Le Fonds mondial

Re: Sécuriser vos systèmes – cyberattaques et transactions financières frauduleuses en temps de pandémie de COVID-19

Chers collègues,

La crise actuelle a pour effet d'augmenter rapidement la portée et l'intensité des cyberattaques et des transactions financières. Avec la croissance exponentielle de l'activité en ligne, les criminels trouvent des manières plus ingénieuses d'intercepter des informations vitales et de détourner des transactions financières.

Le moindre écart lors de la vérification approfondie standard des processus de décaissement/de paiement pourrait conduire, involontairement, à une perte financière importante.

Selon la Note d'orientation sur les systèmes d'information et le partage de données du Fonds mondial, publiée en avril dernier, il a été demandé aux récipiendaires principaux d'effectuer les mises à jour nécessaires de leurs processus internes et d'en confirmer la mise en œuvre.

Pour rappel des bonnes pratiques, les récipiendaires principaux, les sous-récipiendaires et les récipiendaires du financement de l'instance de coordination nationale sont invités à suivre les meilleures pratiques suivantes :

- Adoptez l'attitude « **Ne jamais faire confiance, toujours vérifier** » pour toutes les transactions financières. Les demandes les plus dangereuses semblent souvent provenir d'une adresse ou d'un numéro de téléphone que nous connaissons bien. Dans certains cas, les hackers utilisent de véritables comptes, mais détournent des informations. Toute demande non sollicitée qui inclut une transaction financière doit être traitée avec la plus grande précaution.
- Assurez-vous d'avoir la dernière version de votre **antivirus**.
- Consultez vos banques, afin de connaître les informations actualisées sur la manière de sécuriser votre **logiciel de paiement en ligne**.
- Demandez une **vérification approfondie supplémentaire si le compte bancaire** d'un fournisseur ou d'un bénéficiaire ne se situe pas là où se trouve le fournisseur ou en cas de changement de pays lorsqu'un compte bancaire est hébergé. Vous pouvez demander une lettre dûment signée au fournisseur ou au récipiendaire afin de confirmer l'authenticité d'un compte bancaire.
- Demandez une confirmation supplémentaire par téléphone.
- Instaurez des vérifications supplémentaires finales des paiements effectués vers de nouveaux comptes bancaires.
- Collaborez avec vos départements informatiques afin de bénéficier de formations de mise à niveau pour le personnel en vue d'améliorer la sensibilisation à ces questions. En particulier, formez la direction de l'instance de coordination nationale, le personnel du secrétariat de l'ICN et le personnel du récipiendaire principal sur le courriel d'hameçonnage.