GUÍA DE VIAJE

PARADA 8

ÍNDICE DE CONTENIDOS

1. CIBERSEGURIDAD: CONCEPTOS BÁSICOS

En un mundo cada vez más digitalizado, la ciberseguridad personal es esencial para proteger tu información personal y profesional de amenazas en línea. Esta píldora formativa te proporcionará conocimientos clave y estrategias prácticas para mejorar tu seguridad digital.

¿Qué es la Ciberseguridad Personal?

La ciberseguridad personal se refiere a las prácticas y herramientas que los individuos pueden utilizar para proteger su información en línea de accesos no autorizados, robos y otros tipos de ciberataques.

Importancia de la Ciberseguridad Personal

- **Protección de Datos Personales:** Evita el robo de identidad, el fraude financiero y la violación de la privacidad.
- **Seguridad Profesional:** Protege información sensible relacionada con tu carrera o negocio.
- **Confianza Digital:** Fomenta una mayor confianza al utilizar tecnologías digitales, sabiendo que tus datos están seguros.

Estrategias Clave para Mejorar la Ciberseguridad Personal

1. **Contraseñas Fuertes y Gestores de Contraseñas:**
    - Utiliza contraseñas largas, únicas y complejas para cada cuenta. Considera el uso de gestores de contraseñas para almacenar y gestionar tus contraseñas de forma segura.
2. **Autenticación de Dos Factores (2FA):**

- Activa la autenticación de dos factores en todas las cuentas que lo permitan. Esto añade una capa adicional de seguridad requiriendo un segundo método de verificación además de la contraseña.

3. **Actualizaciones de Software:**
   - Mantén todos tus dispositivos y software actualizados. Las actualizaciones frecuentemente incluyen parches de seguridad que protegen contra vulnerabilidades recién descubiertas.
4. **Redes Seguras:**
   - Evita usar redes Wi-Fi públicas para transacciones importantes. Considera el uso de una red privada virtual (VPN) para cifrar tu conexión a internet.
5. **Formación sobre Phishing:**
   - Familiarízate con las tácticas comunes de phishing y sé cauteloso al abrir correos electrónicos o clickear en enlaces de fuentes desconocidas.
6. **Copias de Seguridad Regulares:**
   - Realiza copias de seguridad regulares de datos importantes para asegurar que puedas recuperar tu información en caso de un ataque cibernético o fallo técnico.

2. ¿POR QUÉ ES IMPORTANTE LA CIBERSEGURIDAD?

La ciberseguridad es un pilar esencial tanto a nivel personal como profesional en el mundo digital. Como futuros profesionales, aprender a cuidar tanto nuestros datos como los de las empresas donde trabajemos, nos posicionará como un activo valioso y responsable.

Los beneficios e impacto de la ciberseguridad abarcan múltiples áreas:

1. Protección de la privacidad personal

- Evita el robo de identidad: Los datos personales (como contraseñas, cuentas bancarias o información privada) son un objetivo prioritario para los ciberdelincuentes.
- Control de tu información: Un mal manejo de la privacidad puede llevar a la divulgación no autorizada de fotos, documentos o datos personales.

2. Garantía de la seguridad económica

- Prevención de fraudes y robos: Sin ciberseguridad, el acceso a cuentas bancarias, tarjetas de crédito o compras online puede ser fácilmente vulnerado.
- Protección ante ransomware: Estos ataques cifran tus archivos y exigen dinero para recuperarlos, lo que puede generar grandes pérdidas económicas.

3. Confianza en el ámbito profesional

- En empresas, la ciberseguridad asegura:
  - Protección de datos sensibles: Como registros de clientes, contratos o estrategias comerciales.

- Continuidad del negocio: Evitar interrupciones en los servicios debido a ataques como DDoS o ransomware.
- Cumplimiento de normativas legales: Muchas leyes, como el RGPD en Europa, exigen medidas estrictas para proteger la información de los usuarios.

4. Defensa frente a amenazas en un mundo interconectado

- IoT (Internet de las Cosas): Con más dispositivos conectados (teléfonos, coches, electrodomésticos), los riesgos aumentan. La ciberseguridad protege estos ecosistemas.
- Redes sociales y comunicaciones: Ataques en plataformas como WhatsApp, Instagram o correo electrónico pueden comprometer tanto la privacidad como la reputación.

5. Fomenta hábitos digitales responsables

- Educación y concienciación: Aprender ciberseguridad permite identificar y evitar amenazas, como correos de phishing, enlaces sospechosos o redes Wi-Fi no seguras.
- Empoderamiento del usuario: Una persona informada y con buenas prácticas digitales está menos expuesta a riesgos.

6. Relevancia en Formación Profesional

- Habilidad transversal clave: Cualquier estudiante de FP necesita comprender la ciberseguridad, independientemente del sector, ya que las amenazas digitales son universales.
- Preparación para el mercado laboral: Conocer la ciberseguridad aumenta la empleabilidad y posiciona a los futuros profesionales como colaboradores confiables.
- Responsabilidad en el trabajo: Desde técnicos de sistemas hasta administrativos, todos manejan información sensible que debe ser protegida.

7. Impacto global

- Sostenibilidad digital: Un entorno ciberseguro fomenta un uso responsable de la tecnología.
- Prevención de cibercrimen: Reducir el número de víctimas dificulta las actividades ilegales en la red.
- Estabilidad en infraestructuras críticas: Sectores como energía, salud y transporte dependen de sistemas digitales que deben ser protegidos.

3. TIPOS DE CIBERATAQUES

Los ciberdelincuentes buscan normalmente: robar información personal o empresarial, acceder a cuentas bancarias y redes privadas y/o dañar económicamente a individuos o empresas. Es por ellos que saber reconocer los ciberataques más frecuentes es fundamental como futuros trabajadores así como para protegernos a nivel personal.

Tipos de ciberataques y ejemplos prácticos para reconocerlos:

1.- **Ataques a Contraseñas**

Descripción:

Los ataques a contraseñas buscan obtener acceso no autorizado a sistemas, cuentas o información sensible mediante la obtención o descifrado de contraseñas. Estos ataques explotan la debilidad de las contraseñas utilizadas por los usuarios.

Métodos Comunes:

- Fuerza Bruta: Intentar todas las combinaciones posibles de caracteres hasta encontrar la contraseña correcta.
- Ataques de Diccionario: Utilizar una lista predefinida de palabras comunes y variaciones para adivinar la contraseña.
- Ataques de Credenciales Robadas: Utilizar contraseñas obtenidas de brechas de datos previas.
- Keylogging: Instalar software malicioso que registra las pulsaciones del teclado para capturar contraseñas.

Ejemplos Prácticos:

- Fuerza Bruta en Sitios Web: Un atacante utiliza un programa automatizado para probar miles de combinaciones de contraseñas en una cuenta de correo electrónico hasta encontrar la correcta.
- Phishing para Obtener Contraseñas: Un usuario recibe un correo electrónico que parece provenir de su banco, solicitando que actualice su contraseña a través de un enlace falso. Al hacerlo, el atacante captura la nueva contraseña.
- Reutilización de Contraseñas: Un atacante obtiene una contraseña de una brecha en un sitio web de redes sociales y la utiliza para acceder a la cuenta del usuario en otro sitio donde el mismo usuario ha reutilizado la contraseña.

2. Ataques por Ingeniería Social

Descripción:

La ingeniería social implica manipular psicológicamente a las personas para que divulguen información confidencial, realicen acciones específicas o cometan errores que faciliten el acceso no autorizado a sistemas o datos.

Métodos Comunes:

- Phishing: Envío de correos electrónicos fraudulentos que parecen ser de fuentes confiables para engañar a los usuarios y que revelen información sensible.
- Spear Phishing: Ataques dirigidos a individuos o empresas específicas, utilizando información personalizada para aumentar la efectividad del engaño.
- Pretexting: Crear una falsa identidad o escenario para obtener información confidencial de una víctima.
- Baiting: Ofrecer algo atractivo (como un dispositivo USB gratis) para que la víctima lo utilice, permitiendo así la instalación de malware.

Ejemplos Prácticos:

- Phishing en Redes Sociales: Un usuario recibe un mensaje directo en una red social de alguien que parece ser un amigo, solicitando que haga clic en un enlace para ver una foto que supuestamente compartieron. El enlace lleva a una página falsa que captura sus credenciales.
- Vishing (Phishing Telefónico): Un atacante llama a una víctima fingiendo ser un representante de soporte técnico de su empresa, solicitando que le proporcione su contraseña para "resolver un problema".
- Pretexting para Acceso a la Oficina: Un atacante se presenta en una empresa afirmando ser un empleado de mantenimiento, y solicita acceso a áreas restringidas bajo el pretexto de realizar reparaciones.

3. Ataques a Conexiones

Descripción:

Estos ataques se enfocan en interceptar o manipular las comunicaciones entre dos partes para robar información, espiar actividades o alterar la transmisión de datos.

Métodos Comunes:

- Man-in-the-Middle (MitM): El atacante intercepta la comunicación entre dos partes sin que estas lo sepan, pudiendo leer, modificar o redirigir la información.
- Ataques de Redirección DNS: Alterar las respuestas del DNS para redirigir a los usuarios a sitios web maliciosos.
- Sniffing de Red: Capturar y analizar el tráfico de datos que circula por una red para obtener información sensible.
- Ataques de Suplantación de IP: Falsificar direcciones IP para hacerse pasar por otra máquina en la red y acceder a recursos restringidos.

Ejemplos Prácticos:

- Wi-Fi Público Vulnerable: Un usuario se conecta a una red Wi-Fi pública no segura. Un atacante en la misma red intercepta las comunicaciones del usuario, capturando información sensible como credenciales de acceso y datos bancarios.
- Suplantación de DNS: Un atacante modifica las entradas DNS de una empresa para que los empleados accedan a una página de inicio de sesión falsa, capturando así sus credenciales.
- Ataque MitM en HTTPS: Aunque HTTPS protege las comunicaciones, un atacante puede intentar interceptar y presentar certificados falsos para engañar al usuario y capturar datos sensibles.

4. Malware

Descripción:

El malware (software malicioso) es cualquier programa o código diseñado para dañar, interrumpir, robar o tomar control de sistemas informáticos y redes. Puede infectar dispositivos sin el conocimiento del usuario y realizar diversas acciones dañinas.

Tipos Comunes:

- Virus: Programas que se adjuntan a archivos legítimos y se replican cuando se ejecutan.
- Troyanos: Programas que aparentan ser legítimos pero contienen funciones maliciosas ocultas.
- Ransomware: Malware que cifra los archivos de la víctima y exige un rescate para desbloquearlos.
- Spyware: Software que espía las actividades del usuario y recopila información sin su consentimiento.
- Adware: Programas que muestran publicidad no deseada de manera intrusiva.
- Rootkits: Conjuntos de herramientas que permiten el acceso privilegiado a un sistema sin ser detectados.

Ejemplos Prácticos:

- Ransomware en Empresas: Una empresa es víctima de un ataque de ransomware que cifra todos sus archivos críticos y exige un pago en criptomonedas para proporcionar la clave de descifrado, paralizando sus operaciones hasta que se resuelve.

- Troyano Bancario: Un usuario descarga un software aparentemente útil, como un reproductor multimedia, que en realidad contiene un troyano diseñado para robar información bancaria y credenciales de acceso.
- Spyware en Dispositivos Móviles: Un empleado descarga una aplicación gratuita para gestionar tareas que incluye spyware, permitiendo al atacante monitorear todas sus comunicaciones y movimientos.
- Virus en Correos Electrónicos: Un usuario abre un archivo adjunto en un correo electrónico que contiene un virus, el cual se propaga a través de la red interna de la empresa, infectando múltiples dispositivos y comprometiendo datos sensibles.
- Adware en Navegadores: Un usuario instala una extensión de navegador gratuita que, sin su conocimiento, muestra anuncios constantemente y ralentiza la navegación, además de recopilar datos de uso para fines publicitarios.

4.- CIBERSEGURIDAD PERSONAL: PROTEGE TU DÍA A DÍA

A continuación te presentamos algunas estrategias claves de Ciberseguridad personal para proteger tu día a día:

Uso de dispositivos móviles y ordenadores:

- Mantén actualizado el sistema operativo y las aplicaciones.
- Activa el cifrado en tus dispositivos.
- Usa un gestor de contraseñas para no repetir claves.

Protección en redes sociales:

- Configura tu privacidad para limitar quién puede ver tus publicaciones.
- No compartas información personal, como tu dirección o ubicación.
- Desconfía de mensajes o solicitudes de desconocidos.

Cuidado al navegar por internet:

- Usa navegadores seguros y verifica que las webs tienen https.
- No descargues archivos de sitios no confiables.
- Elimina cookies y limpia el historial regularmente.

Seguridad en correos electrónicos:

- No abras archivos adjuntos de remitentes desconocidos.
- Revisa los enlaces antes de hacer clic: verifica si la URL es legítima.
- Desconfía de correos con errores gramaticales o urgencias exageradas.

Uso seguro de redes Wi-Fi:

- Evita redes públicas para tareas importantes como banca online.
- Usa una VPN para cifrar tu conexión.
- Configura tu router: cambia la contraseña por defecto y activa el firewall.

Protección ante dispositivos externos:

- Escanea con antivirus cualquier USB antes de usarlo.
- Evita conectar dispositivos de procedencia desconocida.

5. RECURSOS

- https://www.incibe.es/ciudadania/formacion/guias/guia-de-ciberataques
- https://www.incibe.es/ciudadania/formacion/talleres
- https://angeles.ccn-cert.cni.es/es/simuladores