Nouvelle arnaque: livraison de commande en ligne

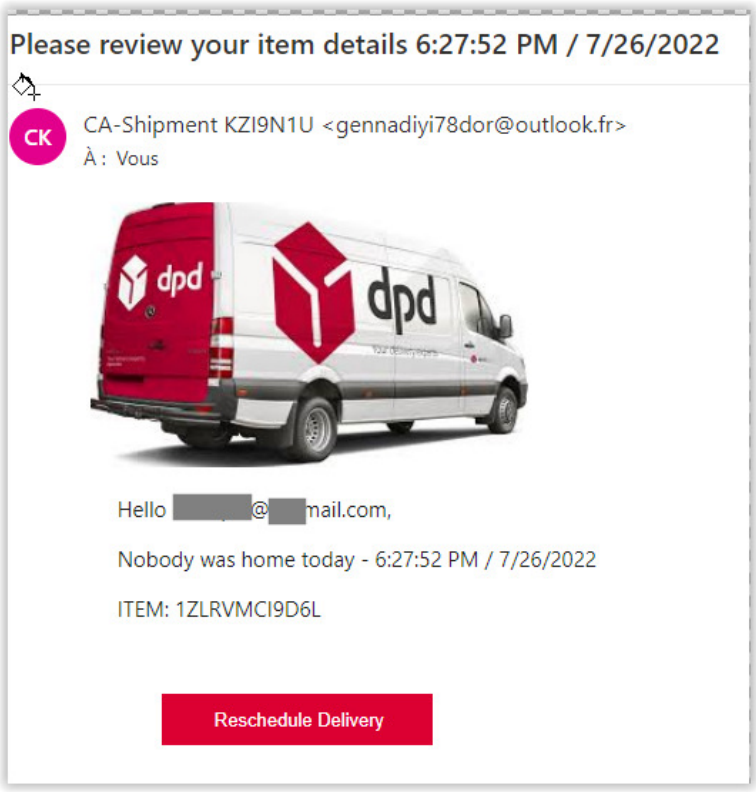
La situation

De nos jours, presque tout le monde effectue des commandes en ligne, et les produits commandés sont livrés chez soi par un livreur (Amazon, Postes Canada, etc.). On s'attend à recevoir un courriel par ce livreur nous informant de la réception de la commande et de la date estimée de livraison.

Or une nouvelle arnaque courriel consiste à vous aviser que votre commande en ligne a subi des problèmes et que vous devrez débourser plus pour recevoir votre commande.

Le scénario

Vous recevez un courriel du genre qui suit :



Recevoir un tel message est logique, car on a effectivement fait une commande en ligne, d'autant plus que DPD est une agence de livraison qui existe vraiment (cela aurait pu aussi bien être Amazon, Postes Canada, etc.). Donc on clique le bouton "*Reschedule Delivery*". Le site du supposé livreur, qui est sécurisé (débute par *https//*) vous informe que vous étiez absent lors de la livraison de votre commande, que le livreur ne pouvait laisser le colis devant la porte car il valait trop cher, et qu'une autre livraison vous occasionnera des frais de $1,50 que vous devrez payez avec une carte de crédit pour avoir une nouvelle date de livraison. Le montant est minime, donc vous vous exécutez avec votre carte de crédit. Le site vous avise que le paiement est refusé, et vous suggère d'utiliser une autre carte de crédit, ce que vous faites: on vous refuse

encore le paiement, qui immanquablement est aussi refusée. Et ainsi de suite pour toutes les cartes que vous utilisez.

Les conséquences

Les arnaqueurs possèdent maintenant tous ce qu'il faut pour cloner une nouvelle carte, et l'utiliser pour effectuer des achats sur vos comptes de crédit. Si vous êtes chanceux, et que votre banque est aux aguets, on vous appellera pour signaler des achats douteux sur votre carte de crédit, qui sera annulée et qui sera remplacée par la banque.

Comment détecter une telle fraude?

D'abord, tout réside dans le courriel lui-même:

- Il ne contient aucune information relative à votre achat, aucun bouton pour la consulter et encore moins votre nom ou l'endroit où vous avez fait l'achat en ligne.
- Il contient bien votre adresse courriel suite à "*Hello…*": c'est certain, sinon vous n'auriez jamais reçu ce courriel! L'arnaqueur ne vous connait pas, il envoie des courriels du genre à tout vent en essayant toutes combinaisons d'adresses courriel en espérant attraper des poissons!
- La date et l'heure de supposée tentative de livraison: même Amazon ne peut livrer avant le lendemain, donc si c'est la date de la commande, c'est louche.
- Aucune compagnie de livraison ne vous demandera des frais supplémentaires **pour quelque raison que ce soit**, car tous les frais ont déjà été encourus lors de l'achat du produit en ligne.
- Si l'on passe la souris sans cliquer sur le bouton "*Reschedude Delivery*" pour voir sur la ligne de statut du navigateur Web en bas de l'écran, l'adresse Web du site pointée par le bouton, on peut voir une adresse Web qui n'a rien à faire avec le livreur de la commande, ou qui ressemble un livreur connu, par exemple https://s3.amazonaws.com/... qui n'est pas le site d'Amazon mais une adresse trompeuse, car le nom de domaine principal (les caractères précédant le dernier point) doit être explicitement *amazon.com* ou *amazon.ca* si vous avez commandé chez Amazon.