S21 SEC

PHISHING

Escenarios de ataque

Durante el primer semestre de 2020, los ataques de *phishing* han sido uno de los **principales riesgos** para empresas y usuarios de internet.

Debido al Coronavirus los phishing se han convertido en uno de los ataques informáticos con más éxito en todo el mundo.

S21 SEC

Mayor facilidad

Para realizar campañas masivas de distribución

+1000

Ataques de *Phishing* al mes

Aumento del 350%

En la creación de dominios maliciosos suplantando a marcas y organizaciones

NUEVAS ESTRATEGIAS EN LOS ATAQUES DE *PHISHING*

Para empresas e instituciones, los *phishing* se convierten en un doble riesgo impactando negativamente en su imagen y actividad.

El 36% de las empresas no tienen claro que sus empleados sean capaces de detectar y evitar un ataque de este tipo.

El 38% de las empresas reconocen haber sido víctimas de este tipo de ataques durante el último año.

Las suplantaciones se realizan de una forma cada vez más profesional, con mayor detalle en la redacción, suplantación de marca o creación de dominios.

PRINCIPALES SECTORES suplantados

Tecnológico

Bancario

Redes sociales

24%

del *mail-phishing*

Está centrado en Microsoft, Outlook y Unicredit

SUPLANTACIONES

de ataques *phishing*

Se realizan mayoritariamente en Google, Amazon, Whatsapp y Facebook

61%

de ataques Web

Involucraron a Google, Amazon y WhatsApp

21:00h

PHISHING móviles

Una nueva realidad

Los ataques *phishing* a móviles han aumentado en un 37% en 2020

La detección de links fraudulentos es más difícil de detectar para los usuarios mediante los mensajes de móvil

Supermercados

Mensajería

Instituciones públicas

Banco

EMPRESAS MÁS SUPLANTADAS

Promoción de descuentos

Confirmación de información personal

Regalos

Reactivación de dispositivos

SEÑUELOS MÁS UTILIZADOS

Email

SMS

Llamadas de voz

Apps mensajería

Apps RRSS

NUEVOS RIESGOS

Usuarios

Empleados

TARGET AMPLIADO

APPS MÁS AFECTADAS

PHISHING en la era de COVID-19

GOOGLE

Confirmó que de los 100 millones de correos electrónicos de *phishing* bloqueados por Gmail, unos 18 millones estaban relacionados con la pandemia.

AMAZON

Se estableció durante los meses de confinamiento como la empresa más suplantada en campañas de *phishing*, dirigidas a usuarios que realizaban sus compras a través de esta plataforma.

OMS

Ha reportado un incremento de este tipo de ataques suplantando su imagen y a trabajadores de la organización para engañar a usuarios y empresas de todo el mundo en diferentes campañas.

CIBERSEGURIDAD

Desde S21sec hemos registrado un aumento de este tipo de ataques desde el inicio de la pandemia, con un 53% de crecimiento.

S21SEC HA OBSERVADO UN CRECIMIENTO EXPONENCIAL EN LA SUPLANTACIÓN DE INSTITUCIONES PÚBLICAS EN CAMPAÑAS DE *PHISHING*

Ciberdelincuentes hacen uso de la imagen de instituciones públicas con fines ilegales.

Operaciones de distribución de código malicioso.

Campañas de robo de credenciales.

- Una de cada tres brechas de seguridad involucró un ataque de *phishing* previo.
- Europa se alza como la primera región del mundo en la recepción de *phishing* o correos electrónicos con contenido malicioso.
- Durante el segundo trimestre de 2020 España, Rusia y Alemania ha recibido el 22,75% del total de ataques con emails peligrosos, archivos adjuntos maliciosos o enlaces a sitios de *phishing*.
- Las campañas de *phishing* y distribución de malware actúan, cada vez, de manera más interrelacionada.

PIENSA ANTES DE DAR CLIC

Nunca abras un adjunto o ingreses en un link de remitentes no identificados.

NO CONFÍES

En promociones, regalos o sorteos. Comprueba siempre las páginas oficiales de las empresas.

VERIFICA LA FUENTE

Especialmente si en el correo se pide confirmación de información personal o financiera.

MANTÉN MEDIDAS

Actualiza tus contraseñas de seguridad periódicamente.

INSTALA SOLUCIONES

De ciberseguridad en tus dispositivos y mantenlas actualizadas.

S21SEC

www.s21sec.com
marketing@s21sec.com