Assurance responsabilité professionnelle Barreau

Maîtres@droits

Service de prévention

Guylaine LeBrun, avocate
Coordonnateur aux activités de prévention

Judith Guérin, avocate
aux activités de prévention

Mars 2020

Prévenir les fraudes et les cyberrisques à l'ère de la COVID-19

Le mois de mars est le mois de la prévention de la fraude au Canada, mais en cette période d'incertitude créée par la COVID-19, les fraudeurs tentent d'en tirer profit et d'exploiter les faiblesses qui peuvent subsister dans nos systèmes de sécurité. Cela est d'autant plus vrai que le contexte actuel amène une surutilisation des technologies de l'information pour interagir et maintenir nos relations d'affaires.

Dans le présent article, nous survolerons les mesures permettant de réduire les risques d'être victime de fraude, notamment par courriel. Puis, nous enchaînerons avec des mesures préventives en lien avec la cybercriminalité et le travail à distance.

Réduction des risques de fraude par courriel :

- Assurez-vous que des mesures de prévention sont prévues, connues et appliquées eu égard aux fraudes par courriel et aux cyberrisques. Une gestion adéquate des cyberrisques comporte également un plan d'intervention en cas d'incidents de cybersécurité. Des personnes responsables de l'application de ce plan doivent être spécifiquement nommées. De même, une version papier du plan devrait être conservée si l'accès à la version numérique s'avérait impossible;

- Sensibilisez les membres de votre équipe, avocats et personnel du cabinet, ainsi que vos clients, d'être prudents à l'égard de toute demande par courriel de transfert de fonds ou de modifications d'instructions de paiement;

- Élaborez une politique selon laquelle ces demandes sont soigneusement examinées et vérifiées directement auprès de la personne qui en fait la demande. Plus précisément, communiquez par téléphone avec le demandeur pour vous assurer que les instructions reçues émanent bel et bien de lui (comparez le numéro de téléphone qui apparaît dans le courriel avec celui qui figure dans vos dossiers ou posez des questions auxquelles seul votre client, votre collègue ou l'avocat adverse connaît les réponses);

- Posez des questions appropriées pour déterminer si la demande est légitime ou non;

- Renforcez vos contrôles internes. Par exemple, exigez que deux avocats examinent et approuvent la transaction en vérifiant les instructions du client. Ici, l'adage « Mieux vaut prévenir que guérir » trouve pleinement application;

- Vérifiez derrière l'adresse courriel affichée de l'expéditeur. Assurez-vous qu'il s'agit de la même adresse et qu'elle est connue. D'autres fraudeurs ne modifient qu'une lettre à l'adresse courriel de l'un de vos contacts. Il faut donc être vigilant et confirmer que l'adresse courriel par laquelle nous parvient la demande de transfert est la même que celle présente au dossier;

- Vérifiez d'où proviennent les demandes de transfert de fonds;

- Dans le cas de la remise d'un effet de commerce (chèque, traite ou autre), assurez-vous qu'il émane d'une institution financière canadienne. Suite au dépôt, obtenez une confirmation écrite auprès de l'institution financière qu'elle a vérifié la validité de l'effet de commerce et que les sommes sont disponibles;

- Dans tous les cas, ne répondez pas aux courriels du fraudeur.

Télétravail et cyberrisques

Par ailleurs, dans un effort pour limiter la propagation de la COVID-19, plusieurs d'entre nous seront en télétravail. Voici quelques mesures préventives en lien avec cette modalité de travail :

- Assurez-vous que les ordinateurs professionnels qui seront utilisés sont adéquatement protégés par des logiciels antivirus, anti-maliciels et coupe-feux (autant pour les avocats que pour le personnel du cabinet);

- Dotez-vous d'un système d'authentification fort. Plus précisément, chaque ordinateur doit être protégé par un mot de passe suffisamment long pour éviter les intrusions;

- Afin d'assurer le respect du secret professionnel et éviter les virus provenant de sites Internet ou d'applications non sécurisés, un ordinateur distinct doit être utilisé pour les activités professionnelles versus les activités familiales et personnelles;

- Portez une attention sur l'usage du cellulaire et mettez en place une politique à cet effet, notamment quant aux applications téléchargées et aux adresses courriel personnelles qui peuvent être l'objet de virus ou de cybercrime. Ceci dit, le cellulaire doit comporter minimalement un mot de passe pour être déverrouillé;

- De la même manière, transmettez des consignes précises quant à l'usage de la messagerie professionnelle. Autrement dit, interdisez l'utilisation de la messagerie personnelle à des fins professionnelles et inversement interdisez l'usage de la messagerie professionnelle à des fins personnelles;

- Protégez les pièces jointes par des logiciels prévus à cette fin;

- Utilisez une connexion à des réseaux privés plutôt qu'à des réseaux Wi-Fi publics autant pour les ordinateurs que pour les téléphones cellulaires. Vu les récentes mesures imposées par le gouvernement du Québec quant à l'accès à certains lieux publics, le respect de cette mesure ne devrait pas poser problème;

- Assurez-vous que l'accès au réseau soit sécurisé. Cela peut notamment se faire avec une clé VPN (réseau privé virtuel).

Ajoutons qu'il importe de maintenir en vigueur une couverture d'assurance adéquate et suffisante relativement à la cybercriminalité.

Bien que cela ne soit pas directement relié à la cybercriminalité, rappelons également l'importance de respecter nos obligations déontologiques relativement au secret professionnel, même si dans un contexte de télétravail, cela nécessite plus de logistique. Aussi, évitez de vous éparpiller et rangez tout dossier ou document confidentiel de façon à respecter le secret professionnel.

Bref, ne tardez plus… En privilégiant la mise en place de ces mesures relativement simples, vous réduirez les risques d'être victime de cybercriminalité et aurez l'esprit plus tranquille.