

# 4 ATAQUES MÁS COMUNES A TRAVÉS DEL CORREO ELECTRÓNICO



1

## PHISHING

El **phishing** de correo electrónico es una técnica de ciberataque que tiene por objetivo **intentar robar información comercial confidencial**.

### ¿En qué consiste?

Simulan que provienen de un contacto conocido.

Se enmascaran con emblemas oficiales de la empresa.

Dirigidos a cuentas vulnerables y empleados de nivel inferior.



La mejor protección contra este tipo de ataque es una red de vigilancia que supervise la comunicación dentro y fuera de la empresa.

### ¿En qué consiste?

Falsifican el **encabezado** de un correo electrónico para que parezca que proviene desde dentro de la empresa.

Se intenta confundir a los empleados para que **proporcionen información sensible** o, en algunos casos, gestiones de tipo **bancarias**

2

## SPOOFING

El **spoofing** o correo electrónico falso es una estrategia utilizada durante los ataques de **spam y phishing**.



Si bien la diligencia es el mejor método para hacer frente a los ataques de suplantación de identidad, las empresas también deben buscar un software que mejore la seguridad del correo electrónico.

3

## MALWARE

El **malware**, o software malicioso, es un **virus** que contiene una codificación programada para atacar y dañar datos, equipos técnicos o sistemas enteros. Los troyanos, virus, spyware, gusanos, adware y botnets entre otros, son tipos de malware.

### ¿En qué consiste?

Se envía por correo electrónico durante los **ataques** de phishing y spam.

Se envían **múltiples correos electrónicos** con un **virus** haciéndose pasar por una empresa

Después de ser **abierto**, el malware infecta el sistema y le causa daños.



Enseñar a los empleados de la empresa es la primera línea de defensa contra el malware. Si alguien recibe un correo electrónico de una fuente desconocida y con un archivo adjunto grande, es mejor que lo elimine inmediatamente.

4

## RAMSOMWARE

El rescate es un tipo específico de malware que ataca todo el sistema informático y bloquea el acceso a los usuarios hasta que se paga la demanda financiera (rescate) al autor.

### ¿En qué consiste?

Las amenazas a la seguridad del correo electrónico como ésta suelen producirse durante otros ataques **a gran escala** cuando se apunta hacia **múltiples usuarios** dentro de la empresa.

