proofpoint.

INFORME

Europa y Oriente Medio

2023 State of The Phish

Una mirada en profundidad a la concienciación, la vulnerabilidad y la resiliencia de los usuarios

proofpoint.com/es

Una encuesta a:

7500
empleados en 15 países

1050
profesionales de seguridad de TI de esos países

Y:

135 millones
de ataques de phishing simulados enviados por nuestros clientes en un período de 12 meses

18 millones
de mensajes de correo electrónico denunciados por los empleados de nuestros clientes en un período de 12 meses

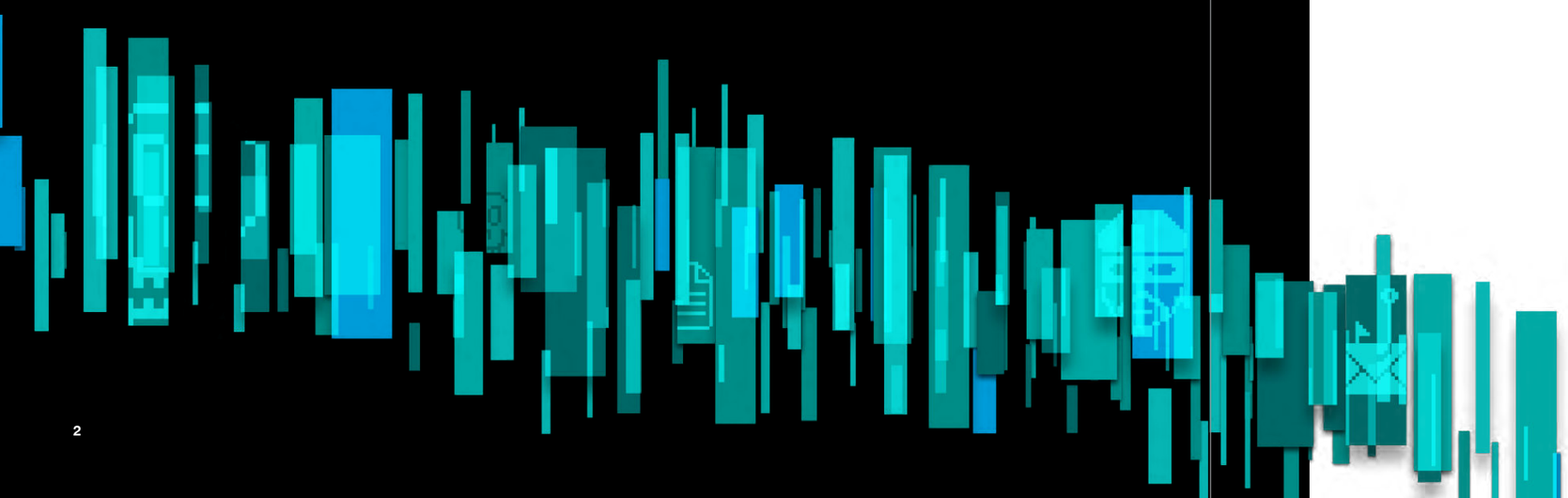
2022: Los ciberdelincuentes se vuelven incluso más creativos

Cada año, los ciberdelincuentes buscan nuevas formas de engañar a las víctimas y eludir las defensas. Y 2022 no ha sido diferente. Las empresas desplegaron nuevos controles de seguridad y los ciberdelincuentes no tardaron en responder.

Incorporaron técnicas complejas como ataques telefónicos y para eludir la autenticación multifactor (MFA). El desconocimiento de estas técnicas por parte de la mayoría de los usuarios permitió a los ciberdelincuentes tomar la delantera, Y el aumento de la sofisticación de los ciberdelincuentes trajo de cabeza tanto a los CISO como a los equipos de seguridad de la información.

En su novena edición, nuestro informe anual *State of the Phish* analiza la concienciación en seguridad, la resiliencia y el riesgo asociado a los usuarios mediante los datos de una encuesta realizada en 15 países. El informe compara el conocimiento de ciberataques y tácticas defensivas comunes. A partir de ahí, examina cómo las lagunas de conocimientos y la ciberhigiene afectan directamente al panorama de ataques reales. La mayoría de los ataques se dirigen contra las personas antes de hacerlo contra los sistemas. Por eso la última sección de este informe analiza las prácticas de formación en materia de seguridad y describe las oportunidades para instaurar y mantener una cultura de concienciación en seguridad en todos los niveles.

Junto con el informe principal de este año, hemos elaborado resúmenes regionales detallados para analizar cómo los matices locales afectan a las lagunas en la concienciación. Este resumen regional incluye datos por país de **Alemania, Emiratos Árabes Unidos (EAU), España, Francia, Italia, Países Bajos, Reino Unido y Suecia**. Se han extraído datos de entrevistas a 4000 empleados y 650 profesionales de seguridad.



ÍNDICE

Conclusiones principales: A nivel mundial

44 %

de las personas piensan que un mensaje de correo electrónico es seguro si contiene elementos de marca familiares

300 - 400 k$

intentos de ataques telefónicos al día, con un pico de 600 000 en agosto de 202

1/3

de los usuarios realizaron alguna acción peligrosa (como hacer clic en enlaces o descargar malware) al enfrentarse a un ataque

76 %

aumento de las pérdidas económicas directas por ataques de phishing

30 millones

fueron los mensajes maliciosos enviados sobre productos de Microsoft o con su marca

> 1 de cada 10

amenazas fueron bloqueadas tras la denuncia de los usuarios

Siguen sin comprenderse incluso algunos conceptos básicos

SOLO 35 %

de las organizaciones realizan simulaciones de phishing

64 %

de las organizaciones infectadas con ransomware han pagado un rescate

90 %

las organizaciones afectadas por el ransomware tenían una póliza de ciberseguro

65 %

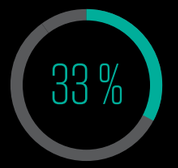
de las organizaciones denunciaron al menos un incidente de pérdida de datos de origen interno

SOLO 56 %

de las organizaciones con un programa de concienciación en seguridad forman a todos sus empleados

de los profesionales de seguridad consideran la seguridad una prioridad en su empresa

VS.



de los empleados afirman que la ciberseguridad no es una de sus principales prioridades en el trabajo

94 %

de las organizaciones suecas eran propensas a sufrir un ataque de phishing

pero...

Solo el 18 %

de las organizaciones suecas forman a los usuarios identificados como objetivos frecuentes

Datos destacados de Europa y Oriente Medio

Observamos importantes variaciones entre los 15 países entrevistados para el informe *State of the Phish*, como cabría esperar cuando se tienen distintos idiomas, culturas y niveles de madurez. Y esto también se hace patente entre los ocho países de este resumen.

De todas las regiones entrevistadas, Europa, Oriente Medio y África (EMEA) es sin duda la región más diversa. Abarca los hemisferios norte y sur, y se trata de un territorio geográfico inmenso que engloba culturas, visiones políticas y economías muy diferentes. Como ocurrió en 2022 en muchos otros lugares, los países de la región EMEA experimentaron cambios geopolíticos y un aumento de la conflictividad. No sorprende que esto se vea reflejado en el panorama de ciberseguridad.

Las organizaciones suecas eran las que más probabilidades tenían de sufrir un ataque de phishing que consiguiera su objetivo comparado con el resto de países, con un 94 %. Por supuesto, los valores atípicos podían ser resultado de varios factores. Una posible explicación es el bajo nivel de formación para concienciar en materia de seguridad del país: solo el 18 % de las organizaciones suecas forman a los usuarios identificados como objetivos frecuentes. También puede que haya mayores tasas de denuncia. Suecia ha sido pionero en el terreno de la seguridad de los datos desde 1970, y aprobó una de las primeras leyes relacionadas con la privacidad digital en Europa. Por lo tanto, puede estar culturalmente más aceptada la admisión de brechas de seguridad, lo que genera denuncias más precisas.

Este año hemos analizado Italia por primera vez, y los resultados fueron sorprendentes. De los 15 países, las organizaciones italianas eran las que menos probabilidades tenían de ser víctimas de muchos tipos de amenazas. Solo el 47 % perdieron datos o propiedad intelectual a través de un ataque externo (frente al 69 % de la media global). En comparación con otros países de este informe, las organizaciones italianas eran las que menos probabilidades tenían de sufrir ataques de phishing que consiguieran su objetivo (79 %). Estos resultados pueden indicar una desconexión o falta de madurez en torno a las normativas de notificación de incidentes de seguridad. También podría reflejar una cultura en la que no prima la transparencia y la apertura de la información.

Si examinamos otras categorías de ciberataques, observamos que los ataques BEC se propagan rápidamente. Países Bajos y Suecia empatan con la tasa más alta de ataques (92 %), frente al 75 % de la media global. Los incidentes aumentaron más rápidamente en Alemania y en España, con una subida interanual del 16,5 %. Un factor importante en el aumento de los ataques BEC podría ser la evolución del idioma utilizado. Históricamente, los mensajes de correo electrónico de los ataques BEC se escribían principalmente en inglés. Recientemente, sin embargo, hemos observado un aumento de ataques BEC en alemán, español, esloveno y otros idiomas. Esto coincide con la creciente sofisticación de los ataques observada de manera general.

Países Bajos tiene el dudoso honor de ser el país más afectado por los ciberataques, tanto por atacantes internos (86 % respecto al 66 % de la media mundial) como externos (84 % frente al 68 %). Sin embargo, la formación también parece ser eficaz. Los empleados holandeses son los menos propensos a dar información personal o contraseñas.

DOMINIO DE LA TERMINOLOGÍA:

Siguen sin comprenderse incluso algunos conceptos básicos: más de un tercio de los usuarios son incapaces de definir "malware", "phishing" y "ransomware"

40 %

de los usuarios saben lo que es el ransomware, un aumento de 9 puntos respecto a 2019; el mayor incremento de los términos sobre los que preguntamos

29 % y 30 %

de los usuarios conocían términos relativamente nuevos como el smishing y el vishing, respectivamente

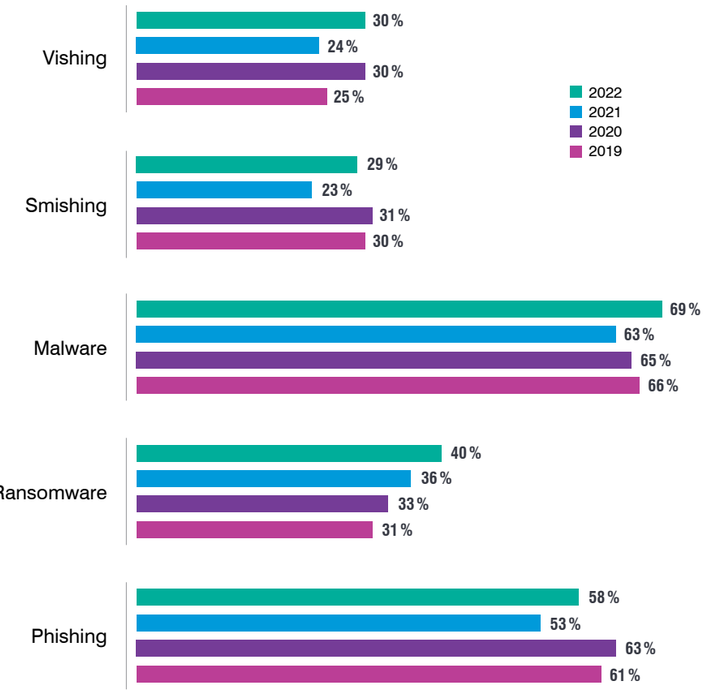
58 %

de los usuarios sabían lo que era el phishing, un aumento de 5 puntos respecto al año pasado, pero 3 puntos por debajo de 2019

Concienciación en seguridad: perspectivas y oportunidades

En los 15 países a nivel mundial, aparece un patrón similar al ponderar el conocimiento de los usuarios sobre términos de seguridad básicos. Amenazas comunes como el phishing ,el ransomware y el malware llevan años entre nosotros, pero los usuarios todavía no tienen un conocimiento claro de lo que son. Y hay incluso menos concienciación sobre amenazas más recientes como el smishihg (phishing por SMS) y el vishing (phishing de voz). Desafortunadamente, nuestros datos muestran pocos cambios año tras año.

El conocimiento de los usuarios muestra pocos cambios año tras año



EL PRINCIPIO DE INCERTIDUMBRE:

69 %

los usuarios de Países Bajos sabían lo que es el phishing, el mayor porcentaje entre los 8 países analizados en esta región

45 %

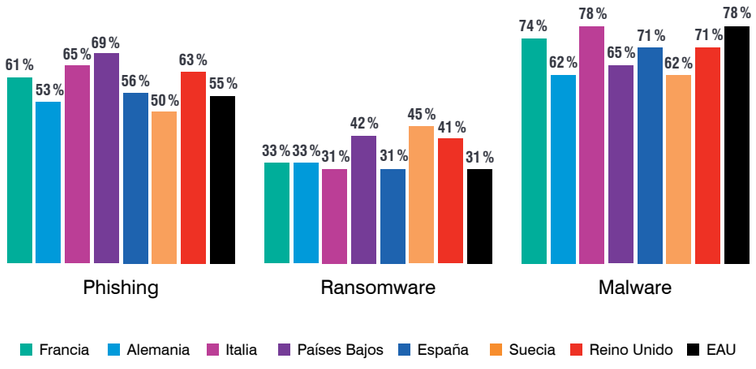
de los suecos conocían el concepto de ransomware, un porcentaje que supera a los otros 7 países

78 %

los usuarios de Italia y de Emiratos Árabes Unidos sabían lo que es el malware, las mayores tasas de conocimiento de los 8 países de esta región

Al comparar el conocimiento de los usuarios sobre las tres amenazas más comunes, surgen varias diferencias notables Los participantes suecos y alemanes fueron los menos capaces de definir "malware" o "phishing". En cambio, los de Emiratos Árabes Unidos e Italia fueron los más capaces de definir "malware", pero se situaron por debajo de la media en el caso del "ransomware".

Conocimiento de amenazas comunes (precisión)



Estas diferencias podrían explicarse por el hecho de que menos del 50 % de las organizaciones europeas y de Oriente Medio forman a sus empleados sobre estos temas. Las medias regionales fueron del 37 % en el caso del phishing, del 34 % para el ransomware, el 40 % para el malware y el 27 % para los ataques BEC.

FORMACIÓN POR TEMAS:

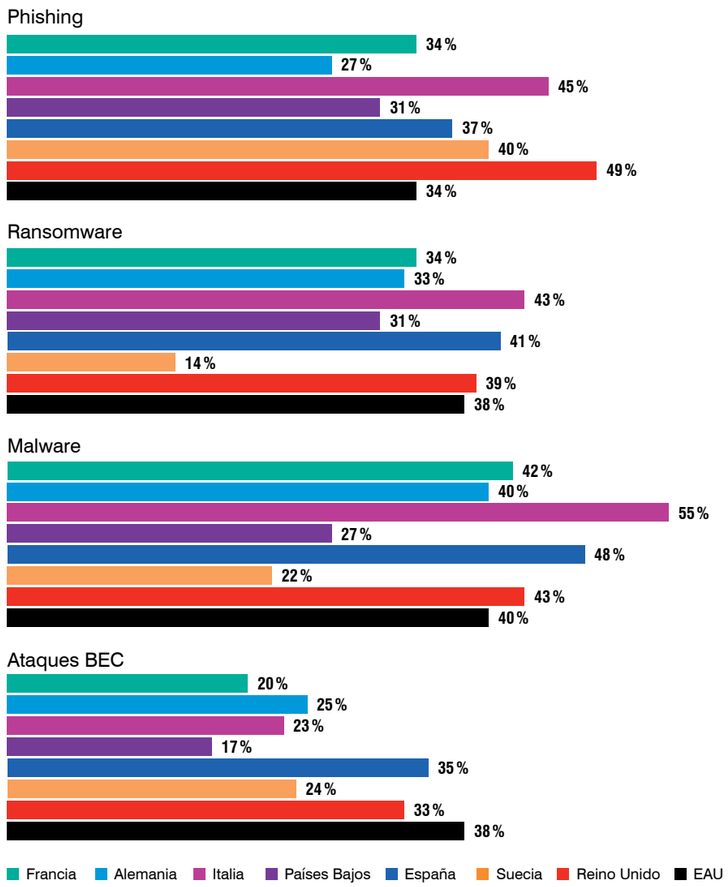
55 %

de las organizaciones italianas forman a los usuarios sobre el malware, el porcentaje más alto de cualquiera de los temas de los países de la región

14 %

de las organizaciones suecas forman a los usuarios sobre el ransomware, el porcentaje más bajo de cualquiera de los temas de los países de la región

Cobertura de temas de amenazas en programas de formación para concienciar en materia de seguridad



Aunque la mayoría de las organizaciones cuentan con un programa de concienciación en materia de seguridad, no todos los empleados reciben formación. Un dato destacado fue el de las organizaciones de Emiratos Árabes Unidos: el 64 % forman a todos los empleados y el 52 % solo a los usuarios identificados como objetivos frecuentes. Además, el 74 % de las organizaciones de EAU forman a sus empleados en temas de seguridad que afectan específicamente a su organización, un porcentaje superior al de los otros 14 países.

CONCIENCIACIÓN PARA TODOS:

64 %

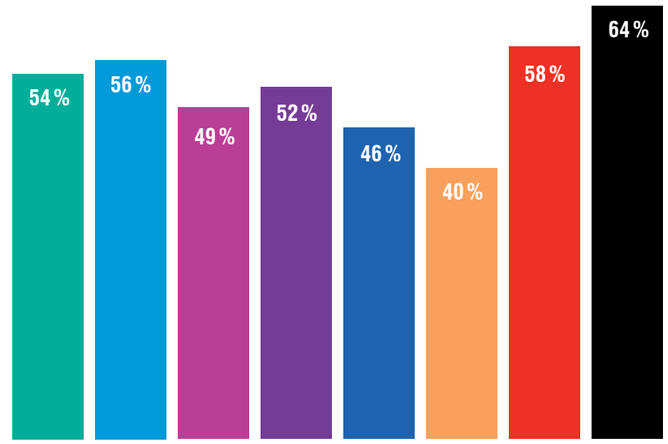
de los empleadores de EAU formaban a todos los empleados de sus organizaciones, el porcentaje más alto de los países entrevistados en Europa y Oriente Medio

40 %

de las organizaciones suecas hicieron lo mismo, el porcentaje más bajo de los países analizados en esta región

Los CISO del Reino Unido parecen estar haciendo bien su trabajo a la hora situar la seguridad como una prioridad en sus organizaciones. Los empleados de Reino Unido fueron los más propensos a expresar confianza en su equipo de TI, así como a afirmar que en su organización la ciberseguridad era una prioridad. Esta opinión puede deberse a la formación recibida; las organizaciones de Reino Unido, junto con las de EAU tienen las mayores tasas de formación para los usuarios identificados como objetivos frecuentes (52 %).

Porcentaje de organizaciones que formaban a todos los empleados en sus programas de concienciación en materia de seguridad



Los ataques simulados de phishing se utilizaron con más frecuencia en España (véanse los gráficos de la página siguiente), con un 48 %. Y el Reino Unido destacó por dar mucha importancia al toque personal, con un 45 % de formación presencial. Dentro de la región, las organizaciones de Reino Unido fueron las más propensas a cubrir el phishing (49 %), pero considerablemente menos propensas que España a utilizar simulaciones de phishing (39 %).

TIPOS DE FORMACIÓN

45 %

de las organizaciones de Reino Unido ofrecían formación presencial, la tasa más alta de los países de Europa y Oriente Medio analizados

50 y 48 %

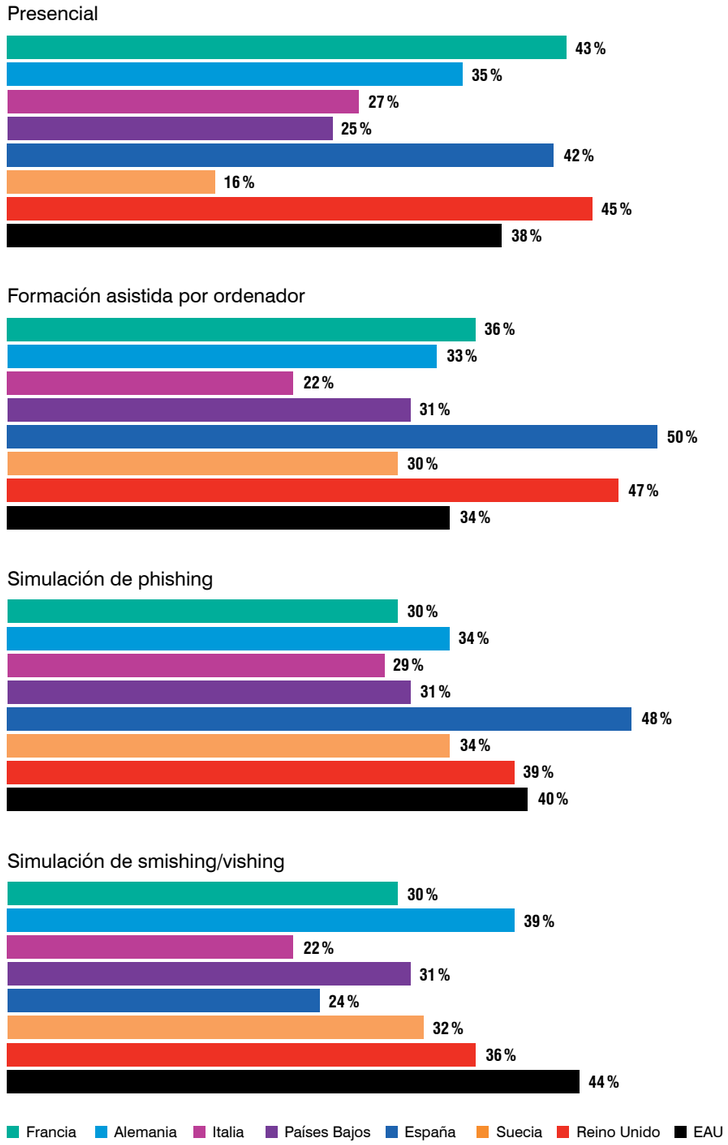
de las empresas españolas ofrecían formación asistida por ordenador y realizaban ataques simulados de phishing, respectivamente, lo que lo convierte en el país más destacado de la región

44 %

de las organizaciones de EAU ejecutaban simulaciones de smishing y vishing, el porcentaje más alto de la región

Los datos de formación de Suecia destacaron porque sugieren que las organizaciones pueden no tomarse suficientemente en serio la seguridad. Muy pocas organizaciones imparten formación presencial (16 %). También son las menos propensas a formar a todos los empleados (40 %) Esto resulta sorprendente si tenemos en cuenta que las infecciones de ransomware son mayores en Suecia que en cualquier otro país analizado en este informe (82 %).

Soportes de formación



AMENAZAS INTERNAS:

71 %

de las organizaciones de la región EMEA perdieron datos por incidentes de origen interno

54 %

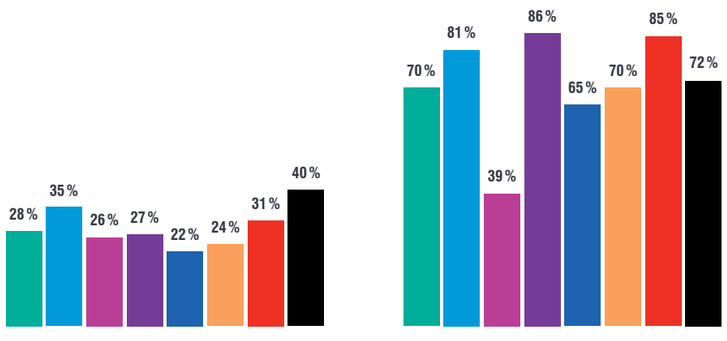
sufrieron tres o más ataques

Concienciación en seguridad: amenazas internas

Este año, hemos ampliado nuestro estudio para reflejar la creciente influencia de las amenazas internas, una categoría que abarca desde el robo de datos malicioso a la pérdida de datos negligente y el robo de credenciales.

De media, el 71 % de las organizaciones de esta región perdieron datos por incidentes de origen interno. Destaca principalmente la desconexión entre el alto nivel de ataques y el bajo nivel medio de formación para concienciar en materia de seguridad, con un 29 %.

Riesgo de pérdida de datos asociado a amenazas internas



Las organizaciones alemanas eran las más propensas a sufrir ataques internos frecuentes (18 %), y los empleados de este país los más proclives a llevarse información de la empresa al salir de la empresa. Esto se debe a que los empleados alemanes piensan que esa información les pertenece; solo el 35 % de las organizaciones alemanas forman a sus empleados sobre las amenazas internas. En las organizaciones de EAU en cambio, experimentan solamente un 4 % de ataques internos frecuentes, aunque la tasa de formación que ofrecen a sus empleados es del 40 %. Esto se debe a que los empleados de EAU son los que presentan las tasas más elevadas de la región (29 %) en lo que se refiere a empleados que entregan información personal o contraseñas de cuentas a personas que no son de confianza.

VACACIONES EN ROMA:

las organizaciones italianas eran menos propensas que otras de los países analizados de la región a sufrir ataques dirigidos en una amplia variedad de categorías.

79 %

sufrieron ataques de phishing

51 %

sufrieron ataques BEC

63 %

sufrieron ataques de ransomware (solo en EAU la tasa fue interior)

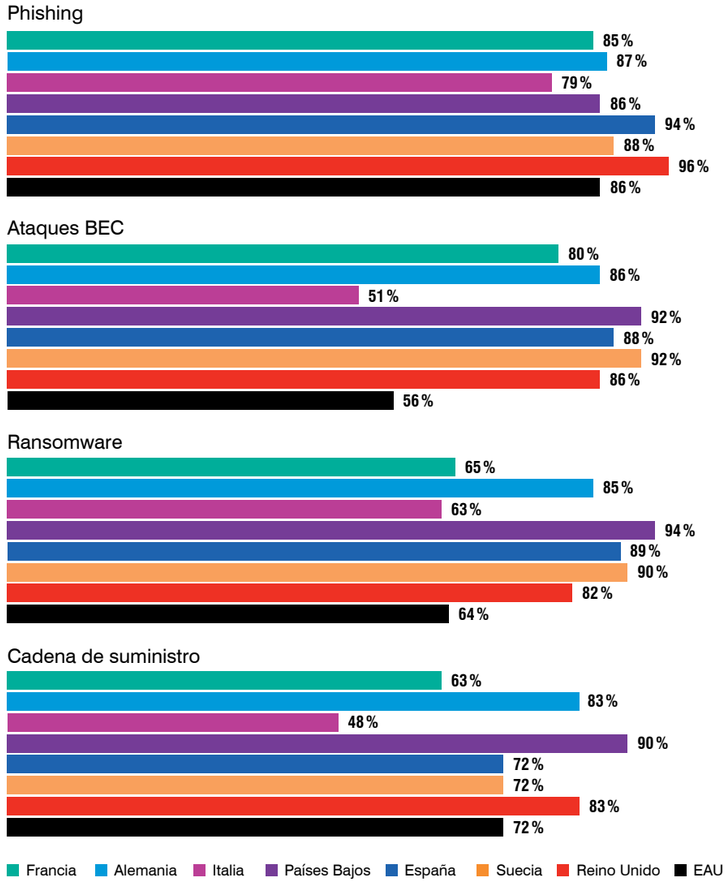
48 %

sufrieron ataques a la cadena de suministro

Tendencias del panorama de amenazas

En general, Francia destacó por situarse sistemáticamente en la mediana de toda la región en cuanto a víctimas de ataques dirigidos. Sospechamos que esto refleja la madurez en ciberseguridad del país.

Porcentaje de organizaciones afectadas por ataques dirigidos



PAGAR O NO PAGAR:

27 %

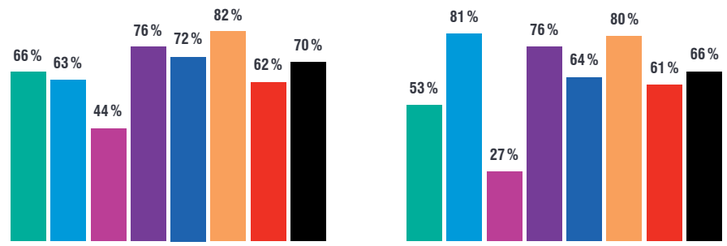
de las organizaciones italianas infectadas por ransomware pagaron el rescate solicitado por los ciberdelincuentes, el porcentaje más bajo de los países de este informe. Las organizaciones italianas también fueron las más propensas a sufrir una infección en primer lugar (44 %) y las que tenían más probabilidades de recibir un reembolso de su aseguradora (56 %).

Ransomware: los seguros echan una mano

El ransomware es un ataque habitual que se produce tras un compromiso inicial. Cinco países de la región EMEA mostraron altas probabilidades de infección de ransomware.

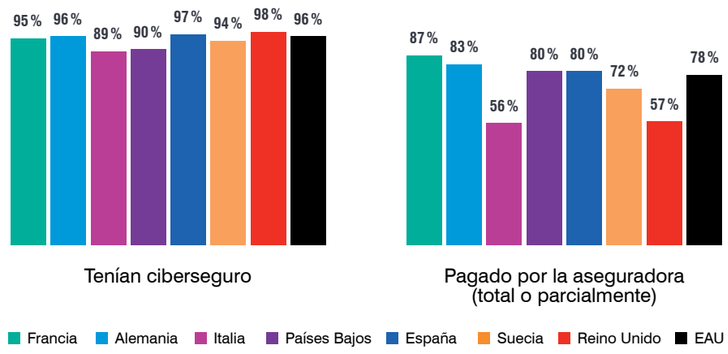
De todos los países analizados en este informe, Suecia era el que menos probabilidades tenía de sufrir una infección con ransomware (82 %). Como uno de los países mejor conectados del mundo, Suecia se encuentra a la vanguardia de la digitalización, tanto en el sector público como en el privado. Es posible que durante la pandemia muchas organizaciones no prestaran tanta atención a la protección frente a los ciberataques.

Infecciones de ransomware y pagos



Mientras que las organizaciones alemanas fueron las más propensas a pagar (81 % frente al 64 % de media global), las del Reino Unido obtuvieron peores resultados generales respecto a los otros 14 países. No solo no consiguieron recuperar el acceso a los datos tras el pago (33 % frente al 52 %), sino que las reclamaciones de ciberseguros fueron denegadas con mayor frecuencia (23 % frente al 7 %).

Infecciones de ransomware y pagos



Recomendaciones

Con tantas variaciones entre mercados y empresas, lo ideal es un programa de seguridad individual adaptado a las amenazas reales y los riesgos asociados a los usuarios. Pero si todavía no dispone de uno, el informe State of the Phish de este año sugiere algunas estrategias útiles.

Reduzca la complejidad haciendo las preguntas adecuadas.

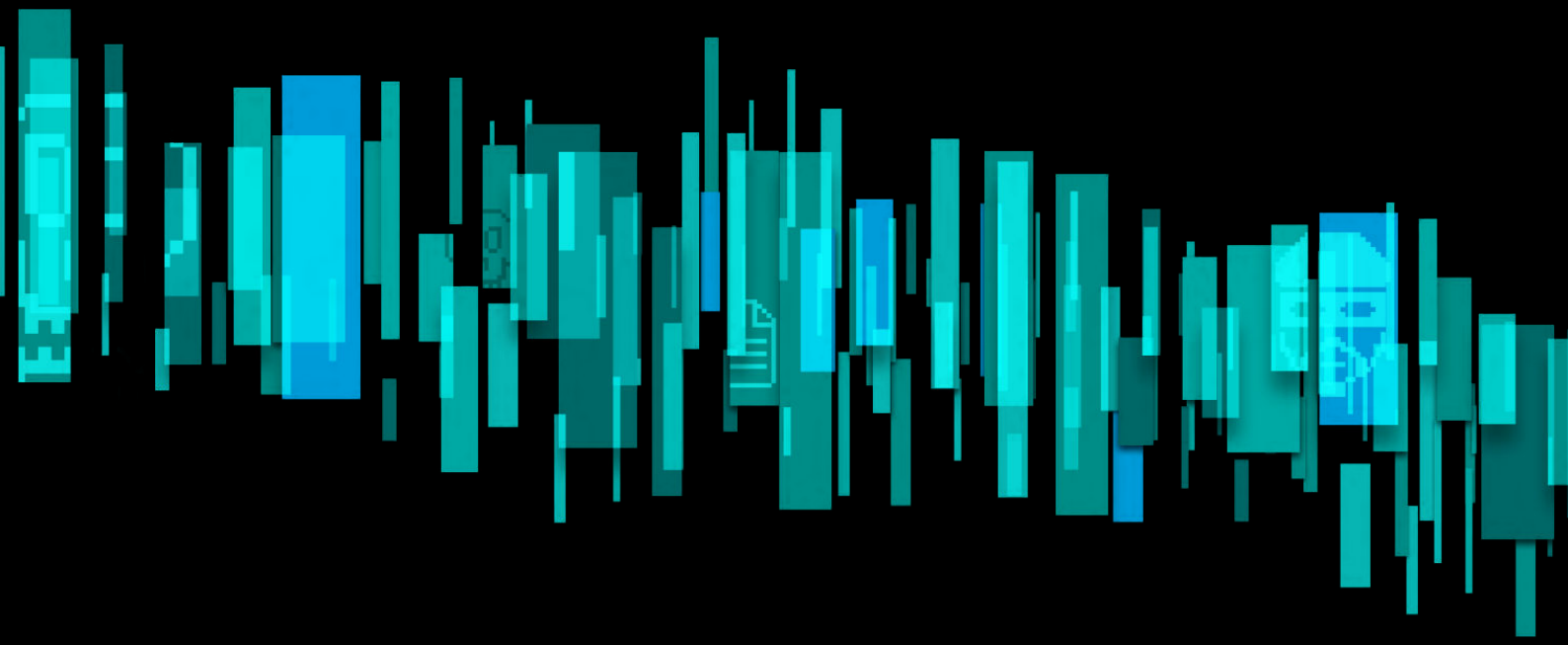
- ¿Quién es objetivo dentro mi organización?
- ¿Dónde se encuentran las lagunas de las defensas actuales?
- ¿Cuáles son mis prioridades para mitigar el riesgo humano?

Combine inteligencia de amenazas con formación para concienciar en materia de seguridad en toda la organización.

- Identifique qué usuarios son más vulnerables a ataques y quién son más propensos a morder el anzuelo.
- Adapte el contenido de la formación a las amenazas en circulación.
- Forme a sus empleados para que reconozcan el phishing utilizando los señuelos que se utilizan contra ellos.

Instaure una cultura de seguridad que vaya más allá de la formación.

- La formación es fundamental pero no suficiente.
- Una sólida cultura de seguridad en el lugar de trabajo animará a los usuarios a tomarse la seguridad de la información más en serio en su vida personal.
- Mida los indicadores que importan y responda con medidas apropiadas y justas.



MÁS INFORMACIÓN

Para obtener más información sobre cómo le ayuda Proofpoint a conocer sus riesgos asociados a los usuarios, y a mitigarlos con una estrategia de ciberseguridad centrada en las personas, visite **proofpoint.com/es**.

ACERCA DE PROOFPOINT

Proofpoint, Inc. es una compañía líder en ciberseguridad y cumplimiento de normativas que protege el activo más importante y de mayor riesgo para las organizaciones: las personas. Gracias a una suite integrada de soluciones basadas en cloud, Proofpoint ayuda a empresas de todo el mundo a detener las amenazas dirigidas, a salvaguardar sus datos y a hacer a los usuarios más resilientes frente a ciberataques. Compañías líderes de todos los tamaños, entre las que se encuentra el 75 % del Fortune 100, confían en las soluciones de Proofpoint para su seguridad centrada en personas y su cumplimiento regulatorio, mitigando los riesgos más críticos en sus sistemas de correo electrónico, cloud, redes sociales y web. Encontrará más información en **www.proofpoint.com/es**.

proofpoint.

0400-013-06-01