everest®

We underwrite opportunity.™

Ciberseguridad

Identificando y evitando el Phishing en ambientes de trabajo

¿Qué es el Phishing?

El Phishing es **cualquier mensaje malicioso** creado para engañar a la víctima y así suplantar su identidad, robarle información y datos personales, como números de tarjeta de crédito, ID o incluso credenciales de acceso.

¿A través de cuáles canales suele ocurrir el Phishing?

- **Email**
- **Mensaje de texto**
- **Redes sociales**
- **Teléfono**

La estrategia principal de un atacante es elaborar un mensaje convincente y sofisticado que imite a fuentes confiables, como contactos de negocio o personas conocidas.

¿Por qué es tan peligroso a nivel empresarial?

- Puede **causar pérdidas económicas considerables** a una organización.
- Puede **dañar de forma permanente la reputación de la organización** ante sus socios, clientes y socios comerciales.

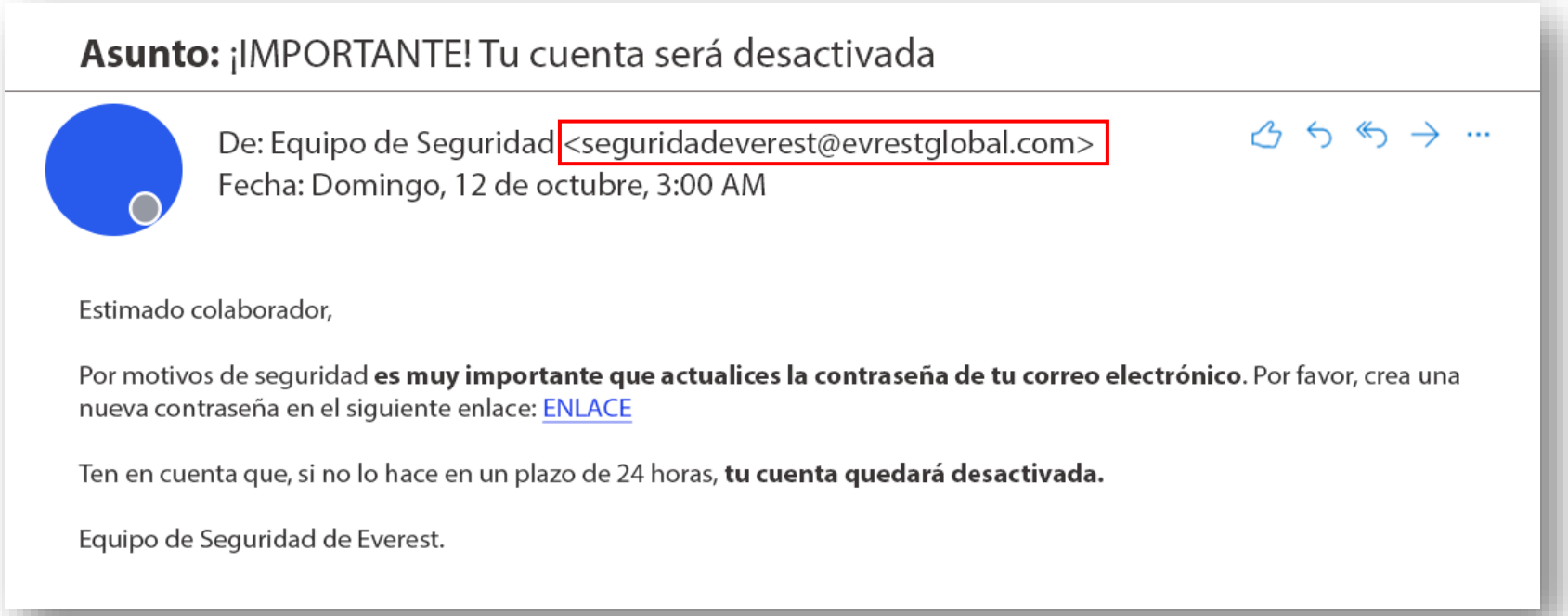
¿Por qué es tan peligroso a nivel personal?

- Puede **robar tu identidad** y utilizarla para cometer fraudes.
- Puede **poner en peligro a tu familia y amigos**, ya que podrían recibir correos electrónicos o mensajes falsos de tu parte.

Señales de Phishing fáciles de reconocer

- ¿De quién es el correo?

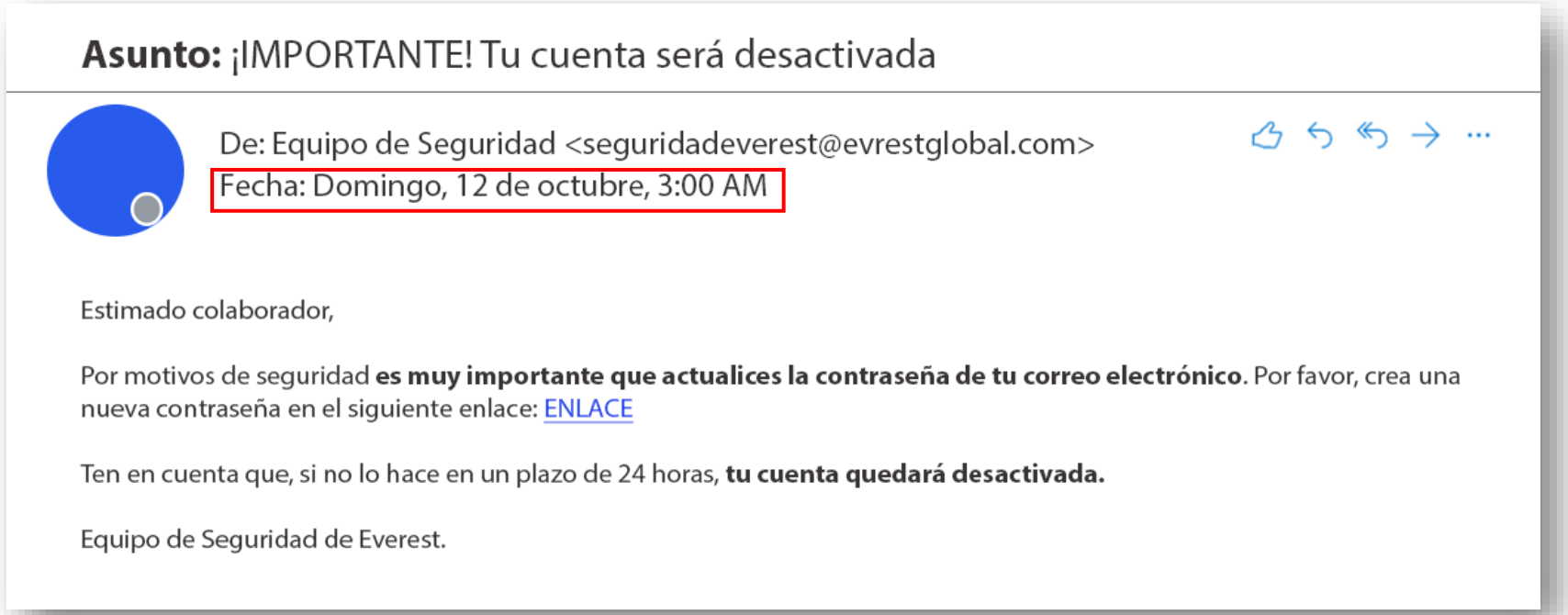
Presta atención a las **direcciones de correo de personas que no conoces o que no esperabas, errores ortográficos, o direcciones que se ven un poco fuera de lo común.** Los ciberdelincuentes suelen suplantar la identidad de personas que conoces utilizando direcciones de correo electrónicos similares. Utiliza tus sitios marcados como favoritos o números de teléfonos que sepas que son legítimos para verificar la solicitud de la fuente verdadera.



Señales de Phishing fáciles de reconocer

- Fecha

Los mensajes enviados a horas poco habituales deben ser una señal de alerta. Un mensaje enviado a las 3:00 a.m., por ejemplo, o incluso mensajes enviados durante los fines de semana.

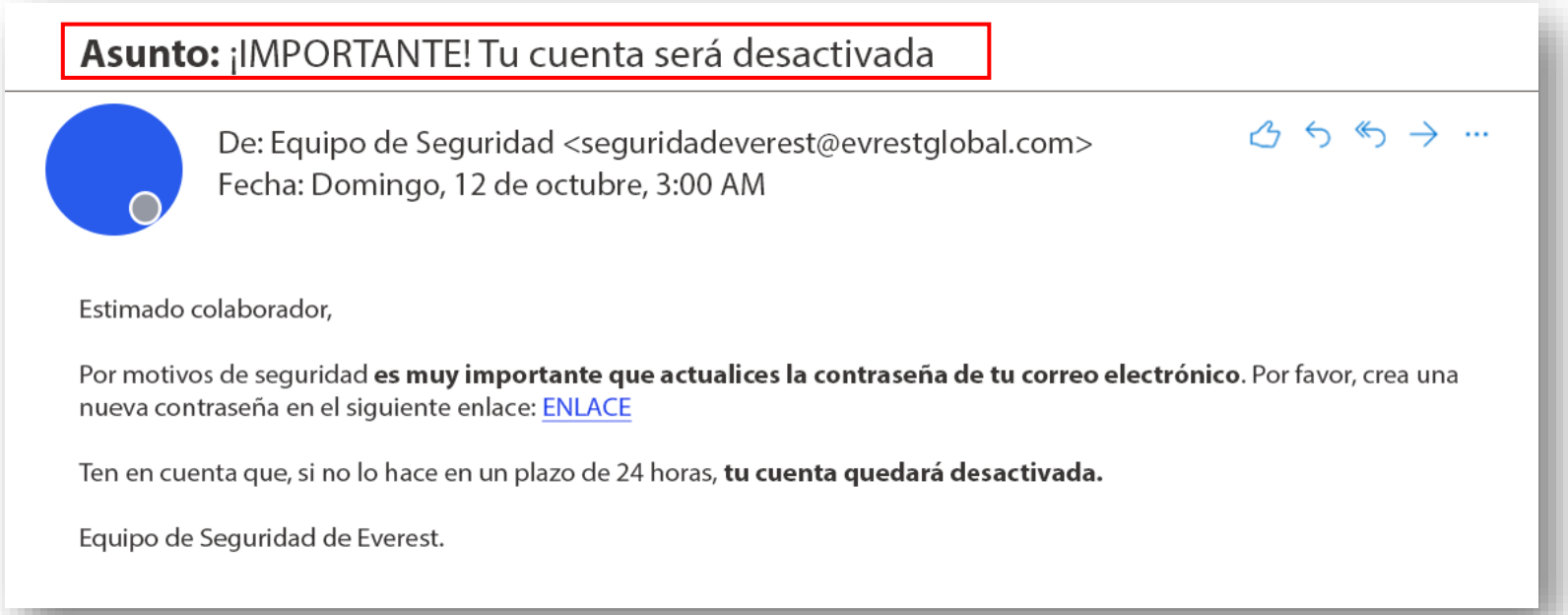


Señales de Phishing fáciles de reconocer

- Asunto

Los ciberdelincuentes usarán el título del asunto para **llamar tu atención e incitarte a interactuar** con el correo. Revisa que el asunto concuerde con el contenido del correo. Pregúntate:

- ¿Es una respuesta a algo que no solicitaste?
- ¿Es un correo reenviado que no debería ser para ti?
- ¿Estabas esperando este mensaje?
- ¿La solicitud concuerda con los conductos regulares de tu compañía?

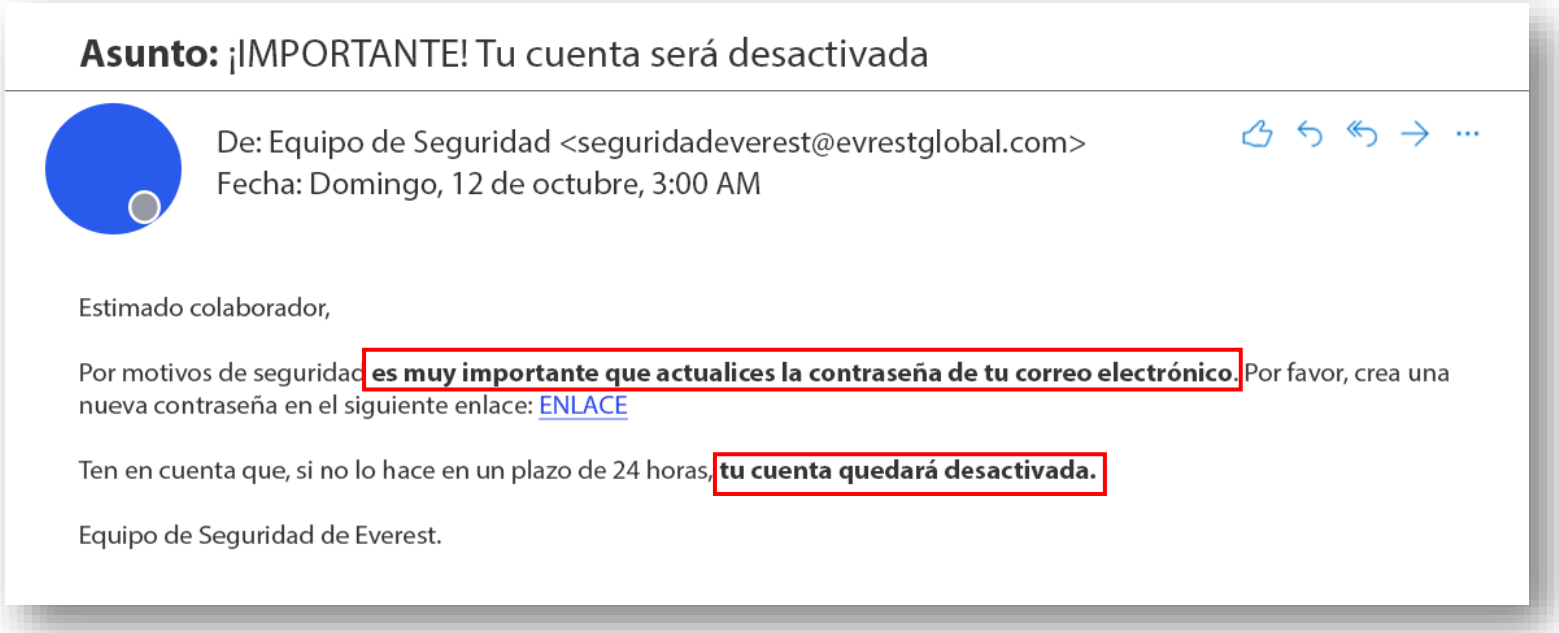


Señales de Phishing fáciles de reconocer

- Sentido de urgencia

Los correos de Phishing por lo general **crean un falso sentido de urgencia para presionarte** a tomar acciones inmediatas. Por ejemplo: “Si no actúas en las próximas horas, tu cuenta será deshabilitada” o “Como medida de seguridad, borraremos tu cuenta si no respondes dentro de las próximas 24 horas”.

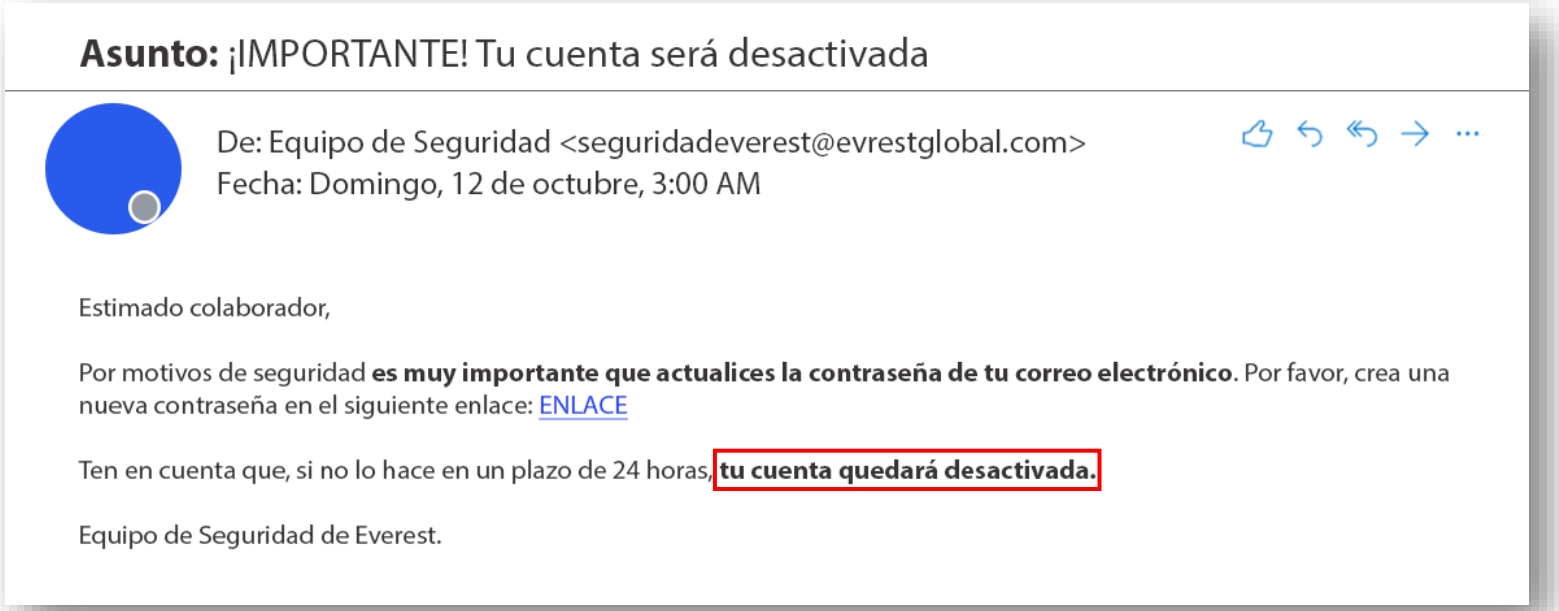
Recuerda: las empresas legitimas, incluida la tuya, nunca te darán plazos tan cortos para verificar tu cuenta, actualizar contraseña o realizar acciones similares.



Señales de Phishing fáciles de reconocer

- Miedo o consecuencias negativas

Otra táctica común en correos de Phishing es generar miedo en el receptor. Estos mensajes pueden incluir **amenazas o advertencias de consecuencias negativas para presionar al usuario** a tomar medidas inmediatas. Los atacantes suelen utilizar información personal básica, fácil de encontrar en Internet, para que el mensaje parezca más personalizado y convincente. Si copias y pegas todo el correo electrónico en un motor de búsqueda, como Google, verás que otros usuarios lo han reportado como una estafa.

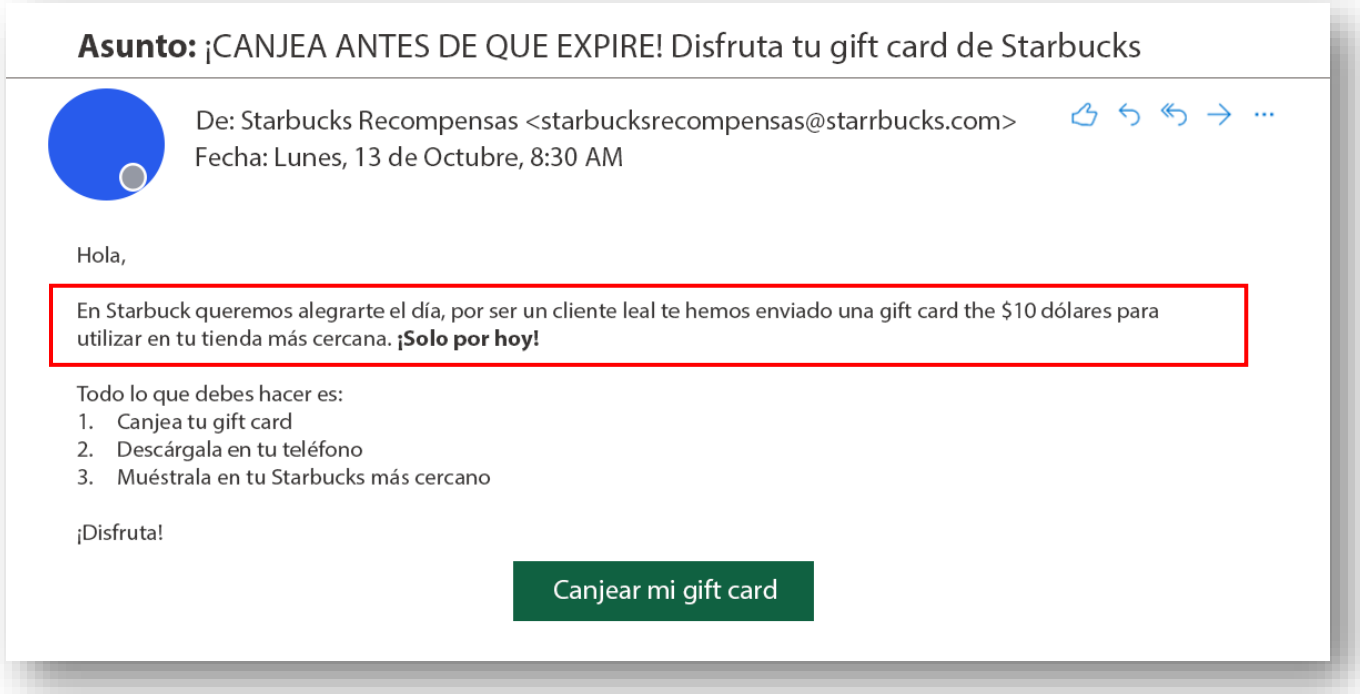


Señales de Phishing fáciles de reconocer

- Promesas de regalos o recompensas

Muchos intentos de Phishing involucran **propuestas falsas como gift cards, premios u ofertas exclusivas** para persuadirte a darle clic a enlaces maliciosos.

No confíes en correos inesperados ofreciendo recompensas. Recuerda, si suena muy bueno para ser cierto, probablemente lo es.



¿Cómo saber si un link es malicioso?

Primero, **posiciona el mouse encima del link para poder ver la URL completa** antes de dar clic y evalúala.

¿Cómo evaluarla? Para entender lo que estás viendo, analicemos la estructura de una URL (concretamente, lo que aparece antes y después del dominio principal)

Subdominio: es lo que precede al nombre del dominio principal, separado por un punto. Algunos ejemplos comunes son:

- **www** → www.everestglobal.com
- **mail** → mail.everestglobal.com
- **blog** → blog.everestglobal.com
- **store** → store.everestglobal.com

Se utilizan para organizar diferentes partes de un sitio web. Pueden ser reales, pero los atacantes pueden falsificarlos para engañarte. El hecho de que veas "paypal" en un subdominio no significa que sea un sitio real de PayPal.

- **Dominio de nivel superior (o TLD por sus siglas en inglés) :** es lo que viene después del nombre de dominio principal. Algunos ejemplos son:
  - **.com** → www.everestglobal.com
  - **.org** → www.everestglobal.org
  - **.net** → www.everestglobal.net
  - **.edu** → www.everestglobal.edu

Ejemplos

Subdominio

- **https://seguridad.everestglobal.com**

  En este caso ‘seguridad’ está separado del dominio principal por un punto lo que convierte a ‘seguridad’ en un **subdominio**. Esto significa que puedes confiar en el sitio, ya que el dominio principal es everestglobal.com

Subdirectorios

- **https://everestglobal.com/seguridad/principal**

  En este caso ‘seguridad’ y ‘principal’ están separados por barras inclinadas y se convierten en **subdirectorios** del sitio original de Everest.

Dominio principal

- **https://everestglobal.seguridad.com**

  En este caso, seguridad.com se convertiría en el **dominio principal** y, al hacer clic en el enlace, se le redirigiría a ese sitio web y no a everestglobal.com. ¡Ten cuidado!

¿Cuáles son otras señales de enlaces maliciosos o falsos?

- **Puntos:** puntos que dividen el nombre de dominio pueden cambiar totalmente el dominio principal, por ejemplo, en el siguiente caso se nos redirigirá a 'global.com':
  - https://everest.global.com
- **Guion:** un guion en el nombre de dominio cambia el dominio real. Se convierte en parte del dominio principal, no solo en una palabra adicional. En el siguiente caso, estás visitando un sitio llamado 'seguridad-everestglobal.com' que no tiene nada que ver con 'everestglobal.com':
  - https://seguridad-everestglobal.com
- **Números:** los números que aparecen antes de un dominio son sospechosos, ya que pueden indicar un potencial riesgo de seguridad, como el Phishing. Sin embargo, si los números aparecen después de un dominio, pueden representar identificadores de contenido, números de página o parámetros de consulta. Por lo tanto, solo cuando veas números antes del dominio principal, no confíes:
  - 192.45.34.72.everestglobal.com
- **URL acortada:** una URL acortada oculta el destino real, lo que facilita disfrazar sitios maliciosos y engañar a las personas para que hagan clic sin conocer el sitio de destino real. Comprueba siempre dos veces antes de hacer clic. Un link acortado se puede ver así:
  - https://bit.ly/49Pd3MK
- **Errores de ortografía:** los errores ortográficos sutiles pueden llevarte a pensar erróneamente que se trata del sitio web legítimo. Comprueba siempre la URL antes de hacer clic:
  - https://evrestglobal.com

Consejos para evitar un intento de Phishing

Para comprobar si un enlace es real, escribe manualmente la URL en un motor de búsqueda como Google. Busca la URL exacta junto con palabras como “reseña”, “estafa” o “falso”. Los resultados deberían dejar claro si el enlace es legítimo o si se trata de un intento de Phishing.

Si alguien que conoces te envía un archivo que no estabas esperando, verifica que realmente sea esa persona utilizando un método de contacto que sepas que es legítimo. No descargues ni ejecutes archivos no solicitados.

Evita acceder a tu correo electrónico o cuentas de redes sociales en ordenadores públicos o redes Wi-Fi abiertas. Estos entornos suelen ser inseguros y los atacantes pueden interceptar tus datos personales más fácilmente, especialmente si la conexión no está encriptada.

everest®

We underwrite opportunity.™

Gracias por ver este curso.