EXEMPLAIRE DE L'ENSEIGNANT(E)

Spam

Pour chaque scénario, déterminez si le message est un spam et si vous devez partager ces informations avec la personne. Veuillez noter votre réponse à chaque question dans l'espace prévu à cet effet.

SCÉNARIO 1 : vous recevez un e-mail d'un avocat vous informant qu'un parent éloigné vous a désigné comme bénéficiaire d'une certaine somme d'argent. On peut y lire : « Pour recevoir l'argent, veuillez nous envoyer votre numéro de compte bancaire et votre IBAN, afin que nous puissions effectuer le dépôt. »

Cet e-mail est très probablement un spam. Même s'ils utilisent correctement le nom de votre proche, ils ne sont pas forcément qui ils prétendent. L'expéditeur aurait pu obtenir les informations sur votre relation par d'autres moyens. Partager les informations relatives à votre compte bancaire est toujours risqué et doit être fait avec prudence. N'envoyez jamais vos informations à une personne sans l'avoir contactée au préalable et, même dans ce cas, soyez très prudent(e). Par exemple, ce n'est probablement pas une bonne idée d'envoyer vos informations par e-mail, car elles ne sont pas cryptées. C'est pourquoi de nombreux hôpitaux, avocats et banques disposent de sites web spéciaux pour communiquer avec vous.

SCÉNARIO 2 : un(e) ami(e) vous envoie un message pour vous dire qu'il (elle) essaie de revoir une photo que vous lui avez montrée plus tôt mais qu'il (elle) n'a pas la permission de la voir. Vous n'avez pas accès à votre ordinateur à ce moment-là pour lui envoyer la photo. Il ou elle répond : « Je peux me connecter à ton compte vite fait pour télécharger la photo, quel est ton mot de passe ? »

Même s'il ne s'agit pas d'un spam, vous ne devriez pas partager vos mots de passe avec d'autres personnes. Une fois qu'elles ont votre mot de passe, elles peuvent éventuellement bloquer votre compte ou accéder à d'autres comptes en ligne avec le même mot de passe. En outre, si des tiers, des pirates ou des passants voient votre message, d'autres personnes pourraient accéder à votre compte à votre insu.

SCÉNARIO 3 : vous recevez un e-mail de votre école, affirmant que de nombreux comptes d'étudiant(e)s ont été piratés. Ils affirment : « Nous avons récemment détecté que de nombreux comptes d'étudiant(e)s ont été compromis. Nous nous excusons et faisons en sorte de résoudre le problème. Pour réinitialiser votre compte, veuillez répondre à cet e-mail en indiquant votre nom d'utilisateur et votre mot de passe. »

La pratique courante consiste à ne pas demander ces informations aux utilisateurs. Même si l'expéditeur semble légitime, vous devez supposer que tout e-mail vous demandant votre mot de passe est un spam.

SCÉNARIO 4 : vous recevez un e-mail de la banque où vous avez un compte légitime. L'e-mail indique qu'ils ont été piratés et que vous devez vous connecter pour changer le mot de passe de votre compte dès que possible, ainsi que ceux de tous les comptes pour lesquels vous utilisez le même.

La bonne marche à suivre est d'ouvrir une nouvelle fenêtre de navigateur et d'accéder au site comme vous le feriez normalement. Un message indiquant que des comptes ont été piratés sera normalement affiché sur le portail client de l'entreprise ou de la banque. Les instructions sur le portail doivent pouvoir être suivies en toute sécurité. Comme pour le scénario 3, aucun acteur légitime ne vous demandera les identifiants associés à votre compte par e-mail.

Meta | Mon Univers Digital