Internet está lleno de ventajas y posibilidades, pero también está lleno de peligros como los fraudes y estafas. Para sacar el máximo provecho de Internet, **necesitamos conocer cómo funcionan los fraudes y estafas más comunes y así evitarlos**. Por lo general, esta clase de engaños emplea la información que los ciberdelincuentes encuentran sobre nosotros, por lo que **tenemos que estar atentos y usar el sentido común**. Por suerte para nosotros, la forma que tienen de actuar es prácticamente la misma, así que una vez aprendas en este nivel cómo funcionan, podrás identificarlos y evitarlos rápidamente.

Una de las formas que tienen los ciberdelincuentes para intentar estafarnos es **mediante la ingeniería social**, es decir, **hacerse pasar por personas o empresas de confianza para aprovecharse de nosotros**. Para identificar esta clase de ataques y defendernos bien, debemos ser pacientes y prestar atención a los detalles. Con estos consejos sabrás en qué cosas fijarte y cómo actuar:

1. **Comprueba de quién es el correo, mensaje o llamada**. Si coincide con la persona o empresa que dice ser, podemos estar más tranquilos. Sin embargo, si no coincide, nos aparece un número desconocido o un correo extraño, se trata de un fraude.

2. **Si nos ha llegado un correo, tenemos que leerlo, no solo el asunto**. La mayoría de los fraudes utilizarán un asunto llamativo para desviar nuestra atención del resto de alertas.

3. **Si te llega un mensaje, es bueno preguntarse qué es lo quieren, cuál es la finalidad**. Por ejemplo, si fuera el banco quien te envía el mensaje, no es lógico que te estén pidiendo datos que ya deberían tener. Esta clase de mensajes suelen llegar con el contexto de necesitar algo urgentemente. De esta forma, los ciberdelincuentes buscan que no prestes atención al mensaje y te des cuenta de que es un fraude.

4. **Observa con cuidado cómo se ha escrito el mensaje o correo que te llega**. Generalmente, si está cargado de faltas ortográficas o da la sensación de que está sacado directamente de “Google Translate”, es muy probable que se trate de un fraude y debemos ignóralo.

5. **Si el mensaje o correo que te envían lleva un enlace, ¡no lo pinches!** Pasa primero el cursor del ratón o mantén el dedo ligeramente encima para ver la dirección de la página web a la que te redirige. Así podemos ver si se trata de un web real o una falsa.

6. **Si el mensaje o correo que te envían lleva un archivo adjunto, antes de descargarlo debes analizarlo con el antivirus para asegurarnos de que no es peligroso**.

7. Por último, **si sospechamos, aunque sea un poco de que puede ser un fraude**, NO debemos hacer caso de las indicaciones que nos dan y NO debemos dar ningún tipo de información. **Lo mejor es que lo ignoremos y se lo contemos a un adulto o a alguien de confianza**.

Los ciberdelincuentes cuentan con más formas para hacernos caer en sus engaños. Veamos otros tipos de fraudes más comunes con los que nos podemos encontrar:

1. **Anuncios maliciosos**: son muy invasivos, apareciendo en medio de la pantalla con letras y colores atractivos. **Suelen aparecer en sitios poco fiables** y, si hacemos clic en ellos, lo más probable es que terminemos en un web falsa o peligrosa. Por lo que, en cierta forma **son un buen indicador para abandonar la página en la que estamos de inmediato**.

2. **Webs falsas**: las webs falsas **copian el estilo de otras webs más famosas o de marcas conocidas**, utilizando sus colores, logo y estructura. Sin embargo, pueden encontrarse diferencias si nos fijamos bien, como imágenes de menor calidad, falta de información sobre la empresa o la URL sin "https" al principio y sin certificado de seguridad.

3. **Concursos falsos**: has ganado un sorteo sin haber siquiera participado, ¿no es un poco raro? **Lo más probable es que sea un fraude**. Si lo que pasa es que has entrado a un formulario para registrarte en un concurso y ves que te piden una cantidad excesiva de datos (como el DNI, el número de la tarjeta del banco, el correo, etc.) o te piden que lo compartas con todos tus contactos para tener más posibilidades de ganar, lo más probable es que sea falso. No hagas nada de lo que te piden y simplemente no participes en nada que no sepas que es de confianza.

4. **Las "fake news"**: las "fake news" son, como su nombre indica, noticias falsas. **La peculiaridad que tienen estas noticias son lo rápido que se propagan**, ya sea por mensajes o por redes sociales. **El principal objetivo de las "fake news" es desinformar para que sea más fácil manipular a las personas**, por lo que los ciberdelincuentes se aprovechan de ellas para hacer de las suyas. Por tanto, si nos topamos con cualquier noticia, **tenemos que verificar que las fuentes son reales y fiables**, que no proceden de páginas web falsas o poco fiables, **fijarnos en los detalles de la noticia** (como las imágenes que la acompañan o si tiene faltas de ortografía) **y aplicar el sentido común** sin dejarnos llevar por las emociones que buscan provocarnos.

Con toda esta información, pensarás que ya se ha terminado el nivel, ¿no? Si ya has hecho otros niveles sabrás que hay algo más que puedes hacer para reforzar todo lo que has aprendido. Abajo se encuentra un botón que te llevará a un test. Si lo superas, quedará demostrado que has aprendido todo lo necesario de este nivel. No hace falta que lo hagas ahora, repasa la lección todo lo que necesites, pero es bueno que en algún momento pongas a prueba tus conocimientos para así finalizar de verdad el nivel.