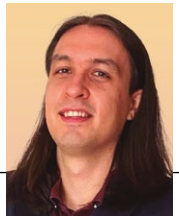
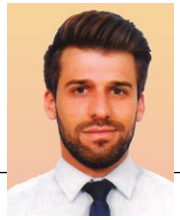
CORREOS: ¿Es una utopía reducir el *phishing*?

El *phishing* es, sin duda, uno de los términos de moda en el ámbito de la ciberseguridad. No existe evento, informe, artículo o análisis relacionado con la ciberseguridad donde no hablemos de ello desde diferentes perspectivas. No es la idea de esta exposición realizar un análisis profundo de la situación actual del *phishing*, de su impacto y de sus números. Probablemente con un clic se tenga toda la información y datos disponibles al respecto. Pero lo que sí podemos obtener como denominador común es que el *phishing*, que no deja de ser un fraude de suplantación de toda la vida, pero en el plano digital, se ha convertido en un serio problema por una cuestión fundamental: a los ciberdelincuentes les funciona muy bien para robar información y dinero. Y no parece que vaya a ir a menos.





Raúl Gómez-Álvarez / Brais Chousa

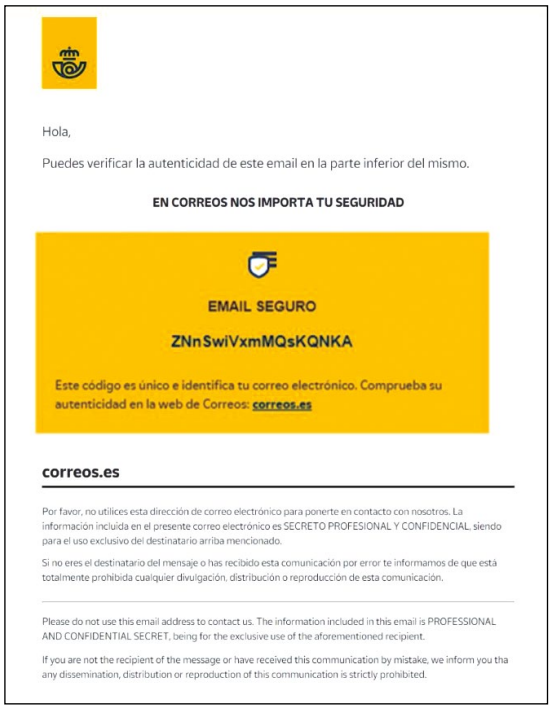
Toda esta problemática ha generado mucha literatura, problemas, soluciones, análisis y perspectivas, pero lo cierto es que sigue aumentando. Y no, ninguna de las respuestas que buscamos son tan simples como que la gente no sabe lo que hace, no tiene suficiente conocimiento o que se crea que le van a regalar un *smartphone* por un euro: hay un problema más complejo de fondo.

La solución propuesta por Correos

Para abordar esta cuestión, en Correos apostamos por convertir nuestras comunicaciones con los clientes en **únicas y verificables** a través de la serialización. Cada *email* de Correos relacionado con la paquetería (envíos, aduanas, cambios, etc.), donde se concentra casi la totalidad del fraude a la marca que sufrimos, se ha normalizado mediante una estructura común reconocible incorporando un código único de identificación. De esta manera, puedes introducir este código en la web junto con la dirección de correo electrónico donde lo has recibido y nuestro verificador te informa si el *mail* es de Correos o, por el contrario, si puede tratarse de un *phishing*.

La idea es, además de concienciar progresivamente a los clientes y usuarios de Correos, ayudarles y potenciar su capacidad de detección. Para ello utilizamos dos principios muy sencillos:

• Reconocimiento visual (el *email* dispone de un código único).



Hola,

Puedes verificar la autenticidad de este email en la parte inferior del mismo.

EN CORREOS NOS IMPORTA TU SEGURIDAD

EMAIL SEGURO

ZNnSwiVxmMQsKQNKA

Este código es único e identifica tu correo electrónico. Comprueba su autenticidad en la web de Correos: correos.es

correos.es

Por favor, no utilices esta dirección de correo electrónico para ponerte en contacto con nosotros. La información incluida en el presente correo electrónico es SECRETO PROFESIONAL Y CONFIDENCIAL, siendo para el uso exclusivo del destinatario arriba mencionado.

Si no eres el destinatario del mensaje o has recibido esta comunicación por error te informamos de que está totalmente prohibida cualquier divulgación, distribución o reproducción de esta comunicación.

Please do not use this email address to contact us. The information included in this email is PROFESSIONAL AND CONFIDENTIAL SECRET, being for the exclusive use of the aforementioned recipient.

If you are not the recipient of the message or have received this communication by mistake, we inform you tha any dissemination, distribution or reproduction of this communication is strictly prohibited.

• Herramienta de verificación en la web (canal alternativo de comprobación).

En primer lugar, distingo el *email* a simple vista porque **siempre disponen de un recuadro inferior destacado con su código único**. En segundo, puedo **comprobarlo por un canal alternativo** (el verificador que está en nuestra web) si tengo dudas de su legitimidad.

Por poner un ejemplo real del enfoque que aplicamos, el funcionamiento es parecido al proceso de detección de billetes falsos. ¿Cómo reconozco un billete falso? Primero por su aspecto y tacto, y si aún tengo dudas, dispongo de una máquina que si la utilizo me indica su veracidad. El concepto es el mismo.

Para desarrollar esta herramienta hemos contado con un sistema sencillo que nos permite centralizar y controlar los envíos por *email,* por lo que la implementación técnica no ha sido compleja.

Contexto

Si analizamos qué tipo de empresas son las que utilizan para realizar la suplantación, en el top anual de marcas utilizadas como señuelo para *phishing* nos encontramos siempre empresas del sector logístico entre las tres primeras. A nivel mundial, más del 15% del *phishing* total utiliza las marcas del sector logístico para realizar fraude.

En este sentido, en Correos combatimos a diario la problemática del *phishing.* Nuestra marca es reconocida, extendida y de confianza, por lo que somos vehículo

***Hasta el momento, ninguna compañía ha intentado probar soluciones nuevas que ayuden a la detección por parte del usuario con herramientas que no sean puramente técnicas o de concienciación. Este es el espacio que cubre, en Correos, nuestra solución de serializar* emails *y ofrecer una propuesta sencilla y novedosa para verificarlos, utilizando además un canal de verificación distinto al de la recepción del* email.**

del fraude y un cebo muy potente para los ciberdelincuentes. Por tanto, la pregunta que nos hacemos es, ¿por qué hay unas marcas más utilizadas que otras? ¿Qué tenemos para que un ciberdelincuente quiera utilizar nuestra marca y no otra?

Enfoque

Desde Correos pensamos que, además del reconocimiento del propio sector y de otras cuestiones relevantes, existe una cuestión clave: cualquier persona de nuestro país puede ver con normalidad que Correos se comunique con ella. **No es nada extraño que Correos se pueda comunicar contigo por cualquier canal**, y además lo más probable es que hayas utilizado alguno de nuestros servicios recientemente. Esto significa que el ciberdelincuente es capaz de romper diversas barreras (confianza, seguridad, fiabilidad, etc.) simplemente utilizando el logo de Correos.

En general, las soluciones que se plantean ante estas problemáticas suelen enfocarse desde la parte técnica, aplicando métodos de 'securización' y autenticación de *mail* tradicionales como son el SPF, DKIM, DMARC y cifrado de canal. Pero los problemas que nos encontramos con este tipo de medidas son dos: por un lado, las restricciones técnicas reducen la usabilidad si se aplican a un nivel alto, llegando a limitar el negocio, y, por otro, no son 100% efectivas. A pesar de todas las medidas que podamos aplicar que nos pueden evitar una suplantación de nuestro dominio legítimo, técnicas como el *cybersquatting* hacen que la efectividad no sea la deseada. Los *emails* fraudulentos siguen llegando y el *phishing* sigue funcionando para los ciberdelincuentes.

Por tanto, ¿estamos aplicando el enfoque adecuado? Desde Correos pensamos que, además de desplegar todas las medidas técnicas necesarias, las soluciones que pueden aportarnos un valor adicional no deben centrarse tanto en el enfoque técnico como en el humano: educar a la sociedad, concienciar y facilitar la detección pueden ser ejes claves para reducir el *phishing*. La gran mayoría de las personas tenemos un ejemplo claro en la cabeza de cómo trabajar estos ejes para concienciar y reducir los casos: la DGT y sus campañas de sensibilización. Hemos conseguido a lo largo de los años que la gente se ponga el cinturón sin pensar, ahora **deberíamos buscar que se detecte el *phishing* de la misma manera.**

Desde esta lógica, y sabiendo que el *phishing* no se puede eliminar, pero sí reducir, en Correos somos conscientes del uso que se le da a nuestra marca para cometer fraude y queremos probar una solución nueva que, según el análisis que hemos hecho, apunte a donde están la mayoría de los riesgos: la parte humana.

Hasta el momento, ninguna compañía ha intentado probar soluciones nuevas que ayuden a la detección por parte del usuario con herramientas que no sean puramente técnicas o de concienciación. Este es el espacio que cubre nuestra solución de serializar *emails* y ofrecer una solución sencilla y novedosa para verificarlos, utilizando además un canal de verificación distinto al de la recepción del *email.*

Nuestra aportación con esta solución, en definitiva, es contribuir a crear conciencia y a dar certezas y tranquilidad a los usuarios, llegando tanto a las personas que puedan tener dudas para resolverlas, como a las que estén más concienciadas, para que puedan confirmar por sí mismas si están o no ante un fraude. Incluso alcanzamos a todas aquellas personas que no tengan, o crean que no lo tengan, ningún conocimiento de ciberseguridad.

Hasta el momento en el que estamos escribiendo este artículo, **1.883.513 personas han utilizado nuestro verificador, siendo 967.354 de ellos visitantes únicos**. Esto significa que hemos ayudado a casi un millón de personas a confirmar sus dudas sobre la legitimidad de una comunicación recibida en nuestro nombre, haciéndoles sentir más seguros con esta comprobación.

Sabemos que es una solución que, como cualquier otra, tiene aspectos de mejora, pero su éxito pasa porque todo el mundo sepa que los *emails* que les enviamos desde Correos son **únicos y verificables.** Creemos que tiene buen recorrido a medio/largo plazo y que incluso el resto de las empresas con la misma problemática pueda implantar soluciones de este tipo, llegando a un consenso general en el que se aplique el enfoque que planteamos en este artículo.

En cualquier caso, aunque no seamos capaces de adivinar el futuro, lo que sí podemos asegurar es que la sociedad sabe que Correos tiene una solución para detectar el *phishing*, que poder verificar el *email* aporta un enfoque adicional valioso y que el ciudadano tiene **una herramienta más para poder defenderse de estas técnicas de fraude**. Como en la **fábula del colibrí y el fuego**, en Correos estamos seguros de que estamos haciendo la parte de trabajo que nos compete desde nuestra función con el objetivo de ayudar a la sociedad a luchar contra el *phishing* y, esta vez sí, reducirlo. ■

Raúl Gómez-Álvarez
Responsable de Cultura Ciber y Auditoría de Cumplimiento
CORREOS

Brais Chousa
Senior Manager
Business Security Solutions
PwC