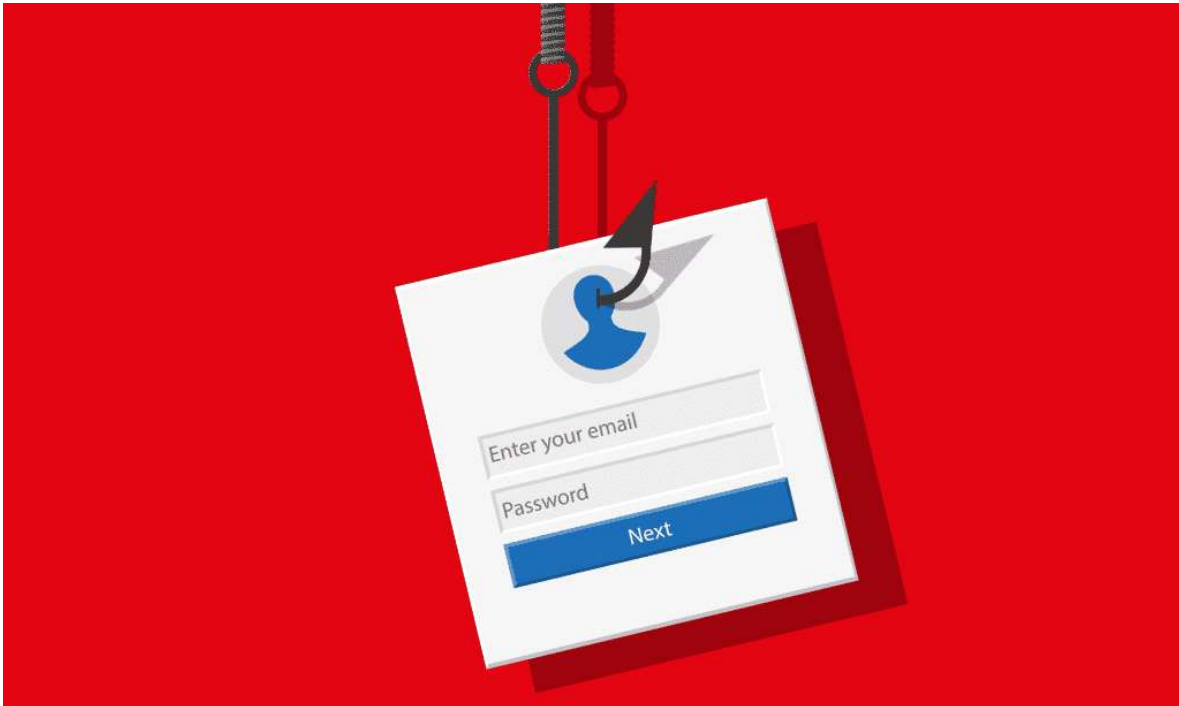


## Advierten sobre nueva estafa de phishing usando Bank of America

- Los ataques de *phishing* actúan disfrazados de correos electrónicos o mensajes de texto confiables. En **El Diario** conversamos con una abogada especialista en seguridad digital sobre cómo actuar para prevenir ser víctima de un fraude en Internet. Foto: Ideas TED



Por Jackelin Díaz

Delincuentes en el ámbito informático aprovechan la inexperiencia de los usuarios para robar sus contraseñas, información privada u obtener control sobre tarjetas y cuentas bancarias. Es una práctica conocida como *phishing*.

Por ejemplo, muchos mensajes de correo electrónico y sitios web falsos enlazan con logotipos reales de empresas de marcas conocidas. Por lo tanto, parecen legítimos.

Un usuario reportó a **El Diario** que había recibido un correo electrónico presuntamente de **Bank of America** en el que se le exigía cambiar su contraseña en un lapso de 24 horas porque su seguridad había sido vulnerada.

En este caso, la dirección de correo no correspondía a la institucional del banco, el nombre de la empresa en el correo estaba mal escrito y tampoco había algún logo referencial.

Lo único que lo asociaba con el banco era el uso de colores azul y rojo, pero ¿qué pasa una vez que se presiona en el link que supuestamente va a direccionar hacia la página de este banco?

Hildamar Fernández, abogada y especialista en seguridad digital, explicó para **El Diario** que existen distintas formas en las que se puede presentar este ataque.

Uno de los formatos más básicos es el del correo que te solicita el ingreso a un sitio web porque alguien intentó acceder de manera sospechosa a tu cuenta, por lo que sugiere que verifiques ciertos datos como número de tarjeta, clave, cédula de identidad, entre otros.

fuelle : <https://eldiario.com/2020/09/27/phishing-estafa-bank-of-america/>