SH13LD-4CE

SHIELD FORCE – IRT

Cyber Security Operation Center (CSOC)

csoc@shieldforce.mx

ventas@shieldforce.mx www.shieldforce.mx

+52.55.53.51.15.56 opc 1

PHISHING EN TIEMPOS DE COVID-19

INCIDENT RESPONSE TEAM SA DE CV

EL PHISHING

- Es una técnica de manipulación (ingenieria social) que los ciber delincuentes usan para engañar a los usuarios y ganara acceso a información personal, confidencial o para que realicen alguna actividad. Se realiza mediante el envío de correos electrónicos o mensajes de texto fraudulentos.
- Su objetivo es información como:
  - Credenciales de acceso, usuario y contraseña.
  - Datos bancarios.
  - Datos personales.

En algunos casos invitan al usuarios a descargar archivos maliciosos.

SH13LD-4CE
IRT

OBJETIVOS DEL PHISHING

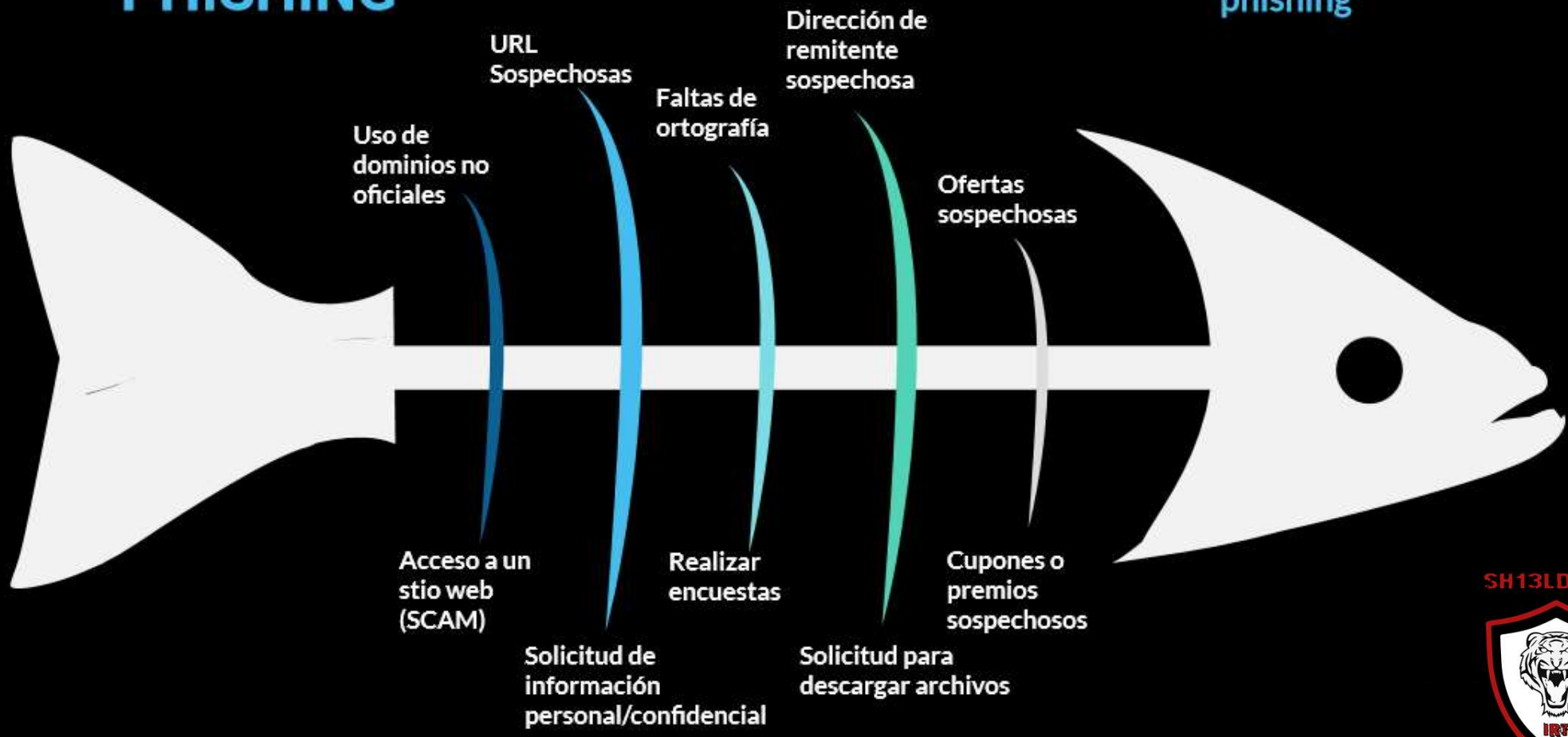
El COVID-19 es uno de los principales motivos para hacer campañas de phishing o spam por los diversos medios existentes, los cuales son:

- Correo Electrónicos
- Redes Sociales
- Mensajería de texto (SMS/WhatsApp)

Aprovechando el miedo y la desinformación de los usuarios durante la cuarentena, durante Marzo y Abril del 2020 las campañas de phishing se han incrementado utilizando los nombres de entidades financieras como bancos, así como empresas, hospitales, gobiernos.

Composicion del PHISHING

Principales aspectos a tener en cuenta para detectar un phishing



SH13LD-4CE

IRF

DETECTAR EL PHISHING

7 Consejos para Detectar Phishing.

- 1. Verifica las direcciones Web y los dominios.
- 2. Los e-mail de phishing tienden a tener faltas de ortografía y un español no muy asertivo.
- 3. Verifica el e-mail del remitente.
- 4. Verifica el "motivo" del e-mail.
- 5. Debes estar atento a las "ofertas", no caigas en engaños
- 6. No descargues los archivos adjuntos, si sospechas del correo
- 7. Consulta fuentes oficiales.
- 8. Utiliza el sentido común, si dudas, no lo abras

SH13LD-4CE

IRF

ACCIONES INMEDIATAS EN CASO DE PHISHING

- 1. Cambia de inmediato tu password.
- 2. No utilices el mismo password para tus aplicaciones.
- 3. Mantén actualizado tu equipo con los últimos parches publicados.
- 4. Ejecuta un escaneo en busca de amenazas con tu solución antimalware.
- 5. Si eres encargado de la seguridad en tu empresa impulsa la implementación de una solución antispam.
- 6. Contacta al equipo de **SHIELDFORCE**.

(55) 5351-1556 op.1 csoc@shieldforce.mx www.shieldforce.mx

SH13LD-4CE

SHIELD FORCE – IRT

Cyber Security Operation Center (CSOC)

csoc@shieldforce.mx

ventas@shieldforce.mx www.shieldforce.mx

+52.55.53.51.15.56 opc 1

9RACIAS

INCIDENT RESPONSE TEAM SA DE CV.