MINISTÈRE
DE L'INTÉRIEUR
*Liberté*
*Égalité*
*Fraternité*

POLICE
NATIONALE

*Direction générale de la police nationale*
*Direction interdépartementale de la police nationale de Seine-et-Marne*
*Circonscription de Police Nationale de Melun Val de Seine*

# LA POLICE NATIONALE VOUS INFORME

L'Association UFC Que Choisir attire l'attention des utilisateurs de voitures électriques, en effet la hausse de ces dernières crée des opportunités pour les escrocs. L'Association vous invite à adopter les bons réflexes pour ne pas tomber dans leurs pièges.

Afin d'améliorer l'expérience utilisateur des propriétaires de véhicules électriques, toutes les nouvelles bornes de recharge devront désormais être équipées d'un terminal de paiement. Jusqu'alors, cette option était marginale. Il fallait soit télécharger l'application du fournisseur et fournir son numéro de carte bancaire, soit posséder une carte de recharge du constructeur ou de type Chargemap. Cela a évidemment inspiré les escrocs en tout genre. Leur but ? Collecter des données personnelles pour les utiliser frauduleusement.

## Arnaque au QR code falsifié

Sur le point de recharge, les aigrefins placent un autocollant avec un QR code imitant celui du fournisseur d'énergie. Quand vous le scannez, vous êtes dirigé vers un site web frauduleux qui réclame moult informations : nom, adresse, numéro de carte de crédit… et même des identifiants de connexion pour le service de recharge légitime.

**Le bon réflexe:** si vous avez un doute, passez par l'appli de la station de recharge pour payer et lancer la session. Avant de scanner le QR code, vérifiez qu'il ne s'agit pas d'un ajout, d'un autocollant posé sur un autre.

## Arnaque au faux abonnement

Cette arnaque n'est pas spécifique à l'univers de la voiture électrique. Sur les réseaux sociaux ou par courriel, vous pouvez recevoir une offre d'abonnement à un tarif particulièrement alléchant. Lors de la souscription, on vous réclame vos données personnelles et coordonnées bancaires. Si vous les fournissez, hop, le tour est joué pour les escrocs.

**Le bon réflexe:** en général, ce type d'escroqueries est vite démasqué. Vérifiez toujours sur Internet si l'offre est sérieuse ou signalée comme malveillante.

## Arnaque à la fausse station

Heureusement, les cas sont encore rares. L'idée est d'indiquer des aires de recharge qui n'existent pas sur les applis de localisation. Y figurent de fausses informations, comme un tarif avantageux et la possibilité de réserver sa place. La suite est identique aux méthodes précédentes, avec pour objectif de récupérer les données de paiement. Attention, cette arnaque peut aussi être utilisée pour vous attirer dans une zone peu fréquentée pour vous soutirer directement de l'argent.

**Le bon réflexe:** si la station semble isolée, vérifiez son existence sur plusieurs sources avant de vous y rendre.

## Arnaque par hameçonnage

Vous recevez un SMS ou un courriel vous intimant de mettre à jour votre carte bancaire pour pouvoir continuer à recharger votre voiture électrique. Mais il vous renvoie vers un site frauduleux ou une application mobile contrefaite qui demanderont vos données personnelles.

**Le bon réflexe:** accédez au site web ou à l'appli officielle du fournisseur de service en tapant l'URL dans votre navigateur, et allez sur votre compte.

**Source:** UFC Que Choisir décembre 2024