

Contenus indésirables

Pour chaque scénario, déterminez si le message est un courrier indésirable ou non, et si vous devez communiquer des informations à la personne mentionnée. Pour chaque question, veuillez écrire votre réponse dans l'espace prévu à cet effet.

Scénario 1

Vous recevez un e-mail de la part d'un avocat, vous informant qu'un parent éloigné vous a nommé comme bénéficiaire d'une certaine somme d'argent. L'e-mail indique « Pour recevoir votre argent, merci de m'envoyer votre numéro de compte bancaire ainsi que le numéro de routage associé afin que nous puissions procéder au virement ».

Scénario 2

Vous recevez un texto d'un ami, indiquant qu'il voudrait voir une photo que vous lui aviez montrée auparavant, mais qu'il n'a pas les autorisations nécessaires pour y accéder. Vous n'avez actuellement pas accès à votre ordinateur et ne pouvez donc pas lui envoyer la photo. Votre ami répond « Je peux me connecter à ton compte quelques minutes pour télécharger la photo, quel est ton mot de passe ? ».

Scénario 3

Vous recevez un e-mail de la part de votre université, indiquant que de nombreux comptes d'étudiants ont été piratés. L'e-mail indique « Nous avons récemment remarqué que de nombreux comptes d'étudiants ont été piratés. Veuillez nous excuser pour la gêne occasionnée, nous nous efforçons actuellement 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 ».

Scénario 4

Vous recevez un e-mail de votre banque. L'e-mail indique que la banque a été piratée et que vous devez vous connecter à son site web afin de modifier le mot de passe associé à votre compte dès que possible, mais aussi modifier tous les mots de passe de tous vos comptes qui utilisent ce même mot de passe.

Contenus indésirables : Copie pour l'éducateur

Pour chaque scénario, déterminez si le message est un courrier indésirable ou non, et si vous devez communiquer des informations à la personne mentionnée. Pour chaque question, veuillez écrire votre réponse dans l'espace prévu à cet effet.

Scénario 1

Vous recevez un e-mail de la part d'un avocat, vous informant qu'un parent éloigné vous a nommé comme bénéficiaire d'une certaine somme d'argent. L'e-mail indique « Pour recevoir votre argent, merci de m'envoyer votre numéro de compte bancaire ainsi que le numéro de routage associé afin que nous puissions procéder au virement ».

Cet e-mail est très certainement un courrier indésirable. Même s'il contient le nom d'un véritable parent éloigné, il se peut que l'expéditeur de l'e-mail ne soit pas la personne qu'elle prétend être. L'expéditeur a pu obtenir des informations concernant ce parent par plusieurs moyens. Le fait de partager des informations concernant votre compte bancaire présente toujours des risques, c'est une décision qui ne doit pas être prise à la légère. N'envoyez jamais de telles informations sans avoir contacté le destinataire au préalable, et même si vous l'avez contacté, restez extrêmement prudent. Par exemple, il n'est pas prudent d'envoyer de telles informations par e-mail étant donné que les e-mails ne sont pas chiffrés. C'est la raison pour laquelle de nombreux établissements de santé, cabinets d'avocats ou banques utilisent des sites web dédiés pour communiquer avec vous.

Scénario 2

Vous recevez un texto de la part d'un ami, indiquant qu'il voudrait voir une photo que vous lui aviez montrée auparavant, mais qu'il n'a pas les autorisations nécessaires pour y accéder. Vous n'avez actuellement pas accès à votre ordinateur et ne pouvez donc pas lui envoyer la photo. Votre ami répond « Je peux me connecter à ton compte quelques minutes pour télécharger la photo, quel est ton mot de passe ? ».

Même s'il ne s'agit pas d'un message indésirable, vous ne devez pas donner vos mots de passe à des tiers. Si une personne détient votre mot de passe, elle pourra vous empêcher d'accéder à votre compte ou accéder à d'autres comptes en ligne pour lesquels vous utilisez ce même mot de passe. Par ailleurs, si une tierce personne, y compris un pirate informatique, a l'occasion de lire votre texto de réponse, elle pourra accéder à votre compte sans même que vous le sachiez.

Scénario 3

Vous recevez un e-mail de la part de votre université, indiquant que de nombreux comptes d'étudiants ont été piratés. L'e-mail indique « Nous avons récemment remarqué que de nombreux comptes d'étudiants ont été piratés. Veuillez nous

excuser pour la gêne occasionnée, nous nous efforçons actuellement 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 ».

Généralement, personne ne demande d'envoyer de telles informations par e-mail. Même si l'expéditeur semble fiable, vous devez considérer comme courrier indésirable tout e-mail vous demandant votre mot de passe.

Scénario 4

Vous recevez un e-mail de votre banque. L'e-mail indique que la banque a été piratée et que vous devez vous connecter à son site web afin de modifier le mot de passe associé à votre compte dès que possible, mais aussi modifier tous les mots de passe de tous vos comptes qui utilisent ce même mot de passe.

La bonne chose à faire consiste à ouvrir une nouvelle fenêtre de navigateur et à accéder au site comme vous le faites d'habitude. Une notification de ce type (par exemple, le piratage de comptes) est généralement affichée sur le portail client de l'entreprise ou de la banque. Les instructions détaillées sur ce portail peuvent généralement être suivies en toute confiance. Tout comme dans le scénario 3, aucune entité de confiance ne vous demandera les codes d'accès à votre compte dans un e-mail.