Ejercicios Adicionales: Identificación de Phishing

Municipalidad de Melipilla

Instrucciones Generales

Estos ejercicios están diseñados para reforzar los conocimientos adquiridos en la capacitación sobre phishing. Para cada escenario, analice cuidadosamente la información proporcionada y determine si se trata de un intento de phishing o una comunicación legítima.

Objetivo: Desarrollar la capacidad de identificar rápidamente las señales de alerta y tomar las decisiones correctas ante posibles amenazas.

Ejercicio 1: Análisis de Correos Electrónicos

Escenario A

De: soporte@bancochile.cl

Para: juan.perez@munimelipilla.cl

Asunto: Verificación de Seguridad Urgente

Contenido:

Estimado cliente,

Hemos detectado actividad sospechosa en su cuenta. Para proteger sus fondos,

necesitamos que verifique su información inmediatamente.

Haga clic aquí para verificar: http://banco-chile-seguridad.com/verificar

Si no verifica en las próximas 24 horas, su cuenta será suspendida.

Atentamente,

Equipo de Seguridad Banco de Chile

Pregunta: ¿Es este correo legítimo o phishing?

Escenario B

De: alcaldia@munimelipilla.cl

Para: personal@munimelipilla.cl

Asunto: Reunión de Personal - Viernes 15 de Agosto

Contenido:

Estimado equipo,

Les informo que tendremos una reunión general de personal el viernes 15 de agosto

a las 10:00 AM en el salón principal.

Temas a tratar:

- Nuevas políticas de seguridad informática
- Actualización de procedimientos administrativos
- Planificación del segundo semestre

Por favor confirmen su asistencia respondiendo a este correo.

Saludos cordiales,

Paula Garate

Alcaldesa de Melipilla

Pregunta: ¿Es este correo legítimo o phishing?

Escenario C

De: noreply@microsoft.com

Para: maria.gonzalez@munimelipilla.cl

Asunto: Su suscripción de Office 365 expirará pronto

Contenido:

Hola Maria,

Su suscripción de Microsoft Office 365 expirará en 7 días.

Para renovar su suscripción y evitar la interrupción del servicio,

haga clic en el siguiente enlace:

Renovar ahora: https://office.microsoft.com/renewal?user=maria.gonzalez

Si no renueva antes del 20 de agosto, perderá acceso a todos sus archivos.

Equipo de Microsoft

Pregunta: ¿Es este correo legítimo o phishing?

Ejercicio 2: Análisis de URLs

Para cada URL, determine si es legítima o sospechosa:

1. `https://www.bancochile.cl/login`
2. `http://banco-chile.security-update.com/login`
3. `https://melipilla.cl/tramites/online`
4. `https://microsoft-office365.renewal-urgent.net/login`
5. `https://www.sii.cl/servicios/declaracion`
6. `http://sii-chile.verificacion-rut.org/validar`

Para cada URL, explique:

- ¿Qué elementos la hacen legítima o sospechosa?

Ejercicio 3: Escenarios de Llamadas Telefónicas (Vishing)

Escenario A

Recibe una llamada de alguien que dice ser del "Departamento de Seguridad Informática de Microsoft". Le informa que su computador está infectado con virus y necesita acceso remoto para solucionarlo. Le pide que descargue un programa para darle acceso.

Preguntas:

1. ¿Es esta una llamada legítima?
2. ¿Qué señales de alerta identifica?
3. ¿Cómo debería responder?

Escenario B

Recibe una llamada del número principal de la Municipalidad. La persona se identifica como del departamento de Informática y dice que necesita verificar su contraseña para una actualización de seguridad urgente.

Preguntas:

1. ¿Qué elementos son sospechosos en esta llamada?
2. ¿Cómo puede verificar la legitimidad de la llamada?
3. ¿Qué acciones debe tomar?

Ejercicio 4: Mensajes de Texto (Smishing)

Analice los siguientes mensajes SMS:

Mensaje 1

BANCO CHILE: Su tarjeta ha sido bloqueada por seguridad.

Para desbloquear visite: bit.ly/banco-desbloqueo

Código de verificación: 4829

Mensaje 2

Municipalidad Melipilla: Su permiso de circulación está listo.

Retire en horario de oficina con su cédula de identidad.

Consultas: 2-829-5000

Mensaje 3

¡FELICIDADES! Ha ganado $500.000 en nuestro sorteo.

Para reclamar su premio envíe sus datos a:

premios-chile@gmail.com

Para cada mensaje:

1. Identifique si es legítimo o fraudulento
2. Señale las características que lo delatan
3. Explique qué acciones tomaría

Ejercicio 5: Casos Complejos

Caso 1: El Compañero de Trabajo

Recibe un correo de un compañero de trabajo conocido solicitando que transfiera fondos urgentemente para un proyecto. El correo viene de su dirección oficial, pero el tono es inusual y la solicitud es extraña.

Análisis requerido:

- ¿Qué factores considera para evaluar este correo?
- ¿Qué verificaciones realizaría antes de actuar?
- ¿Cómo procedería paso a paso?

Caso 2: La Actualización del Sistema

Recibe un correo del "Administrador del Sistema" informando que debe actualizar su contraseña debido a una nueva política de seguridad. El correo incluye un enlace a un formulario para cambiar la contraseña.

Análisis requerido:

- ¿Qué elementos evaluaría en este correo?
- ¿Cómo distinguiría entre una actualización legítima y phishing?
- ¿Cuál sería el protocolo correcto a seguir?

Ejercicio 6: Simulación de Respuesta a Incidentes

Escenario

Usted ya hizo clic en un enlace sospechoso y proporcionó su nombre de usuario y contraseña en un sitio web que parecía ser el portal interno de la Municipalidad. Ahora se da cuenta de que puede haber sido víctima de phishing.

Tareas:

1. Identifique a quién debe contactar

2. Describa qué información debe proporcionar en su reporte

3. Explique qué medidas preventivas implementaría para el futuro

Respuestas y Explicaciones

Ejercicio 1 - Respuestas

Escenario A: PHISHING

Señales de alerta:

- URL sospechosa (banco-chile-seguridad.com en lugar de bancochile.cl)

- Creación de urgencia
- Solicitud de verificación por correo
- Amenaza de suspensión de cuenta

Escenario B: LEGÍTIMO

Elementos que lo confirman:

- Remitente oficial conocido
- Contenido apropiado para el cargo
- No solicita información personal
- Propósito claro y profesional

Escenario C: POTENCIALMENTE LEGÍTIMO

Requiere verificación adicional:

- URL parece legítima
- Contenido coherente con servicios de Microsoft
- Sin embargo, debe verificarse independientemente

Ejercicio 2 - Respuestas

1. LEGÍTIMA - Dominio oficial, HTTPS

2. SOSPECHOSA - Dominio falso, subdominio engañoso

3. LEGÍTIMA - Dominio oficial municipal

4. SOSPECHOSA - Dominio falso que imita Microsoft

5. LEGÍTIMA - Dominio oficial del SII

6. SOSPECHOSA - Dominio falso que imita al SII

Evaluación Personal

Después de completar todos los ejercicios, reflexione sobre:

1. ¿Qué tipos de phishing le resultan más difíciles de identificar?

2. ¿Qué señales de alerta debe reforzar en su práctica diaria?

3. ¿Qué aspectos de la verificación necesita mejorar?

4. ¿Cómo puede aplicar estos conocimientos en su trabajo diario?

Recursos Adicionales

Para Mantenerse Actualizado

- Revise regularmente los boletines de seguridad de la Municipalidad
- Participe en las capacitaciones periódicas
- Consulte sitios oficiales de ciberseguridad como ANCI Chile

Para Reportar Incidentes

- Email de Informática: informatica@munimelipilla.cl

Recuerde: La práctica constante es clave para desarrollar la capacidad de identificar amenazas de phishing. Manténgase alerta y no dude en consultar cuando tenga dudas.