proofpoint.

State of The Phish: de un vistazo

INTRODUCCIÓN

La ciberseguridad puede ser complicada en tiempos normales. Pero en tiempos "no tan normales" (como una pandemia global que obliga a cambios drásticos en los entornos laborales) puede resultar una tarea realmente abrumadora. En el último año, los profesionales de seguridad de la información han tenido que enfrentarse a un aluvión de timos de phishing sobre temas relacionados con el coronavirus, así como a un fuerte incremento de los ataques de ransomware. Al mismo tiempo, han tenido que hacer un esfuerzo importante para garantizar la seguridad de los usuarios en medio de una repentina adopción del teletrabajo.

Nuestro informe *State of the Phish* de 2021 explora las grandes tendencias actuales y sus efectos a través del análisis de ejercicios de phishing simulado, entrevistas y ciberataques reales. Repasa, además las mayores vulnerabilidades asociadas a los usuarios. Y más importante aún, ofrece información detallada sobre las medidas que se pueden adoptar para resolverlas.

A continuación ofrecemos un resumen de los principales hallazgos de este año.

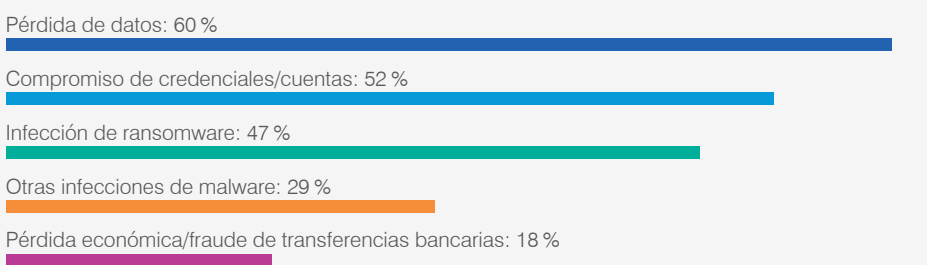
LAS AMENAZAS SIGUEN CRECIENDO

2020 fue un año excepcional para los ataques de phishing, que afectaron a las víctimas de una gran cantidad de maneras.

El **57 %**

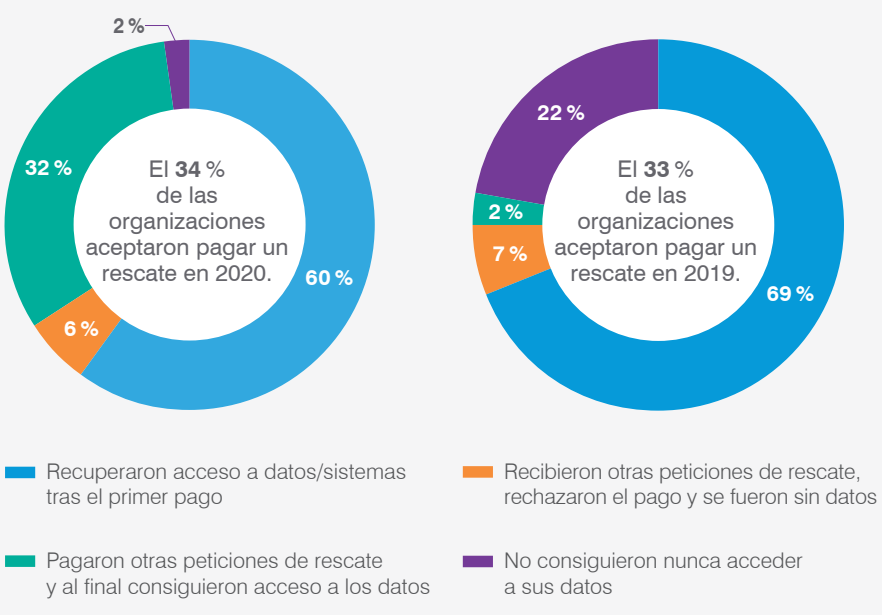
de los participantes en una encuesta independiente afirmaron que su organización había sufrido un ataque de phishing en 2020, lo que supone un aumento respecto al **55 %** de 2019

Impacto de los ataques de phishing



Un porcentaje ligeramente superior de víctimas de ransomware pagaron a los ciberdelincuentes para recuperar acceso a sus datos y sistemas. Pero muy pocos consiguieron lo que se les había prometido, y casi un tercio terminó pagando una cantidad adicional por el rescate.

Resultados tras los pagos del rescate (2020 vs. 2019)



INTERNACIONAL

El **68 %** de las organizaciones de EE. UU. afirmaron haber pagado un rescate en 2020; esto supone el doble de la media mundial.

El **41 %** de las organizaciones españolas rechazaron pagar un rescate tras sufrir una infección, siendo las menos propensas a negociar con los ciberdelincuentes.

El **78 %** de las organizaciones francesas pudieron recuperar el acceso a sus datos y sistemas tras pagar un solo rescate, el porcentaje más alto de todas las regiones estudiadas (EE. UU. se situó en segundo lugar con un **76 %**)

El **14 %** de las organizaciones alemanas rechazaron pagar un segundo rescate, el mayor porcentaje de las regiones estudiadas

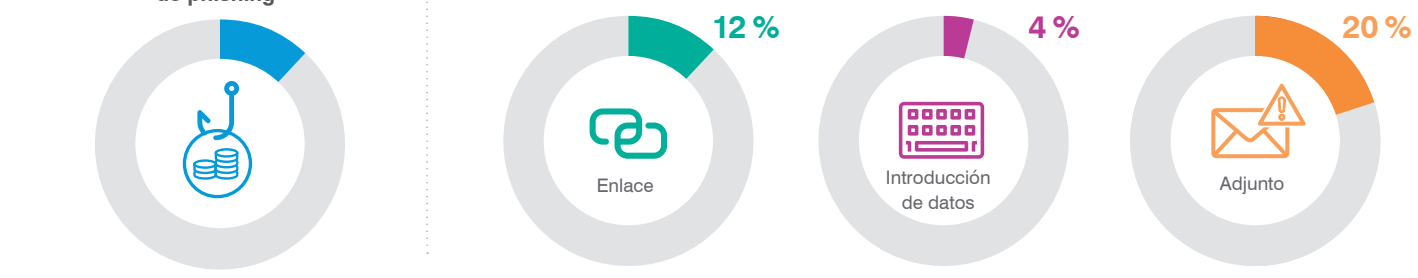
DÓNDE SON MÁS VULNERABLES LOS USUARIOS

El objetivo de los ciberataques actuales no es la tecnología; son las personas. Saber cuál es el punto débil de los usuarios es una parte fundamental para su preparación para una mayor resiliencia.

Más de 1 de cada 10 usuarios hizo clic en un mensaje de correo electrónico de phishing simulado. En el caso de pruebas de phishing con adjuntos, esa cifra fue de 1 de cada 5.

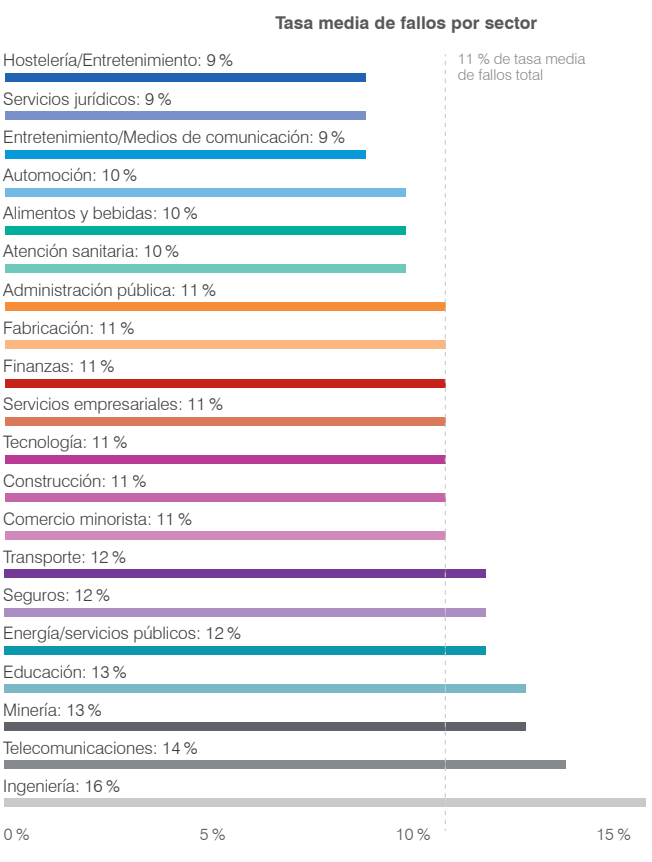
Un 11 % de tasa media de fallos en pruebas de phishing

Tipos de plantillas de phishing: tasas medias de fallos

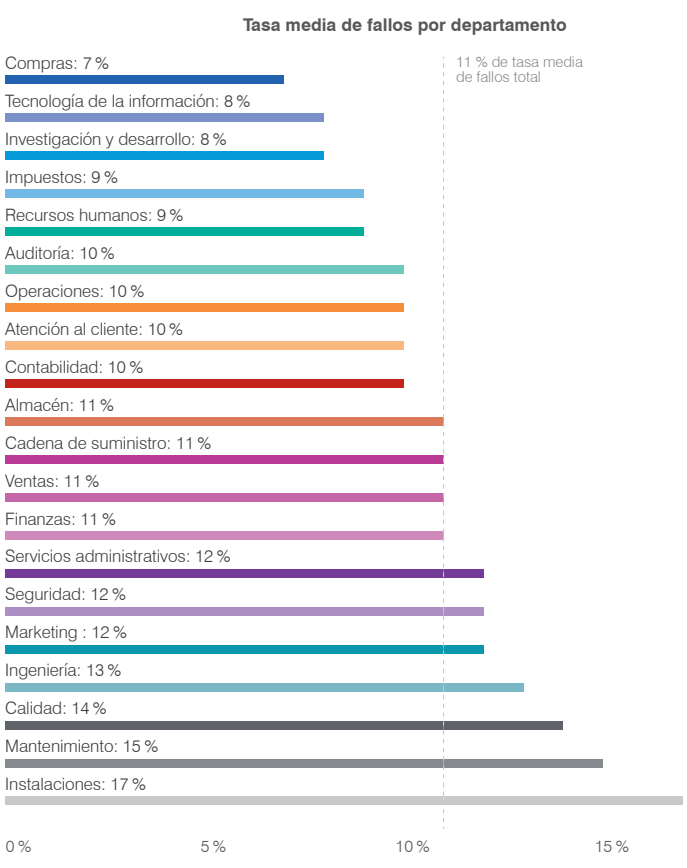


Los usuarios de algunos sectores son más vulnerables que otros. Lo mismo ocurre con los usuarios de distintos departamentos.

Tasa media de fallos por sector



Tasa media de fallos por departamento



Los líderes de TI están absolutamente familiarizados con los términos de ciberseguridad más habituales, pero muchos usuarios los desconocen por completo.

Nuestra encuesta pedía a los usuarios que definieran términos de ciberseguridad clave, ofreciendo tres respuestas con varias opciones y una opción "No lo sé". Los usuarios que desconocen la respuesta pueden plantear tanto riesgo como los que contestan incorrectamente.

¿Qué es el **PHISHING?**

Correcto **63 %** | Incorrecto **22 %** | No lo sé **15 %**

Los trabajadores de EE. UU. consiguieron la peor puntuación (52 %)

Los trabajadores de Reino Unido consiguieron la mejor puntuación (69 %)

¿Qué es el **RANSOMWARE?**

Correcto **33 %** | Incorrecto **36 %** | No lo sé **31 %**

Solo el 26 % de los trabajadores alemanes respondieron correctamente.

El 42 % de los trabajadores australianos respondieron correctamente

¿Qué es el **MALWARE?**

Correcto **65 %** | Incorrecto **21 %** | No lo sé **14 %**

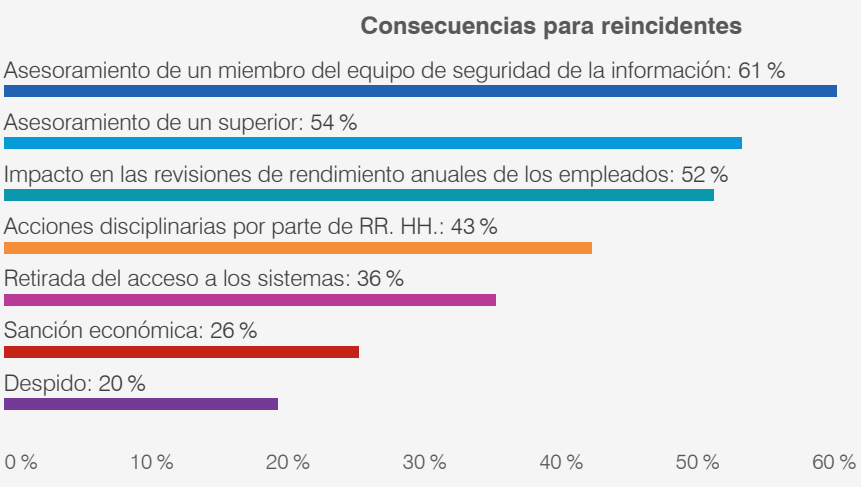
Los trabajadores españoles consiguieron la mejor puntuación (75 %)

Los trabajadores de EE. UU. consiguieron la peor puntuación (54 %)

CÓMO ESTÁN RESPONDIENDO LAS ORGANIZACIONES

Aunque no recomendamos castigar a los usuarios por errores de buena fe, algunas organizaciones aplican un modelo de consecuencias a los "usuarios reincidentes".

Consecuencias para reincidentes



INTERNACIONAL

El **82 %** de las organizaciones de EE. UU. utilizan un modelo de consecuencias, el porcentaje más alto de las regiones estudiadas

El **72 %** de las organizaciones australianas involucraron al departamento de RR. HH. para castigar a los reincidentes

El **35 %** de las organizaciones españolas utilizan un modelo de consecuencias, el porcentaje más bajo de las regiones estudiadas

El **32 %** de las organizaciones de Reino Unido afirmaron que su modelo de consecuencias no ha modificado la concienciación de los empleados

El **30 %** de las organizaciones de EE. UU. incluyeron el despido como consecuencia, el porcentaje más alto de las regiones estudiadas

OBTENGA EL INFORME COMPLETO

¿Quiere más detalles? El informe *State of the Phish* 2021 incluye datos de:

Una entrevista independiente de	Un estudio independiente de	Más de	Casi
3500	**600**	**60 M**	**15 M**
trabajadores en activo en los siete países (Australia, Francia, Alemania, Japón, España, Reino Unido y Estados Unidos).	profesionales de seguridad de TI en los mismos siete países	ataques de phishing simulados enviados por nuestros clientes en un período de 12 meses	de mensajes denunciados por los usuarios de nuestros clientes

Consiga el informe para tener una imagen detallada de las amenazas de phishing actuales y de las medidas a tomar para desarrollar una estrategia de ciberseguridad centrada en las personas que contribuya a mejorar la concienciación de los usuarios, reducir los riesgos y hacer más resilientes a sus empleados.

www.proofpoint.com/es/resources/threat-reports/state-of-phish

proofpoint.