GUIA METODOLOGICA

PARA LA PREVENCION SOCIAL POLICIAL

AREA EDUCATIVA

ADOLESCENTES

PHISHING

Para la capacitación para adolescentes sobre el riesgo de phishing, es importante cubrir temas clave relacionados con la seguridad en línea y cómo protegerse contra estafas en línea. Aquí hay una lista de lo que un adolescente debe saber en una sesión de capacitación sobre phishing

"Protegiéndote del Phishing en Línea"

Duración de la Sesión: Aproximadamente 60-90 minutos

Objetivos de la Sesión:

- Educar a los adolescentes sobre qué es el phishing y cómo funciona.
- Enseñar a los adolescentes a reconocer las señales de phishing en línea.
- Proporcionar consejos para prevenir el phishing y proteger su información personal en línea.

Estructura de la Sesión:

1. **Introducción**
   - Saludo y presentación de los servidores públicos policiales.
   - Explicación de los objetivos de la sesión.

2. **Qué es el Phishing**
   - Definición de phishing y cómo funciona, que implica engañar a las personas para obtener información personal o financiera confidencial a través de mensajes de correo electrónico, sitios web falsos y otros métodos engañosos
   - Ejemplos de ataques de phishing.

3. **Cómo Funciona el Phishing**
   - Explicación de cómo los atacantes utilizan técnicas de engaño para obtener información personal. Describir cómo los estafadores utilizan técnicas de ingeniería social para engañar a las personas, incluyendo la suplantación de identidad y la creación de sitios web falsos.
   - Descripción de la ingeniería social en el phishing.

4. **Señales de Phishing**
    - Enseñanza de señales comunes de phishing, como errores de ortografía y gramática, direcciones de correo electrónico sospechosas y URLs falsas.
    - Ejemplos de correos electrónicos y sitios web de phishing.

5. **Cómo Reconocer el Phishing**
    - Estrategias para reconocer intentos de phishing, como verificar la autenticidad del remitente, no hacer clic en enlaces sospechosos y no compartir información confidencial en respuesta a correos electrónicos no solicitados.

6. **Consecuencias del Phishing**
    - Discusión sobre las posibles consecuencias de caer en un ataque de phishing, como el robo de identidad y la pérdida de datos personales.

7. **Cómo Protegerse**
    - Consejos para protegerse contra el phishing, que incluyen la activación de la autenticación, el uso de contraseñas seguras y la actualización de software.

8. **Denuncia de Phishing:**
    - Información sobre cómo denunciar intentos de phishing a las autoridades o a los proveedores de servicios en línea.

9. **Ejercicio Práctico**
    - Ejercicio interactivo donde los adolescentes evalúan correos electrónicos o sitios web para detectar señales de phishing.

10. **Denuncia de Phishing**
    - Información sobre cómo denunciar ataques de phishing a las autoridades o proveedores de servicios en línea.

11. **Recursos de Apoyo**
    - Proporcionar información sobre recursos adicionales, como sitios web de seguridad en línea y organizaciones de seguridad cibernética.

12. **Preguntas y Discusión**
    - Invitar a los adolescentes a hacer preguntas y compartir sus experiencias o preocupaciones relacionadas con la seguridad en línea.

13. **Cierre**
    - Agradecer a los adolescentes por su participación.
    - Entrega de materiales impresos o enlaces a recursos de seguridad en línea.

- La seguridad en línea es un tema crítico en la sociedad actual, y es fundamental que los adolescentes estén bien informados para protegerse contra amenazas cibernéticas, es importante proporcionar recursos y referencias para buscar ayuda en caso de necesidad.

Recursos Necesarios:

- Servidores Públicos Policiales con conocimiento en seguridad cibernética y phishing.
- Material educativo, como presentaciones en PowerPoint y ejemplos de phishing.
- Computadoras o dispositivos para el ejercicio práctico.

Evaluación: Puede evaluar la comprensión de los adolescentes sobre el phishing al final de la sesión mediante una breve evaluación o una discusión de grupo.