PRUEBA DE

INGENIERÍA SOCIAL PHISHING

Objetivo:
Evaluar la conciencia y preparación de los empleados frente a correos maliciosos de tipo Phishing.

DATOS DE LA PRUEBA

Figura 1. Email enviado - Phishing

- Correos enviados: **4.395 (100%)**
- Correos abiertos: **550 (12,5%)**
- Clicks en enlace malicioso: **662 (120%*)**

**Múltiples clics por usuario*

- Información confidencial entregada: **76 (14%)**
- Correos respondidos (aceptación total): **7 (1,2%)**

ANÁLISIS DE RIESGO

RIESGO EXTREMO

0 reportes de incidente tras abrir el correo.

662 clics en enlace fraudulento.

Alta vulnerabilidad: exposición a malware que compromete confidencialidad, integridad y disponibilidad.

RIESGO ALTO

76 usuarios entregaron usuario y contraseña.

7 funcionarios respondieron al correo, indicando confianza total en el emisor.

¿Cómo Identificar un Correo Phishing?

- El remitente **simula ser confiable.**
- Crea **urgencia**: "¡Cambia tu contraseña ya!".
- Enlaces **aparentemente legítimos.**
- **Pide datos** como usuario y contraseña.
- Puede contener **archivos con virus** o spyware.

BUENAS PRÁCTICAS DE SEGURIDAD DIGITAL

Infórmate:
Participa en talleres y charlas sobre seguridad digital.

Verifica:
Si tienes dudas, no hagas clic ni respondas.

Cuida tus datos:
No entregues datos sensibles por correo.

Mantente alerta:
Entidades serias nunca solicitan información confidencial por e-mail.

Recomendación Final

Se sugiere capacitar a usuarios de áreas críticas como:

- Procesos misionales con datos sensibles.
- Finanzas, contabilidad, presupuesto y afines.

LA SEGURIDAD ES UN COMPROMISO DE TODOS

Actúa con responsabilidad y protege la información institucional.

ALCALDÍA DE
SANTIAGO DE CALI