TECNOLÓGICA DEL ORIENTE
INSTITUCIÓN DE EDUCACIÓN SUPERIOR

COMPETENCIAS DIGITALES

IDENTIFICACIÓN Y PREVENCIÓN DE CIBERAMENAZAS

IDENTIFICACIÓN Y PREVENCIÓN DE *CIBERAMENAZAS*

Entendiendo las *ciberamenazas*

- ¿Qué son las ciberamenazas? Las ciberamenazas son intentos maliciosos de acceder, dañar o robar información en entornos digitales. Estas amenazas pueden afectar dispositivos, cuentas personales y datos, exponiéndose a riesgos como fraude, robo de identidad y pérdida de información confidencial.

Tipos de *ciberamenazas* comunes

- ***Phishing:*** es una técnica en la que los atacantes intentan engañar para que se comparta información personal a través de correos, mensajes o sitios web falsos. Identificarlos implica reconocer correos o mensajes de remitentes desconocidos, con enlaces sospechosos, errores de gramática o solicitudes urgentes de información.
- ***Malware:*** es un software malicioso que puede instalarse en el dispositivo sin consentimiento. Puedes identificar su presencia si el dispositivo funciona más lento de lo normal, recibe anuncios emergentes constantes o muestra aplicaciones desconocidas.
- **Ataques de fuerza bruta:** Este ataque intenta acceder a las cuentas mediante la adivinación de contraseñas. Notar intentos fallidos de inicio de sesión en las cuentas es una señal de un posible ataque de fuerza bruta.
- **Ataques de ingeniería social:** Estos ataques se basan en la manipulación psicológica para obtener datos o accesos. Los atacantes pueden hacerse pasar por personas de confianza para obtener información. La clave para detectarlos es ser cauteloso con desconocidos que buscan información privada.

Herramientas y prácticas para la prevención de *ciberamenazas*

- **Antivirus y *software* de seguridad:** Instalar y mantener actualizado un antivirus en los dispositivos es esencial. Un buen antivirus puede detectar y bloquear malware y otras amenazas en tiempo real, además de escanear regularmente para eliminar cualquier amenaza potencial.
- **Autenticación en dos factores (2FA):** Activar la autenticación en dos factores para las cuentas más importantes es una forma de protección contra accesos no autorizados. Con 2FA, además de la contraseña, se necesita una segunda verificación, como un código enviado al teléfono.
- **Actualización de *software* y parches de seguridad:** Mantener el sistema operativo, navegador y aplicaciones actualizadas es crucial para reducir el riesgo de ataques.
- **Contraseñas fuertes y únicas:** Crear contraseñas largas y complejas para cada cuenta ayuda a reducir el riesgo de ataques de fuerza bruta. Un gestor de contraseñas permite almacenar contraseñas de forma segura sin necesidad de memorizarlas.

Buenas prácticas para evitar phishing y malware

- No abrir enlaces y archivos adjuntos sospechosos: Si recibes un mensaje de un remitente desconocido, evita abrir enlaces o descargar archivos. Verifica la autenticidad revisando el remitente y confirmando con la persona o entidad.
- Verificación de la autenticidad de los sitios web: Antes de ingresar datos en una página, asegúrate de que la URL esté bien escrita y comience con “https://”.
- Educación y conciencia digital: Mantenerse informado sobre técnicas y tendencias de ciberamenazas permite estar alerta y mejor preparado para identificar intentos de fraude.