Spam

Identifica en cada situación si el mensaje es spam y si deberías compartir información con esa persona. Escribe tu respuesta a cada pregunta en el espacio que se te ha proporcionado.

Primera situación

Recibes un correo electrónico de un abogado que te informa de que un familiar lejano te ha dejado en herencia determinada cantidad de dinero. El mensaje dice: “Para hacerte llegar el dinero, necesitamos que nos envíes tu número de cuenta bancaria y tu número de ruta para poder finalizar el ingreso”.

Segunda situación

Un amigo te envía un mensaje en el que te dice que está buscando una foto que le enseñaste antes, pero que no tiene permiso para verla. No puedes acceder al ordenador en ese momento para enviarle la foto. Te responde: “Puedo entrar en tu cuenta rápidamente y descargar la foto, ¿cuál es tu contraseña?”.

Tercera situación

Recibes un correo electrónico dirigido a ti en nombre de tu centro educativo que alerta de que han hackeado las cuentas de varios estudiantes. El mensaje afirma: “Hemos detectado que han atacado recientemente las cuentas de varios estudiantes. Pedimos perdón por esta situación y estamos trabajando para arreglar el problema. Para restablecer tu cuenta, responde a este correo electrónico con tu nombre de usuario y contraseña”.

Cuarta situación

Recibes un correo electrónico de tu banco, donde tienes una cuenta legítima. El correo electrónico dice que les han hackeado y que deberías entrar en tu cuenta para cambiar la contraseña lo antes posible, así como cambiarla también en otras cuentas que tengan la misma contraseña.

Spam: copia para el educador

Identifica en cada situación si el mensaje es spam y si deberías compartir información con esa persona. Escribe tu respuesta a cada pregunta en el espacio que se te ha proporcionado.

Primera situación

Recibes un correo electrónico de un abogado que te informa de que un familiar lejano te ha dejado en herencia determinada cantidad de dinero. El mensaje dice: “Para hacerte llegar el dinero, necesitamos que nos envíes tu número de cuenta bancaria y tu número de ruta para poder finalizar el ingreso”.

Lo más probable es que este mensaje de correo electrónico sea spam. Incluso si el nombre de tu familiar es correcto, probablemente no son quienes dicen ser. El remitente puede haber obtenido esa información sobre ti por otros medios. Siempre es arriesgado compartir la información de tu cuenta bancaria y deberías hacerlo con cuidado. Nunca envíes tu información a nadie; a no ser que hayas contactado antes con esa persona, e incluso así debes seguir teniendo cuidado. Por ejemplo, posiblemente no sea buena idea enviar tu información por correo electrónico, ya que esta no está encriptada. Por ello, muchos hospitales, abogados y bancos cuentan con sitios web especiales para comunicarse contigo.

Segunda situación

Un amigo te envía un mensaje en el que te dice que está buscando una foto que le enseñaste antes, pero que no tiene permiso para verla. No puedes acceder al ordenador en ese momento para enviarle la foto. Te responde: “Puedo entrar en tu cuenta rápidamente y descargar la foto, ¿cuál es tu contraseña?”.

Esto no es spam, pero no deberías compartir tu contraseña con nadie. Si alguien tiene tu contraseña, puede dejarte sin acceso o entrar en otras de tus cuentas que tengan la misma contraseña. Además, si un tercero, un hacker o cualquier observador ve tu mensaje, puede que varias personas entren en tu cuenta sin que lo sepas.

Tercera situación

Recibes un correo electrónico dirigido a ti en nombre de tu centro educativo que alerta de que han hackeado las cuentas de varios estudiantes. El mensaje afirma: “Hemos detectado que han atacado recientemente las cuentas de varios estudiantes. Pedimos perdón por esta situación y estamos trabajando para arreglar el problema. Para restablecer tu cuenta, responde a este correo electrónico con tu nombre de usuario y contraseña”.

El procedimiento común es no pedir a los usuarios esta información. Incluso si el

remitente parece legítimo, deberías dar por hecho que cualquier correo electrónico que pida tu contraseña es spam.

Cuarta situación

Recibes un correo electrónico de tu banco, donde tienes una cuenta legítima. El correo electrónico dice que les han hackeado y que deberías entrar en tu cuenta para cambiar la contraseña lo antes posible, así como cambiarla también en otras cuentas que tengan la misma contraseña.

El procedimiento correcto es abrir una nueva ventana de navegador y acceder al sitio como lo harías normalmente. Este tipo de revelación (que ha habido cuentas hackeadas) figurará normalmente en el portal para clientes del banco o la empresa. Las instrucciones del portal deberían poder seguirse con seguridad. Como en la tercera situación, ningún remitente legítimo solicitará las credenciales de tu cuenta por correo electrónico.