Conseils pour se protéger contre les techniques de phishing

- Selon les politiques de financement et de contrôle de Sidel Group, Sidel applique un système de double autorisation, y compris pour les modifications en matière d'ordres de paiement. Tout changement doit être approuvé au préalable, par écrit et par deux personnes autorisées par une entité juridique Sidel. Ces changements d'ordres de paiement sont extrêmement rares. Sidel demande rarement à modifier un paiement d'une banque vers une autre, notamment vers un pays tiers.
- Une facture Sidel est toujours jointe à toute demande de paiement. Par conséquent, vous devez immédiatement vous méfier des demandes ne contenant pas une facture correcte.
- Dans tout rappel ou toute demande de suivi concernant un paiement, vous trouverez systématiquement une référence à la demande initiale et la facture incluse. Par conséquent, vous devez immédiatement vous méfier des demandes ne contenant aucune référence à la demande initiale et aucune facture.
- En cas de modifications apportées à vos demandes et ordres de paiement de la part des entités juridiques ou agents Sidel (même si l'expéditeur semble bien être Sidel), nous vous recommandons de toujours confirmer l'ordre verbalement en appelant votre contact Sidel de confiance au numéro habituel. **N'utilisez pas** les coordonnées fournies par l'expéditeur figurant sur les demandes de paiement et changements d'ordre de paiement. Appelez votre contact Sidel de confiance au numéro habituel. Ceci est particulièrement important si vous recevez une demande de transfert de fonds ou d'informations sensibles pour l'entreprise à partir d'une adresse électronique qui semble différente du format prénom.nom@sidel.com.
- Sidel utilise uniquement les adresses électroniques sidel.com telle que prénom.nom@sidel.com. Sidel n'utilise pas d'adresses mail comme sidel.net, side1.com, sidei.com, etc.
- N'ouvrez pas et ne répondez pas à des spams provenant de tiers
- Ne réagissez pas aux courriels ou appels vous demandant des informations commerciales sensibles ou personnelles. Vérifiez toujours la source (en enregistrant les informations relatives à la demande initiale puis en appelant la personne nommée par téléphone à son numéro habituel).
- Lorsque vous envoyez des informations commerciales sensibles par e-mail, veillez à crypter votre message.
- Lorsque vous accédez à un site Internet via un moteur de recherche connu, assurez-vous de son authenticité en vérifiant l'adresse URL, souvent affichée dans le moteur de recherche.
- Vérifiez toujours l'identité de la personne avec laquelle vous communiquez par voie électronique (par e-mail par exemple) et le but de sa demande si vous avez des doutes.
- Méfiez-vous des e-mails externes contenant des liens vers des sites Web, aussi officiel que le message puisse paraître.
- Ne cliquez jamais sur un hyperlien (tel qu'un lien vers une page Web) dans un e-mail si vous avez des doutes sur le message ou sur l'expéditeur. Si vous êtes dirigé vers

un site Sidel à partir d'un e-mail, vérifiez toujours que l'adresse du site est une adresse sidel.com.

- Les principaux sites Web que Sidel utilise pour sa communication externe sont www.sidel.com, www.sidel.de, www.sidel.pt, www.sidel.es, www.sidel.cn, www.sidel.fr et www.sidel.ru. Si vous êtes invité dans un e-mail à accéder à un autre site Sidel, ne cliquez pas sur le lien et vérifiez d'abord par téléphone en appelant votre contact Sidel habituel.
- Procédez toujours à la mise à jour des ordinateurs avec les derniers correctifs de sécurité. Les systèmes d'exploitation (comme Windows) sont régulièrement améliorés par leurs fournisseurs offrant ainsi plus de garanties en termes de sécurité. Windows, par exemple, permet aux utilisateurs d'installer automatiquement des correctifs de sécurité via http://windowsupdate.microsoft.com.
- Les navigateurs Internet (comme Internet Explorer, Mozilla Firefox, Google Chrome, Safari (Apple), etc.) offrent désormais une protection contre les sites Web frauduleux et ont des fonctionnalités anti-phishing dans leurs menus. Votre ou vos navigateur(s) doivent aussi être régulièrement mis à jour avec la dernière version.
- Tous les logiciels sur les ordinateurs doivent être régulièrement mis à jour. Les vendeurs font régulièrement apparaître des messages pop-up pour vous proposer une mise à jour de leur logiciel.
- Envisagez l'installation de logiciels antivirus et anti-espion (qui sont souvent disponibles dans le même produit) et assurez-vous qu'ils soient à jour. Vous devez également faire une mise à jour régulière de ces logiciels.
- La plupart des logiciels antivirus s'appuient sur une base de données de virus, qui peut être mise à jour plusieurs fois par jour. L'antivirus peut être configuré pour installer automatiquement ces mises à jour de base de données afin d'assurer une protection maximale. Vous pouvez envisager de scanner votre ordinateur après l'installation ou la mise à jour de l'antivirus pour vérifier toute éventuelle infection.
- Envisagez l'activation d'un pare-feu personnel. Cela vous permet de protéger l'ordinateur contre les intrusions et de contrôler le trafic entrant et sortant.
- Sécurisez votre e-mail. Votre logiciel de messagerie doit être équipé d'un filtre anti-spam. L'accès à votre messagerie doit être protégé par un login et un mot de passe robuste.
- Si vous pensez que votre adresse e-mail a été piratée, pensez à utiliser une nouvelle adresse e-mail et à la communiquer à tous vos contacts.

Enfin, n'oubliez pas de toujours revérifier toutes les demandes de modification de financement ou de coordonnées bancaires, et de vérifier l'identité de l'expéditeur autorisé. Confirmez la demande en appelant l'expéditeur à son numéro habituel (n'utilisez pas les coordonnées figurant dans l'e-mail).

Pour plus d'informations, conseils et consignes, rendez-vous sur les sites de support internationaux http://www.stopthinkconnect.org/ et http://www.antiphishing.org/.