Termes et conditions applicables à la communication par courriel

Les présents termes et conditions générales applicables à la communication par courriel constituent une partie intégrante du Contrat de Communication par courriel conclu entre le(s) titulaire(s) du compte, le(s) client(s) et les parties au contrat (dénommées ci-après conjointement « le Client ») et Rothschild & Co Bank AG (la « Banque »).

Le Client et les Destinataires / Expéditeurs confirment par la présente avoir pris connaissance des informations ci-dessous, termes et conditions qui s'appliquant à la communication par courriel avec la Banque. Il a / Ils ont conscience qu'il existe certaines menaces dans l'environnement moderne des communications mondiales, et qu'il est essentiel de veiller à un traitement sécurisé de ses/leurs données dans le cadre de ses/leurs activités bancaires.

Risques

Le Client et les Destinataires / Expéditeurs confirment avoir pris connaissance qu'un ordre, une notification ou une communication envoyée par courriel est transmis via un réseau ouvert, accessible au public et parfois à l'étranger, et peut par conséquent, en principe, et s'il n'est pas chiffré, être vu par des tiers, qui pourraient en conclure qu'une relation bancaire existe avec la Banque. Le Client et les Destinataires / Expéditeurs confirment également avoir pris connaissance que le contenu linguistique et électronique d'un ordre, d'une notification ou d'une communication envoyé par courriel non chiffré peut être modifié et manipulé par des tiers.

Si la communication entre la Banque et le Destinataire / l'Expéditeur est cryptée, le contenu de la communication faite au moyen des adresses courriel ou du nom de domaine donnés sera protégé. Le Client et les Destinataires / Expéditeurs prennent note que seul le contenu est protégé, mais pas l'adresse courriel de la Banque ni les adresses courriel ou le nom de domaine donnés, ceux-ci ne sont pas anonymes, le fait qu'il y a une communication avec la Banque reste donc visible.

Dans cette mesure, le Client et les Destinataires / Expéditeurs libèrent expressément la Banque de toute obligation de protection des données et du secret bancaire.

De plus, des personnes non autorisées pourraient obtenir un accès non autorisé aux installations informatiques (l'ordinateur personnel par exemple) du Client ou du Destinataire / de l'Expéditeur pendant une session Internet. Le Client et les Destinataires / Expéditeurs savent et confirment avoir pris connaissance qu'un tel risque peut être accru lorsque l'on indique seulement / également un nom de domaine. Il incombe donc à chaque utilisateur de prendre toutes les précautions techniques nécessaires pour minimiser les risques inhérents à l'utilisation d'Internet et de veiller à ce que son système informatique soit équipé des dispositifs les plus récents en matière de protection contre les logiciels malveillants (virus, vers, chevaux de Troie) et les pirates informatiques (en installant notamment un pare-feu).

Le Client et les Expéditeurs / Destinataires confirment avoir pris connaissance du fait que la transmission d'un ordre, d'une notification ou d'une communication peut être retardée, interrompue ou rendue totalement impossible en raison d'erreurs de transmission, de défauts techniques, de coupures, de pannes, d'une intervention illégale, de surcharge du réseau ou du blocage injustifié de l'accès électronique par des tiers ou d'autres défaillances de la part des opérateurs de réseau. En outre, des retards peuvent également survenir en raison du temps nécessaire à la Banque pour traiter un courriel.

Usurpation d'identité

L'usurpation d'identité est un des délits connaissant la plus forte augmentation dans le secteur financier, et affecte des millions de personnes tous les ans. L'usurpation d'identité consiste à voler l'identité / les informations personnelles de quelqu'un, comme son nom, sa date de naissance, son adresse, son courriel, etc. et à ce que ces informations soient ensuite utilisées par des escrocs à des fins d'enrichissement personnel. Par exemple, les escrocs peuvent utiliser les données relatives à l'identité pour réaliser des paiements et des transferts de fonds, ou utiliser les informations d'une carte de crédit pour acheter des biens et services aux frais de la personne dont l'identité a été volée. Pour obtenir des informations relatives à l'identité, il est courant que les escrocs piratent un compte mail afin d'accéder à la correspondance par courriel et d'identifier les relations de la personne, voire de les exploiter.

Courriels frauduleux

Les escrocs utilisent souvent les courriels pour recueillir les informations personnelles des particuliers. De tels courriels peuvent demander au destinataire de mettre à jour ou de vérifier leurs informations financières ou personnelles, dont leur date de naissance, leurs identifiants, les informations de leur compte, le numéro de leur carte de crédit, etc. Généralement, ces courriels prétendent venir d'une organisation légitime telle qu'une banque ou un commerçant en ligne. Le courriel contient un lien qui renvoie vers un faux site web ressemblant exactement (ou étant quasi-similaire) au vrai site de l'organisation. L'escroc peut alors recueillir les données personnelles telles que les mots de passe lorsque vous les saisissez, ou charger des programmes malveillants sur votre ordinateur.

Si un Client ou les Destinataires / Expéditeurs reçoivent un mail contenant des demandes spécifiques à ses informations bancaires dont ils ne sont pas sûrs que la source soit bien la Banque, le Client ou les Destinataires / Expéditeurs doit / doivent alors contacter son / leur Conseiller par téléphone afin de procéder à une vérification. Si le Client et les Destinataires / Expéditeurs ont le moindre doute quant au fait qu'un compte e-mail depuis lequel il a / ils ont communiqué avec la Banque puisse être compromis, le Client et les Destinataires / Expéditeurs doit / doivent alors immédiatement en informer la Banque.

Protection

Afin de réduire le risque que son / leur compte e-mail ne soit compromis ou victime d'usurpation d'identité, le Client et les Destinataires / Expéditeurs doit / doivent suivre les recommandations de sécurité suivantes :

- Toujours rester vigilant sur Internet, et faire très attention à qui et où l'on donne ses données personnelles.
- Ne pas envoyer de mots de passe par courriel, et ne pas les donner à d'autres personnes. La Banque ne vous demandera jamais vos mots de passe.
- Ne pas répondre à des courriels non sollicités ou indésirables, et ne jamais donner d'informations personnelles ou sur son compte bancaire si c'est demandé mais qu'il n'y a aucune certitude absolue quant au destinataire. La Banque ne contactera ses Clients ou les Destinataires / Expéditeurs que via le Conseiller Client respectif.
- Ne pas cliquer sur les liens figurant dans les courriels suspects. Cliquer sur un lien de ce type peut entraîner le téléchargement sur l'ordinateur de logiciels malveillants tels qu'un virus, et permettre ainsi à un pirate ou un escroc d'accéder aux informations personnelles.
- Pour protéger ses comptes e-mail, utiliser un mot de passe difficile à deviner. Un mot de passe fort doit comprendre au moins huit caractères et contenir des lettres majuscules, des chiffres et des caractères spéciaux tels que / $ _ # - + etc. Il est également recommandé d'utiliser des mots de passe différents pour chaque application et chaque compte.
- Utiliser un anti-virus sur l'ordinateur personnel, et le mettre à jour en chargeant les nouvelles versions.
- Vérifier et rapprocher régulièrement les relevés de compte afin de s'assurer que toutes les transactions sont bien légitimes. De même, toujours vérifier les relevés de compte afin de contrôler s'il y a eu des transferts non autorisés.

La solution de communication sécurisée de la Banque

La Banque propose *Secure Email*, un environnement de communication sécurisé avec la Banque. *Secure Email* offre au Client les avantages de sécurité suivants :

- La correspondance par courriel entretenue avec Rothschild est séparée de vos autres courriels personnels, et l'accès aux courriels requiert un nom d'utilisateur et un mot de passe supplémentaires. Ainsi, un pirate ayant accédé à votre compte personnel n'aurait pas connaissance des courriels et informations échangés avec Rothschild.
- Les courriels du Client ou de tout Destinataire / Expéditeur sont stockés exclusivement dans les systèmes de la Banque et ne quittent jamais les locaux de la Banque.
- Les systèmes de la Banque sont sûrs et soumis à des contrôles de sécurité réguliers effectués par des sociétés spécialisées en cybersécurité.
- Secure Email est facile à utiliser et fonctionne sur la plupart des appareils.