Blainville, le 16 août 2021

Cher partenaire,

Il a été porté à notre attention qu'en ce moment il y a en circulation un courriel frauduleux laissant croire avoir été envoyé par Ralik. Celui-ci porte la mention de « Bon de paiement » avec un faux numéro de bon de commande. Il s'agit d'un « courriel d'hameçonnage ». Soyez assuré que nous avons pris les actions nécessaires pour régler la situation et nous sommes désolés des inconvénients que cette situation a pu vous occasionner.

Si vous êtes victime de cet envoi, nous vous demandons de ne pas ouvrir le courriel et de transmettre cette information au responsable des I.T. de votre entreprise. Veuillez cependant ne pas bloquer l'adresse comptabilite@ralik.ca car celle-ci est bien une adresse réelle de Ralik.

Nous vous invitions à communiquer avec nous pour toutes questions en lien avec ce message. Nous vous remercions de votre diligence et nous vous souhaitons une agréable journée !

L'équipe Web, Ralik
450 420 0022

Ne pas ouvrir ce courriel
Do not open this email

De : Comptabilité Ralik <comptabilite@ralik.ca>
Envoyé : 16 août 2021 08:35
À : ********@*******.com
Objet : ********@*******.com Bon de paiement

Bon de paiement 001005I.htm
49 KB

******* **Vous avez reçu un virement *SWIFT TRANSFER*.**

Time:	8:35:05 AM
Date:	Août 16, 2021
Recepient:	VOTRE ADRESSE COURRIEL
Message:	Le versement ci-joint décrit le dépôt direct envoyé à votre banque.
	Veuillez prévoir 1 à 3 jours ouvrables pour le traitement.

COMPTABILITÉ RALIK
450 420.0022, poste 215 \\ 1 800 99RALIK \\ **ralik.ca**
80, rue Omer-DeSerres, Blainville, Québec J7C 5V6

SIMPLIFIEZ VOTRE APPROVISIONNEMENT
PURCHASING MADE EASY

Qu'est-ce que l'hameçonnage?

L'hameçonnage est un cybercrime basé sur la tromperie pour voler des informations privées et confidentielles aux individus et aux compagnies.

L'hameçonnage consiste à piéger les victimes pour les amener à révéler des informations pourtant confidentielles. Comme les cybercriminels se font passer pour une personne de confiance, les victimes ne remettent pas la demande en doute. Elles croient agir dans le meilleur intérêt de tous.

En général, les cybercriminels demandent des informations telles la date de naissance, le numéro d'assurance sociale, le numéro de téléphone, les détails de la carte de crédit et l'adresse à la maison. Ils peuvent également demander de réinitialiser le mot de passe.

Les cybercriminels utilisent ensuite cette information pour personnifier la victime et commettre différentes actions frauduleuses en son nom comme se procurer une carte de crédit, demander un prêt ou ouvrir un compte de banque. Certains cybercriminels utilisent les informations recueillies par hameçonnage pour lancer une cyberattaque plus ciblée qui nécessite de connaître des détails sur la victime.