Universidad Politécnica de San Luis Potosí

Ingeniería en Tecnologías de la Información

Creando una campaña de phishing

SET (Social Engineer Toolkit)

Reporte técnico académico

Integrantes:

Coronado Noriega Jesús Olaf	178991
De La Rosa Rodríguez Erik	177700
González Reyes Felipe de Jesús	181134
Mendoza Aguado Karina	179859
Serrano Zermeño Leonardo	177301
Pérez Ventura Juan Alejandro	180370

Materia:

CNG V: Seguridad Informática

Nombre del docente:

Mtro. Servando López Contreras

San Luis Potosí, S.L.P.

27 de abril de 2026

Índice

1 Resumen ejecutivo

Este reporte documenta la actividad *Creando una campaña de phishing: SET (Social Engineer Toolkit)*, desarrollada en un contexto escolar para la asignatura de Seguridad Informática. La práctica consistió en diseñar y enviar correos simulados de phishing mediante Social Engineer Toolkit (SET), con el propósito de observar cómo un atacante puede explotar factores humanos como autoridad, urgencia y miedo a consecuencias académicas.

La campaña simulada utilizó mensajes relacionados con seguridad de cuenta, límite de faltas e irregularidades de reinscripción. En cada caso se analizaron los elementos que aumentan la credibilidad del engaño, los indicadores técnicos visibles y las medidas de prevención aplicables a estudiantes e instituciones.

2 Relación con la actividad de clase

El material de la asignatura ubica esta práctica dentro del segundo parcial, correspondiente a técnicas de explotación de vulnerabilidades y seguridad en entornos tecnológicos. En ese bloque se revisan phishing e ingeniería social, tipos de phishing por propagación, señales de identificación y recomendaciones de prevención. La actividad específica solicita crear una campaña de phishing utilizando SET, por lo que este documento se enfoca en evidenciar el flujo de simulación, analizar el pretexto usado y proponer controles defensivos.

3 Alcance, límites y consideraciones éticas

La actividad se considera válida únicamente bajo un contexto académico controlado. Una campaña de phishing real contra terceros requiere autorización formal, alcance definido, población delimitada, métricas permitidas y mecanismos de contención. Ejecutarla sin autorización puede afectar cuentas, datos personales, infraestructura institucional y confianza de los usuarios.

3.1 Alcance de la práctica

- Simular la creación de correos de phishing con temática escolar.
- Evaluar el uso de pretextos basados en autoridad institucional, urgencia y consecuencias académicas.
- Documentar el uso del módulo de correo de SET dentro de un entorno de prueba.
- Revisar los correos recibidos y detectar indicadores de phishing.
- Proponer medidas técnicas y educativas para reducir el riesgo.

3.2 Límites de seguridad recomendados

- No almacenar contraseñas reales ni información de sesión de usuarios.
- No utilizar dominios, logos o cuentas institucionales reales sin autorización expresa.
- No enviar campañas masivas fuera del grupo o alcance aprobado.
- No publicar evidencias con datos personales en espacios abiertos.
- Orientar el reporte a defensa, concientización y mejora de controles.

4 Objetivos

4.1 Objetivo general

Analizar el funcionamiento de una campaña simulada de phishing mediante SET, identificando los elementos técnicos, narrativos y visuales que aumentan la probabilidad de engaño, así como los controles necesarios para prevenir este tipo de ataques en un entorno escolar.

4.2 Objetivos específicos

1. Diseñar pretextos de ingeniería social asociados a procesos escolares.
2. Generar evidencia técnica del proceso de composición, configuración y envío de mensajes simulados.
3. Analizar las señales de alerta presentes en los correos recibidos.
4. Relacionar los hallazgos con controles de seguridad aplicables a usuarios e instituciones.
5. Elaborar recomendaciones orientadas a prevención, detección y respuesta.

5 Marco teórico

5.1 Phishing

El phishing es una técnica de ingeniería social en la que el atacante intenta engañar a una persona para que realice una acción perjudicial: ingresar credenciales, abrir enlaces, descargar archivos, autorizar accesos o revelar información. En un entorno escolar, este riesgo aumenta cuando el mensaje usa asuntos relacionados con reinscripción, calificaciones, faltas, becas, pagos, seguridad de cuenta o trámites administrativos.

5.2 Ingeniería social

La ingeniería social no depende únicamente de vulnerabilidades técnicas. Su fuerza está en manipular decisiones humanas. En las evidencias de esta práctica se observan tres disparadores psicológicos relevantes:

- **Autoridad:** el mensaje aparenta provenir de servicios escolares, control escolar o seguridad institucional.

- **Urgencia:** se establece una ventana de tiempo reducida para actuar.
- **Miedo a pérdida:** se amenaza con suspensión de cuenta, baja temporal, bloqueo de calificación o pérdida de derecho a examen.

5.3 Social Engineer Toolkit (SET)

SET es una herramienta utilizada en laboratorios de seguridad para simular escenarios de ingeniería social. Permite construir vectores de ataque controlados como correos, páginas clonadas, payloads o enlaces. En esta práctica se utilizó el módulo de correo para documentar una simulación académica y analizar sus implicaciones defensivas.

5.4 Phishing por correo electrónico

El phishing por correo electrónico es una de las modalidades más comunes porque permite distribuir mensajes con apariencia institucional, incluir enlaces externos y presionar al usuario mediante asuntos urgentes. El riesgo no está solamente en la herramienta técnica, sino en la combinación entre pretexto creíble, identidad aparente del remitente y falta de validación del destinatario.

6 Diseño de la campaña simulada

La campaña se construyó con tres variantes de mensaje. Todas mantienen una temática escolar porque ese contexto resulta creíble para estudiantes universitarios y aprovecha procesos que suelen generar presión: seguridad de cuenta, asistencia y reinscripción.

Tabla 1: Variantes de pretexto utilizadas en la campaña simulada

Variante	Pretexto	Riesgo buscado
Seguridad de cuenta	Aviso de actividad inusual y supuesta vinculación obligatoria de seguridad.	Inducir al usuario a validar identidad mediante un enlace externo.
Límite de faltas	Alerta de inasistencias superiores al porcentaje permitido.	Generar urgencia por miedo a perder derecho a examen ordinario.
Reinscripción	Supuesta irregularidad en el estatus de inscripción del ciclo escolar.	Forzar una acción rápida para evitar suspensión de materias o acceso a plataforma.

6.1 Características narrativas del mensaje

Los mensajes se diseñaron con tono formal, estructura institucional y consecuencias directas. Esto aumenta la credibilidad inicial, pero también permite observar indicadores de riesgo: remitentes no oficiales, enlaces acortados, dominios ajenos a la institución y errores de redacción.

6.2 Flujo general de la simulación

El flujo ejecutado puede resumirse en cinco fases:

1. Selección del vector de correo dentro de SET.
2. Redacción de asunto, cuerpo HTML y pretexto escolar.
3. Configuración del remitente visible, destinatario y servidor SMTP de laboratorio.
4. Envío hacia cuentas definidas para la práctica.
5. Revisión del mensaje recibido y análisis de indicadores de phishing.

7 Evidencias de la práctica

Las siguientes evidencias muestran el proceso de simulación de la campaña. Se conservan íntegras para que el docente pueda revisar datos visibles del remitente, destinatario, asunto, enlaces y contenido del mensaje.

7.1 Selección del módulo de correo en SET

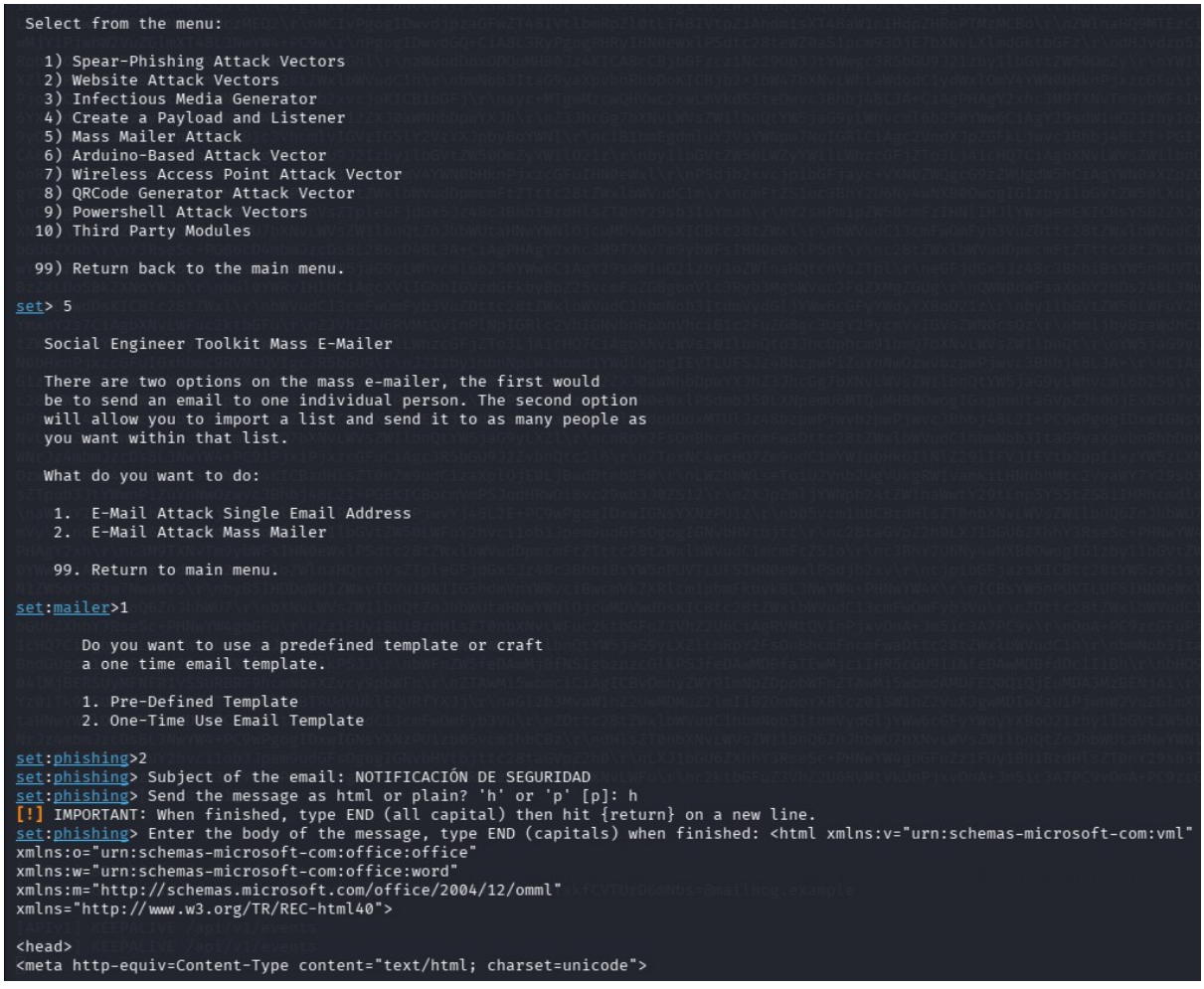

Figura 1: Menú de SET con selección del módulo *Mass Mailer Attack*, definición de mensaje HTML y asunto *NOTIFICACIÓN DE SEGURIDAD*.

7.2 Configuración del envío simulado

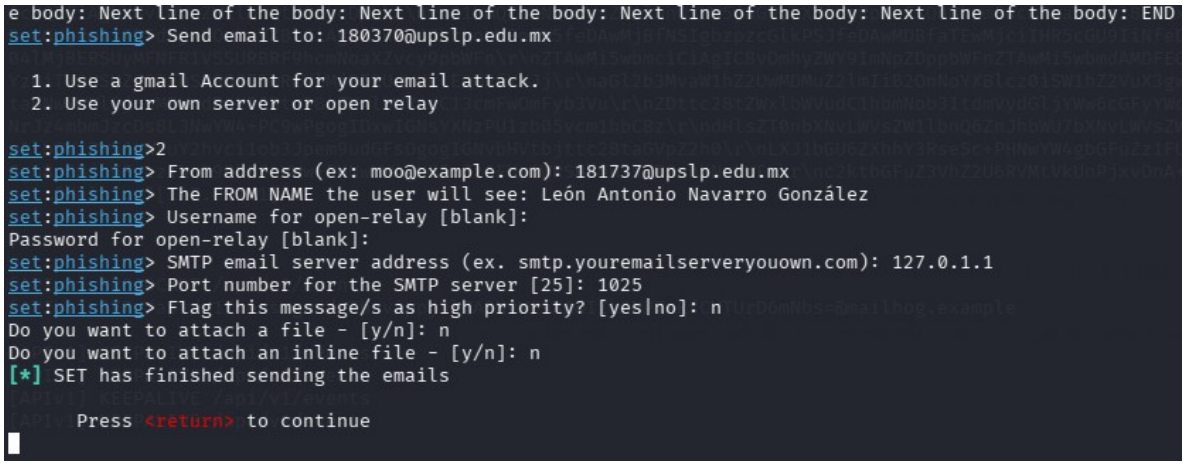

Figura 2: Configuración del envío: destinatario, remitente visible, nombre mostrado, servidor SMTP local y confirmación de envío.

7.3 Recepción del mensaje de seguridad

Figura 3: Vista inicial del correo recibido con asunto *NOTIFICACIÓN DE SEGURIDAD*; se observan remitente, destinatario y cuerpo del mensaje.

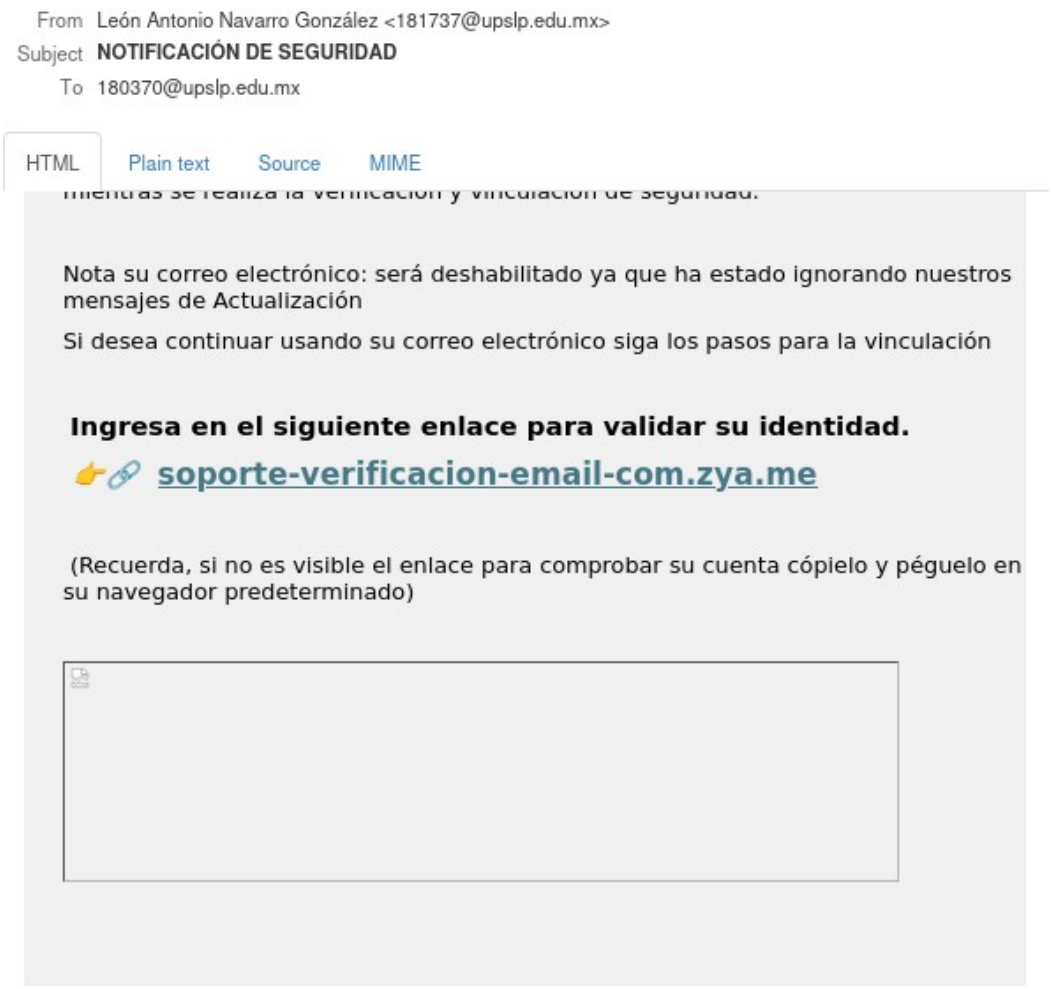

Figura 4: Vista inferior del mismo correo, donde se observa el llamado a validar identidad mediante el enlace mostrado en la evidencia.

7.4 Variantes

ALERTA: Límite de faltas excedido - Acción inmediata requerida Inbox ×

Servicios Escolares <servicios-escolares-upslp@gmail.com> 5:30 PM (2 minutes ago)
to me

Estimado alumno,

El sistema automatizado de control de asistencia ha detectado que en una o más de sus asignaturas registradas en el presente ciclo, usted ha alcanzado o excedido el **15% de inasistencias permitidas** según el Reglamento General de Alumnos.

De acuerdo con la normativa institucional, el exceder este límite genera automáticamente un estatus de **"Sin Derecho"** a examen ordinario.

Si usted considera que esto es un error de registro por parte del docente o cuenta con justificantes médicos no capturados, debe ingresar de inmediato al portal de **Autogestión de Asistencias** para realizar la aclaración antes del cierre de actas parciales:

https://bit.ly/3P409Fe

Pasos para la aclaración:

1. Inicie sesión en el módulo de autoservicio con su cuenta institucional.
2. Identifique la materia con la alerta roja.
3. Suba su evidencia en formato digital o solicite la revisión manual.

Nota: Tiene hasta las 23:59 horas del día de hoy para realizar este proceso; de lo contrario, el sistema bloqueará el registro de calificación para el parcial en curso.

Atentamente, Dirección de Servicios Escolares Universidad Politécnica de San Luis Potosí

Reply Forward

Figura 5: Correo simulado sobre límite de faltas excedido. El mensaje utiliza urgencia, autoridad escolar y una consecuencia académica directa.

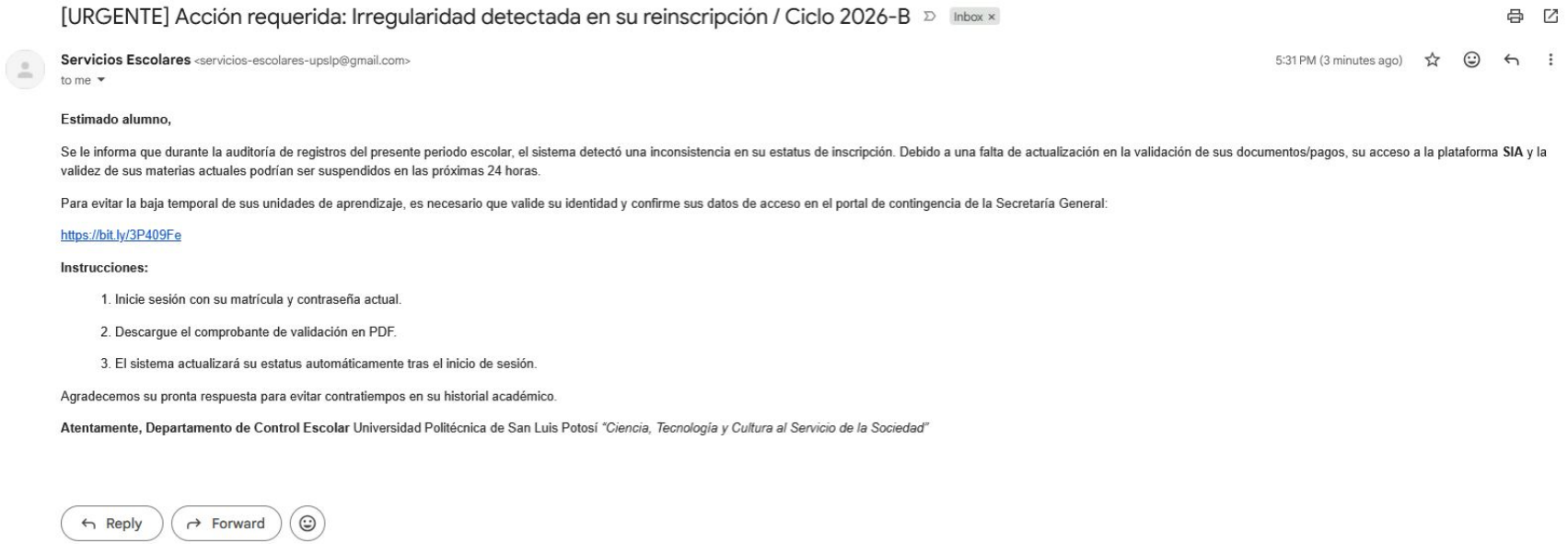

Figura 6: Correo simulado sobre irregularidad de reinscripción. El mensaje intenta dirigir al usuario a un enlace externo para validar identidad y confirmar datos de acceso.

8 Análisis técnico de los correos

La campaña demuestra que un correo visualmente simple puede ser suficiente para generar riesgo si explota presión académica. Sin embargo, las evidencias también muestran señales claras que permitirían detectar el ataque.

Tabla 2: Indicadores de phishing identificados

Indicador	Observación en la evidencia	Interpretación defensiva
Remitente no verificable	Se simula un nombre institucional o un área escolar, pero la dirección no prueba por sí misma que el mensaje sea legítimo.	El usuario no debe confiar solo en el nombre visible del remitente. Debe revisar dominio, firma y canal oficial.
Uso de cuenta genérica para comunicación institucional	En las variantes de faltas y reinscripción se observa un remitente con apariencia de área escolar, pero no corresponde al dominio institucional formal.	Una universidad normalmente debe comunicarse desde dominios oficiales y consistentes, no desde cuentas genéricas.
Lenguaje de urgencia	Se menciona bloqueo, suspensión, límite de tiempo, baja temporal o pérdida de derecho académico.	La urgencia es un disparador común para reducir el análisis crítico del usuario.
Enlace externo o acortado	Se observan ligas externas y acortadas dentro de los mensajes recibidos.	Las ligas acortadas y dominios no institucionales deben considerarse sospechosos.
Solicitud de validación de identidad	El correo pide continuar con un proceso de vinculación, aclaración o confirmación.	Cualquier solicitud de inicio de sesión debe verificarse entrando manualmente al portal oficial, no desde el enlace recibido.
Errores de redacción y formato	Algunos mensajes presentan frases poco naturales, acentos inconsistentes o imágenes rotas.	Los errores no prueban por sí solos que sea phishing, pero elevan el nivel de sospecha.
Consecuencia desproporcionada	Se amenaza con bloquear cuentas, materias o calificaciones en poco tiempo.	Los procesos institucionales críticos normalmente tienen canales formales y plazos claros.

8.1 Evaluación de impacto

Tabla 3: Riesgo estimado por variante

Variante	Nivel de riesgo	Justificación
Seguridad de cuenta	Alto	Combina autoridad tecnológica, amenaza de deshabilitación y solicitud de validación de identidad.
Límite de faltas	Alto	Ataca un miedo académico directo: perder derecho a examen. El plazo corto incrementa presión.
Reinscripción	Medio-alto	Usa una consecuencia seria, aunque puede ser detectado si el usuario revisa el dominio y confirma en plataforma oficial.

9 Controles recomendados

9.1 Para estudiantes y usuarios finales

- No abrir enlaces de correos que amenacen con consecuencias inmediatas sin verificar primero en el portal oficial.
- Revisar el dominio completo del remitente, no solo el nombre visible.
- Desconfiar de enlaces acortados o dominios externos cuando el trámite supuestamente sea institucional.
- No ingresar contraseña después de abrir un enlace recibido por correo. Es mejor escribir manualmente la URL oficial en el navegador.
- Reportar correos sospechosos al área correspondiente antes de reenviarlos a otros usuarios.

9.2 Para la institución

- Implementar y monitorear SPF, DKIM y DMARC para reducir suplantación de dominio.
- Usar campañas periódicas de concientización con ejemplos reales y simulados.
- Establecer una ruta oficial de reporte de phishing visible para estudiantes y personal.
- Bloquear o advertir sobre URL acortadas y dominios recién creados cuando se usen en correos institucionales.
- Aplicar autenticación multifactor en portales escolares y cuentas institucionales.
- Mantener plantillas oficiales de comunicación para que los usuarios reconozcan diferencias de estilo, dominio y firma.

10 Buenas prácticas para campañas éticas de concientización

Una campaña de phishing ética no debe buscar humillar ni castigar al usuario. Su objetivo correcto es medir exposición, enseñar señales de alerta y mejorar controles. Para que sea válida, debe cumplir al menos con los siguientes criterios:

1. Autorización formal por escrito antes de ejecutar la prueba.
2. Alcance limitado: población, fechas, dominios, mensajes y métricas permitidas.
3. Protección de datos personales y prohibición de almacenar contraseñas reales.
4. Página educativa posterior, en caso de que el usuario haga clic.
5. Reporte agregado de resultados, evitando señalar públicamente a personas específicas.
6. Plan de mejora posterior con capacitación y endurecimiento técnico.

11 Conclusiones

La práctica evidencia que el usuario sigue siendo un punto crítico en la seguridad informática. Un correo con estructura sencilla puede generar riesgo si utiliza elementos de autoridad, urgencia y miedo a consecuencias académicas. La parte técnica de SET facilita la simulación, pero el éxito del engaño depende principalmente del contexto psicológico del mensaje.

También se comprobó que existen señales detectables: remitentes no oficiales, ligas acortadas, dominios ajenos, solicitudes de validación de identidad y presión temporal. Por ello, la defensa no debe depender únicamente de filtros de correo; necesita combinar controles técnicos, capacitación, autenticación multifactor y canales claros de verificación.

El aprendizaje principal es directo: una institución puede tener buenas herramientas técnicas, pero si sus usuarios no tienen criterios de validación, una campaña de ingeniería social puede comprometer cuentas, información académica o accesos internos.

Referencias

- Cybersecurity and Infrastructure Security Agency. (s. f.). *Avoiding social engineering and phishing attacks*. https://www.cisa.gov/
- Hadnagy, C. (2018). *Social Engineering: The Science of Human Hacking* (2nd ed.). Wiley.
- López Contreras, S. (2026). *CNG V: Seguridad Informática*. Material de clase, Universidad Politécnica de San Luis Potosí.
- MITRE. (s. f.). *Phishing, Technique T1566 - Enterprise ATT&CK*. https://attack.mitre.org/techniques/T1566/
- National Institute of Standards and Technology. (2018). *Building an Information Technology Security Awareness and Training Program* (SP 800-50). https://csrc.nist.gov/

- TrustedSec. (s. f.). *The Social-Engineer Toolkit*. https://github.com/trustedsec/social-engineer-toolkit