CÓMO DETECTAR UN CORREO ELECTRÓNICO DE PHISHING EN

LA ERA DE LA IA

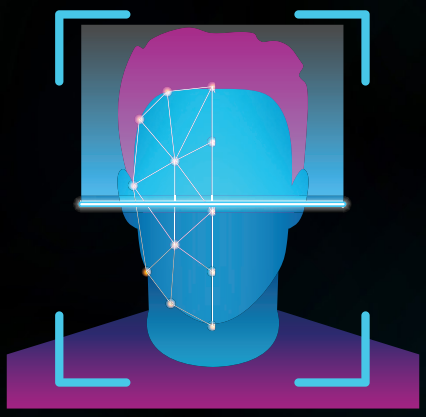
HORNETSECURITY

INTRODUCCIÓN

El concepto de implicar a los usuarios finales en la defensa de tu empresa frente a las ciberamenazas no es nuevo, pero en los últimos años ha cobrado fuerza el concepto de organización ciberresiliente. Esto es importante, ya que los delincuentes son cada vez más prolíferos y persistentes en sus ataques, como lo demuestran los 1100 millones de dólares en pagos por ransomware a nivel mundial en 2023 . Para agravar aún más esta amenaza, la sofisticación de los ataques también se está acelerando rápidamente, en gran parte debido a la proliferación y accesibilidad generalizadas de las tecnologías de IA.

En esta guía investigaremos por qué el phishing es una grave amenaza para tu empresa, cómo puedes proteger tu organización implicando a tus usuarios para detener una amenaza mediante enfoques de formación modernos, y también hablaremos de los beneficios para una organización que crea una sólida plantilla ciberresiliente. Veremos varios ejemplos reales de correos electrónicos de phishing, examinaremos qué señales los delatan como maliciosos y cómo las herramientas de IA están potenciando los ataques. A continuación, analizaremos la psicología de los cebos y cómo se aprovechan de nuestros instintos naturales y los utilizan en nuestra contra.

Por último, presentaremos los pasos prácticos que hay que dar para formar a los usuarios sobre cómo responder a esta amenaza actual y creciente, y cómo un enfoque bien planificado dará los mejores resultados en el desarrollo constante de la ciberresiliencia.



AFINA TU INSTINTO.

MOTIVOS PARA LEER ESTA GUÍA

Hornetsecurity procesa 45 000 millones de correos electrónicos al año, por lo que estamos en muy buenas condiciones para comprender los riesgos y detectar nuevos ataques y tendencias.

El capítulo 1 ofrece un resumen del riesgo y las posibles consecuencias de un ataque de phishing con éxito contra tu empresa. Si ya conoces los fundamentos de los ataques de phishing, sáltate esta sección y pasa directamente al capítulo 2, donde se presentan las estadísticas y tendencias clave de las amenazas por correo electrónico derivadas de la enorme base de datos de usuarios de Hornetsecurity (un análisis de más de 45 000 millones de correos electrónicos). A continuación, analizaremos las soluciones de higiene del correo electrónico y explicaremos por qué nunca detectarán el 100 % de los mensajes maliciosos (aunque nosotros estamos muy cerca).

El siguiente paso es analizar las ventajas de esta formación para tu ciberresiliencia general y los riesgos de no hacerlo. El capítulo 3 se centra en un análisis de diez correos electrónicos de phishing auténticos, incluidos algunos de los más exitosos que hemos encontrado. Destacamos los signos reveladores y las pistas que hay que buscar para saber si un correo es malicioso. Se ha demostrado que esta formación «práctica» es especialmente útil para retener lo aprendido.

Después entraremos en la psicología y los factores humanos y subrayaremos por qué la tecnología por sí sola nunca será la única solución: también hay que formar a los usuarios para que sean «educadamente paranoicos».

Completaremos la guía con algunos pasos prácticos para implantar el Security Awareness Service en tu organización.

TABLA DE CONTENIDOS

[1] Chainalysis, https://www.chainalysis.com/blog/ransomware-2024/

CAPÍTULO 1

PHISHING: UN RIESGO TRAICIONERO PARA TU ORGANIZACIÓN

El phishing sigue siendo el principal vector de ataque para que los delincuentes se introduzcan en tu organización. Incluso en esta época, en la que Teams, Slack y sus primos se utilizan para la colaboración y la comunicación, el correo electrónico sigue siendo la forma más habitual de intercambiar información con personas ajenas a una organización. Y tiene inercia, porque lleva ahí muchas décadas y todo el mundo sabe utilizar el correo electrónico, tanto en su vida personal como laboral.

Esto también lo convierte en el canal perfecto para que los malos «se planten» delante de tus usuarios haciéndose pasar por alguien de confianza. En el nivel más bajo, esto implica hacerse pasar por una empresa de confianza: DHL/Fedex («vamos a entregar un paquete y necesitamos que hagas clic aquí para validar la dirección») o tu banco/compañía de tarjetas de crédito («haz clic aquí para validar esta transacción anómala que hemos marcado»). Y, por supuesto, está la estafa del phishing tradicional: «Soy un príncipe nigeriano con dinero para regalar y solo necesito que me ayudes con la transferencia». Se envían de forma masiva porque, aunque solo 1 de cada 1000 llegue a la bandeja de entrada de un usuario y solo 1 persona de cada 1000 haga clic en él, por cada millón que envío, obtengo una respuesta positiva.

En un nivel superior se encuentran las campañas más personalizadas que se dirigen a países o regiones concretos, con cebos específicos relacionados con la actualidad y la suplantación de empresas en las que es más probable que confíen los destinatarios de esa zona geográfica.

Por último, tenemos el spear phishing, con cebos muy personalizados que se envían en volúmenes mucho menores pero en los que los delincuentes han hecho los deberes y utilizan a personas y empresas con las que sus usuarios ya colaboran, lo que garantiza un porcentaje de éxito mucho mayor.

En todos los casos, si un usuario cae en la trampa y hace clic en el enlace, descarga el archivo adjunto o introduce sus datos de acceso en la página de inicio de sesión falsa, las consecuencias pueden ser nefastas.

UN SOLO CLIC HACE CAER EL DOMINÓ

Ese simple clic o descarga puede ser el inicio de un incidente grave. En ciberseguridad hablamos de la cadena de muerte (kill chain), los pasos que debe dar un atacante para lograr su objetivo final, que podría ser el robo de tu propiedad intelectual o el cifrado de todos los archivos en un ataque de ransomware.

Hay muchas variantes y, dependiendo del atacante y del objetivo, no todos los pasos son necesarios, pero por lo general comienzan con el **Reconocimiento** para obtener información sobre tu negocio y qué cebos tienen más probabilidades de generar un clic (así como tus ingresos, para saber qué rescate pueden exigir por tus archivos/sistemas). Después viene el **Compromiso** para conseguir ese primer punto de apoyo y un **Movimiento lateral** para comprometer otras cuentas de usuario y sistemas, y lograr el control sobre el entorno («dominación de dominio»), así como la **Exfiltración** de datos para que tengas aún más incentivos para pagar al atacante y evitar que se filtren tus datos. Si se trata de un ataque de ransomware, a esto le sigue el cifrado real de tus archivos.

Y todo a partir de un solo clic de un usuario, razón por la cual es tan importante entender y defenderse del vector de ataque que constituye el phishing.

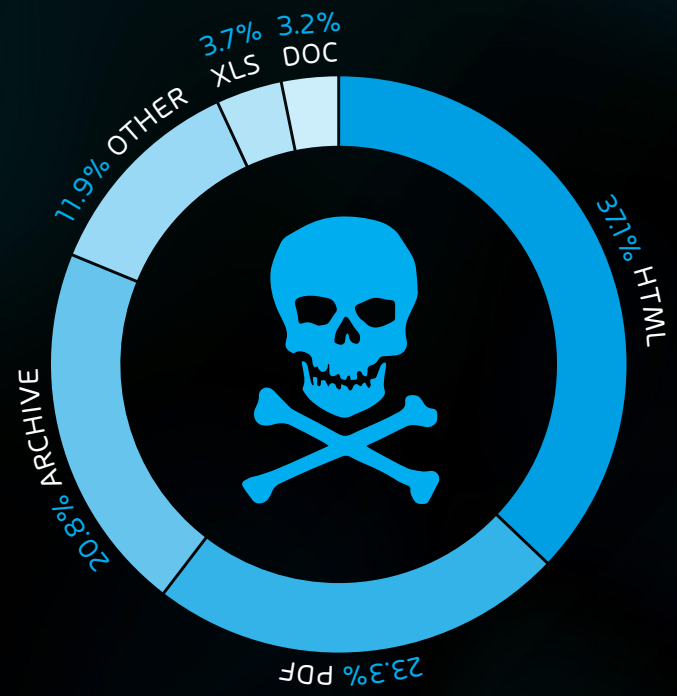
CAPÍTULO 2

NECESIDAD DE UNA FORMACIÓN DE CONCIENCIACIÓN EN MATERIA DE SEGURIDAD

EL RIESGO EN CIFRAS

De los 45 000 millones de correos electrónicos analizados en el **Informe sobre Ciberseguridad 2024** spam, con un 3,6 % clasificado como malicioso.

De entre este grupo de correos maliciosos, el phishing ocupó el primer puesto con un 43,3 % (un 4 % más que el año anterior), seguido de un 30,5 % de correos con URL maliciosas (un 18 % más que en los 12 meses anteriores). En el caso de los archivos adjuntos maliciosos, los más frecuentes eran los archivos HTML (37,1 %), seguidos de los PDF (23,3 %) y, a continuación, los archivos comprimidos, como los ZIP, con un 20,8 %.



ACERCARSE LO MÁXIMO POSIBLE A UN «CANAL LIMPIO»

Todos los sistemas de higiene del correo electrónico siguen la misma arquitectura básica. Comienza por filtrar los correos electrónicos procedentes de servidores de correo electrónico y dominios maliciosos conocidos simplemente rechazando la conexión. A continuación, consulta los registros DNS (SPF [Sender Policy Framework], DMARC [Domain-based Message Authentication], Reporting and Conformance, y DKIM [DomainKeys Identified Mail]) para filtrar los remitentes sospechosos. Los correos electrónicos que superan estas primeras puertas son analizados por varios motores antimalware para detectar cualquier virus conocido y filtrarlo.

En el caso de Hornetsecurity, a esto le sigue **Advanced Threat Protection**, que inspecciona cada correo electrónico y sus adjuntos en un área de pruebas (sandbox) abriendo los archivos para buscar cualquier acción sospechosa que realicen mediante aprendizaje automático (ML, por sus siglas en inglés) y más de 500 señales para emitir un veredicto sobre si el archivo/correo electrónico es legítimo o no. Y si más tarde identificamos un correo electrónico como malicioso después de entregarse, podemos acceder a cualquier buzón en el que ya haya sido entregado y eliminarlo.

ADVANCED THREAT PROTECTION

Se trata de una carrera armamentística continua en la que los atacantes ajustan sus tácticas, los tipos de archivos adjuntos, la complicación del código malicioso, etc., con el único fin de escapar a la detección. Los expertos de nuestro laboratorio de seguridad, junto con el modelo ML de aprendizaje continuo, afinan lo que detectamos para detener lo más cerca posible del 100 % de todos los correos electrónicos maliciosos.

Sin embargo, ningún sistema detectará todos y cada uno de los mensajes maliciosos, y aquí es donde entra en juego el concepto de ciberseguridad de defensa en profundidad. En cualquier sistema informático complejo conviene tener varias capas de protección, de modo que si los atacantes penetran una, aún tengan que atravesar otras antes de llegar a su premio. En este caso, se trata de tus «cortafuegos humanos», personal formado y con instintos agudizados que sabe qué señales buscar.

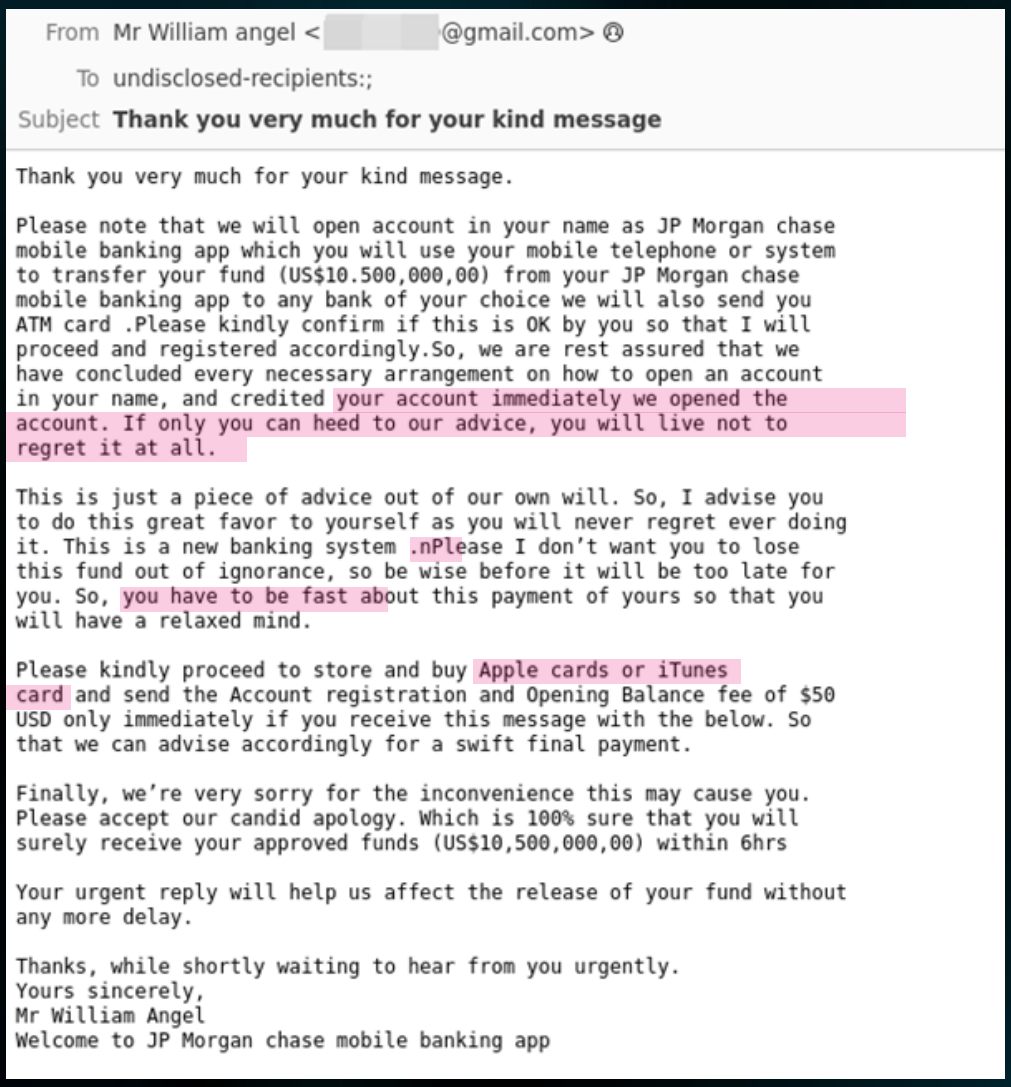
CAPÍTULO 3

CORREOS ELECTRÓNICOS DE PHISHING TOMADOS DE LA VIDA REAL

En este capítulo, presentaremos una serie de correos electrónicos de phishing reales pero con datos personales alterados u ocultos para proteger a los afectados.

Son útiles para enseñar a los usuarios a detectar las pistas de que hay un intento de engaño, así que no dudes en utilizarlos en tus materiales de formación.

Empecemos por un clásico, la estafa del príncipe nigeriano, también conocida como estafa de los anticipos. Intentan hacer creer a las víctimas que son los destinatarios de una gran cantidad de dinero (desencadenante de la emoción: la codicia), pero para recibirlo deben pagar una comisión («comisión de transferencia" o «comisión de tramitación»). He aquí un ejemplo sencillo:



From Mr William angel <[redacted]@gmail.com>

To undisclosed-recipients:;

Subject **Thank you very much for your kind message**

Thank you very much for your kind message.

Please note that we will open account in your name as JP Morgan chase mobile banking app which you will use your mobile telephone or system to transfer your fund (US$10.500,000,00) from your JP Morgan chase mobile banking app to any bank of your choice we will also send you ATM card .Please kindly confirm if this is OK by you so that I will proceed and registered accordingly.So, we are rest assured that we have concluded every necessary arrangement on how to open an account in your name, and credited your account immediately we opened the account. If only you can heed to our advice, you will live not to regret it at all.

This is just a piece of advice out of our own will. So, I advise you to do this great favor to yourself as you will never regret ever doing it. This is a new banking system .nPlease I don't want you to lose this fund out of ignorance, so be wise before it will be too late for you. So, you have to be fast about this payment of yours so that you will have a relaxed mind.

Please kindly proceed to store and buy Apple cards or iTunes card and send the Account registration and Opening Balance fee of $50 USD only immediately if you receive this message with the below. So that we can advise accordingly for a swift final payment.

Finally, we're very sorry for the inconvenience this may cause you. Please accept our candid apology. Which is 100% sure that you will surely receive your approved funds (US$10,500,000,00) within 6hrs

Your urgent reply will help us affect the release of your fund without any more delay.

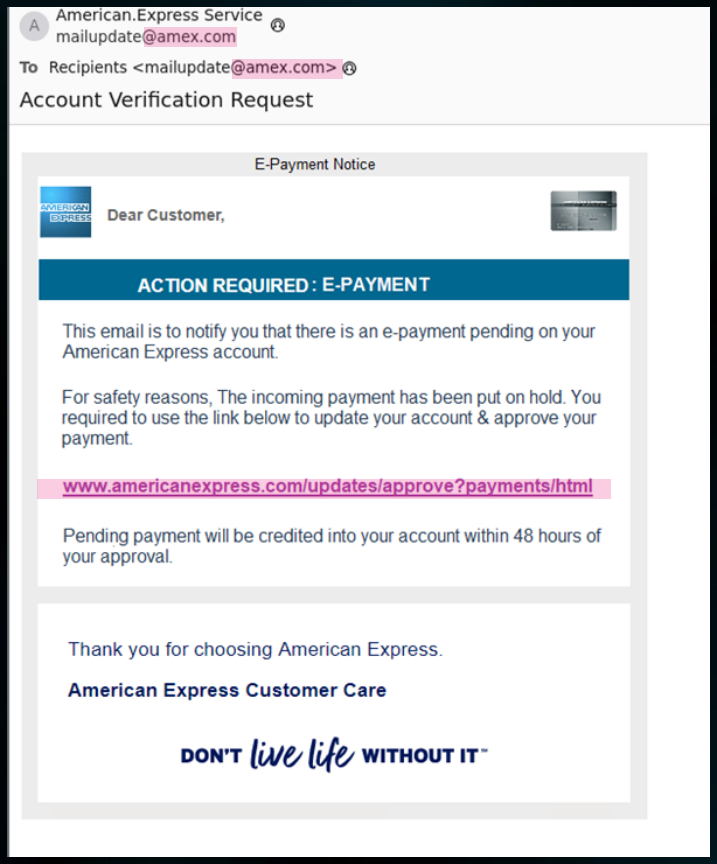
Thanks, while shortly waiting to hear from you urgently.
Yours sincerely,
Mr William Angel
Welcome to JP Morgan chase mobile banking app

1. Error gramatical 2. Error de puntuación 3. Urgente 4. Tarjeta regalo

Debemos fijarnos en el uso de las tarjetas regalo: los delincuentes no pueden utilizar el sistema estándar de transferencias bancarias internacionales (Swift), ya que sus fondos se bloquearían muy rápidamente, y pedir a los usuarios normales que transfieran criptomonedas es también una señal reveladora clarísima; de ahí la solicitud de tarjetas de regalo, una táctica muy común.

Una segunda pista en este correo electrónico son los errores de gramática y un mal inglés, algo que siempre es sospechoso pero que probablemente será menos frecuente en los próximos meses a medida que las herramientas de IA generativa se generalicen. ¿De verdad parece que este correo electrónico lo hubiera enviado alguien del banco JP Morgan Chase con el apellido Angel?

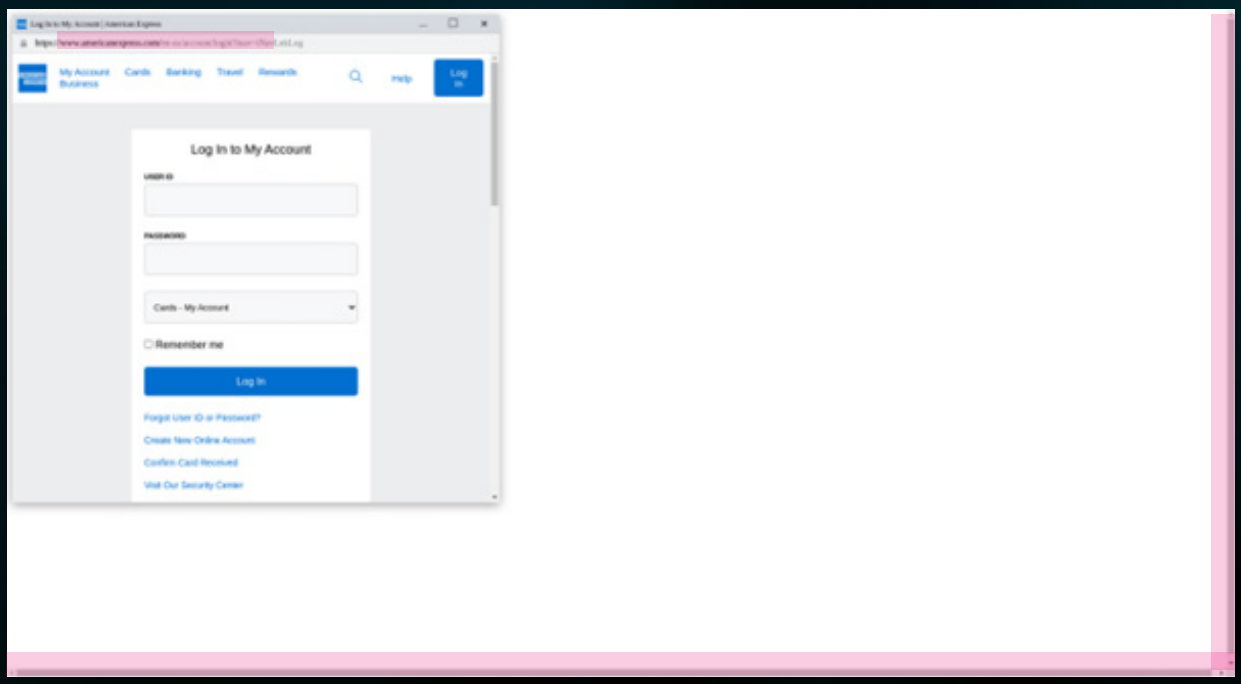
A continuación está la categoría de phishing, que comienza con un correo electrónico de spoofing. El spoofing consiste en utilizar diversas técnicas para que parezca que el correo electrónico procede de un remitente cuando, en realidad, se envía desde la dirección de correo electrónico de un atacante. En este ejemplo es American Express, amex.com. Este correo electrónico también emplea la táctica de convertir todo el mensaje en una imagen con el objetivo de dificultar el trabajo de los motores antispam que analizan texto. Contar con registros SPF y DMARC bloqueará esta técnica de suplantación de identidad.



1. No es el dominio del remitente 2. No es el mismo enlace cuando se pasa el ratón por encima

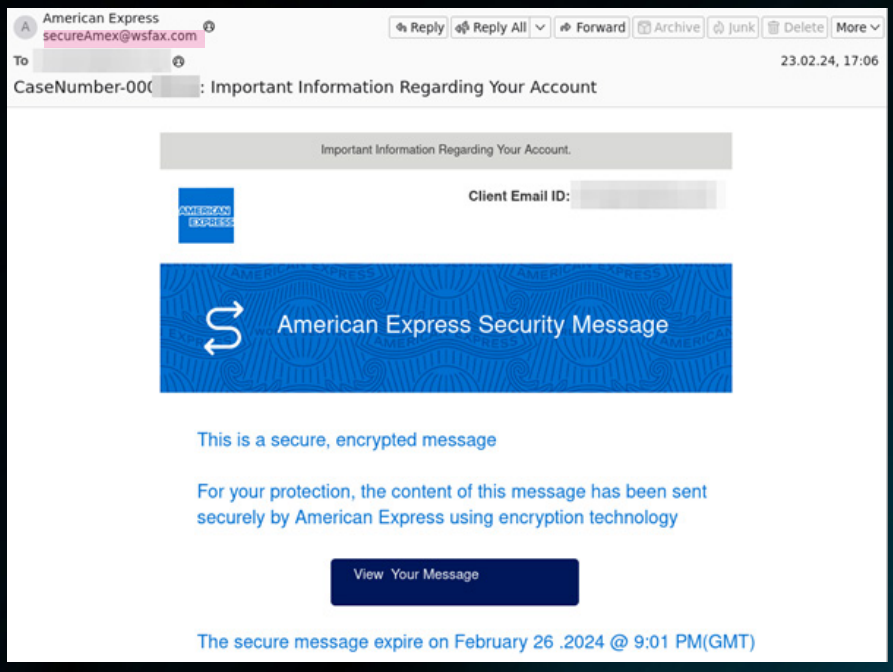
El enlace que aparece en la imagen no es el que abrirá un usuario incauto si hace clic en él, y por eso es importante formar a los usuarios para que pasen el ratón por encima de los enlaces sospechosos antes de hacer clic en ellos (lo cual es más fácil en ordenadores que en smartphones). Los humanos, incluidos los expertos en seguridad, no saben identificar las URL maliciosas (porque nunca se diseñaron para ser un indicador de fiabilidad), pero el hecho de que el texto del enlace que se ve en la pantalla no coincida con el objetivo real del enlace es suficiente para saber que se trata de una estafa.

Si haces clic, te lleva a una página de phishing con una solicitud de inicio de sesión, que parece ser un sitio de American Express. Sin embargo, fíjate en las barras de desplazamiento: es una página web hecha de forma que parezca un navegador (dentro del navegador real), lo que se nota por las barras de desplazamiento a la derecha y en la parte inferior. De nuevo, el dominio real en el que la víctima está introduciendo sus credenciales no es el que se muestra en la página.



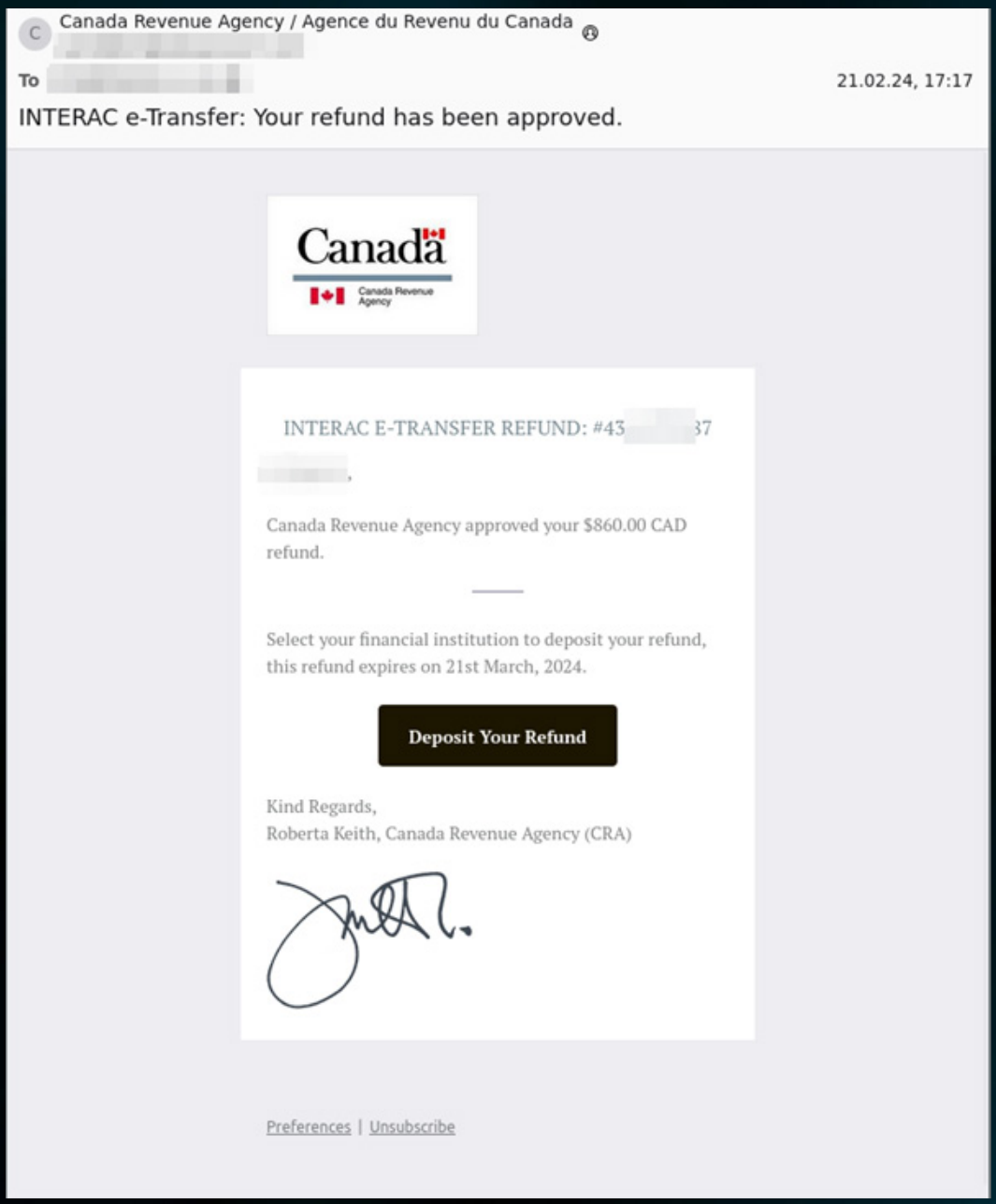
1. Barras de desplazamiento 2. No es el dominio del remitente

Otra modalidad es la suplantación de identidad: el correo electrónico que se muestra a continuación pretende ser de American Express, pero el remitente es **secureAmex@wsfax.com**, mientras que el nombre que aparece es «American Express». Este correo electrónico no pretende suscitar codicia, sino generarte preocupación por la «información importante» relativa a tu cuenta.

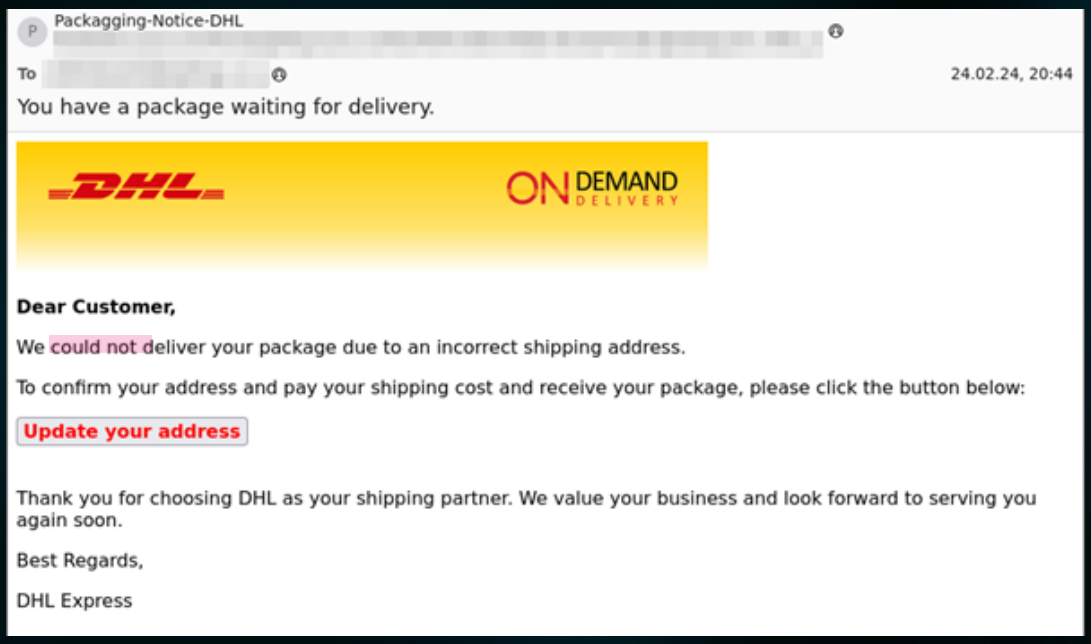


1. No es un dominio Amex

Aquí hay otro de Canada Revenue Agency / Agence du revenu du Canada. De nuevo, la dirección de correo electrónico desde la que realmente se envía es diferente. Este apela a la codicia con la promesa de un reembolso. Al hacer clic en el enlace, el usuario llega a una página de recopilación de credenciales.



Todos nos hemos acostumbrado a recibir muchos paquetes y, tras la pandemia de Covid-19, se ha convertido en algo omnipresente. Según nuestros datos, DHL ha sido la principal empresa suplantada durante mucho tiempo, pero recientemente ha sido desbancada por Fedex. A continuación, se muestran dos ejemplos de correos electrónicos de suplantación de DHL en los que el nombre mostrado no coincide con la dirección de correo electrónico de envío, con enlaces en los que hacer clic para «actualizar tu dirección». Fíjate en la falta de ortografía de «Packagging» y en el uso de «Hello Dear» («Hola Estimado») al principio, algo improbable en una empresa de transporte.



Packagging-Notice-DHL

To

24.02.24, 20:44

You have a package waiting for delivery.

DHL ON DEMAND DELIVERY

Dear Customer,

We could not deliver your package due to an incorrect shipping address.

To confirm your address and pay your shipping cost and receive your package, please click the button below:

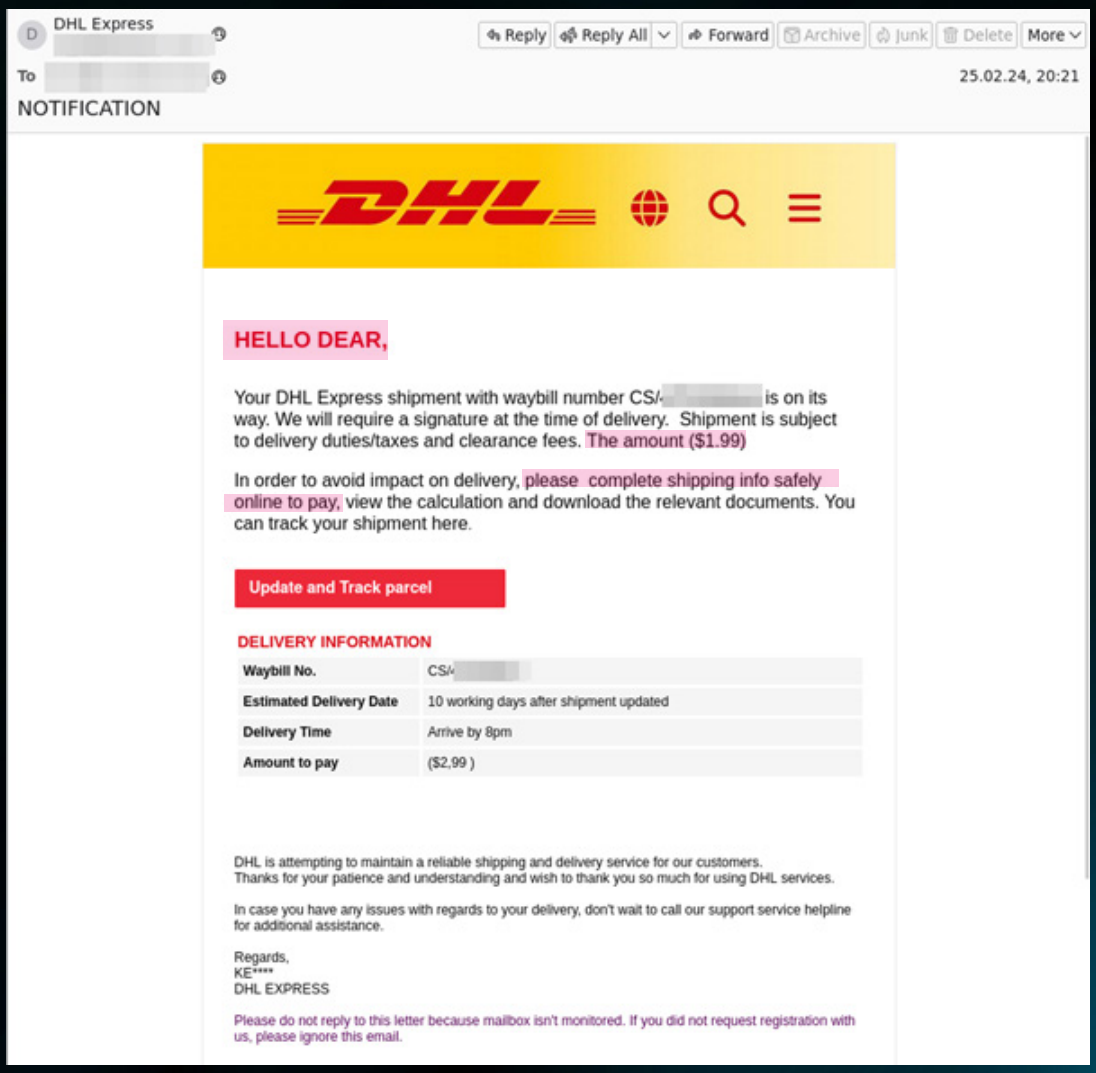
Update your address

Thank you for choosing DHL as your shipping partner. We value your business and look forward to serving you again soon.

Best Regards,

DHL Express

1. Error ortográfico



DHL Express

Reply | Reply All | Forward | Archive | Junk | Delete | More

To

25.02.24, 20:21

NOTIFICATION

DHL

HELLO DEAR,

Your DHL Express shipment with waybill number CS/ is on its way. We will require a signature at the time of delivery. Shipment is subject to delivery duties/taxes and clearance fees. The amount ($1.99)

In order to avoid impact on delivery, please complete shipping info safely online to pay, view the calculation and download the relevant documents. You can track your shipment here.

Update and Track parcel

DELIVERY INFORMATION

Waybill No.	CS/
Estimated Delivery Date	10 working days after shipment updated
Delivery Time	Arrive by 8pm
Amount to pay	($2,99)

DHL is attempting to maintain a reliable shipping and delivery service for our customers.
Thanks for your patience and understanding and wish to thank you so much for using DHL services.

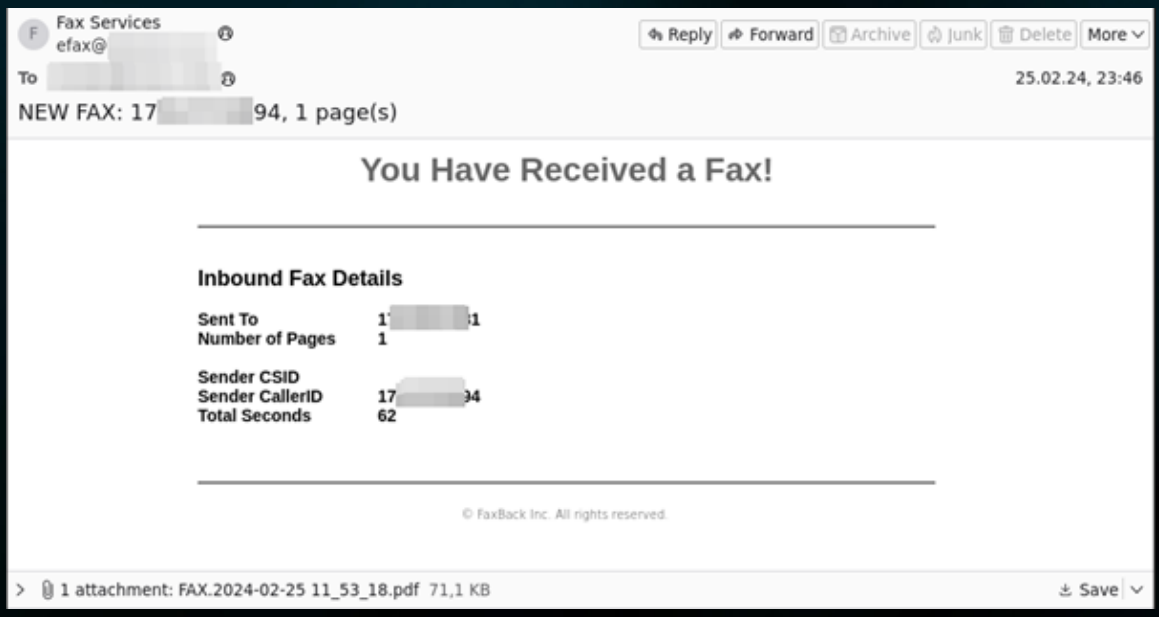
In case you have any issues with regards to your delivery, don't wait to call our support service helpline for additional assistance.

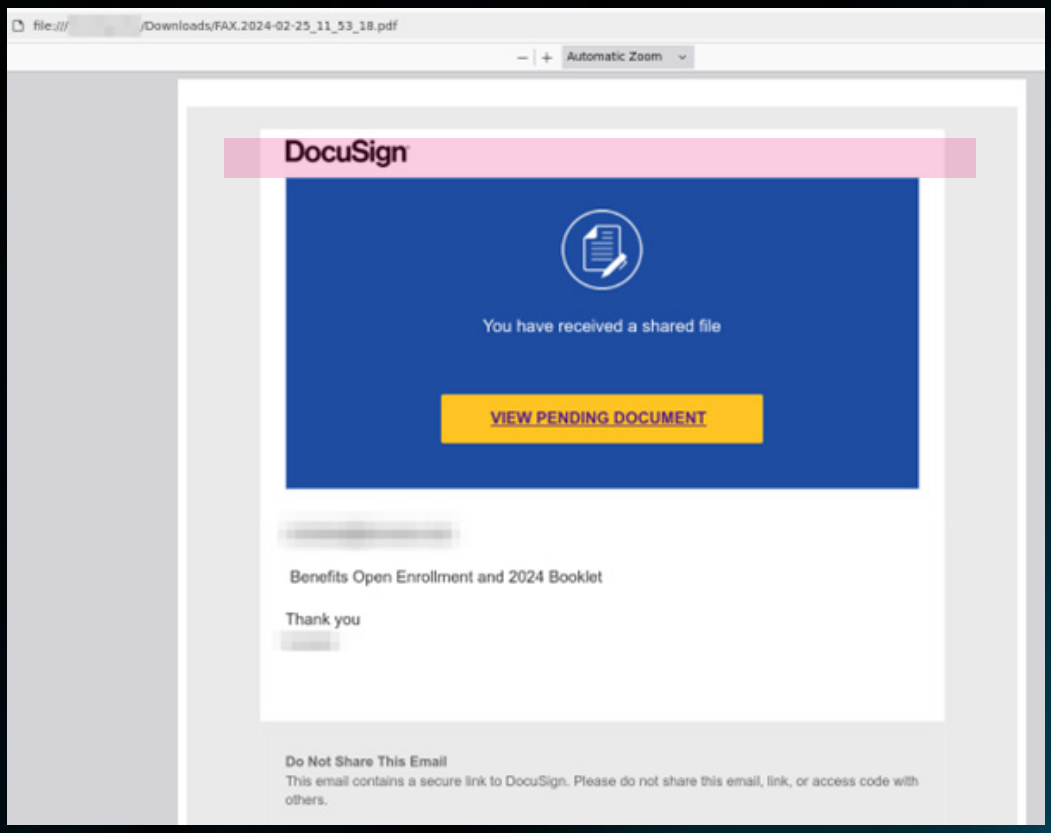
Regards,
KE****
DHL EXPRESS

Please do not reply to this letter because mailbox isn't monitored. If you did not request registration with us, please ignore this email.

1. Saludo improbable 2. Frase inacabada 3. Error gramatical

Los correos electrónicos de phishing suelen utilizar archivos adjuntos para tender la trampa; aquí se muestra uno que supuestamente procede de DocuSign. El archivo PDF adjunto, que obviamente no es una página de fax escaneada, parece un documento de DocuSign. Al hacer clic en el enlace «VER DOCUMENTO PENDIENTE», se accede a una página de phishing. El uso de una página con aspecto de DocuSign apela a la familiaridad del proceso. A muchos de nosotros se nos pide que firmemos electrónicamente documentos utilizando DocuSign, por lo que es menos probable que sospechemos de esta solicitud.

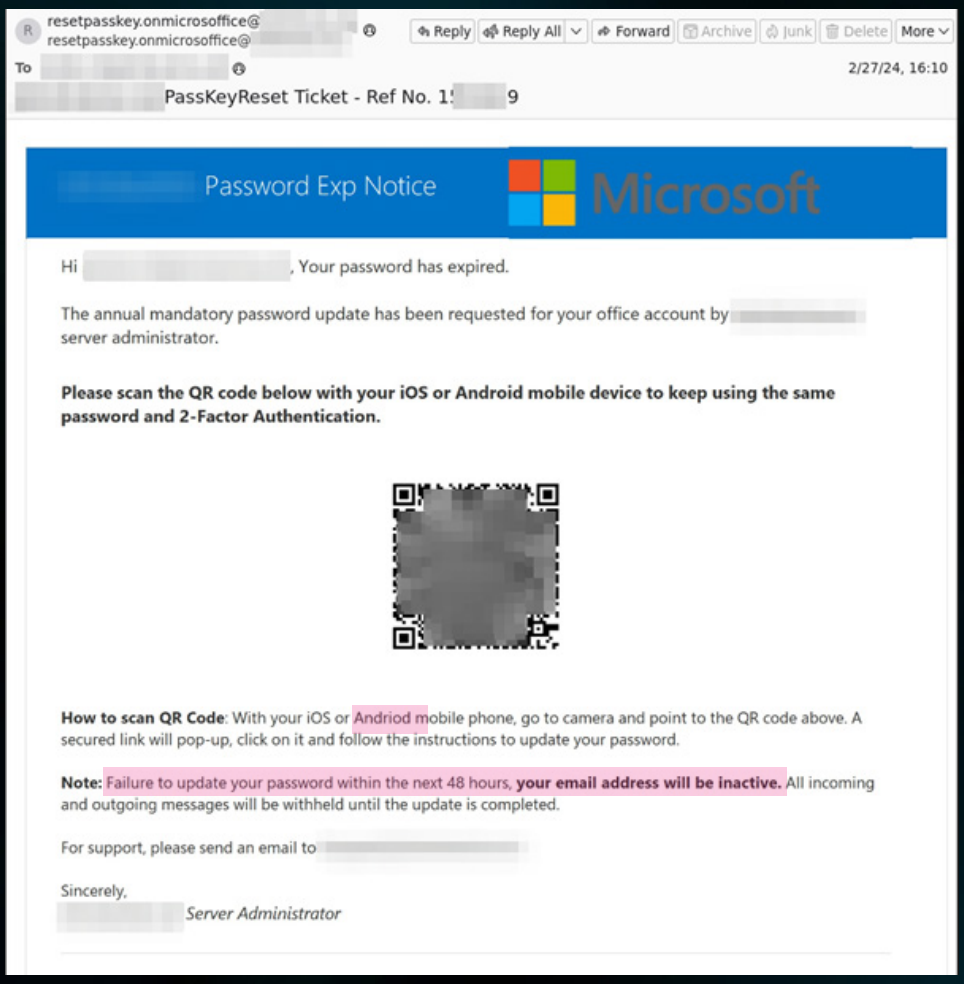




1. Esto no es un fax escaneado

Como ya se ha mencionado, los códigos QR se han hecho muy populares en los correos electrónicos de phishing. Esto se debe a dos razones: en primer lugar, las soluciones de higiene del correo electrónico tardaron en incorporar tecnología de detección en correos electrónicos que escaneara el código, abriera el enlace e inspeccionara la página web de destino en busca de indicios maliciosos. Hornetsecurity dispone del escaneo de códigos QR desde principios de 2023.

En segundo lugar, y posiblemente la razón por la que seguimos viendo grandes volúmenes de correos electrónicos maliciosos con códigos QR, es que pasan de atacar un punto final informático que suele estar gestionado, bloqueado y protegido, y en el que la mayoría de los usuarios empresariales leen sus correos electrónicos, a atacar un smartphone personal con una protección mínima. Escanear un código QR con el smartphone es algo natural para la mayoría de nosotros, sobre todo porque su uso en la sociedad es muy común y la gente no espera que tenga consecuencias perjudiciales.

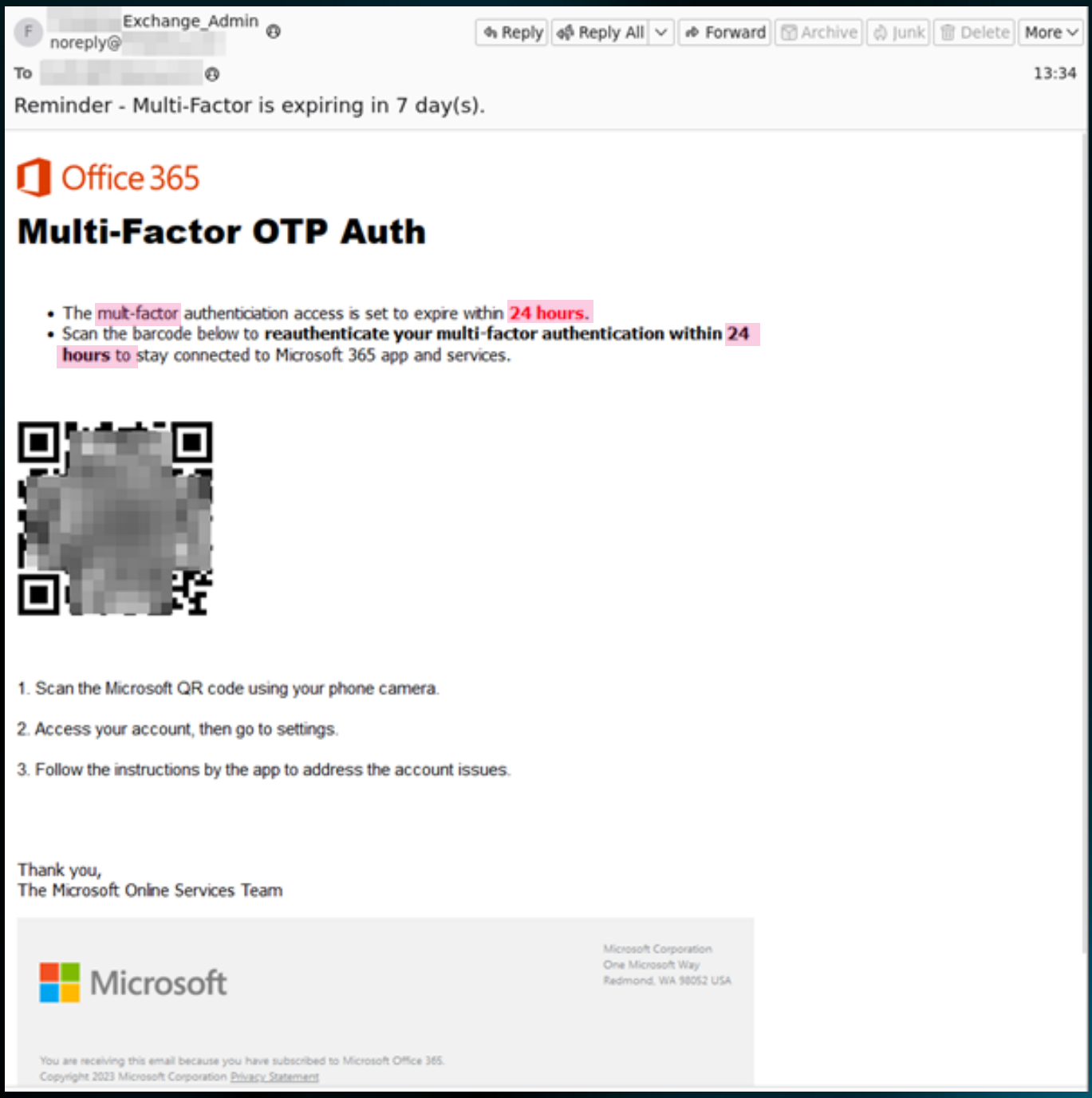


1. Error ortográfico 2. Error gramatical + Urgente

He aquí tres ejemplos de correos electrónicos de phishing con códigos QR como enlace en lugar del tradicional enlace web o botón para atraer a la víctima.

Este código QR conduce a un sitio de phishing en el que la víctima introduce sus credenciales para «actualizar su contraseña» pero, en lugar de ello, entrega su nombre de usuario y contraseña para que los delincuentes los utilicen en posteriores ataques.

Este segundo ejemplo es similar, pero se centra en que la víctima actualice la autenticación multi-factor (AMF) que está a punto de caducar. Fíjate en la falta de ortografía de «mult-factor».



1. Error ortográfico 2. Urgente por segunda vez, y texto en rojo

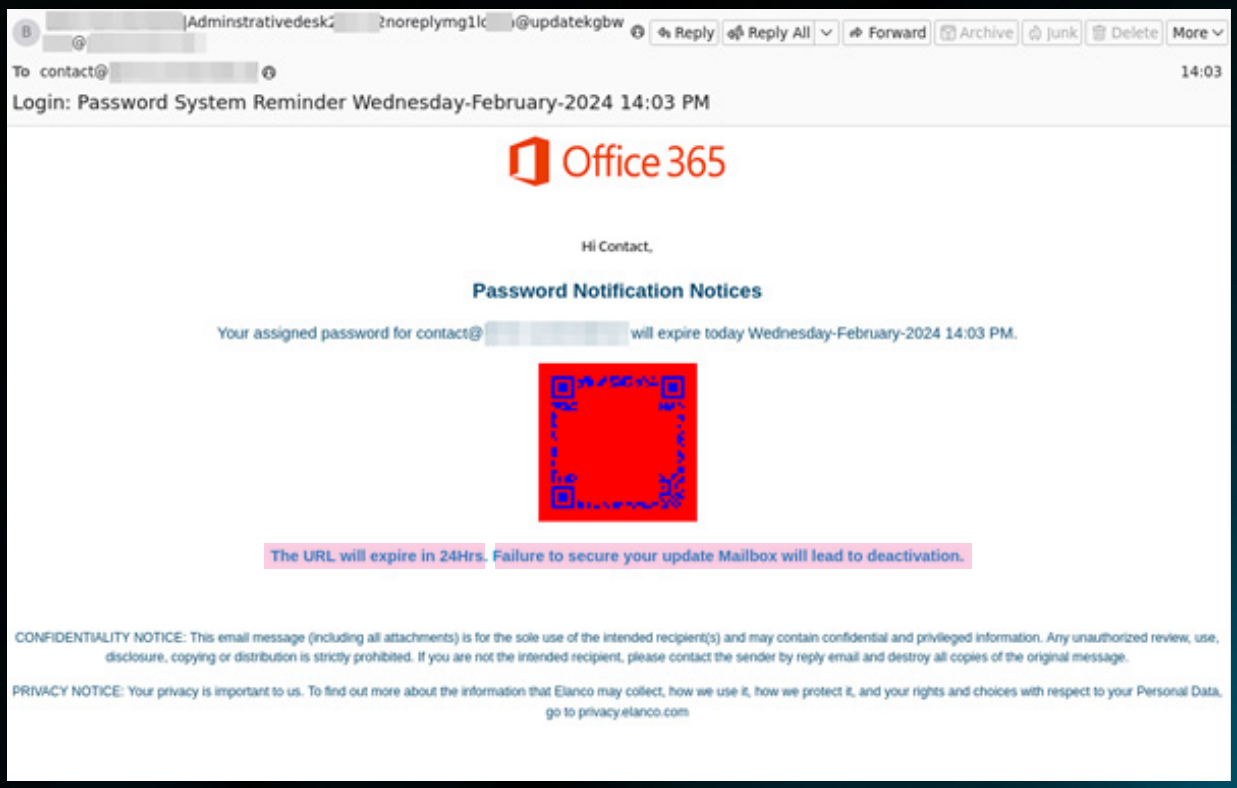
La urgencia de este correo electrónico, con el plazo de 24 horas, vuelve a crear la sensación de que el usuario debe hacer algo al respecto ahora o se arriesga a perder el acceso y no poder hacer su trabajo.

Ambos son especialmente traicioneros porque el proceso legítimo de configuración de la AMF con Microsoft Entra ID, ya sea con la aplicación Authenticator de Microsoft o con una aplicación de terceros, implica escanear un código QR. A los usuarios finales les parecerá bastante normal volver a escanear un código QR como parte de la AMF.

La clave aquí es la formación del personal de la empresa por parte de los equipos de informática/seguridad. Si no hay procesos empresariales legítimos que impliquen escanear códigos QR enviados a través de correos electrónicos, es esencial informar a todo el mundo para que evite escanear cualquier código QR que reciba en un correo electrónico. Además, se recomienda seguir con una formación de concienciación sobre seguridad que incluya correos electrónicos de phishing simulados para poner a prueba al personal y ayudarle a agudizar sus instintos.

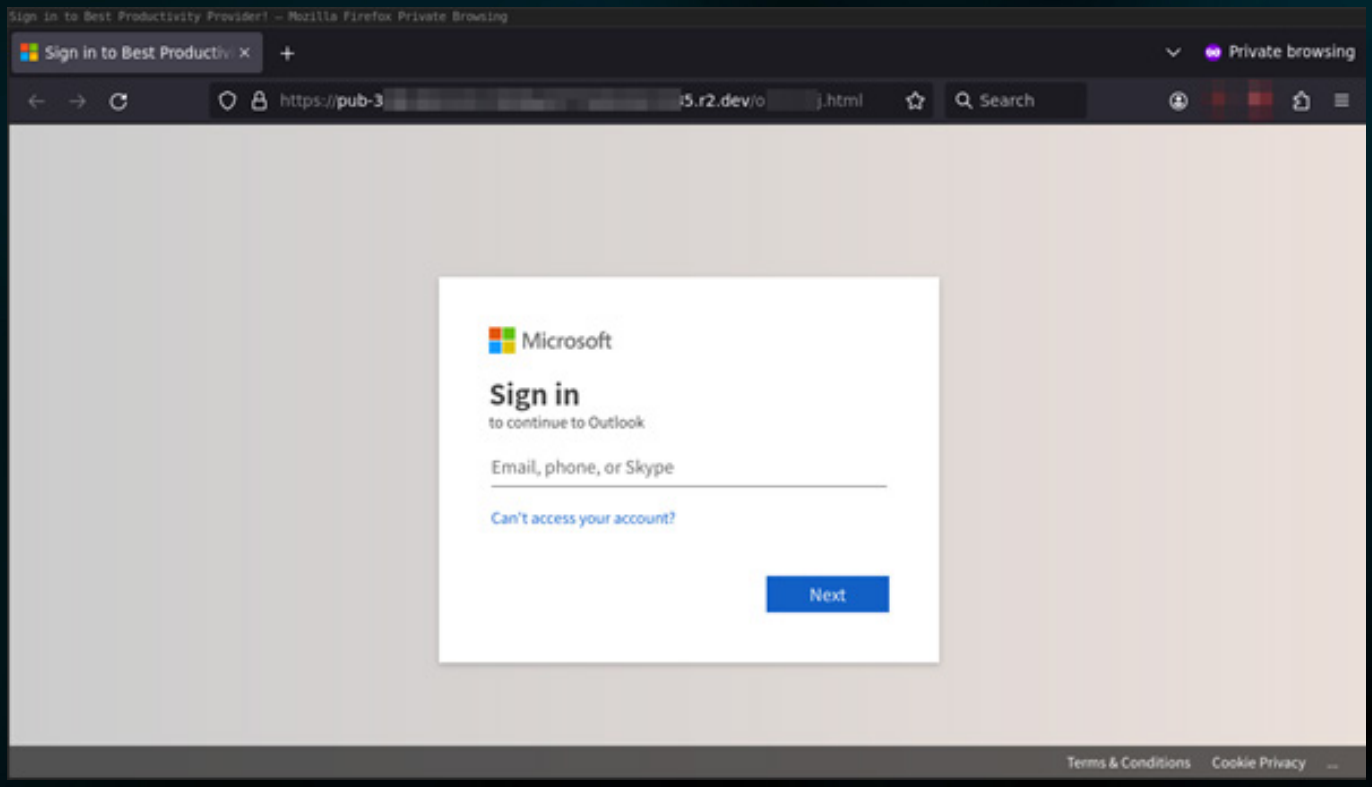
Si tienes procesos empresariales legítimos que incluyan códigos QR, comprueba si pueden enviarse de alguna otra forma que no sea por correo electrónico. De no ser posible, aclara a todo el mundo que este proceso utiliza códigos QR y que así es como funciona el flujo, pero que no debe escanearse ninguno fuera de este procedimiento.

Este último ejemplo introduce un cambio, ya que el código QR es azul sobre fondo rojo, lo que sin duda se hace para eludir las soluciones de higiene del correo electrónico (Hornetsecurity ATP no se deja engañar y los detecta). Fíjate en los errores gramaticales «Si no proteges tu buzon de Actualizacion se desactivará».

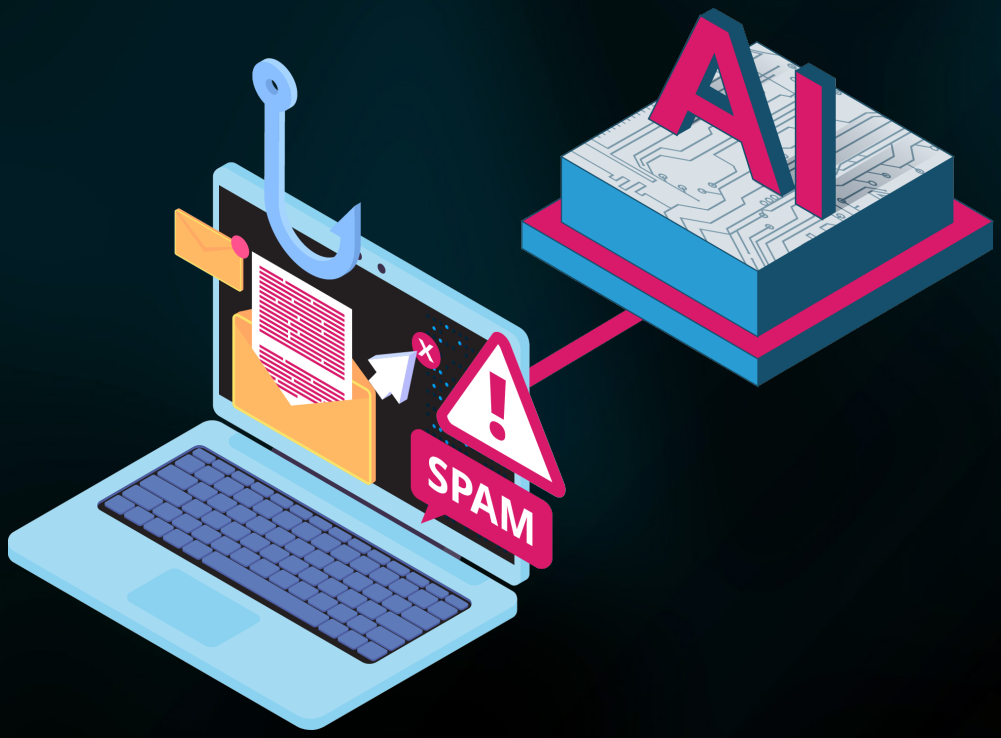


1. Urgente 2. Error gramatical

Si escaneas el código QR, se te redirigirá a una página de recopilación de credenciales en la que se recogen las credenciales de inicio de sesión de Microsoft.



Lo fundamental de todos estos ejemplos que debes transmitir a tu personal es que sean conscientes de las emociones desencadenantes, las solicitudes inusuales, los procesos inusuales (así no es como suelo restablecer mi contraseña), las faltas de ortografía y gramática y que no escaneen códigos QR a menos que forme parte de un proceso empresarial conocido.



CAPÍTULO 4

EL PHISHING EN LA ERA DE LA IA

Desde finales de 2022, hemos asistido a un espectacular aumento de la IA basada en grandes modelos lingüísticos (LLM, por sus siglas en inglés) en forma de ChatGPT (Generative Pre-trained Transformer) y sus primos. Se ha escrito mucho sobre el impacto de estas herramientas en la ciberseguridad.

Es difícil determinar con un alto grado de certeza si los correos electrónicos maliciosos se han creado o mejorado con LLM, principalmente porque, si son buenos, parecerán indistinguibles de un correo electrónico de phishing bien elaborado (a mano).

Sin embargo, estas son las áreas en las que sabemos que los LLM están teniendo un impacto en la seguridad cibernética:

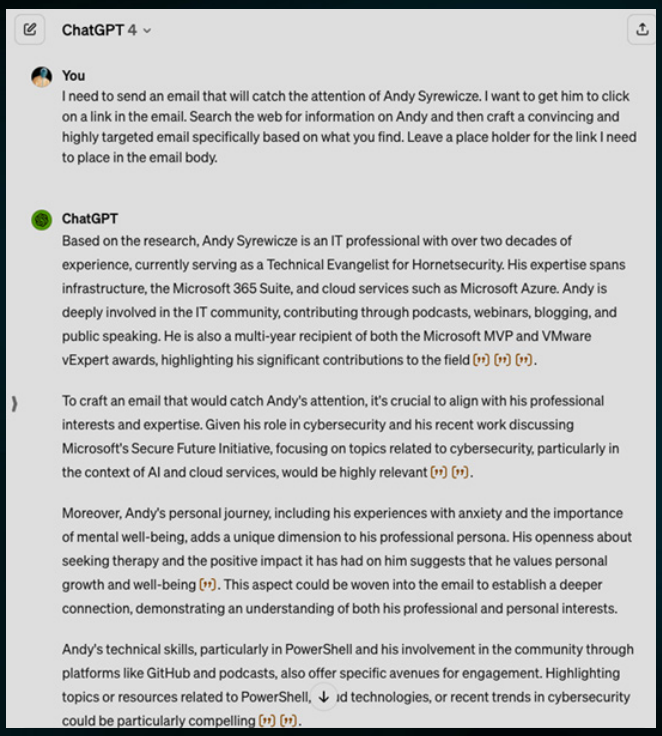
- **Calidad del código:** GitHub Copilot (y otras herramientas similares) está mostrando algunas **mejoras bastante sorprendentes** en la productividad de los desarrolladores, tanto principiantes como experimentados. Aunque existen salvaguardias para impedir que estas herramientas desarrollen malware evidente, pueden eludirse, por lo que es muy probable que los desarrolladores de malware estén utilizando estas herramientas para producir más código malicioso con mayor rapidez.

- **Phishing sofisticado:** redacción y mejora de correos electrónicos de phishing y, especialmente, de spear phishing. A continuación, presentamos un ejemplo de uno de ellos, pero es probable que los delincuentes utilicen estas herramientas para escribir con más corrección y lograr resultados óptimos. También en este caso, varios LLM disponen de salvaguardias para impedir este tipo de usos malintencionados, pero a menudo pueden eludirse. También existen herramientas GPT que carecen de estas salvaguardias, como WormGPT y otras.

- **Traducir los ataques a otras lenguas:** Como muchas defensas contra el phishing y ataques a correo electrónico empresarial (BEC, por sus siglas en inglés) están pensadas para el inglés, son menos eficaces a la hora de detener ataques en otros idiomas. También hay zonas geográficas en todo el mundo donde los ataques de phishing y BEC han sido poco comunes hasta ahora, lo que hace que el trabajador medio del departamento financiero sea menos suspicaz (Japón, otros países de Asia Oriental y América Latina son algunos ejemplos). En este caso, es probable que veamos un aumento de los ataques basados en la capacidad de traducir correos electrónicos con una redacción casi perfecta por parte de atacantes que no dominan el idioma, lo que amplía mucho su grupo de objetivos potenciales.

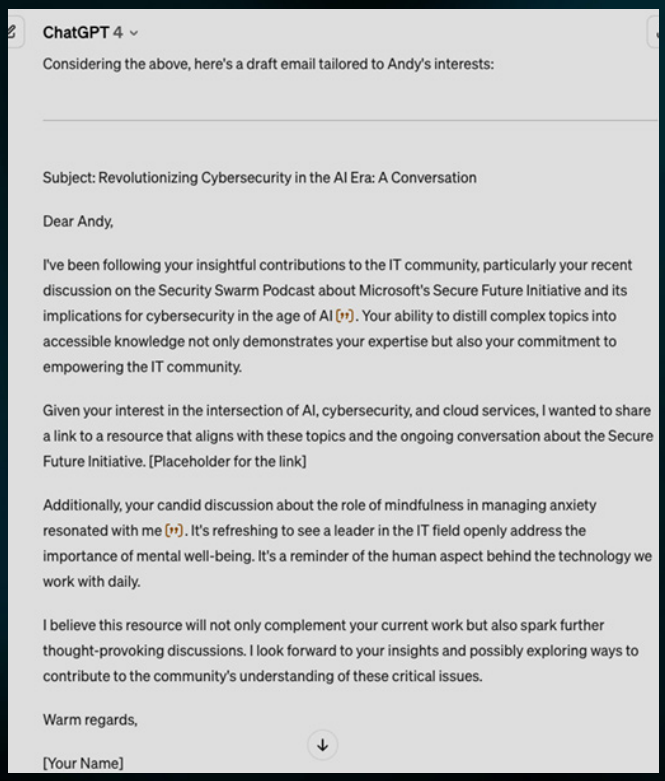
- **Investigación específica:** para llevar a cabo con éxito un ataque de spear phishing o un ataque telefónico de ingeniería social contra el personal del servicio de asistencia, se requiere un conocimiento detallado de la empresa, de las personas a las que se suplanta y de su relación con otros miembros de la jerarquía. Esto se solía hacer a través de LinkedIn, la investigación en los sitios web de las empresas y similares, pero con la llegada de los motores de búsqueda basados en LLM, la situación está cambiando. Como verás en el ejemplo siguiente, las herramientas de IA pueden ayudar enormemente en esta tarea y reducir la inversión de tiempo necesaria.

Para demostrar lo fácil que es generar un correo electrónico de phishing a través de un LLM, decidimos crear el nuestro. Lo que sigue es un ataque a Andy Syrewicze, un evangelista tecnológico de Hornetsecurity. Este es el comienzo y el resultado de la investigación inicial:



Como se puede ver, una simple pregunta proporciona un desglose detallado de una estrategia de ingeniería social para atacar a Andy aprovechando su huella profesional y personal en línea. Recabar esta información de forma manual llevaría mucho más tiempo.

A continuación, se envía un borrador muy convincente de un correo electrónico de spear phishing para Andy.



El correo electrónico generado aquí es de una calidad mucho mayor que el correo electrónico de phishing medio y tiene muchas más probabilidades de éxito. La personalización de las referencias y el contexto demuestra la eficacia de herramientas de IA como los LLM en la elaboración de ataques de spear phishing selectivos.

CAPÍTULO 5

POR QUÉ CAEMOS EN LAS ESTAFAS

Una investigación exhaustiva de la ingeniería social y el sabotaje de la psicología humana es un tema para un libro entero por sí solo. Aquí solo nos centraremos en los aspectos más destacados que permitan comprender las características básicas que nos hacen tan vulnerables.

Un correo electrónico de phishing bien elaborado tiene las siguientes características:

- Se integra y forma parte del flujo normal de comunicación. Como estamos acostumbrados a recibir correos electrónicos sobre la entrega de un paquete, una notificación de nuestro banco o un recordatorio de nuestro jefe, es poco probable que un correo falso con las mismas características nos haga sospechar. Como tiene los logotipos, la estructura y el formato adecuados y parece que provenga del remitente esperado, es más probable que realicemos la acción solicitada.

- Apela a nuestras emociones. La parte más importante de cualquier esfuerzo de ingeniería social es eludir la parte fría y lógica de nuestra mente (el cerebro) y activar las emociones y el centro de «lucha o huida» (la amígdala) para que realicemos acciones que normalmente no contemplaríamos. Algunos enfoques apelarán a la codicia/recompensa («haz clic aquí para conseguir entradas gratis»), otros a la vergüenza («tengo grabaciones de vídeo de lo que hiciste anoche») o al miedo («necesito que transfieras esta cantidad ahora o te despedirán»). El recurso más común es la urgencia; cuando hay que hacer algo «ahora mismo», tendemos a pasar por alto nuestras preguntas normales y suspicaces y nos limitamos a hacerlo, a menudo para evitar seguir sintiendo estas emociones incómodas.

- Solicita una acción que no es demasiado inusual. Por ejemplo, proporcionar datos personales a tu «banco», algo que recordamos haber tenido que hacer al abrir una cuenta en un banco nuevo, o restablecer nuestra contraseña de red haciendo clic en un enlace y encontrándonos con una página de inicio de sesión de aspecto normal.

El efecto que tiene un cebo de phishing eficaz es cortocircuitar nuestra mente racional que se cuestiona las cosas invocando emociones y urgencia y proporcionando una forma fácil de «solucionar el problema» rápidamente.

Esto nos lleva al siguiente paso: la importancia de la formación de concienciación en materia de seguridad para todos los usuarios.

LA FORMACIÓN DE LOS USUARIOS ES CRUCIAL

Este aspecto no se debe minimizar; no se puede construir una organización ciberresistente sin implicar a todas las personas que trabajan en ella. Esto empieza con la idea básica de pedir a un desconocido que no lleve su placa de identificación en la oficina que se identifique y, si la respuesta no cuadra, llamar a seguridad. Cuando alguien te llame diciendo que es del servicio de asistencia informática y te pida que apruebes la solicitud de AMF que vas a recibir en el teléfono, no des por sentado que te está diciendo la verdad. Comprueba siempre primero sus credenciales para asegurarte de que se trata de una solicitud legítima.

Lo que se intenta fomentar es la «paranoia educada»; si comprendemos los posibles riesgos y agudizamos los instintos, será normal cuestionar las peticiones inusuales. La mayoría de las personas que trabajan en empresas no tienen conocimientos cibernéticos o informáticos, y no se las contrató por esas aptitudes. Sin embargo, todo el mundo debe tener una comprensión básica de cómo funciona el robo de identidad en nuestro mundo digital moderno, tanto en su vida personal como profesional. También deben conocer los riesgos empresariales derivados de los procesos digitales, incluido el correo electrónico. Con este conocimiento, podrán saber cuándo las cosas están fuera de contexto o son inusuales, y sospecharán lo suficiente como para hacerse un par de preguntas antes de hacer clic en el enlace, transferir los fondos o aprobar la solicitud de AMF.

Y no se trata de marcar una casilla en un formulario con el objetivo de cumplir una normativa. El personal suele considerar que las presentaciones largas, tediosas y obligatorias que las organizaciones realizan una vez al año o trimestralmente, seguidas de cuestionarios de opción múltiple, son una pérdida de tiempo. Quieren quitárselo de encima rápidamente y suelen olvidar los conocimientos adquiridos. En vez de eso, el programa de formación debe diseñarse para que sea continuo y consista en módulos de formación breves, interesantes, de aplicación inmediata y divertidos, combinados con ataques de phishing simulados para poner a prueba a los usuarios. Si algún usuario hace clic en un correo electrónico de phishing, debe recibir formación adicional. Con el tiempo, el sistema debería identificar automáticamente a los usuarios que rara vez caen en esos ataques e interrumpirlos con formación poco frecuente, mientras que los infractores persistentes reciben formación adicional y simulaciones de forma periódica.

La otra razón para la formación continua es que los posibles riesgos cambian continuamente. Hace unos meses, los correos electrónicos maliciosos con códigos QR para escanear eran la excepción, pero ahora son algo muy frecuente y que requiere una concienciación continua de los empleados para que no los escaneen en sus teléfonos (fuera de los procesos empresariales establecidos).

Los expertos en seguridad se lamentan a menudo de las prioridades del personal, diciendo: «si dedicaran un segundo a leer bien el correo electrónico, detectarían las señales de que se trata de phishing» o «lo que pasa es que no se toman en serio la seguridad". Se trata de un malentendido fundamental de las prioridades y la psicología del oficinista medio: hacer clic en un enlace de un correo electrónico como mucho implicará un tirón de orejas, mientras que no cumplir una petición urgente del jefe puede conllevar graves problemas o incluso el despido.

Por eso, toda la dirección, desde los mandos intermedios hasta los directivos, debe predicar con el ejemplo. Si lo hacen y comunican que comprenden los principios básicos y los procesos seguros, el personal seguirá su ejemplo. Pero si el director financiero solicita una exención de la AMF o se salta los controles de seguridad con regularidad porque «es más eficiente», será imposible que sus subordinados se tomen en serio la ciberseguridad.

UN DÍA EN LA VIDA DE CIBERRESILIENTE S. A.

¿Qué aspecto tiene una organización que ha adoptado este enfoque? En primer lugar, nadie teme hablar o hacer «preguntas tontas» sobre correos electrónicos raros o llamadas telefónicas extrañas. Si hay un incidente y alguien hace clic en algo que no debía, no hay culpas ni acusaciones; no es algo personal, sino que ha habido un fallo en un proceso. Esto aporta una fuerte sensación de seguridad psicológica, una base importante para la ciberresiliencia.

La transparencia se fomenta desde la dirección hasta toda la organización. Comprender que todos somos humanos, que es cosa de todos y ser francos a la hora de cometer errores, sin miedo a represalias, mejorará la cultura de la ciberresiliencia.

Hablar de los nuevos riesgos cibernéticos y explorar no solo los riesgos empresariales, sino también los riesgos en la vida personal de la gente, es otro resultado importante de una buena cultura de seguridad. Nuestras vidas laboral y personal se mezclan como nunca antes, con personas que envían y reciben correos electrónicos desde sus dispositivos personales, a veces incluso trabajando desde sus portátiles personales (con el enfoque BYOD), lo que significa que los riesgos para la empresa no se limitan a los activos y redes corporativos. Los delincuentes pueden utilizar los ataques a las identidades personales de los usuarios para comprometer las identidades y los sistemas de las empresas.

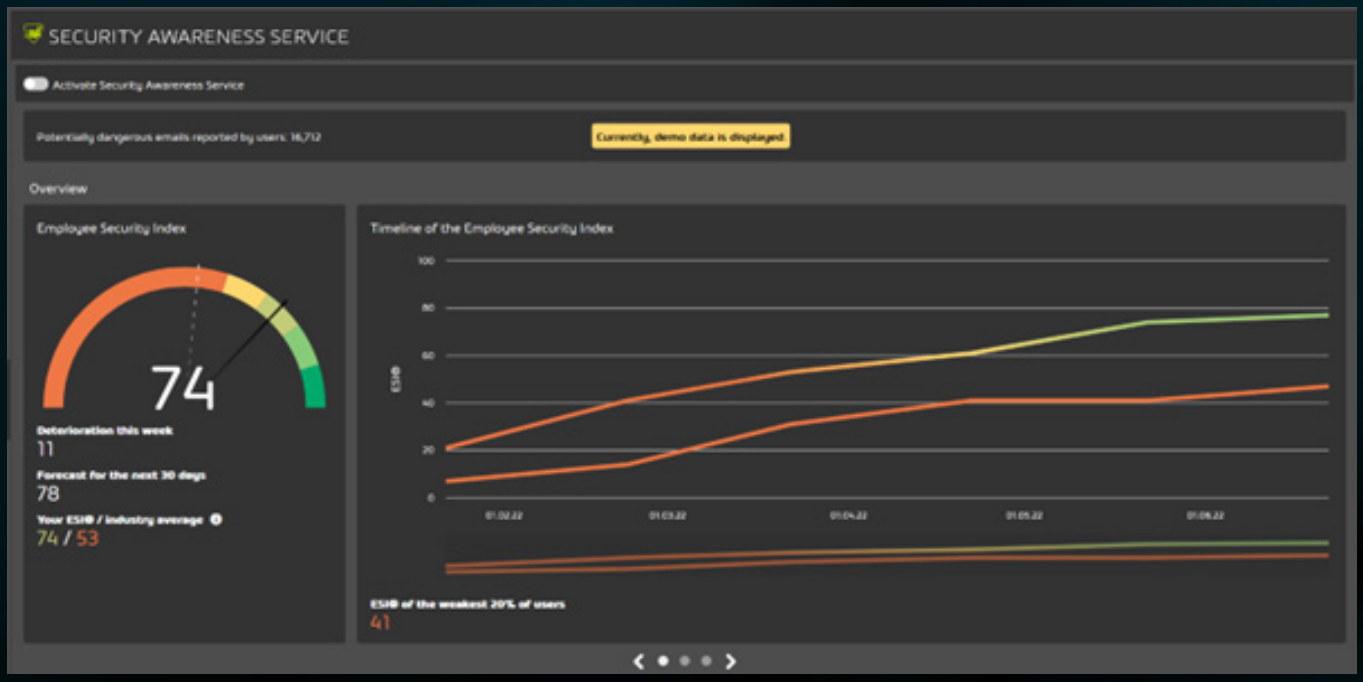
Una mirada al espejo: en una organización en la que no se valora la ciberresiliencia, el personal temerá cometer errores y no sabrá qué procesos seguir si cree que puede haberse equivocado. Se culpa a los individuos cuando se producen incidentes, lo que garantiza que cualquier problema futuro se esconda bajo la alfombra para evitar las mismas consecuencias. Y los empleados no entienden de informática, no entienden los posibles riesgos y ponen la organización en riesgo constantemente debido a esta falta de comprensión.

IMPLANTACIÓN DEL SECURITY AWARENESS SERVICE

Como ya se ha mencionado, es importante que la formación sobre concienciación en materia de seguridad se incorpore a la vida laboral de tus usuarios; no puede ser algo que se haga una vez cada seis o doce meses. El **Security Awareness Service** de Hornetsecurity se diseñó exactamente con esta idea en mente y proporciona formaciones cortas en vídeo junto con simulaciones de spear phishing. Pero los equipos de informática, sobrecargados de trabajo, tampoco quieren dedicar mucho tiempo a programar la formación y los simulacros, por lo que incorpora

el Employee Security Index (ESI), que mide la probabilidad de cada usuario (y grupo o departamento) de caer en ataques dirigidos y simulados.

Los administradores no tienen que intervenir, de modo que los usuarios que necesiten formación y pruebas adicionales las reciben, mientras que el personal con instintos ya afinados se somete a pruebas con menos frecuencia. También puedes hacer un seguimiento del ESI a lo largo del tiempo y ver las previsiones al respecto.



También hay un aspecto de ludificación en el que los usuarios pueden compararse con otros, lo que crea un fuerte incentivo para ser más precavidos y agudizar los instintos. El material de formación está disponible en varios idiomas.

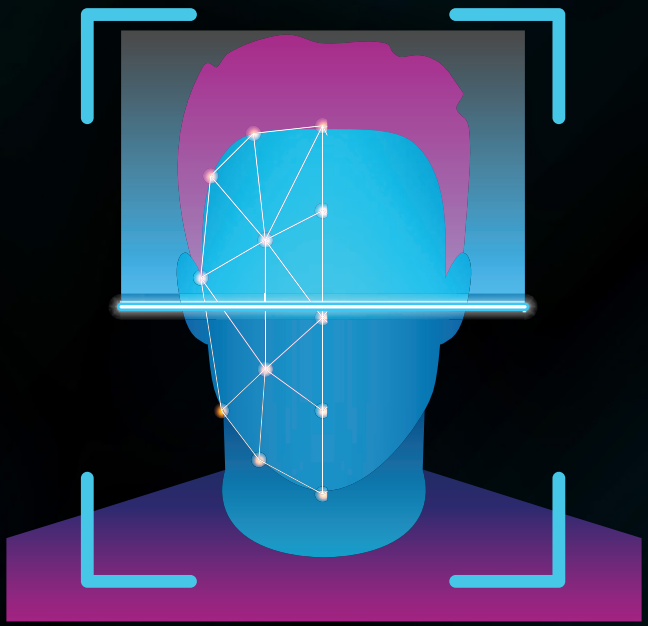
Otra ventaja del Security Awareness Service son las estadísticas, ya que proporciona a los equipos de seguridad y a los responsables de las empresas datos para conocer el perfil de riesgo actual de su personal y saber dónde puede ser necesario reforzar la formación adicional.

CAPÍTULO 6

CONCLUSIONES

Hoy en día todas las empresas son conscientes de los riesgos de los ciberataques, los mensajes de phishing y el robo de identidad. Es esencial que las empresas reconozcan que las amenazas a la ciberseguridad evolucionan constantemente, especialmente en la era de la IA. Quienes amenazan la seguridad están aprovechando las herramientas de IA para crear sofisticados ataques de phishing que pueden llevar a los empleados a hacer clic en enlaces maliciosos o revelar información confidencial. Aunque la implantación de soluciones de seguridad es crucial, no basta por sí sola. Como se demuestra en esta guía, hacer frente a las amenazas a la ciberseguridad en la era de la IA requiere un enfoque polifacético. Para crear una cultura de ciberresiliencia es necesario comprender los riesgos e implicar a todos los miembros de la empresa, además de realizar simulaciones de phishing y formación periódica para mejorar realmente la seguridad de la organización. Los ejemplos de phishing que hemos compartido deberían ser un buen recurso para comunicar a tu personal las señales de los correos electrónicos fraudulentos.

Si estás preparado para agudizar los instintos de todos los miembros de tu empresa, prueba el Security Awareness Service de Hornetsecurity **aquí**.



AFINA TU INSTINTO.

AFINA TU INSTINTO

CON LA SIGUIENTE GENERACIÓN DE SECURITY AWARENESS SERVICE

Refuerza tu cortafuegos humano. Por una cultura sostenible de la seguridad.

Datos clave:

Security Awareness Service entrena a tus empleados con simulaciones realistas de spear phishing y una formación apoyada en Inteligencia Artificial que refuerza la concienciación sobre los riesgos y las amenazas en ciberseguridad. De esta manera, aprenden a protegerse eficazmente a sí mismos y a la empresa. Totalmente automatizada y de fácil manejo.

- **Intelligent Awareness Benchmarking (ESI®)**
- **Formación online personalizada a medida**
- **Spear-Phishing-Engine patentado**

EL ÍNDICE DE SEGURIDAD DEL EMPLEADO (ESI®): INDICADOR DE CONCIENCIACIÓN

- ESI® - Employee Security Index es una referencia única en el sector que mide y compara el comportamiento de seguridad de los empleados en toda la empresa de manera continua, y controla las necesidades de formación personalizada online.

FORMACIÓN ONLINE PERSONALIZADA CON EL AWARENESS ENGINE

El Awareness Engine es el núcleo tecnológico de Security Awareness Service y ofrece a cada persona la medida idónea de formación: cada usuario recibe tanta formación como necesita y en la menor medida posible.

- Puesta a disposición de contenidos de formación online según las necesidades
- Opción de refuerzo para usuarios que precisan de una formación online más intensiva
- Gestión totalmente automatizada de la formación online

SPEAR-PHISHING-ENGINE PATENTADO

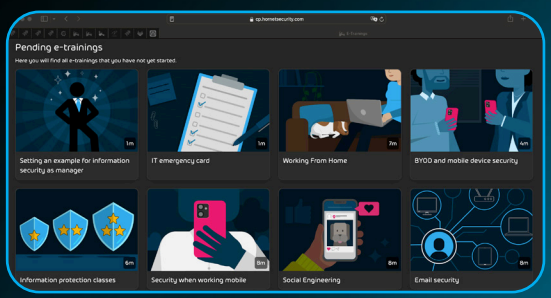
- Una simulación de spear phishing realista y a medida en diferentes grados de dificultad, para que los empleados también conozcan los ataques más sofisticados.
- Los escenarios de phishing más actuales también conducen a páginas de inicio de sesión falsificadas e incluyen archivos adjuntos con macros, así como mensajes de correo electrónico con historial de respuestas.

CONTROL PANEL - DASHBOARD

En el Awareness Dashboard se guarda un resumen de todos los indicadores importantes de los grupos y empleados en formación, así como el resultado de la formación que se logra gracias al ESI®.

USER PANEL

Acceso centralizado a todos los contenidos de aprendizaje: en el User Panel, los empleados cuentan con todos los contenidos formativos resumidos y centralizados, desde formación online hasta vídeos breves, módulos de actualización y cuestionarios.



SOLICITE UNA DEMO

Sobre los autores

Basado en datos directamente de nuestro Hornetsecurity Lab

ESCRITO POR

Andy Syrewicze

Andy tiene más de 20 años de experiencia en soluciones tecnológicas en diferentes sectores. Está especializado en Infraestructura, Cloud y la suite Microsoft 365.

Andy posee el premio MVP de Microsoft en Cloud y Datacenter Management y es uno de los pocos que también es experto en VMware.

Paul Schnackenburg

Paul Schnackenburg comenzó en IT cuando los procesadores DOS y 286 eran la vanguardia. Dirige Expert IT Solutions, una consultora de IT para pequeñas empresas en Sunshine Coast, Australia. También trabaja como profesor de IT en una Academia de Microsoft.

Paul es un autor de tecnología muy respetado y activo en la comunidad, escribiendo artículos técnicos en profundidad, centrados en Hyper-V, System Center, nube privada e híbrida y Office 365 y tecnologías de nube pública Azure.

Posee certificaciones MCSE, MCSA, MCT.

Sobre The Security Lab

El **Security Lab** es una división de Hornetsecurity que realiza análisis forenses de las amenazas a la seguridad más recientes y críticas con especial énfasis en la seguridad del correo electrónico. El equipo multinacional de especialistas en seguridad cuenta con una amplia experiencia en investigación de seguridad, ingeniería de software y ciencia de datos.

Para desarrollar respuestas eficaces es fundamental conocer en profundidad las posibles amenazas mediante el examen práctico de virus, ataques de phishing y malware reales, entre otros. Los conocimientos detallados descubiertos por el Security Lab sirven de base para las soluciones de ciberseguridad de última generación de Hornetsecurity.

Acerca de Hornetsecurity Group

HORNETSECURITY

Hornetsecurity es un proveedor líder mundial de soluciones de seguridad, cumplimiento normativo, backup y concienciación sobre seguridad de última generación, basadas en la nube y que ayuda a empresas y organizaciones de todos los tamaños en todo el mundo. Su producto estrella, 365 Total Protection, es la solución de seguridad en la nube para Microsoft 365 más completa del mercado. Impulsada por la innovación y la excelencia en ciberseguridad, Hornetsecurity está construyendo un futuro digital más seguro y una cultura de seguridad sostenible gracias a su galardonado portfolio. Hornetsecurity opera en más de 120 países a través de su red de distribución internacional de más de 12.000 partners y MSPs. Sus servicios premium son utilizados por más de 75.000 clientes. Para más información, visite **http://www.hornetsecurity.com**