29 jan 2022 -14:05

Payer pour un certificat COVID ? C'est absurde ! Nouveaux cas d'e-mails de phishing

Depuis ce samedi 29 janvier 2022, nous avons identifié de nouvelles tentatives de phishing (hameçonnage) qui donnent l'impression d'être envoyées à partir de l'eBox. Ces derniers messages de phishing sont particulièrement convaincants et donc d'autant plus dangereux.

Comment reconnaître ces e-mails frauduleux ?

Dans les nouveaux e-mails de phishing, on vous demande de payer pour un certificat COVID. Toutefois, ces certificats sont gratuits. Le meilleur conseil pour reconnaître les courriers et messages de phishing est de bien réfléchir au message. On vous demande de payer pour un service gratuit ? Vous avez reçu un message concernant

Ces conseils peuvent également vous aider à reconnaître le phishing via eBox :

- Les messages officiels qui proviennent de My e-Box s'adressent toujours à leur destinataire en mentionnant leur nom (« Chère Madame/Monsieur suivi de votre prénom et nom ») et non « Chère Madame, Cher Monsieur, ou encore Cher citoyen».
- My e-Box ne va jamais vous demander de compléter des données bancaires ou d'autres identifiants que vos clés numériques CSAM nécessaires pour vous connecter.

- Si vous avez reçu un email dont vous n' êtes pas sûr, nous vous invitons à naviguer vers https://myebox.be et accéder à l'application via le lien « Ouvrir My e-Box » qui se trouve sur la page d'accueil. S'il n y'a pas de nouveau message dans votre My e-Box, l'email que vous venez de recevoir est une tentative d'hameçonnage.

Vous soupçonnez qu'un e-mail est un e-mail de phishing ? Veuillez contacter Safe on Web. Ne cliquez surtout pas sur le lien qui figure dans cet e-mail et ne complétez en aucun cas des données bancaires.

SPF Stratégie et Appui
WTC III
boulevard Simon Bolivar30
1000 Bruxelles
Belgique

Laurence Mortier
Contact presse
+32 477 962682
laurence.mortier@bosa.fgov.be