MANUAL DE CAPACITACIÓN

BUENAS PRACTICAS

JOAQUIN JESUS FEDERICI | JOAQUINFEDERICI@GMAIL.COM

RESUMEN

EN ESTE MANUAL REPASAREMOS LA BUENAS PRACTICAS DE SEGURIDAD EN LA GESTION DE CONTRASEÑAS E INFORMACION PARA EMPRESAS.

REPASAREMOS COMO FUNCIONA EL PHISHING, QUE ES Y COMO UNO PUEDE DARSE CUENTA DE CORREOS MALICIOSOS.

INTRODUCCIÓN Y OBJETIVOS

OBJETIVO

Este manual busca capacitar a los empleados para identificar y prevenir ataques de phishing y manejar informacion confidencial de manera segura. Ademas se buscara que los mismos puedan utilizar lo aprendido en su vida privada.

CONTEXTO

Buscamos explicar la relevancia de la seguridad informatica en el entorno laboral y el impacto potencial de una brecha de seguridad por parte del capital humanos

EL POR QUE

El capital humano es lo mas importante en una empresa y al ser de este modo es el mas vulnerable a cyberataques orientados al robo de informacion, esto puede ocacionar perdidas de informacion, tardanzas indeseadas, entorpecimiento de operaciones, entre otras.
Por eso mismo es importante que el capital humano este capacitado en como resguardarse de estos cyberataques.

https://fr.freepik.com/vecteurs-libre/concept-compte-phishing_8184219.htm

¿QUÉ ES EL PHISHING?

DEFINICIÓN Y TIPOS COMUNES DE PHISHING

El phishing es una técnica de fraude en línea que busca engañar a las personas para que revelen información sensible, como contraseñas, números de tarjetas de crédito o datos personales. A continuación, describo algunos intentos comunes de suplantación de identidad mediante correos electrónicos falsos:

- **Phishing por correo**:

1. **Correos de Entidades Financieras**

   Los atacantes se hacen pasar por bancos u otras instituciones financieras, enviando correos electrónicos que parecen oficiales.

   Pueden incluir logotipos y direcciones de correo similares a las de la entidad real, junto con mensajes que indican problemas con la cuenta o que requieren verificación.

2. **Ofertas y Promociones Falsas**

   Correos que ofrecen descuentos increíbles, sorteos o regalos.

   Utilizan líneas atractivas en el asunto y un lenguaje persuasivo para crear urgencia.

3. **Alertas de Seguridad**

   Correos que advierten sobre una actividad sospechosa en cuentas de correo o redes sociales.

   Dan instrucciones para "verificar" la cuenta mediante un enlace que lleva a una página de inicio de sesión falsa.

4. **Correos de Recursos Humanos o Servicios Técnicos**

   Intentos de phishing que parecen provenir de recursos humanos de una empresa o soporte técnico.

   Incluyen mensajes que parecen auténticos sobre actualizaciones de políticas o solicitudes de información adicional.

5. **Correos de Redes Sociales**

   Correos que indican que se ha recibido un mensaje o notificación en una red social.

   Ofrecen enlaces a "nuevos mensajes" que dirigen a sitios de phishing.

- **Phishing en Mensajes de Texto (Smishing)**:

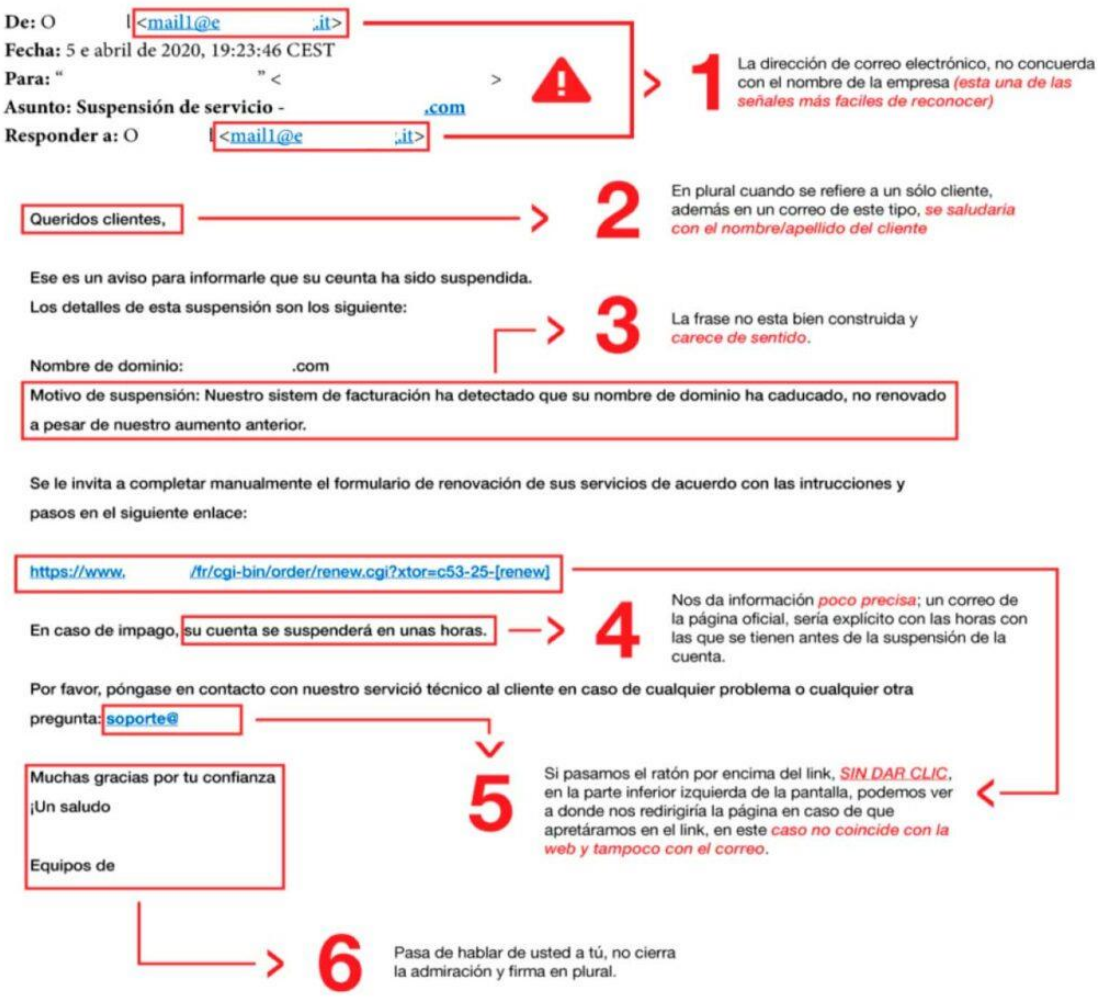
  Es una forma de phishing que utiliza mensajes de texto (SMS) para engañar a las personas y obtener información confidencial o inducirlas a realizar acciones perjudiciales.

  Los tipos de smishing son similares a los tipos de phishing exceptuando por un tipo importante:

  Falsas Ofertas de Empleo

  Mensajes que ofrecen trabajos o entrevistas, solicitando información personal.

  Estos piden a los usuarios que envíen información a un número de teléfono o sitio web.



IDENTIFICACIÓN Y PREVENCIÓN DE PHISHING

SEÑALES DE ALERTA EN CORREOS Y MENSAJES

Remitente Extraño

- **Revisar el Dominio del Remitente:**
    - Es fundamental prestar atención a la dirección de correo electrónico del remitente. Aunque el nombre de la persona o la empresa puede parecer legítimo, el dominio (la parte después del @) puede ser un indicativo de fraude.

    - **Ejemplo:** Un correo que supuestamente proviene de tu banco puede tener un dominio como "tu-banco-algo.com" en lugar de "tu-banco.com". Si el dominio es inusual o tiene errores, es una señal de alerta.

Errores en Ortografía y Gramática

- **Qué Buscar en un Correo Falso:**
    - Los correos electrónicos de phishing suelen contener errores gramaticales, ortográficos o de puntuación. Esto puede incluir frases confusas o el uso incorrecto de términos técnicos.

    - **Ejemplo:** Mensajes que dicen "Verifique su acount" o "Su cuenta será bloqued" son indicativos de un intento de fraude. Las empresas legítimas suelen tener un cuidado riguroso en su comunicación.

Urgencia Exagerada

- **Ejemplos de Palabras y Frases:**
    - Los atacantes a menudo intentan crear un sentido de urgencia para que el destinatario actúe rápidamente sin pensar. Palabras y frases como "Última oportunidad", "Su cuenta será suspendida", "Actúe ahora" o "Urgente: respuesta requerida" son típicas de los correos de phishing

    - **Consejo:** Siempre toma un momento para evaluar la situación y no actúes de inmediato ante mensajes alarmantes.

BUENAS PRÁCTICAS PARA EVITAR EL PHISHING

Verificación de Enlaces

- **Cómo Revisar la URL Sin Hacer Clic:**
    - Antes de hacer clic en un enlace, pasa el cursor sobre él para ver la dirección URL real en la parte inferior de tu navegador. Esto puede revelar si el enlace lleva a un sitio web legítimo o a uno falso.

    - **Consejo:** Si la URL no coincide con la del sitio oficial de la empresa, no hagas clic en ella.

No Descargar Archivos Desconocidos

- **Explicación de los Riesgos:**
    - Los archivos adjuntos en correos de remitentes desconocidos pueden contener malware, virus o ransomware. Estos pueden comprometer la seguridad de tu dispositivo y tu información personal.

    - **Consejo:** No descargues archivos de correos sospechosos. Si esperabas un archivo de alguien, verifica primero con el remitente a través de otro canal de comunicación.

Usar Autenticación Multifactor (2FA)

- **Beneficios de Añadir una Segunda Capa de Seguridad:**
    - La autenticación multifactor añade una capa adicional de seguridad, requiriendo no solo una contraseña, sino también otro método de verificación (como un código enviado a tu teléfono o una aplicación de autenticación).

    - **Beneficio:** Incluso si un atacante obtiene tu contraseña, necesitará el segundo factor para acceder a tu cuenta, lo que reduce significativamente el riesgo de acceso no autorizado.

GESTION SEGURA DE CONTRASEÑAS

CREACION DE CONTRASEÑAS FUERTES

Elementos de una Contraseña Segura

Para garantizar una buena protección, las contraseñas deben cumplir ciertos criterios que las hagan difíciles de adivinar o descifrar mediante ataques de fuerza bruta.

- **Longitud:**
    - Se recomienda que las contraseñas tengan al menos **12 caracteres** para incrementar su seguridad. Cuanto más larga sea la contraseña, más difícil será descifrarla.
- **Complejidad:**
    - Una contraseña segura debería incluir una combinación de **letras mayúsculas y minúsculas, números y caracteres especiales**. Esta variedad hace que la contraseña sea más robusta.

Ejemplos

- **Ejemplo seguro:** Tr0ub4dor&3!
    - Esta contraseña es segura porque combina letras, números y un símbolo especial.
- **Ejemplo débil:** contraseña123
    - Es fácil de adivinar, carece de complejidad y es demasiado común.

Consejo:
Si tienes dificultad para recordar contraseñas seguras, considera el uso de una frase única y personalizada, con variaciones de letras, números y símbolos.

GESTORES DE CONTRASEÑAS

Los gestores de contraseñas son aplicaciones que almacenan de forma segura todas tus contraseñas, permitiéndote crear contraseñas complejas sin necesidad de recordarlas. Algunas opciones populares incluyen:

- **LastPass:** Ofrece almacenamiento seguro de contraseñas y sincronización entre dispositivos.
- **Bitwarden:** Una opción de código abierto que también permite la gestión segura de contraseñas y notas.

Ventajas del Uso de Gestores

- **Simplificación:** Permiten crear y almacenar contraseñas seguras sin tener que recordarlas todas.
- **Acceso Seguro:** Los gestores suelen proteger tus datos con cifrado avanzado y requieren autenticación para acceder a tus contraseñas.
- **Generación de Contraseñas Fuertes:** Pueden crear automáticamente contraseñas complejas, lo que ahorra tiempo y mejora la seguridad.

POLÍTICAS DE CAMBIO DE CONTRASEÑAS

Cuándo Cambiar Contraseñas

Para maximizar la seguridad de tus cuentas, es recomendable:

- **Cada 6 meses:** Realizar un cambio de contraseñas regularmente ayuda a minimizar el riesgo de que queden obsoletas o comprometidas.
- **Después de un incidente:** Si detectas un posible acceso no autorizado a tu cuenta o has sido víctima de un ataque de phishing, cambia inmediatamente tu contraseña.

Ejercicio: Crear una Contraseña Segura

- **Instrucción:** Pensa en una frase que te resulte significativa y conviértela en una contraseña segura añadiendo complejidad. Por ejemplo, si tu frase es "Me gusta la música de los 90", puedes transformarla en Mg!st4Mú$1ca90.

GESTIÓN DE INFORMACIÓN CONFIDENCIAL

PRÁCTICAS PARA LA PROTECCIÓN DE INFORMACIÓN SENSIBLE

Política de Pantalla Limpia

- La política de pantalla limpia busca reducir el riesgo de exposición de información confidencial al asegurar que las pantallas de computadoras no contengan información visible cuando el usuario se ausenta de su puesto.

- **Consejo:** Configura el dispositivo para que se bloquee automáticamente tras unos minutos de inactividad y evita dejar documentos o datos sensibles en el escritorio físico y virtual.

- **Beneficio:** Esta práctica ayuda a minimizar los riesgos de visualización accidental o no autorizada de información.

Evitar Anotar Contraseñas en Lugares Públicos

- Es común que los usuarios apunten sus contraseñas en notas adhesivas o libretas accesibles, lo cual representa un riesgo si alguien tiene acceso al lugar donde están anotadas.

- **Riesgo:** Si una persona no autorizada accede al espacio de trabajo, podría ver o tomar una foto de estas contraseñas, lo que comprometería la seguridad.

- **Consejo:** Utiliza un gestor de contraseñas en lugar de anotar credenciales de acceso en papel.

Cifrado de Archivos

- El cifrado convierte la información en datos ilegibles sin una clave de acceso, protegiéndola en caso de que el dispositivo sea robado o accedido sin permiso.

- **Herramientas:**
  - **BitLocker** (Windows): Permite cifrar discos completos y unidades extraíbles.
  - **FileVault** (Mac): Ofrece cifrado de disco para proteger toda la información en el sistema.

- **Beneficio:** Protege datos confidenciales al asegurar que, sin la clave de cifrado, la información sea inaccesible para terceros.

CONTROL DE ACCESO A LA INFORMACIÓN

Limitación de Acceso

- La gestión de acceso implica restringir la información confidencial únicamente a quienes necesitan conocerla para realizar su trabajo.

- **Consejo:** Define roles y permisos claros para asegurar que solo el personal autorizado pueda acceder a datos sensibles.

- **Ejemplo:** Documentos financieros solo deben estar accesibles para el equipo de contabilidad.

EJERCICIO DE SIMULACIÓN

- Imagina que eres un analista de datos y has recibido una solicitud de un colega que trabaja en el área de marketing. El colega te pide acceso a los informes de ventas detallados que contienen información de clientes.

- **Pregunta de Análisis:** ¿Cómo evaluarías si la información puede ser compartida y bajo qué condiciones?
  - **Consideraciones:**
    - ¿El colega de marketing necesita esta información para su función específica?
    - ¿Hay un nivel de acceso designado en la política de la empresa que defina quién puede ver esos datos?
    - Si el acceso está permitido, ¿se puede proporcionar una versión limitada o anonimizada de los datos?

Objetivo del Ejercicio: Este ejercicio ayuda a practicar la evaluación de accesos para proteger la confidencialidad de la información, asegurando que solo se compartan los datos necesarios y siempre con las personas adecuadas.

RESPUESTA A UN INCIDENTE DE PHISHING

PROCEDIMIENTO EN CASO DE SOSPECHA DE PHISHING

Cómo Reportar un Correo Sospechoso

- Reportar correos sospechosos es esencial para proteger tanto al usuario como a la organización de posibles amenazas.

- **Pasos:**
    1. **No interactuar** con el correo (evitar abrir enlaces o responder).

    2. **Informar al equipo de TI:** Envía una captura de pantalla y, si es seguro, el encabezado del correo para que el equipo de TI pueda investigar.

    3. **Eliminar el mensaje** después de reportarlo para evitar el riesgo de interacción accidental.

Evitar Responder o Hacer Clic en Enlaces

- **Descripción de los Riesgos:**

    - Interactuar con un correo de phishing puede desencadenar ataques adicionales, como el robo de credenciales, la descarga de malware o el espionaje.

    - **Consejo:** Incluso si el mensaje parece urgente, mantén la calma y verifica primero con el área de TI para evitar riesgos.

RESTAURACIÓN Y PROTECCIÓN POSTERIOR A UN INCIDENTE

Cambio de Contraseñas

- **Recomendaciones:**
    - Cambia las contraseñas de todas las cuentas vinculadas o con credenciales similares al instante. Usa una contraseña fuerte y considera el uso de autenticación multifactor (2FA) para reforzar la seguridad.

    - **Consejo:** Usa un gestor de contraseñas para generar y almacenar nuevas contraseñas seguras.

Evaluación de Daños y Mejores Prácticas

- **Evaluación de Daños:** Si se compartió información por error, revisa qué datos fueron expuestos y notifica a las partes relevantes, incluyendo el área de TI, para monitorear posibles consecuencias.

- **Mejores Prácticas:**
    - **Revisión de Actividad en las Cuentas:** Revisa los registros de inicio de sesión y detecta cualquier actividad inusual.

    - **Refuerzo de la Conciencia:** Aprender de la experiencia mejora la capacidad de detectar futuros intentos de phishing.

CONCLUSIÓN Y RECURSOS ADICIONALES

REFLEXIÓN FINAL

- **Responsabilidad Individual:** La seguridad de la información es una responsabilidad compartida. Cada persona juega un papel crucial en la protección de los datos, al estar alerta y aplicar buenas prácticas en su gestión.

- **Importancia del Aprendizaje Continuo:** La ciberseguridad evoluciona rápidamente; estar al día y capacitarse regularmente permite mantenerse protegido.

RECURSOS PARA PROFUNDIZAR

- **Sitios Oficiales y Guías de Ciberseguridad:**
    - **CISA** (Cybersecurity and Infrastructure Security Agency): Recursos y guías sobre amenazas cibernéticas https://www.cisa.gov/

    - **CyberAware:** Consejos y artículos de concientización sobre ciberseguridad https://www.cyberaware.gov.uk/

    - **OWASP** (Open Web Application Security Project): Recursos y buenas prácticas en seguridad de aplicaciones web https://owasp.org/

EJERCICIO DE REVISIÓN FINAL

- **Instrucciones:** Responde a las siguientes preguntas de opción múltiple para evaluar tu comprensión:

1. Ejercicio de Verdadero o Falso
Lee cada afirmación y marca si es Verdadero (V) o Falso (F). Justifica las respuestas falsas.

- **(V/F) Es seguro abrir cualquier correo si conoces al remitente.**
- **(V/F) Las políticas de pantalla limpia ayudan a proteger la información confidencial cuando no estás en tu puesto de trabajo.**
- **(V/F) Si un mensaje tiene un enlace, debes hacer clic en él para verificar si es legítimo.**
- **(V/F) Las contraseñas seguras deben tener al menos 12 caracteres e incluir letras, números y símbolos.**

Respuestas:

- **Falso: Es seguro abrir cualquier correo si conoces al remitente. Justificación: A veces, las cuentas de remitentes conocidos pueden ser comprometidas y utilizadas para enviar correos de phishing.**
- **Falso: Si un mensaje tiene un enlace, debes hacer clic en él para verificar si es legítimo. Justificación: No se debe hacer clic en enlaces sospechosos; es mejor pasar el cursor sobre ellos para ver la URL sin hacer clic.**

---

2. Caso Práctico

Imagina que recibes el siguiente correo en tu trabajo:
De: soporte@bancointernacional.com
Asunto: ¡Atención! Su cuenta será suspendida
Mensaje: Estimado cliente,
Por razones de seguridad, necesitamos que verifique su cuenta. Por favor, haga clic en el enlace a continuación y proporcione sus credenciales.
Enlace: Verificar cuenta

Instrucciones:
Identifica los pasos que deberías seguir según las recomendaciones del manual:

1. **¿Cómo identificarías las señales de alerta en este correo?**
2. **¿Qué harías a continuación? Describe los pasos para reportarlo y evitar la interacción con el correo sospechoso.**

3. Análisis de Mensajes Sospechosos

A continuación, se muestran dos mensajes. Identifica cuál podría ser un intento de phishing y cuál es legítimo. Explica tus razones.

Mensaje A:
De: notificaciones@empresa.com
Asunto: Factura de este mes
"Estimado usuario, adjuntamos la factura correspondiente al mes. Por favor, revise el archivo adjunto."

Mensaje B:
De: seg.social@su-gobierno.co
Asunto: ¡URGENTE! Debe actualizar su información ahora
"Hemos detectado un problema con su cuenta. Para evitar la suspensión, ingrese aquí: www.actualice-info-gobierno.com"

---

4. Ejercicio de Creación de Contraseñas

Usando las recomendaciones del manual, crea una contraseña segura para una cuenta de correo de trabajo. La contraseña debe tener al menos 12 caracteres, incluir letras mayúsculas y minúsculas, números y símbolos.
Ejemplo de respuesta:
Mi cumpleaños es el 3 de enero y mi color favorito es el azul → Contraseña segura: C0l0rAzul!03

---

5. Evaluación de Escenarios de Acceso

Lee los siguientes escenarios y decide si concederías acceso a la información confidencial solicitada. Justifica tu respuesta.

1. **Escenario A: Un colega del área de Marketing solicita acceso a los datos de ventas detallados, argumentando que necesita analizarlos para una campaña.**
    - **¿Le concederías acceso? Explica tu respuesta según el control de acceso descrito en el manual.**
2. **Escenario B: Un miembro del equipo de finanzas te pide ver los detalles de los pagos recientes a proveedores.**
    - **¿Le concederías acceso? Justifica tu respuesta en función de las prácticas de gestión de información.**

6. Ejercicio de Identificación de Información Confidencial

Imagina que trabajas en un banco y estás organizando los archivos de la oficina. Identifica cuáles de los siguientes documentos requieren medidas de protección adicional y explica por qué.

- **Documento A: Nómina de empleados, que incluye nombres, direcciones y números de cuenta bancaria.**
- **Documento B: Análisis de mercado de la competencia, con datos públicos.**
- **Documento C: Contratos de clientes que contienen información personal y financiera.**