Spam

En cada situación, identifica si el mensaje es spam o si deberías compartir información con la persona. Escribe la respuesta a cada pregunta en el espacio proporcionado.

Situación 1

Recibes un correo electrónico de un abogado que te comunica que un pariente lejano te nombró beneficiario de una suma de dinero. El mensaje dice: "Para recibir el dinero, envíame tu número de cuenta y número de ruta bancarios, para que podamos completar el depósito".

Situación 2

Un amigo te envía un mensaje de texto donde te cuenta que está buscando una foto que le mostraste hace poco, pero no tiene permiso para verla. En ese momento no puedes acceder a tu computadora para enviarle la foto. Esta es su respuesta: "Yo puedo iniciar sesión en tu cuenta muy rápido para descargar la foto, ¿cuál es tu contraseña?".

Situación 3

Recibes un correo electrónico con el remitente de tu escuela. El mensaje dice que alguien hackeó las cuentas de muchos estudiantes: "Recientemente detectamos que la seguridad de las cuentas de muchos estudiantes se vio comprometida. Te pedimos disculpas. Estamos trabajando para solucionar el problema. Para restablecer tu cuenta, responde este mensaje con tu nombre de usuario y contraseña".

Situación 4

Recibes un correo electrónico del banco en donde eres titular de una cuenta. El mensaje dice que alguien hackeó su sistema y debes iniciar sesión en tu cuenta para cambiar tu contraseña lo antes posible y cambiarla también en otras cuentas donde usaras la misma contraseña.

Spam: texto del educador

En cada situación, identifica si el mensaje es spam o si deberías compartir información con la persona. Escribe la respuesta a cada pregunta en el espacio proporcionado.

Situación 1

Recibes un correo electrónico de un abogado que te comunica que un pariente lejano te nombró beneficiario de una suma de dinero. El mensaje dice: "Para recibir el dinero, envíame tu número de cuenta y número de ruta bancarios, de modo que podamos completar el depósito".

Lo más probable es que sea spam. Incluso si la persona menciona el nombre correcto de un pariente, puede no ser quien dice. El remitente pudo obtener la información del parentesco por otros medios. Compartir información de cuentas bancarias siempre implica un riesgo y se debe hacer con cautela. Nunca le envíes esta información a nadie que no hayas contactado primero, e incluso en ese caso, ten mucho cuidado. Por ejemplo, probablemente no es buena idea enviar la información por correo electrónico, ya que no está cifrado. Esa es la razón por la que muchos hospitales, abogados y bancos tienen sitios web especiales para comunicarse con sus clientes.

Situación 2

Un amigo te envía un mensaje de texto donde te cuenta que está buscando una foto que le mostraste hace poco, pero no tiene permiso para verla. En ese momento no puedes acceder a tu computadora para enviarle la foto. Esta es su respuesta: "Yo puedo iniciar sesión en tu cuenta muy rápido para descargar la foto, ¿cuál es tu contraseña?".

Esto no es spam, pero te recomendamos que no compartas tu contraseña con otras personas. Alguien que posea tu contraseña podría bloquear el acceso a tu cuenta o acceder a otras cuentas en internet donde uses la misma contraseña. Además, si un tercero, hacker o alguien que está cerca ven tu mensaje, más personas podrían acceder a tu cuenta sin que tú lo sepas.

Situación 3

Recibes un correo electrónico con el remitente de tu escuela. El mensaje informa que alguien hackeó las cuentas de muchos estudiantes: "Recientemente detectamos que la seguridad de las cuentas de muchos estudiantes se vio comprometida. Te pedimos disculpas. Estamos trabajando para solucionar el problema. Para restablecer tu cuenta, responde este mensaje con tu nombre de usuario y contraseña".

Lo habitual es no pedir a los usuarios esta información. Incluso si el remitente parece legítimo, debes considerar como spam cualquier correo electrónico donde te pidan tu contraseña.

Situación 4

Recibes un correo electrónico del banco en donde eres titular de una cuenta. El mensaje dice que alguien hackeó su sistema y debes iniciar sesión en tu cuenta para cambiar tu contraseña lo antes posible y cambiarla también en otras cuentas donde usaras la misma contraseña.

Los pasos indicados que debes seguir consisten en abrir una nueva ventana del navegador y acceder al sitio web como sueles hacerlo. Por lo general, un aviso de este tipo (sobre cuentas hackeadas) se publicará en el portal para clientes de la empresa o el banco. Las instrucciones del portal deben poder seguirse de manera segura. Como en la situación 3, ningún agente legítimo te solicitará las credenciales de tu cuenta en un correo electrónico.