**¿Qué es la Ciberseguridad?**

En palabras sencillas, la ciberseguridad es el conjunto de **prácticas, tecnologías y procesos** que se diseñan para proteger las **redes, dispositivos, programas y datos** de **ataques, daños o accesos no autorizados**.

es como tener un **guardaespaldas digital**, para todo lo que haces en tu computadora, teléfono o en internet

El objetivo principal es garantizar tres cosas para tu información:

**Confidencialidad:** Que solo tú y las personas autorizadas puedan ver tus datos (como si fuera un sobre sellado).

**Integridad:** Que tus datos no sean modificados o borrados sin tu permiso (que un documento no sea alterado).

**Disponibilidad:** Que puedas acceder a tus sistemas y datos cuando los necesites (que tu cuenta bancaria esté accesible).

**¿De qué protege?**

Protege contra amenazas como:

**Virus y Malware:** Programas maliciosos que intentan dañar o tomar el control de tu dispositivo.

**Hackers:** Personas que intentan entrar en tus sistemas para robar información o causar problemas.

**Phishing:** Engaños (a menudo por correo electrónico) para que reveles contraseñas u otra información sensible.

La **Ingeniería Social** y el **Fraude** son amenazas cibernéticas que se basan en la manipulación psicológica del usuario en lugar de aprovechar vulnerabilidades técnicas del sistema.

La **Ingeniería Social** se define como el conjunto de técnicas empleadas por los delincuentes para **engañar a los usuarios**. El objetivo principal de estas técnicas es lograr que la víctima les facilite datos de valor, como **credenciales** o información sensible sobre los sistemas o servicios instalados.

Ataques y Amenazas Específicas

Diversas amenazas y ataques se basan en la suplantación de identidad y el engaño que proporciona la ingeniería social:

|  |  |
| --- | --- |
| Amenaza/Ataque | Descripción y Propósito |
| Phishing | Es una técnica o tipo de ataque en el que alguien **suplanta a una entidad/servicio** (usando suplantación de identidad) para conseguir las **credenciales** o información de tarjeta de crédito de un usuario. Esto se logra mediante un correo electrónico o mensaje instantáneo que contiene un enlace a un sitio web fraudulento que suplanta al legítimo. |
| Spear Phishing | Es una modalidad de *phishing* **dirigida contra un usuario u organización en concreto**. Los atacantes buscan información confidencial mediante un correo electrónico que aparenta ser de un conocido o de una empresa. |
| Caza de Ballenas (Whaling) | Es un **ataque de ingeniería social** que constituye una variante del *spear phishing*. Está dirigido a **ejecutivos de alto nivel** de la organización. Su fin es obtener sus claves, contraseñas e información confidencial para acceder y controlar los sistemas de información de la empresa. |
| Scareware | Es un tipo de estafa que usa **técnicas de ingeniería social** mediante ventanas emergentes repetitivas que intentan hacer creer al usuario que su equipo es víctima de una amenaza seria, para así venderle un **software falso**. A través de esta trampa, los atacantes buscan obtener datos bancarios y acceder al dispositivo de la víctima. |
| Cartas Nigerianas  Estafa N°419 | Es una comunicación inesperada (correo electrónico, carta o mensajería instantánea) donde el remitente promete **negocios muy rentables**. El gancho es la expectativa de ganar dinero fácil para involucrar a las víctimas en una situación engañosa y conseguir que transfieran una fuerte cantidad de dinero para llevar a cabo la supuesta operación. |
| Bulo (Noticia Falsa) | Es un mensaje falso muy llamativo que busca difundir mentiras, lograr que el usuario visite una web maliciosa o recopilar direcciones de correo electrónico. |

Principales Tipos de Malware

• **Virus**: Es un malware que **infecta ficheros ejecutables**. Su principal característica es que se adjunta a aplicaciones existentes para poder replicarse.

• **Gusano (Worm)**: A diferencia de los virus, los gusanos **se propagan automáticamente a través de redes**, creando copias de sí mismos para infectar otros ordenadores sin necesidad de intervención humana.

• **Troyano (Trojan)**: Es un malware que se disfraza para engañar al usuario. Su función más común es crear una **puerta trasera (*backdoor*)** en el equipo infectado para que un atacante pueda controlarlo remotamente. Los ordenadores infectados por troyanos se conocen como **bots o zombies**. Más del 80% del malware actual corresponde a troyanos.

• **Spyware (Programa espía)**: Recopila información de un ordenador, como las teclas que se pulsan (**keylogger**), y la envía a una entidad remota sin el conocimiento del usuario.

• **Ransomware**: Este tipo de malware **"secuestra" la información** de un dispositivo, usualmente cifrándola, y exige el pago de un rescate a la víctima para poder recuperarla.

• **Adware**: Es un software que muestra anuncios para financiarse. En algunos casos, se considera malware, especialmente si se instala sin consentimiento y recopila datos del usuario.

• **Rootkit**: Permite a un atacante obtener un **acceso continuo y oculto a un dispositivo** con privilegios de administrador, dificultando su detección.

• **Bomba Lógica**: Es un código malicioso insertado en un programa que permanece oculto hasta que se cumple una condición preprogramada, momento en el que se activa.

• **Scareware**: Es una estafa que utiliza la **ingeniería social**. Muestra ventanas emergentes que intentan asustar al usuario haciéndole creer que su equipo está infectado para venderle un falso software de seguridad.

El Malware en el Contexto de los Ataques

El malware es el vehículo para ejecutar diversos tipos de ataques:

• **Ataques Combinados**: Son ataques muy agresivos que utilizan una combinación de virus, gusanos y troyanos para propagarse rápidamente y causar daños graves.

• **Amenazas Avanzadas Persistentes (APT)**: Son ataques sigilosos y de larga duración, a menudo patrocinados por estados o grandes organizaciones. Utilizan malware y *exploits* (programas que aprovechan vulnerabilidades) para vigilar y robar datos de forma continua.

• **Ataques de Ingeniería Social**: Técnicas como el **phishing** a menudo utilizan malware. Un correo fraudulento puede contener un enlace a una web maliciosa o un fichero adjunto que, al ejecutarse, instala un troyano u otro malware en el equipo de la víctima.

Las extorsiones telefónicas más comunes identificadas por las Autoridades de Seguridad Pública / Ciudadana y Procuración de Justicia Mexicanas:

1. **Por Amenaza Directa y Secuestro:**
   * **Secuestro virtual de un familiar:** El más agresivo; amenaza de violencia o asesinato contra un familiar supuestamente secuestrado (incluso con simulación de voz) exigiendo grandes sumas rápidamente.
   * **Amenaza de muerte o secuestro:** Se utiliza un tono agresivo, se afirma que la víctima o su familia están vigiladas (a veces con datos reales obtenidos en línea) y se exige dinero para evitar el daño.
2. **Por Simulación de Problemas Legales o Detención:**
   * **Extorsión carcelaria:** Simulan la detención de un conocido de la víctima y exigen dinero para su liberación, usando un tono profesional y apurado.
   * **Familiar proveniente del extranjero detenido:** Se hacen pasar por un familiar lejano detenido en aduanas por traer regalos y piden dinero para su liberación.
   * **Amenaza de supuestos funcionarios gubernamentales:** El delincuente se identifica como una autoridad federal y exige dinero para no remitir a un familiar supuestamente detenido a las autoridades competentes.
   * **Extorsión por adeudo:** Usan tono profesional y confidencial, con información parcial de la víctima, y exigen el pago rápido de una supuesta deuda (a veces con un conocido como aval) bajo amenaza de consecuencias, pidiendo colocar objetos de valor en una maleta para ser recogidos.
   * **Deudas contraídas:** Simulan ser una institución bancaria o cobradora, utilizando términos financieros para convencer a la víctima de pagar una deuda (a veces inexistente) para evitar un embargo, alternando tonos agresivos y amables.
3. **Por Engaño o Suplantación de Identidad:**
   * **Extorsión familiar:** Se hacen pasar por un familiar o pariente cercano (a veces iniciando con preguntas ambiguas como "¿está mi tío?") para solicitar dinero bajo pretextos como pagar una deuda o comprar un regalo.
   * **Extorsión por negocios:** Llaman a un local comercial, se hacen pasar por socios o de otra sucursal y exigen una transferencia rápida de dinero por una supuesta emergencia.
4. **Por Falsa Recompensa:**
   * **Extorsión por recompensa:** Notifican falsamente a la víctima sobre la obtención de un premio (viaje, auto, dinero, etc.) y condicionan la entrega a un depósito bancario, insistiendo en que el valor del premio es mayor al depósito solicitado.

**Elementos Clave en la Extorsión Telefónica:**

* **Urgencia y Presión:** En modalidades como el **secuestro virtual** o la **extorsión carcelaria** y **por adeudo**, el delincuente impone un lapso de tiempo corto para el pago. El objetivo es evitar que la víctima cuelgue, piense, o consulte a un familiar o a la policía.
* **Manipulación Emocional:** El **secuestro virtual** y la **amenaza de muerte** utilizan el miedo y la preocupación por la seguridad de la familia. La **extorsión familiar** usa lazos afectivos o de confianza.
* **Uso de Información (Ingeniería Social):** Los delincuentes a menudo inician con preguntas vagas ("¿eres José?") para que la víctima **provea la información crucial** (como nombres de familiares) o utilizan **datos reales** obtenidos de directorios, redes sociales o internet para hacer la amenaza más creíble, como en la **amenaza de muerte o secuestro** y la **extorsión por adeudo**.
* **Simulación de Autoridad o Profesionalismo:** En la **extorsión carcelaria**, por **adeudo**, o de **supuestos funcionarios gubernamentales**, el tono es apurado, profesional o de autoridad, lo que dificulta que la víctima cuestione la legalidad o veracidad de la llamada.
* **Bloqueo Mental:** El uso de tonos agresivos, vulgares, o la presentación de datos reales provoca un **bloqueo mental** en la víctima, haciendo que sea más vulnerable a las demandas del extorsionador.
* **Fácil Mecanismo de Pago:** La exigencia de depósitos bancarios, transferencias rápidas o la entrega de objetos de valor en una maleta son métodos que buscan la **rapidez** y la **anonimidad** del delincuente.