Temario - Charla de Ciberseguridad

1. Introducción a la Ciberseguridad

- **¿Qué es la ciberseguridad?**
  - Definiciones y conceptos básicos: orientado hacia software
  - Enfocado por qué la ciberseguridad es importante para las personas y las organizaciones (datos personales, seguridad financiera, continuidad comercial).
- **Ciberataques en la vida real**
  - Hablaremos de los ataques más famosos y sus consecuencias (e.g., Equifax breach, ransomware attacks) Hablar del caso WannaCry
  - Cómo esto afecta a cada uno de nosotros (identity theft), businesses (financial loss, reputation), and society (infrastructure damage).

2. Las amenazas de ciberseguridad más comunes

- **Malware (Viruses, Ransomware, Trojans)**
  - Explicaremos cómo funciona el software malicioso y cómo infecta los dispositivos.
  - Veremos el impacto de los ataques de ransomware (por ejemplo, bloqueo de archivos y pago del rescate).
- **Phishing Attacks**
  - El phishing como intentos de engañar a las personas para que revelen información confidencial (por ejemplo, credenciales de inicio de sesión, números de tarjetas de crédito).
  - Ejemplos de correos electrónicos de phishing y cómo detectarlos (por ejemplo, enlaces sospechosos, lenguaje urgente).
- **Social Engineering**
  - Cómo los atacantes manipulan a las personas para que infrinjan los protocolos de seguridad (por ejemplo, mediante pretextos o provocaciones).
  - Consejos sencillos para evitar ser víctima de estas tácticas.
- **Data Breaches**
  - ¿Qué sucede cuando se roban datos (por ejemplo, información personal o datos financieros)?
  - Ejemplos de infracciones recientes y sus efectos.

3. Cómo y cuándo ocurre un Cyberataque

- **Vulnerabilidad en sistemas y software**
  - Qué son las vulnerabilidades (fallas en el software, contraseñas débiles, sistemas obsoletos).

    - Ejemplos de vulnerabilidades: software sin parches, políticas de contraseñas deficientes, comunicaciones sin cifrar.
- **Cibercriminales y sus motivos**
    - Hacker de sombrero negro y sombre blanco
    - Crimen organizado y Nation-state hackers
    - Motivos que los mueven: financieros, espionaje, activismo, etc.

4. Puntos básicos de Cyber Hygiene (Qué hacer para estar a salvo)

- **Prácticas de contraseñas fuertes**
    - Por qué es importante tener contraseñas seguras y únicas.
    - Presentar el concepto de los administradores de contraseñas.
- **Autenticación de dos factores (2FA)**
    - Explicar qué es la 2FA y por qué es fundamental para una protección adicional.
    - Dar ejemplos de cómo funciona la 2FA (códigos SMS, aplicaciones de autenticación).
- **Actualizaciones y parches de software**
    - Por qué mantener actualizado el software y los dispositivos es esencial para la seguridad.
    - Explicar cómo las actualizaciones corrigen vulnerabilidades y protegen contra ataques.
- **Reconocer actividades sospechosas**
    - Cómo detectar correos electrónicos de phishing, enlaces sospechosos o actividad extraña en la cuenta.
    - Asesoramiento para verificar la legitimidad de las solicitudes de datos confidenciales.

5. La importancia de la privacidad

- **Qué son datos personales**
    - Datos personales (nombre, dirección, correo electrónico, número de documento, información de seguro, etc.).
    - Analice por qué los datos personales son valiosos y cómo pueden utilizarse de forma maliciosa. Sobre todo en entornos financieros y de salud.
- **Opciones de seguridad en redes sociales y servicios online**
    - Cómo configurar los ajustes de privacidad en plataformas populares (Facebook, Instagram, etc.).
    - Los riesgos de compartir demasiada información en línea y cómo proteger la información personal.

6. La importancia del encriptamiento

- **¿Qué es el encriptamiento?**
    - Presentar el concepto de cifrado en términos simples

    - Por qué el cifrado es crucial para proteger la información confidencial, tanto en reposo (en los dispositivos) como en tránsito (a través de las redes).
- **Encriptamiento en nuestro día a día**
    - Ejemplos: HTTPS en navegadores web, aplicaciones de mensajería cifrada (por ejemplo, Signal, WhatsApp).

7. Ciberseguridad para negocios y organizaciones

- **Seguridad más allá del individuo**
    - Cómo las empresas necesitan prácticas sólidas de ciberseguridad para proteger los datos de los clientes, la propiedad intelectual y la continuidad operativa.
    - La importancia de la capacitación y la concientización de los empleados.
- **Medidas básicas de seguridad para las empresas**
    - Firewalls, software antivirus y sistemas de detección de intrusiones.
    - La necesidad de auditorías y monitoreo de seguridad regulares.

8. Lo legal y lo ético en Ciberseguridad

- **Leyes y normativas de protección de datos**
    - Mencione las principales normativas, como el RGPD (Europa), la CCPA (California) y la HIPAA (datos sanitarios). Podríamos enfocarnos en temas de datos en Panamá
    - Por qué las empresas y los particulares deberían preocuparse por el cumplimiento normativo. ¿Qué hace el SIP para esto?
- **Hackeo ético y ciberdefensa**
    - Qué hacen los hackers éticos (o hackers de sombrero blanco) para proteger los sistemas.
    - El papel de los expertos en ciberseguridad en la defensa contra los ataques.

9. El futuro de la ciberseguridad

- **Amenazas emergentes**
    - Las amenazas emergentes (por ejemplo, ataques impulsados por IA, deepfakes).
    - Cómo está evolucionando la ciberseguridad para combatir estos nuevos desafíos.
- **El creciente papel de la ciberseguridad en la sociedad**
    - Cómo la ciberseguridad se está integrando cada vez más en la vida diaria, con dispositivos inteligentes, IoT y monedas digitales.
    - La necesidad constante de concienciación y educación sobre ciberseguridad a medida que avanza la tecnología.

10. Conclusiones

- **La seguridad es responsabilidad de todos**
    - Reforzar la idea de que todos, no solo los profesionales de TI, desempeñan un papel en la ciberseguridad.
    - Fomentar la acción personal: adoptar buenas prácticas de seguridad, estar alerta y mantenerse informado.