

Recharger son cellulaire sur un port USB public, c'est risqué

Crédit et remerciements à Madame Lise Langlois, membre du CIVBDL

Pour le partage du sujet, reçu par courriel :

À la suite de l'écoute de l'émission « On va se le dire », il a été également confirmé de ne jamais charger vos appareils en utilisant uniquement votre câble de recharge USB

Eh oui, dans les endroits publics tels que les hôtels, aéroports, centres commerciaux, etc. il est possible d'infiltrer votre système informatique.

Pour recharger vos appareils (ordinateur, tablette, cellulaire), toujours utiliser une prise électrique (donc mettre l'embout au bout du fil et brancher au mur).

Cette façon est sécuritaire.

NDLR : en collaboration avec



Question à Microsoft Copilot (IA) :

Question sur la cybersécurité et les endroits publics pour recharger mon cellulaire, dois-je le brancher dans une fiche secteur ou via un port de mon ordinateur ?

Semble-t-il que en rechargeant port à port, il y aurait des risques de me faire arnaquer

Réponse de Microsoft Copilot (IA) :

La cybersécurité est un sujet important, surtout lorsqu'il s'agit de recharger votre cellulaire dans des lieux publics.

Il est vrai que brancher votre cellulaire à des ports USB publics peut présenter des risques de sécurité, comme le "juice jacking"*

[C'est une technique où des logiciels malveillants peuvent être installés sur votre appareil ou des données peuvent être volées lorsque vous utilisez un port USB public.](#)

* Le “juice jacking” est un type de cyberattaque qui cible les appareils électroniques lorsqu’ils sont branchés à des ports USB publics pour se recharger.

Ces ports USB peuvent également servir de port de transfert de données, ce qui permet aux attaquants d’installer des logiciels malveillants sur l’appareil ou de voler des données.

Voici quelques exemples de ce qui peut se produire lors d’une attaque de juice jacking:

Installation de logiciels malveillants:

Un attaquant peut installer un malware sur votre appareil pendant qu’il est branché à un port USB compromis.

Vol de données:

Des informations sensibles comme des photos, des messages et des données d’authentification peuvent être extraites de votre appareil.

Attaques ciblées:

Les attaquants peuvent cibler des lieux spécifiques comme des aéroports ou des hôtels pour atteindre un grand nombre de victimes ou des individus spécifiques.

Pour se protéger contre le juice jacking, il est recommandé d’utiliser des prises secteur plutôt que des ports USB publics, d’utiliser un bloqueur de données USB, et de ne jamais faire confiance aux câbles ou chargeurs qui ne sont pas les vôtres.

Voici quelques conseils pour minimiser les risques :

- Utilisez des prises secteur plutôt que des ports USB publics et branchez-y votre propre chargeur.
- Envisagez d’utiliser un bloqueur de données, qui permet seulement à l’électricité de passer.
- Refusez toute demande d’accès ou d’installation de logiciel lors de la connexion à un port USB public.
- Gardez une batterie externe chargée avec vous pour éviter d’utiliser les ports USB publics.

[Ces mesures peuvent aider à protéger votre téléphone et vos données personnelles contre les cyberattaques dans les lieux publics.](#)

Question à Microsoft Copilot (IA) :

Quels sont les signes d'une attaque juice jacking ?

Réponse de Microsoft Copilot (IA) :

Les signes d’une attaque de juice jacking ne sont pas toujours évidents, car les cyberattaques sont souvent conçues pour être discrètes.

[Cependant, voici quelques signaux qui peuvent indiquer une attaque potentielle:](#)

- **Comportement inhabituel de l'appareil:**
Si votre téléphone ou tablette commence à se comporter de manière inattendue après avoir été chargé via un port USB public, cela peut être un signe d'interférence malveillante.
- **Demandes de permissions inattendues:**
Si des demandes d'accès ou d'installation de logiciels apparaissent soudainement, cela peut indiquer une tentative d'installation de logiciels malveillants.
- **Ralentissement de l'appareil:**
Un ralentissement notable de la performance de l'appareil peut être le résultat d'un logiciel malveillant opérant en arrière-plan.
- **Utilisation élevée des données:**
Une augmentation inexplicquée de l'utilisation des données peut signifier que des données sont transférées à votre insu.
- **Changements dans les fichiers ou les applications:**
Des modifications non autorisées dans vos fichiers ou applications peuvent être le résultat d'une attaque.

[Il est important de rester vigilant et de prendre des mesures préventives pour protéger vos appareils contre le juice jacking, comme utiliser des prises secteur ou des bloqueurs de données USB.](#)

Si vous suspectez une attaque, il est conseillé de faire analyser votre appareil par un professionnel de la cybersécurité.

Question à Microsoft Copilot (IA) :

Est-il sûr d'utiliser des chargeurs sans fil dans les lieux publics?

Réponse de Microsoft Copilot (IA) :

[L'utilisation de chargeurs sans fil dans les lieux publics est généralement considérée comme sûre, car ces chargeurs utilisent des standards comme Qi ou MagSafe qui ne permettent pas le transfert de données.](#)

Cela signifie qu'il n'y a pas de risque de juice jacking ou de vol de données lors de l'utilisation de ces chargeurs sans fil.

[Cependant, il est toujours bon de rester vigilant et de s'assurer que les stations de recharge sans fil publiques sont fournies par des sources fiables.](#)

Pour une sécurité optimale, voici quelques conseils :

- **Vérifiez la source:**
Assurez-vous que la station de recharge sans fil est fournie par une source ou un établissement de confiance.

- **Surveillez votre appareil:**
Gardez un œil sur votre téléphone pendant qu'il se recharge.
- **Utilisez des accessoires de confiance:**
Si possible, utilisez vos propres accessoires de recharge sans fil, comme des coussins ou des étuis de recharge.

[En suivant ces conseils, vous pouvez profiter de la commodité des chargeurs sans fil tout en minimisant les risques de sécurité](#)

Références supplémentaires pour en savoir plus :

Titre : Recharger votre cellulaire sur un port USB public vous fait courir de gros risques

Lien : [Recharger votre smartphone sur un port USB public vous fait courir de gros risques \(tomsguide.fr\)](#)

Titre : Recharger son smartphone sur un port USB public, c'est risqué

Lien : [Recharger son smartphone sur un port USB public, c'est risqué | 60 Millions de Consommateurs \(60millions-mag.com\)](#)

Titre : En chargeant votre téléphone dans un aéroport ou une gare, vous vous exposez à un risque

Lien : [En chargeant votre téléphone dans un aéroport ou une gare, vous vous exposez à un risque \(journaldesfemmes.fr\)](#)

Titre : Chargeur USB : pourquoi il est dangereux de brancher votre smartphone sur des bornes publiques

Lien : [Chargeur USB : pourquoi il est dangereux de brancher votre smartphone sur des bornes publiques \(phonandroid.com\)](#)

Titre : Recharger son smartphone dans un lieu public peut s'avérer très dangereux

Lien : [Recharger son smartphone dans un lieu public peut s'avérer très dangereux \(science-et-vie.com\)](#)

Titre : Le FBI alerte sur les risques de recharger son téléphone dans les lieux publics

Lien : [Le FBI alerte sur les risques de recharger son téléphone dans les lieux publics : Femme Actuelle Le MAG](#)

Recherche et mise en page par:

Michel Cloutier

CIVBDL

20240205

"C'est ensemble qu'on avance"