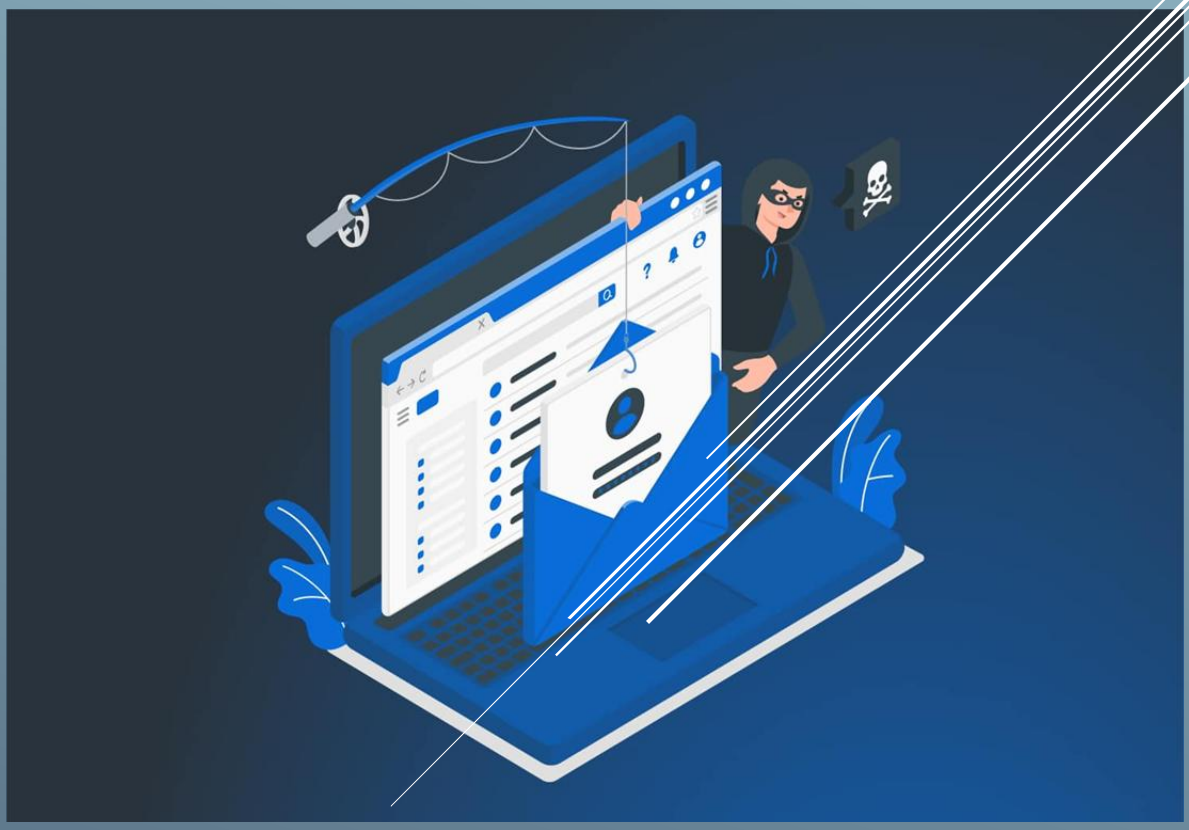


THE PHISHING

CONCEPTOS BASICOS VER. 1.0

Contenido

1. Introducción al phishing

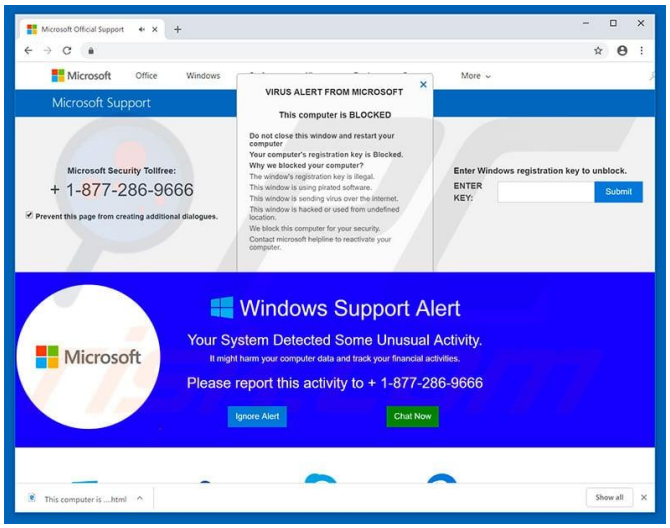
El phishing es una técnica utilizada por ciberdelincuentes para engañar a los usuarios y que proporcionen información confidencial, como contraseñas, números de tarjetas de crédito o credenciales de inicio de sesión. Esto se logra mediante correos electrónicos, mensajes o sitios web falsos que se hacen pasar por entidades confiables (bancos, servicios en línea, empresas reconocidas).

Objetivo del curso:

Capacitar a personas sin conocimientos informáticos para que reconozcan los intentos de phishing y actúen con seguridad.

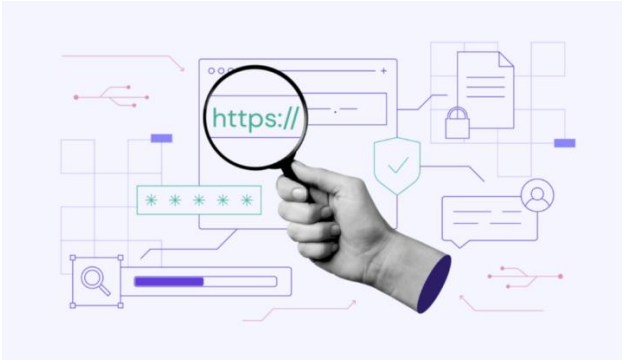
2. Características de los correos electrónicos de phishing

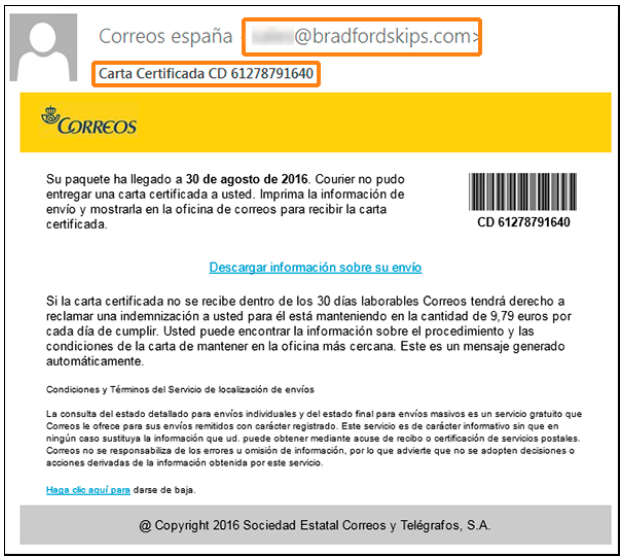
Remitente sospechoso: direcciones de correo electrónico inusuales o incorrectas (p. ej., "micros0ft@support-tech.com").



Mensajes urgentes o alarmantes: "Su cuenta ha sido bloqueada", "Verifique su información ahora".

Enlaces sospechosos: Los enlaces parecen oficiales, pero conducen a sitios falsos. Al pasar el cursor sobre ellos, se revela la URL real.




Correos españa @bradfordskips.com>

Carta Certificada CD 61278791640

CORREOS

Su paquete ha llegado a **30 de agosto de 2016**. Courier no pudo entregar una carta certificada a usted. Imprima la información de envío y mostrarla en la oficina de correos para recibir la carta certificada.

CD 61278791640

Descargar información sobre su envío

Si la carta certificada no se recibe dentro de los 30 días laborables Correos tendrá derecho a reclamar una indemnización a usted para él está manteniendo en la cantidad de 9,79 euros por cada día de cumplir. Usted puede encontrar la información sobre el procedimiento y las condiciones de la carta de mantener en la oficina más cercana. Este es un mensaje generado automáticamente.

Condiciones y Términos del Servicio de localización de envíos

La consulta del estado detallado para envíos individuales y del estado final para envíos masivos es un servicio gratuito que Correos le ofrece para sus envíos remitidos con carácter registrado. Este servicio es de carácter informativo sin que en ningún caso sustituya la información que ud. puede obtener mediante acuse de recibo o certificación de servicios postales. Correos no se responsabiliza de los errores u omisión de información, por lo que advierte que no se adopten decisiones o acciones derivadas de la información obtenida por este servicio.

Haga clic aquí para darse de baja.

@ Copyright 2016 Sociedad Estatal Correos y Telégrafos, S.A.

Errores ortográficos y gramaticales: Los correos electrónicos fraudulentos suelen contener errores.

3. Tipos comunes de phishing

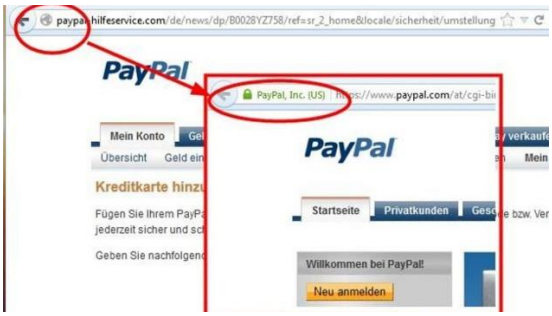
Phishing clásico por correo electrónico.

Ejemplos de phishing por correo electrónico uup.es

Phishing selectivo: Ataques personalizados que utilizan datos específicos del usuario.

Smishing: Mensajes de texto fraudulentos.

Pharming: Redireccionamiento a sitios web falsos al intentar acceder a un sitio web real.



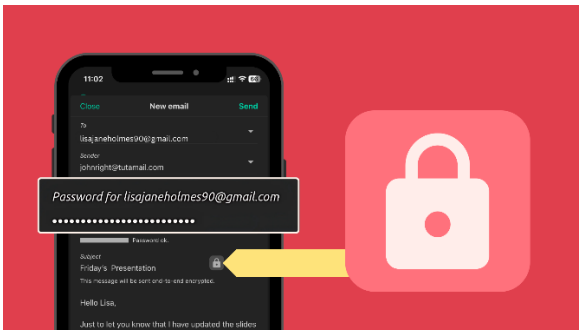
4. Mejores prácticas para evitar estafas de phishing

Nunca haga clic directamente en enlaces de correos electrónicos sospechosos.

Acceda manualmente a los sitios web escribiendo la dirección en su navegador.

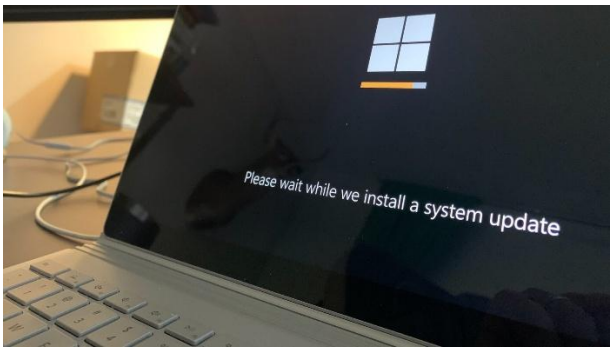
Verifique el remitente y busque errores ortográficos.

No comparta información confidencial por correo electrónico ni por teléfono si no está completamente seguro.



Utilice la autenticación de dos factores siempre que sea posible.

Mantenga su antivirus y sistema operativo actualizados.



5. Glosario Básico

Phishing: Robo de identidad mediante engaño digital para obtener datos confidenciales.

Spear phishing: Phishing dirigido específicamente a una persona u organización.

Smishing: Phishing mediante mensajes SMS.

Vishing: Phishing realizado mediante llamadas de voz.

URL (Localizador Uniforme de Recursos): Dirección web.

Spoofing: Técnica para falsificar la identidad digital.

2FA (Autenticación de Dos Factores): Autenticación en dos pasos para mayor seguridad.

6. Referencias bibliográficas.

Google. (s.f.). Cuestionario de Phishing. https://phishingquiz.withgoogle.com/

Instituto Nacional de Ciberseguridad (INCIBE). (s.f.). Protección contra el phishing. https://www.incibe.es

Oficina de Seguridad del Internauta (OSI). (s.f.). Campañas de Fraude. https://www.osi.es/es/reporte-de-fraudes

Hernández, A. (2022). Ciberseguridad para todos: Guía práctica para principiantes. Digital Segura Publishing.