Campagne de mails frauduleux à destination des entreprises Qualibat RGE

Mise à jour 07/11/2023 : Des courriels usurpant frauduleusement la marque et le logo de l'organisme de qualification Qualibat sont envoyés aux entreprises qualifiées Qualibat ou RGE depuis quelques semaines. Soyez vigilants et ne partagez pas vos données personnelles !

Certaines entreprises de bâtiment qualifiées Qualibat ou RGE ont reçu un message les invitant à transmettre des documents officiels avec les adresses **contact@qualibat-pro.fr** ou **rge@qualibat-certification.**

Il s'agit d'une tentative de phishing (hameçonnage), avec utilisation frauduleuse du logo de Qualibat. Il ne faut surtout pas répondre à ces emails !

Qualibat a engagé une procédure pour bloquer le nom de domaine xxx@qualibat-certification.com, mais il est possible que durant le laps de temps d'autres courriels soient envoyés avec ce nom. Restez par conséquent vigilants.

L'arnaque a été signalée aux entreprises qualifiées et certifiées Qualibat, à l'administration, l'ADEME, la DGCCRF et sur la plateforme PHAROS. Si vous êtes victime de cette fraude, déclarez-la sur la plateforme PHAROS et sur SIGNAL CONSO de la DGCCRF.
Les organismes de qualification ne demanderont jamais de cliquer sur un lien pour effectuer un paiement, un changement de coordonnées bancaires ou de données personnelles, en dehors d'un espace sécurisé.

Si vous avez un doute sur un message reçu, les précautions d'usage sont les suivantes :

- N'ouvrez surtout pas les pièces jointes, ne cliquez pas et ne répondez pas ;
- Ne cliquez par sur un lien ;
- Supprimez le message puis videz la corbeille ;
- Contactez votre service informatique et le responsable de la sécurité des systèmes d'information de votre entreprise pour vérification. Attendez leur réponse avant de supprimer le courrier électronique.

Si vous avez répondu et transmis les renseignements et pièces demandées :

1. Prenez immédiatement RDV avec la police ou la gendarmerie pour un dépôt de plainte en signalant spécialement la transmission de la copie de la carte d'identité (risque d'usurpation d'identité)
2. Contactez www.cybermalveillance.gouv.fr pour être accompagné dans le processus de réponse.
3. Testez votre système informatique et vérifiez l'absence de virus (contactez votre service informatique).
4. Prévenez vos salariés afin d'éviter des cas de « fraude au président » (cette fraude consiste souvent en un appel de mauvaise qualité sonore d'une personne se faisant passer pour le chef d'entreprise ou en un mail urgent du pseudo chef d'entreprise, demandant à un collaborateur du chef d'entreprise d'exécuter très rapidement une action, souvent un virement).

5. Si les clients dont les données ont filtré n'ont pas encore payé l'intégralité des travaux : prévenez-les de la « recrudescence de cas d'escroqueries » et rappelez-leur que les coordonnées RIB n'ont pas changé et ne changeront pas…
6. Vérifiez sur le fichier FICOBA que des tiers n'ont pas créé de compte bancaire à votre nom (n'hésitez pas à demander conseil à votre banquier).
7. Enfin, une fois ces opérations prioritaires réalisées, transmettez le mail frauduleux à Qualibat pour que l'organisme puisse se rendre compte de l'ampleur du phénomène et agir de son côté.

Pour tout savoir sur la cybersécurité, découvrez notre dossier spécial et 12 bonnes pratiques cybersécurité à mettre en place dans votre entreprise.