Los 5 correos electrónicos de phishing que más atraen a los empleados

El **91%** de todos los ataques cibernéticos comienzan con un correo electrónico de phishing y las técnicas de phishing están involucradas en el **32%** de las violaciones de datos exitosas, según estimaciones de Deloitte.

Se realizó un estudio sobre recopilación de un simulador de phishing, proporcionado voluntariamente por **29,597** empleados de 100 países.

¿En qué consistió el análisis?

De acuerdo con información de especialistas, es una herramienta que ayuda a las organizaciones a verificar si su personal puede distinguir un correo electrónico de phishing de uno real sin poner en riesgo los datos corporativos. Un administrador elige del conjunto de plantillas, imitando escenarios comunes de phishing, o crea una plantilla personalizada, luego la envía al grupo de empleados sin advertirles previamente y realiza un seguimiento de los resultados.

El hecho de que una gran cantidad de usuarios haga clic en el enlace, es una clara indicación de que se requiere capacitación adicional en concientización sobre seguridad cibernética. Según campañas recientes de simulación de phishing efectuados por esta empresa, los cinco tipos de correo electrónico de phishing más eficaces son:

- Asunto: Intento de entrega fallido: lamentablemente, nuestro mensajero no pudo entregar su artículo. Remitente: Servicio de entrega de correo. Conversión de clics: 18.5%.

- Asunto: No se entregaron los correos electrónicos debido a servidores de correo sobrecargados. Remitente: El equipo de asistencia de Google. Conversión de clics: 18%.

- Asunto: Encuesta en línea a empleados: ¿Qué mejorarías del trabajo en la empresa? Remitente: Departamento de RRHH. Conversión de clics: 18%.

- Asunto: Recordatorio: Nuevo código de vestimenta en toda la empresa. Remitente: Recursos Humanos. Conversión de clics: 17.5%.

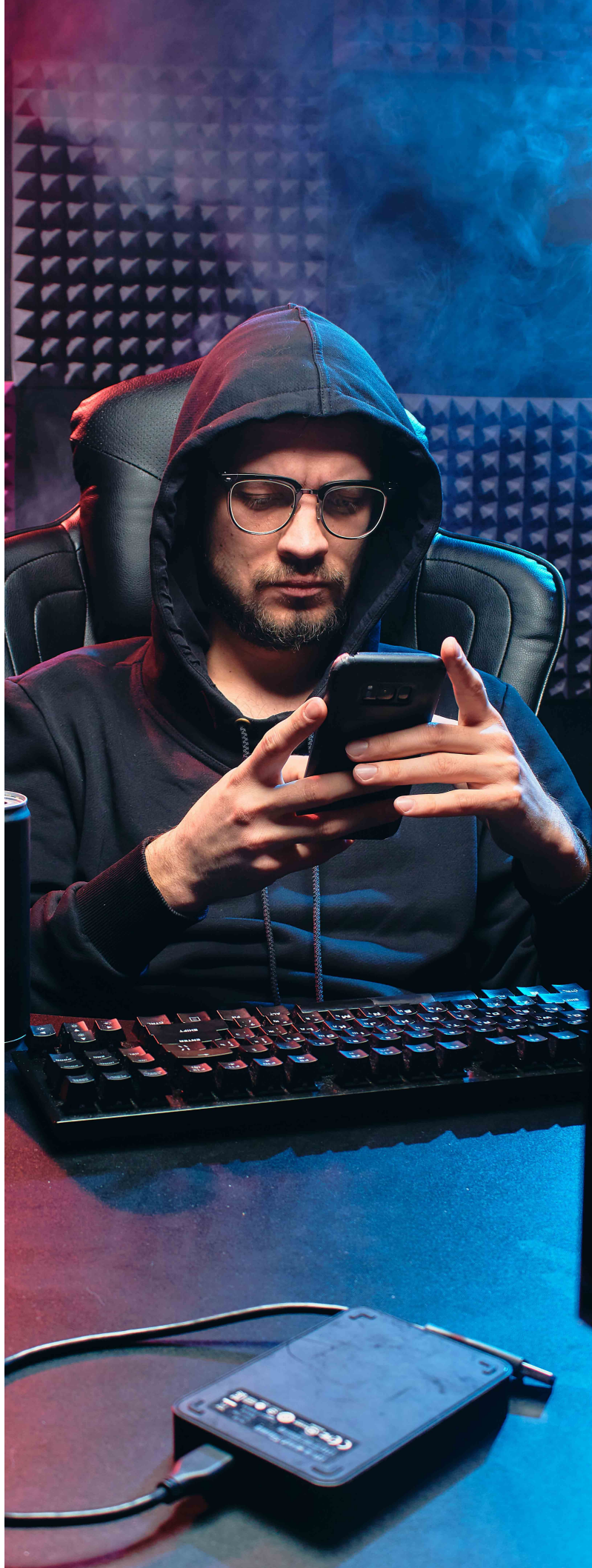
- Asunto: Atención a todos los empleados: nuevo plan de evacuación del edificio. Remitente: Departamento de Seguridad. Conversión de clics: 16%.

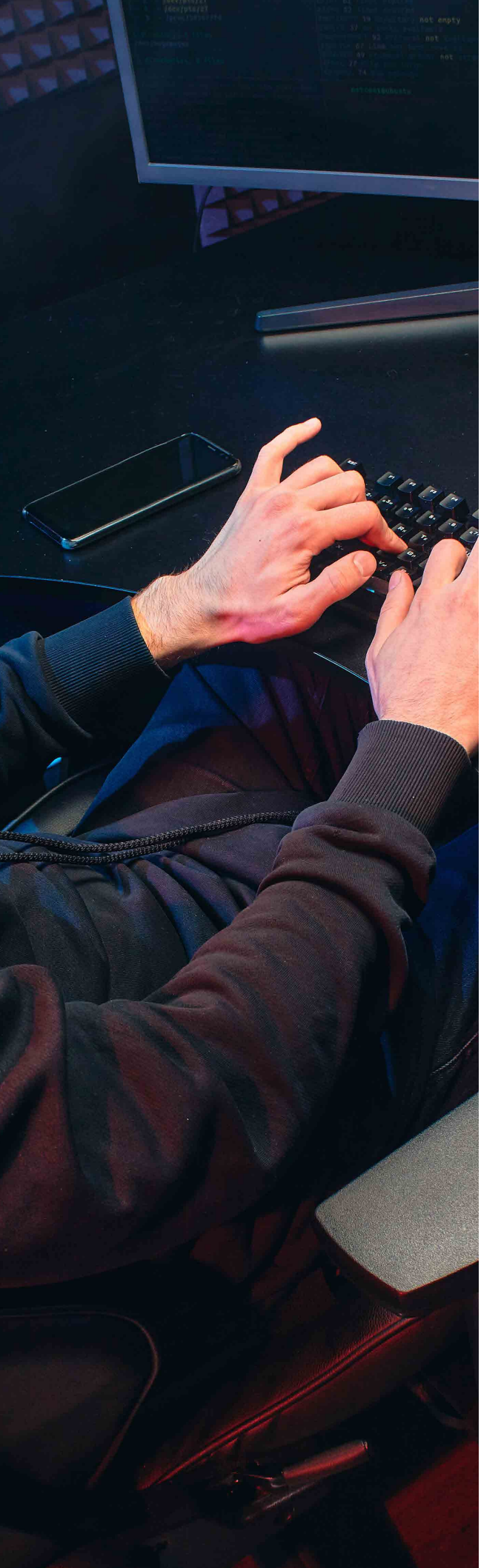
Entre los otros correos electrónicos de phishing que obtuvieron una cantidad considerable de clics se encuentran: confirmación de reservaciones de un servicio para ese fin **(11%)**, una notificación sobre la realización de un pedido **(11%)** y un anuncio de concurso de IKEA **(10%).**

Por otro lado, los correos electrónicos que amenazan al destinatario u ofrecen beneficios instantáneos parecen ser menos "exitosos". Una plantilla cuyo asunto era "Le pirateé su computadora y conozco su historial de búsqueda" obtuvo el **2%** de los clics, mientras que las ofertas de Netflix gratis y **1,000** dólares con sólo hacer clic en un enlace engañaron únicamente al 1% de los empleados.

"Dado que los métodos utilizados por los ciberdelincuentes cambian constantemente, la simulación debe reflejar las tendencias actualizadas de ingeniería social, junto con los escenarios comunes de ciberdelincuencia. Es crucial que los ataques simulados se lleven a cabo regularmente y se complementen con la capacitación adecuada, de modo que los usuarios desarrollen una fuerte habilidad de vigilancia que les permita evitar caer en ataques dirigidos o el llamado **spear-phishing"**, explicó especialista.

.





¿Qué hacer?

Para evitar filtraciones de datos y cualquier pérdida financiera y de reputación relacionadas a un ataque de phishing, se recomienda a las empresas:

• Recuerde a sus empleados las señales básicas de los correos electrónicos de phishing. Un asunto urgente, errores tipográficos y de otro tipo, direcciones irregulares de los remitentes y enlaces sospechosos.

• Si tiene alguna duda sobre el correo electrónico recibido, verifique el formato de los archivos adjuntos antes de abrirlos y la precisión del enlace antes de hacer clic. Esto se puede lograr pasando el cursor sobre estos elementos: asegúrese de que la dirección parezca auténtica y que los archivos adjuntos no estén en un formato ejecutable.

• Denuncie siempre los ataques de phishing. Si detecta un ataque de phishing, informe a su departamento de seguridad de TI y, si es posible, evite abrir el correo electrónico malicioso. Esto permitirá que su equipo de ciberseguridad reconfigure las normas antispam y prevenga un incidente.

• Proporcione a sus empleados conocimientos básicos de ciberseguridad. La educación debe estar orientada a cambiar el comportamiento de los alumnos y enseñarles a enfrentarse a las amenazas.

Puesto que los intentos de phishing pueden confundir y no hay garantía de evitar todos los clics accidentales, proteja sus dispositivos de trabajo con una seguridad en la que pueda confiar. Elija una solución que proporcione funciones antispam, rastree comportamientos sospechosos y cree una copia de seguridad de sus archivos en caso de ataques de ransomware.

Fuente de información: cio.com.mx