L'accusation de pédophilie

Un mail aux multiples en-têtes "Europol", "Police fédérale", "Direction générale de la police judiciaire" vous est adressé. Un policier vous accuse de pédophilie après une pseudo-saisie informatique. Il indique que vous faites l'objet de poursuites judiciaires parce que vous avez envoyé des images dénudées à des mineurs ou consulté des sites pédophiles et que le procureur va vous envoyer en prison, sauf si vous répondez et que vous payez une amende.
La gendarmerie, ou la police ne convoquent jamais par mail, surtout pour des faits de cette nature. Il faut être attentif aux fautes d'orthographe et la justice ne demande jamais d'argent pour arrêter des poursuites judiciaires.

L'assurance maladie

Le SMS est lapidaire et des centaines de personnes le reçoivent chaque jour en ce moment : "Malheureusement votre carte vitale est arrivée à expiration, veuillez renouveler votre carte en cliquant sur ce lien" peut-on y lire.
Face à ces tentatives d'hameçonnage (Phising), l'assurance maladie invite à la plus grande prudence.
La commande ou le renouvellement de la carte vitale ne s'effectue que sur le compte Ameli. La Sécurité Sociale ne vous demandera jamais la transmission par mail ou SMS de vos coordonnées bancaires ni vos informations personnelles.

Les ventes sur le boncoin.fr...

L'escroquerie touche les échanges sur le boncoin.fr, Vinted et autres sites où vous avez déposé des objets à la revente. Une personne se dit intéressée, vous contacte mais indique qu'elle ne peut payer que par Paypal. Vous n'avez pas ce moyen de règlement ? L'escroc vous dit alors qu'il vous envoie de quoi créer le compte Paypal, puis vous demande de verser 1000 € qui seront restitués.
Si vous voulez vendre quelque chose sur ces sites, ce n'est pas à vous de verser de l'argent ! N'envoyez les objets que lorsque la somme est créditée sur votre compte.

La publicité en ligne

Cette arnaque fleurit sur beaucoup de sites en ligne où, tout d'un coup, un témoin assure sur une publicité vidéo qu'il a gagné beaucoup d'argent avec un investissement minime et autres recettes miraculeuses pour faire fructifier ses économies.
Quand c'est trop beau, c'est forcément une arnaque !

Le SMS du faux paiement

Vous recevez un message affirmant que vous avez effectué un paiement de telle ou telle somme et demandant, si vous n'en êtes pas l'auteur, de composer un numéro.
On vous demande de fournir vos coordonnées bancaires.
Ne rappelez jamais ces numéros ! en plus, il se peut qu'ils soient surtaxés.

L'arnaque bancaire par téléphone

Une variante du SMS mais avec un appel. La banque vous téléphone indiquant qu'il y a eu une utilisation frauduleuse de votre carte bancaire et vous redemande la date d'expiration et le code cryptogramme, car il s'agit d'un achat en ligne Là, la victime reçoit un SMS qui demande de rentrer un code pour valider le blocage… En fait, l'opérateur a fait des achats en ligne.
Ne fournissez jamais vos codes de CB. Appelez immédiatement votre conseiller bancaire.

L'escroquerie aux sentiments

Technique ancienne mais redoutablement efficace et plus que jamais d'actualité. Votre adresse mail a été piratée et tous vos contacts reçoivent le même message : vous êtes soi-disant bloqué à l'étranger, empêtré dans une sale affaire ou touché par une grave maladie, vous ne pouvez pas téléphoner, mais vous avez un besoin urgent d'argent via des cartes de prépaiement.