bibliographie Vous citez le ou les documents présentés.	
Crédits Vous citez tous les membres du groupes (même celles et ceux que ne parlent pas), en respectant le nom ou pseudonyme choisi.	

Lucie Ronfaut, lefigaro.fr, *Sécurité : la* Cnil *accuse deux jouets connectés d'atteinte grave à la vie privée des enfants*, 4 décembre 2017.

http://www.lefigaro.fr/secteur/high-tech/2017/12/04/32001-20171204ARTFIG00098-securite-la-cnil-accuse-deux-jouets-connectes-d-atteinte-grave-a-la-vie-privee-des-enfants.php

Lundi, la CNIL a mis en demeure la société Genesis Industries, fabricant hongkongais de deux jouets connectés, pour « atteinte grave à la vie privée en raison d'un défaut de sécurité ». Il s'agit du robot i-Que et de la poupée Cayla, qui sont tous les deux commercialisés en France. « Ces vérifications ont permis de relever que la société collecte une multitude d'informations personnelles sur les enfants et leur entourage : les voix, le contenu des conversations échangées avec les jouets (qui peut révéler des données identifiantes comme une adresse, un nom…) mais également des informations renseignées dans un formulaire [d'une application] », précise l'autorité.

[…]

Les jouets intelligents peuvent poser plusieurs problèmes de sécurité. […] Par exemple, il est reproché au robot i-Que et à la poupée Cayla de ne pas sécuriser la connexion Bluetooth nécessaires pour les faire fonctionner. N'importe qui pouvait utiliser son smartphone pour se connecter au jouet, et donc le contrôler, sans remplir un code d'accès ou un mot de passe. On peut aussi les utiliser pour communiquer avec les enfants, en appelant le téléphone connecté ou en diffusant des sons pré-enregistrés. « Les contrôleurs de la CNIL ont constaté qu'une personne située à 9 mètres des jouets à l'extérieur d'un bâtiment, peut connecter (ou "appairer") un téléphone mobile aux jouets grâce au standard de communication Bluetooth sans avoir à s'authentifier », note la CNIL.

[…]

« Ce ne sont pas des problèmes simples à détecter, c'est difficile de s'en rendre compte soi-même », juge Justine Massera, juriste chez UFC Que-Choisir. Leurs conséquences peuvent pourtant être graves. En 2015, un internaute est parvenu à récupérer les données personnelles de cinq millions de parents et de 6 millions de jeunes propriétaires de jouets fabriqués par VTech. Parmi ces informations personnelles, des photos d'enfants. Plus récemment, en 2017, les peluches de Spiral Toys ont également été victimes d'une grave faille de sécurité, rendant accessibles plus de 200.000 enregistrements vocaux d'enfants.

Allyson Chiu, The Washington Post, *She installed a Ring camera in her children's room for 'peace of mind.' A hacker accessed it and harassed her 8-year-old daughter* (traduit par Louis Paternault), 12 décembre 2019.

https://www.washingtonpost.com/nation/2019/12/12/she-installed-ring-camera-her-childrens-room-peace-mind-hacker-accessed-it-harassed-her-year-old-daughter/

Dans un échange glaçant capturé en vidéo la semaine dernière, les LeMay racontent [qu'un étranger] a pu interagir avec leur fille après avoir piraté une caméra de vidéosurveillance Ring qui avait été installée récemment dans la chambre partagée par Alyssa et ses deux petites sœurs. Durant plusieurs minutes, l'homme a proféré des insultes racistes à son encontre, et a essayé de la persuader de faire des bêtises […].

Les LeMay, pourtant, ne sont pas les seules personnes à avoir vécu ce cauchemar ces dernières semaines. Plusieurs utilisateurs dans tous le pays ont raconté que leur système de sécurité a aussi été infiltré par des pirates qui les ont harcelés grâce à la fonction de discussion de la caméra.

SNT > INFORMATIQUE EMBARQUÉE > ENJEUX JOUETS

Lucie Ronfaut, lefigaro.fr, *Sécurité : la* Cnil *accuse deux jouets connectés d'atteinte grave à la vie privée des enfants*, 4 décembre 2017.

http://www.lefigaro.fr/secteur/high-tech/2017/12/04/32001-20171204ARTFIG00098-securite-la-cnil-accuse-deux-jouets-connectes-d-atteinte-grave-a-la-vie-privee-des-enfants.php

Lundi, la CNIL a mis en demeure la société Genesis Industries, fabricant hongkongais de deux jouets connectés, pour « atteinte grave à la vie privée en raison d'un défaut de sécurité ». Il s'agit du robot i-Que et de la poupée Cayla, qui sont tous les deux commercialisés en France. « Ces vérifications ont permis de relever que la société collecte une multitude d'informations personnelles sur les enfants et leur entourage : les voix, le contenu des conversations échangées avec les jouets (qui peut révéler des données identifiantes comme une adresse, un nom…) mais également des informations renseignées dans un formulaire [d'une application] », précise l'autorité.

[…]

Les jouets intelligents peuvent poser plusieurs problèmes de sécurité. […] Par exemple, il est reproché au robot i-Que et à la poupée Cayla de ne pas sécuriser la connexion Bluetooth nécessaires pour les faire fonctionner. N'importe qui pouvait utiliser son smartphone pour se connecter au jouet, et donc le contrôler, sans remplir un code d'accès ou un mot de passe. On peut aussi les utiliser pour communiquer avec les enfants, en appelant le téléphone connecté ou en diffusant des sons pré-enregistrés. « Les contrôleurs de la CNIL ont constaté qu'une personne située à 9 mètres des jouets à l'extérieur d'un bâtiment, peut connecter (ou "appairer") un téléphone mobile aux jouets grâce au standard de communication Bluetooth sans avoir à s'authentifier », note la CNIL.

[…]

« Ce ne sont pas des problèmes simples à détecter, c'est difficile de s'en rendre compte soi-même », juge Justine Massera, juriste chez UFC Que-Choisir. Leurs conséquences peuvent pourtant être graves. En 2015, un internaute est parvenu à récupérer les données personnelles de cinq millions de parents et de 6 millions de jeunes propriétaires de jouets fabriqués par VTech. Parmi ces informations personnelles, des photos d'enfants. Plus récemment, en 2017, les peluches de Spiral Toys ont également été victimes d'une grave faille de sécurité, rendant accessibles plus de 200.000 enregistrements vocaux d'enfants.

Allyson Chiu, The Washington Post, *She installed a Ring camera in her children's room for 'peace of mind.' A hacker accessed it and harassed her 8-year-old daughter* (traduit par Louis Paternault), 12 décembre 2019.

https://www.washingtonpost.com/nation/2019/12/12/she-installed-ring-camera-her-childrens-room-peace-mind-hacker-accessed-it-harassed-her-year-old-daughter/

Dans un échange glaçant capturé en vidéo la semaine dernière, les LeMay racontent [qu'un étranger] a pu interagir avec leur fille après avoir piraté une caméra de vidéosurveillance Ring qui avait été installée récemment dans la chambre partagée par Alyssa et ses deux petites sœurs. Durant plusieurs minutes, l'homme a proféré des insultes racistes à son encontre, et a essayé de la persuader de faire des bêtises […].

Les LeMay, pourtant, ne sont pas les seules personnes à avoir vécu ce cauchemar ces dernières semaines. Plusieurs utilisateurs dans tous le pays ont raconté que leur système de sécurité a aussi été infiltré par des pirates qui les ont harcelés grâce à la fonction de discussion de la caméra.