CONSEIL NATIONAL DES BARREAUX
LES AVOCATS

FLASH INFO

Samedi 11 avril 2020 #20

Covid-19 et confinement : Point sur votre cyber-sécurité

> Tentatives d'hameçonnage : Le CNB vous accompagne pour les déceler durant la crise sanitaire

Chaque jour, de nombreuses tentatives d'hameçonnage (phishing) ont lieu et en particulier depuis le début du confinement. Cette technique qu'utilisent les fraudeurs vous incite à leur communiquer des données personnelles en se faisant passer pour un tiers de confiance.

Vous pouvez déceler ces tentatives en prêtant attention aux indices suivants :

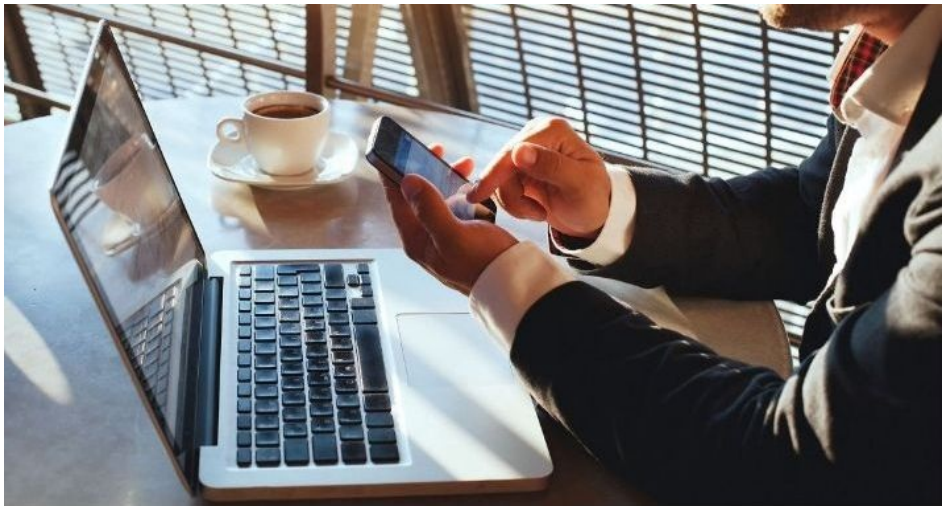
- Le mail ne vous est pas réellement destiné ;
- Le message évoque un dossier, une facture, un thème qui ne vous parle pas ;
- Le message comporte un lien cliquable (URL) dont la structure n'est pas cohérente avec celle de l'expéditeur du message ;
- Le message vous demande de communiquer des informations personnelles ;
- Il vous est demandé de payer des frais sans que vous n'en ayez été informé au préalable ;
- Le mail contient des menaces irréalistes ;
- Le mail semble émaner d'un acteur de référence (impôts, sécurité sociale) mais n'a pas la structure habituelle des messages que vous recevez.

Si vous avez un doute sur un message reçu, il y a de fortes chances que celui-ci ne soit pas légitime.

Que faire si vous êtes face à une tentative d'hameçonnage ?

- N'ouvrez surtout pas les pièces jointes ou les liens URL présents dans le mail et ne répondez-pas ;
- S'il s'agit de votre compte de messagerie professionnel et que l'adresse expéditrice contient l'identification du CNB : écrivez-nous à donneespersonnelles@cnb.avocat.fr en joignant le mail en pièce jointe. Nous le signalerons aux autorités compétentes ;
- Si vous avez reçu l'escroquerie dans vos courriers indésirables (spams) et qu'elle ne contient pas l'identité du CNB, vous pouvez le signaler sur ce site ;
- Supprimez le message puis videz la corbeille.

> Télétravail et cyber-sécurité : 10 recommandations à suivre durant le confinement



En cette période de crise sanitaire liée au Covid-19, de nombreux Confrères ont recours au télétravail pour assurer la poursuite de leur exercice professionnel. Ce dispositif a souvent dû être mis en place dans l'urgence, ce qui augmente les risques de sécurité auxquels les Confrères sont exposés. Pour vous aider à appréhender ce nouveau mode de travail tout en restant vigilant sur votre cybersécurité, le site cybermalveillance.gouv a établi plusieurs recommandations à suivre :

Les 10 recommandations de sécurité pour le télétravail

1. Si vous disposez d'équipements professionnels, séparez vos usages. L'activité professionnelle doit se faire uniquement sur vos moyens professionnels ;
2. Appliquez strictement les consignes de sécurité de votre cabinet ;
3. Ne faites pas en télétravail ce que vous ne feriez pas au bureau ;
4. Appliquez les mises à jour de sécurité sur tous vos équipements connectés (PC, tablette, smartphone…) ;
5. Vérifiez que vous utilisez bien un antivirus et scannez vos équipements ;
6. Renforcez la sécurité de vos mots de passe ;
7. Sécurisez votre connexion WiFi avec un mot de passe long et complexe ;
8. Sauvegardez régulièrement votre travail sur plusieurs supports dont au moins un autre que le disque dur de votre ordinateur ;
9. Méfiez-vous des messages inattendus ;
10. N'installez vos applications que dans un cadre « officiel » et évitez les sites suspects.

En savoir plus

> Secret professionnel et fuite de données personnelles : Restez vigilant

Pendant la crise sanitaire, veillez également à assurer la sécurité de vos données personnelles et adoptez les bonnes pratiques concernant le secret professionnel. En collaboration avec le barreau de Paris et la Conférence des bâtonniers, le CNB a créé un guide pratique RGPD pour vous informer de manière concrète sur les bonnes pratiques à mettre en œuvre tant en qualité de responsable de traitement que de conseil auprès de vos clients.

Lire le guide

Afin de compléter vos connaissances en termes de sécurité informatique, l'Agence nationale de la sécurité des systèmes d'information a conçu un guide d'hygiène informatique comprenant 42 mesures à adopter pour renforcer la sécurité de votre système d'information.

RESTONS CONNECTÉS

Site institutionnel du CNB | Plateforme de consultations juridiques en ligne

+33 (0)1 53 30 85 60 | Nous contacter par mail

Conseil national des barreaux 180 boulevard Haussmann, 75008 Paris