CÓMO NO SER UNA PRESA EN INTERNET

Johan Astudillo

CÓMO NO SER UNA PRESA EN INTERNET
https://www.filetechn.com

Dedicatoria

Quiero agradecer primeramente a Dios y a la vida por permitirme arribar hacia el conocimiento, logrando los objetivos propuestos. También agradecer a mis padres por la orientación y apoyo en el camino recorrido, sobre todo en la carrera que siempre me ha apasionado, la cual me llevó a escribir este libro.

SINOPSIS

El objetivo de este libro es analizar la seguridad informática, desde el punto de vista de la víctima, descubrir cuáles son sus debilidades ante los cambios tecnológicos en el mundo, sobre todo conocer cuáles son los ataques que más utilizan los cibercriminales para robar, extorsionar, espiar o corromper nuestra información.

Todos existimos digitalmente, nuestras cuentas bancarias, las compras que realizamos en línea gracias al comercio electrónico, nuestros perfiles en redes sociales, los chats que enviamos a diario, los datos que recopilan las empresas y el gobierno, sabiendo esto, es imposible no pensar en cómo proteger nuestra seguridad dentro de Internet.

Este libro fue escrito para que personas no técnicas, profesionales y empresas, se introduzcan a la seguridad informática y puedan navegar a través de la Web y el Internet de manera segura, explicando cómo no convertirte en una presa en Internet con ejercicios prácticos.

INDICE

Dedicatoria 2

SINOPSIS 3

INDICE 4

AUTOR DEL LIBRO 8

1. INTRODUCCIÓN Y CONCEPTOS 9

1.1. QUÉ DEBEMOS PROTEGER 9

1.1.1. Cuentas bancarias o tarjetas de crédito 9

1.1.2. Nuestras identidades 10

1.1.3. Contraseñas. 10

1.1.4. Conversaciones 11

1.1.5. Fotos y vídeos 11

1.1.6. Claves Wi-fi 12

1.1.7. Cualquier dispositivo electrónico 12

1.2. DE QUIÉN NOS PROTEGEMOS 12

1.2.1. Hackers de sombrero negro 12

1.2.2. Script kiddies 13

1.2.3. Familiares 13

1.2.4. Amigos 13

1.2.5. Pareja 13

1.2.6. Asaltantes 13

1.3. DIFERENCIA ENTRE INTERNET Y WEB 14

1.4. PROTOCOLOS 14

2. CONSERVA TUS CUENTAS Y REDES SOCIALES SEGURAS 16

2.1. CONTRASEÑAS SEGURAS Y NO SEGURAS 16

2.1.1. Consejos para una contraseña segura 17

2.1.2. Escoge tu contraseña segura. 18
2.2. AUTENTICACIÓN EN DOS PASOS 23
2.2.1. Activar autenticación en dos pasos 24
2.3. SEGURIDAD EN REDES SOCIALES 27
2.3.1. Cuentas privadas y suplantación de identidad 28
2.3.2. Ubicaciones 29
2.3.3. Marketing dirigido al comportamiento 29
2.3.4. Tor y DuckDuck Go 30
2.4. POSIBLES ATAQUES 31
2.4.1. Ataque de fuerza bruta 31
2.4.2. Ataque de diccionario 31
2.4.3. Phishing 32
2.4.4. Keylogger 32
3. COMPRAS ONLINE SEGURAS 33
3.1. PRINCIPALES MIEDOS A COMPRAR EN LÍNEA. 33
3.2. COMBATIR EL MIEDO DE COMPRAR ONLINE 34
3.3. CUIDADO CON LOS SITIOS NO SEGUROS 34
3.4. CUIDADO CON LOS NOMBRES DE DOMINIO 35
3.5. PHISHING POR CORREO ELECTRÓNICO 35
3.6. NÚMERO DE SEGUIMIENTO 36
3.7. COMPRAS EN TIENDAS DE INSTAGRAM 36
3.8. ¿POR QUÉ LOS PRECIOS SON MÁS BAJOS? 37
3.9. POSIBLES ATAQUES 37
3.9.1. Troyanos 37
3.9.2. Spyware 38
3.9.3. Phishing 38
3.9.4. Keylogger remoto 38

4. SEGURIDAD EN REDES LOCALES E INALÁMBRICAS 39
4.1. REDES LAN Y WAN 39
4.2. NAVEGACIÓN SEGURA 40
4.3. REDES INALÁMBRICAS 41
4.4. PROTOCOLOS WI-FI 41
4.4.1. Saber cuál es la seguridad de mi red Wi-Fi 43
4.5. PERSONAS CONECTADAS A MI RED 44
4.6. POSIBLES ATAQUES 46
4.6.1. ARP Spoofing 46
4.6.2. Ataque de hombre en el medio 46
4.6.3. Ataque de denegación de servicio 47
4.6.4. Escaneo de puertos 47
4.6.5. OS Finger Printing 47
5. INGENIERIA SOCIAL 49
5.1. VULNERABILIDADES HUMANAS 49
5.2. POSIBLES ATAQUES DE INGENIERÍA SOCIAL 50
5.2.1. Dumpster diving o trashing 50
5.2.2. Eavesdropping 51
5.2.3. Phishing 51
5.2.4. Piggybacking y tailgating 52
5.2.5. Llamadas y mensajes falsos 52
5.2.6. Deepfake 53
5.2.7. Baiting 54
5.2.8. Bribing 54
5.2.9. Office snooping 55
5.2.10. Shoulder surfing 56
5.2.11. Suplantación 56

5.2.12. Extorsión 57
5.3. INGENIERÍA SOCIAL CON UNA MIRADA POSITIVA 58
6. SEGURIDAD EN DISPOSITIVOS 59
6.1. PROTECCIÓN DE MALWARE 59
6.2. TIPOS DE MALWARE 61
6.2.1. RootKit 61
6.2.2. Ransomware 62
6.2.3. Adware 62
6.2.4. Gusanos 62
6.2.5. Botnet 62
6.2.6. Virus informático 63
7. ATAQUES QUE NO PUEDES EVITAR 64
7.1. EXPLOITS 64
7.2. ZERO DAY 64
7.3. VULNERABILIDADES MÁS PELIGROSAS 65
7.4. CIBERGUERRA 66
7.5. EJEMPLO DE ZERO DAY 66
7.6. CONTRAMEDIDAS 67

AUTOR DEL LIBRO

JOHAN ASTUDILLO

Ingeniero de Sistemas y especialista en Seguridad informática en: Universidad Santiago de Cali, Universidad Autónoma de Occidente. Actualmente, me desempeño como Ingeniero de datos en reconocida empresa Internacional con casa matriz en Inglaterra. Creador de FileTech Tecnología y Tutoriales (filetechn.com) y desarrollador móvil independiente de aplicaciones como: **ImagePDF, TranslatorPRO, ImageText, LinkaaP, CopyText**, entre otras.

1. INTRODUCCIÓN Y CONCEPTOS

Todos somos vulnerables, nuestros dispositivos electrónicos tienen una infinidad de información que cualquier atacante le gustaría interceptar y aprovechar, para ello debemos contar con pequeños conceptos de seguridad que nos ayudaran a la hora de poder navegar en internet y usar nuestros dispositivos electrónicos con seguridad y confianza.

La seguridad de nuestra información es importante, todos tenemos algo que proteger, algo que no queremos enseñar al mundo y no tenemos que irnos muy lejos, nuestras identidades están en la nube, nuestras cuentas bancarias también se encuentran en la nube, podemos tener más información digitalizada en nuestros dispositivos y redes que la de un gobierno, personas o entidades puedan saber sobre nosotros. Por lo anterior, se concluye que todos somos vulnerables, la diferencia es que todos no cuidamos la misma información.

¿Qué información tenemos en nuestros dispositivos? ¿Qué podemos hacer para protegernos?

¿Cómo los atacantes roban nuestra información? ¿Qué técnicas usan?

Te responderás estas preguntas a medida que avances en el libro, verás la importancia de la seguridad informática en la sociedad y en general en el mundo actual también sabrás como defenderte de cualquier atacante.

1.1. QUÉ DEBEMOS PROTEGER

1.1.1. Cuentas bancarias o tarjetas de crédito

Tienes una cuenta de Amazon, Netflix, Mercado libre, eBay, Wish o en cualquier servicio electrónico y realizas alguna compra, probablemente habrás puesto tu tarjeta de crédito. ¿sabías que algunos de estos servicios no dejan que quites tu

tarjeta? Si tienen la opción, no es clara para los usuarios, obviamente para que compren más en sus servicios. Pero ¿qué pasaría si un atacante entra a tu cuenta y empieza hacer cobros masivos a tu tarjeta de crédito?

Los atacantes también usan un ataque llamado phishing para capturar tus tarjetas de crédito, si tu ingresas tus datos en un formulario que se ve como "una página oficial" de tu banco, así lograran obtener tu tarjeta de crédito.

1.1.2. Nuestras identidades

Es muy fácil robar nuestra identidad, compartimos absolutamente todo y a todas las personas, en redes sociales tenemos públicas nuestras fotos, significa que personas que no son nuestros amigos pueden acceder a ellas; en Instagram tenemos nuestra cuenta pública, cualquiera que quiera suplantar nuestra identidad puede hacerlo por medio de las redes por eso tenemos que poner configuraciones de seguridad.

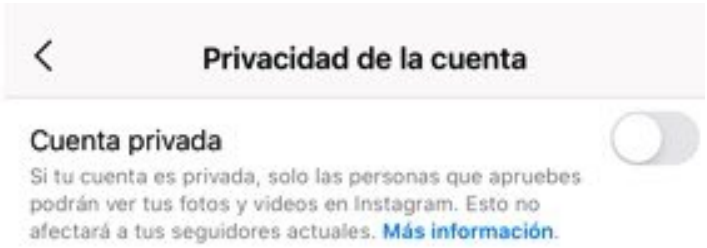


Figura 1.1. Imagen de ejemplo de una cuenta pública en Instagram

1.1.3. Contraseñas.

Hace poco leí en un libro de seguridad informática que decía: "si ocultas el pin cuando insertas la tarjeta en un cajero automático, ¿por qué no tener ciertas precauciones con el teclado del PC?" (Jesús Costas, 2011).

Las contraseñas no se deben compartir con nadie, nuestras contraseñas siempre deben estar seguras ya que normalmente es el primer paso para autenticarnos. Veremos cómo mantenerlas seguras en el siguiente capítulo.

1.1.4. Conversaciones

Los famosos y empresarios no son los únicos que se deben cuidar en este sentido, la mayoría de las personas tienen conversaciones con amigos, familia y pareja que deben mantener confidenciales; imagina una situación donde hables de otra persona, por ejemplo, hablar de un familiar de una manera ofensiva y esa persona se entere, ¿qué podría pasar? Las conversaciones privadas son otra manera en que nos podrían extorsionar si no tenemos precauciones.

1.1.5. Fotos y vídeos

Google Fotos y la biblioteca de fotos de iCloud en iPhone, pueden tener nuestras fotos confidenciales, incluso sólo en nuestro smartphone tenemos cantidad de fotos y muchas de estas no quisiéramos que las viera todo el mundo. ¿Sabías que las fotos no se eliminan cuando le das el botón de eliminar? Lo que se borra es la ruta del archivo, no la foto, así la foto no se va encontrar como anteriormente lo hacíamos antes de borrarla, el dispositivo muestra espacio disponible que antes era el de la foto y se va modificando mientras usamos el almacenamiento de nuestro dispositivo, después de varias modificaciones la foto queda casi irrecuperable, con un simple programa de recuperación de imágenes, podemos volver a tenerla si aún no se ha modificado y si alguien captura tus fotos borradas hace años, con fines maliciosos no dudara usarlas en tu contra.

Figura 1.2. Ejemplo donde está nuestra nube de fotos de un iPhone en icloud.com

Incluso los metadatos de las fotos dicen información precisa de la foto, los metadatos son datos que describen otros datos, por ejemplo, fecha y hora de la foto, ubicación precisa donde se capturo la foto, modelo del dispositivo y la versión del sistema operativo. Mucha información precisa que por supuesto puede ser sensible.

1.1.6. Claves Wi-fi

Cada vez que estas conectado a una red Wi-Fi y envías datos a través de esa red, ya sea para comunicarte con alguien o consumir multimedia, todas las peticiones ingresan a tu Router, así que para las personas que se encuentran en la red no será muy difícil saber los protocolos por los que navegas y pueden interceptar todo el tráfico que pasa por tu red. A los cibercriminales se les hace un trabajo más sencillo si se encuentran conectados a la red de su objetivo; por esa y muchas razones la contraseña del Wi-Fi no se comparte con ningún desconocido. Una empresa por lo general aísla su red cableada con su red inalámbrica precisamente con este fin, pero como no somos una empresa, normalmente el Wi-Fi está conectado con nuestra red de cable.

1.1.7. Cualquier dispositivo electrónico

Los dispositivos electrónicos cada vez tienen más información sobre nosotros, en este punto se trata de abarcar todo, ya que tenemos una computadora en nuestras manos y una gran cantidad de información, todos accedemos a infinidad de aplicaciones móviles en las cuales compartimos nuestros datos, esto se traduce a que si logran entrar a nuestro dispositivo accederán a toda la información y podrán usarlo con fines maliciosos.

1.2. DE QUIÉN NOS PROTEGEMOS

En este apartado, se mostrará de quien debemos protegernos, ya hemos visto que debemos proteger, pero exactamente, ¿quiénes son esas personas?

1.2.1. Hackers de sombrero negro

Los hackers de sombrero negro son los cibercriminales, los que roban, los que extorsionan, los que envían virus masivos, no se debe confundir con los hackers de sombrero blanco, que son los buenos quienes trabajan en empresas y mejoran la seguridad de los sistemas. Aunque tú no creas que un hacker de sombrero negro se fijaría en ti, en realidad es que las personas del común son las más vulnerables, ya que normalmente son fáciles de hackear y extorsionar. En una persona sin "poder" o sin fama, se les hace menos complicado robar sus tarjetas de crédito, suplantar la identidad, extorsionar o cualquier objetivo maligno que se planteen.

1.2.2. Script kiddies

Contrario a los hackers de sombrero negro, los scripts kiddies son personas sin conocimiento técnico que usan herramientas de otros para vulnerar sistemas, sin saber cómo funcionan y su único objetivo es impresionar sin el fin de conseguir dinero como los hackers de sombrero negro, sólo quieren llamar la atención. Sin embargo, un script kiddies puede entrar a tus cuentas, ver toda tu información con tal de satisfacer su necesidad.

1.2.3. Familiares

En este caso se refiere a cualquier persona que viva contigo, que comparta la misma red, no necesariamente un familiar tuyo que quiera corromper tu información, sino que, al compartir la misma red, todos son vulnerables en ella. Si un dispositivo llega a infectarse de malware, puede replicarse en la red en la que se encuentra, como un gusano informático que se replica a través de una red de computadoras y pueden ralentizar tus equipos.

1.2.4. Amigos

Es cierto que no todos son tus verdaderos amigos, muchos pueden hacerse pasar por ti, tal vez no sean los amigos que tienes hace mucho tiempo, aunque podría ser, esto normalmente ocurre con los que conoces recientemente. Estas personas usan algo llamado "ingeniería social" para conseguir su objetivo de corromper tu información y si la forma es ganando tu confianza tu confianza para ser tu amigo, el hará todo lo posible para que también confíes en él. En otros capítulos hablaremos más de la ingeniería social.

1.2.5. Pareja

Eres de los que creen que su pareja nunca haría esto o incluso eres de los que piensa hacer algo así, debes saber que es ilegal, no importa si dices "lo hago por amor" o "es mi pareja yo puedo hacerlo" esto trae muchas consecuencias en las leyes de delitos informáticos de diferentes países, a parte de una multa, puedes ir a la cárcel.

1.2.6. Asaltantes

En este caso los asaltantes hurtan nuestros equipos, al tener nuestra información en el dispositivo, pueden entrar a estos, si no contamos con medidas de

seguridad, ¿qué crees que un ladrón podría hacer con tu información? Seguro pedir alguna recompensa, depende de la clase que sea, divulgarlo sin problemas.

1.3. DIFERENCIA ENTRE INTERNET Y WEB

Internet y web no son lo mismo, aunque pueda existir cierta ambigüedad entre estos dos términos, su significado es totalmente diferente, pese a que se complementan.

Internet, es una red masiva, es la llamada red de redes, ya que comunica a todas las redes del mundo en una, siempre y cuando los computadores se encuentren conectados a internet, toda la información que viaja por aquí funciona a través de protocolos como la familia de protocolos TCP/IP para intercambiar archivos.

En cambio, la World Wide Web (Web) es una manera en la que accedemos a la información que se encuentra en internet, así que la web es parte de internet, lo que se confunde es que cuando accedemos al navegador todo lo que aparece en ellos suele formar parte de la web, así que tú usas internet para acceder a la web, en la web las páginas están interconectadas a través de los links y la web usa el protocolo http.

1.4. PROTOCOLOS

Los protocolos son la forma de comunicación entre las computadoras, son unas reglas en las cuales se estandariza el intercambio de información en las actividades informáticas, no es tan diferente cuando dos personas se encuentran y se saludan, los dispositivos también tienen reglas de comunicación y lo hacen por medio de los protocolos, estos garantizan compatibilidad entre los dispositivos conectados.

Algunos protocolos son:

- FTP: Protocolo de transferencia de ficheros, se usa para él envió y la recepción de archivos a través de una red.
- HTTP: Protocolo de transferencia de hipertexto, permite realizar peticiones de datos y recursos, es el protocolo de la web.

- HTTPS: Extensión del HTTP que cifra los datos de extremo a extremo, por lo tanto, es un canal seguro de comunicación y no se pueden interceptar los datos.
- POP: Protocolo de oficina postal, es el protocolo de correo electrónico para clientes de Email, como Outlook o Gmail.
- Telnet: Protocolo que permite tener acceso a equipos remotos
- TCP: Está diseñado para proporcionar un servicio comunicación punto a punto entre dos hosts.

2. CONSERVA TUS CUENTAS Y REDES SOCIALES SEGURAS

Si alguna vez te han hackeado una cuenta de alguna red social o alguna cuenta a través de Internet, es probable que no hayas contado con los mecanismos de defensa para evitar posibles ataques. Vamos a explorar los diferentes mecanismos de defensa que podemos implementar para proteger nuestra información en la red social Facebook ya que es de las más usadas en la actualidad, pero puede funcionar con Gmail o cualquier otra cuenta por Internet.

2.1. CONTRASEÑAS SEGURAS Y NO SEGURAS

Cuales NO son contraseñas seguras:

- Nombre de la mascota.
- Nombre de los familiares.
- Nombre de la pareja.
- Fechas importantes o de nacimientos.
- Números secuenciales
- Celebridades favoritas.
- Películas y series favoritas.
- Contraseñas sin alguna mayúscula.
- Contraseñas sin números.
- Contraseñas sin caracteres.
- Animales
- Usar palabras de diccionario

Ejemplos de contraseñas inseguras:

- daniel1998.

- 123thewalkingdead.
- qwerty.
- 123456siete.
- elefante1.
- maria2017.
- 1234.
- Contraseña.
- admin.
- Misifugato.
- pusilánime.

2.1.1. Consejos para una contraseña segura

Los que quieran descubrir tu contraseña, intentaran con miles de ataques y formas para que la contraseña se revele, para ello debemos contar con algunos conceptos de una contraseña segura y aplicarlos.

- Una contraseña ideal debe tener mínimo 10 y 14 caracteres.
- Usa mayúsculas, número y caracteres además de texto.
- Usa palabras y frases que te sean fáciles de recordar a excepción de las más obvias para algún atacante, como las que mostramos.
- Si la plataforma lo permite, usa también la barra espaciadora.
- **Cámbialas constantemente**, por ahí cada mes o cada 3 meses, en los sitios que más usas o más te preocupan su información.
- **No uses la misma contraseña** para todas tus redes sociales y cuentas.
- **No confíes en las preguntas de seguridad,** esas preguntas que cuando olvidas tu contraseña te aparecen como modo de recuperación, tienes que utilizar palabras que no son las verdaderas, por si alguien las averigua, podría hacer un ataque de ingeniería social.

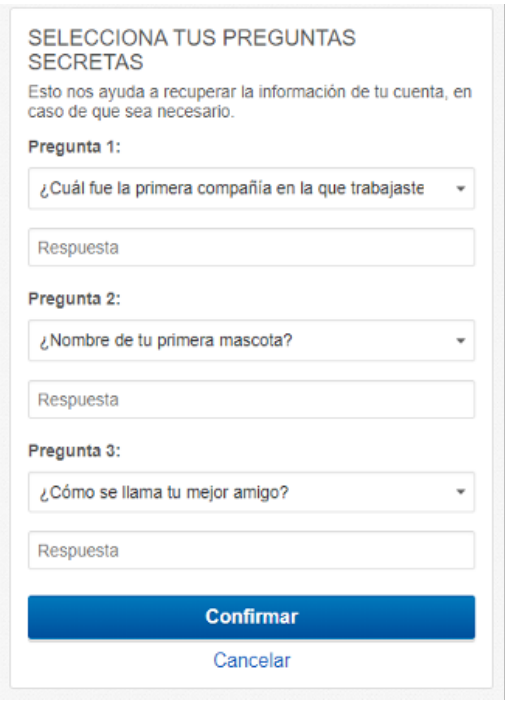


Figura 2.1. Ejemplo de preguntas de seguridad de Ebay.com

2.1.2. Escoge tu contraseña segura.

Para lograr una contraseña segura, **vamos a pensar algo fácil de recordar como una frase "este día es para sonreír"** esta es perfecta, a pesar de servirnos como contraseña, tiene dos tildes asegurando una capa más de seguridad, ¿Sabías que los programas de hackeo no detectan la ñ ni tildes? Normalmente se basan en texto y números en la computación la ñ y las letras con tilde son tomados como caracteres y no texto plano, continuando con el proceso de la contraseña podemos cambiar letras por números de la manera siguiente **"3st3 dí4 3s p3rf3ct0 p4r4 s0nr3ír"** dejando las tildes si es que la aplicación lo permite y aún podemos hacerla más segura, poniendo 2 mayúsculas **"3st3 Dí4 3s p3rf3ct0 P4r4 s0nr3ír"** ahora para hacerla más segura podemos agregar caracteres reemplazando algunos espacios (los espacios cuentan como caracteres) y agregando uno al principio por ejemplo **"_3st3 Dí4_3s p3rf3ct0 P4r4_s0nr3ír".** A una computadora moderna por más rápida que sea le llevaría muchísimos años descifrar una contraseña de este tipo.

La contraseña inicial quedaría:
este día es perfecto para sonreír

La contraseña final:
_3st3 Dí4_3s p3rf3ct0 P4r4_s0nr3ír

Lo que haremos es dirigirnos a Facebook o cualquier otra cuenta y cambiaremos la contraseña insegura por una segura.

Figura 2.2. Ejemplo de configuración en Facebook imágenes capturadas con fines educativos

1. Vamos a dirigirnos al panel derecho y vamos a seleccionar configuración.

2. Ahora en el panel izquierdo seleccionamos la opción de **seguridad e inicio de sesión** y en **cambiar contraseña le damos editar** y escogemos la contraseña.

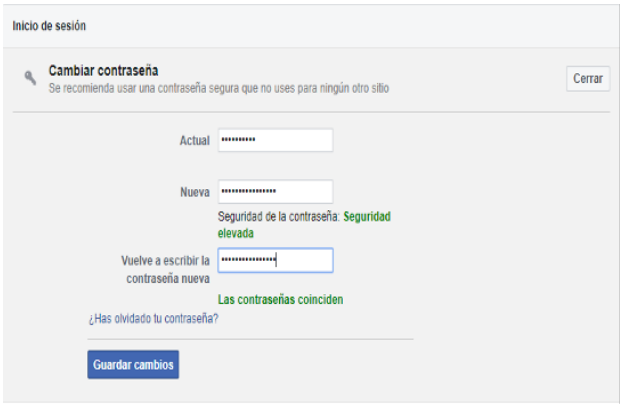


Figura 2.3. Cambio de contraseña

3. La contraseña se habrá actualizado, para mayor seguridad le vamos a dar revisar otros dispositivos, para ver si no nos hemos conectado en una ubicación desconocida.

***Figura 2.4.** La contraseña se cambió correctamente.*

El problema de una contraseña segura es que la gente la olvida muy fácil y ya no se pueden acordar, pero aquí te enseño algunas herramientas que pueden descargar en la Play Store para Android o App Store para iPhone, un administrador de contraseñas, esto les va a servir para almacenar sus contraseñas en un sitio "seguro".

Algunas herramientas que pueden descargar son: **LastPass, 1Password, Dashlane.** Veamos cómo proteger tus contraseñas con **LastPass:**

1. Una vez descargado LastPass desde la Playstore o App Store, vamos a abrir la aplicación y **nos vamos a crear una cuenta**.

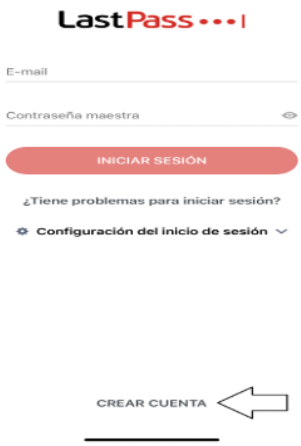


Figura 2.5. Crear cuenta en LastPass

2. Nos solicitara nuestro correo electrónico, ponemos un correo que usemos y que se encuentre activo, agregamos una contraseña que podamos recordar con las características que nos pide.

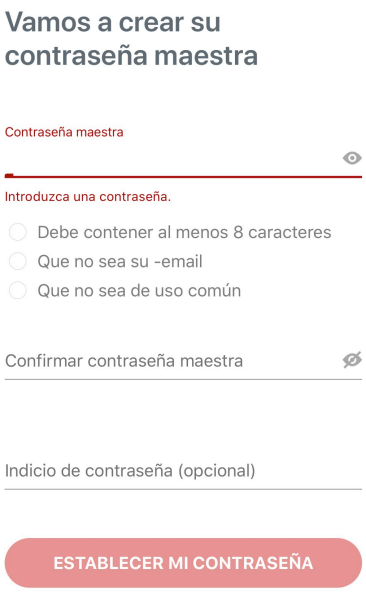


Figura 2.6. Crear una nueva contraseña

3. Si queremos podemos usar una autenticación biométrica, por ejemplo, con un iPhone con reconocimiento facial podemos usar Face ID

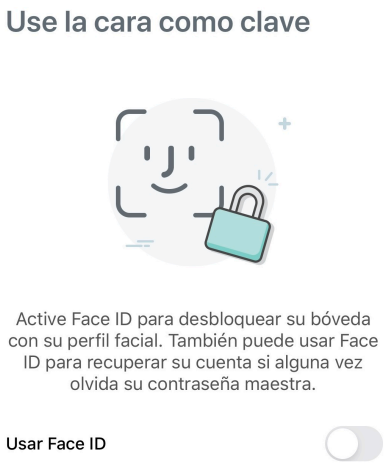


Figura 2.7. Activar Face ID

4. Seleccionamos en cual cuenta queremos guardar nuestra contraseña, este caso fue Facebook.

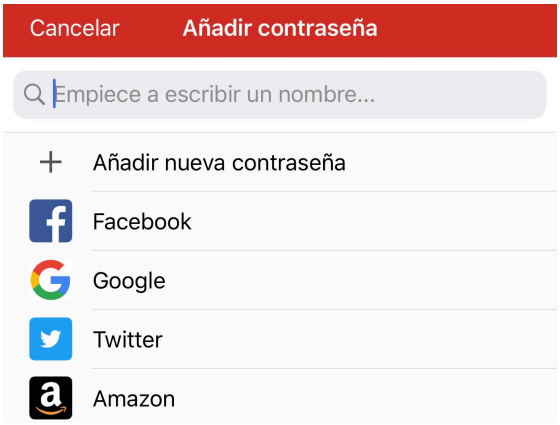


Figura 2.8. Seleccionar cuenta

5. En nombre de usuario **introducir nuestro Email y en contraseña nuestra clave** segura.

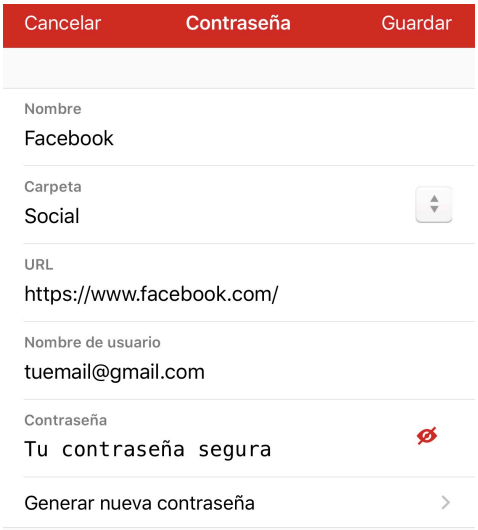


Figura 2.9. Introducir datos

6. Después podemos acceder a nuestra contraseña cada vez que la necesitemos.

Figura 2.10. Contraseña guardada

2.2. AUTENTICACIÓN EN DOS PASOS

Sin embargo, te estarás preguntando, ¿si entran a mi LastPass encuentran todas mis claves? Esto es completamente cierto, si encuentran como acceder a tu

administrador de contraseñas robaran todas tus claves, una forma de defenderse de que pase esto, es la autenticación en dos pasos.

La autenticación en dos pasos es un nivel de seguridad más, además de las contraseñas, es otra forma de validar que efectivamente somos nosotros que estamos intentando acceder a la información.

En palabras simples como define la autenticación la página de Google.com/landing/2step.

1. Introducimos nuestra contraseña

2. Se nos pedirá algo más, como un código que llega a nuestro teléfono mediante mensajes, llaves o llamadas de voz.

2.2.1. Activar autenticación en dos pasos

Para este ejemplo volveremos a usar la red social Facebook y procederemos a activar la autenticación en dos pasos, debemos tener en cuenta que esto sirve para otras cuentas como la de Google, Microsoft y muchos servicios diferentes.

1. En **configuración** en el panel izquierdo, volvemos a ir a **seguridad e inicio de sesión** y **seleccionamos la opción de autenticación en dos pasos**

Figura 2.11. Autenticación en dos pasos

2. Seleccionamos cual será nuestra autenticación en dos pasos, en este caso **seleccionare por mensaje de texto (SMS)**

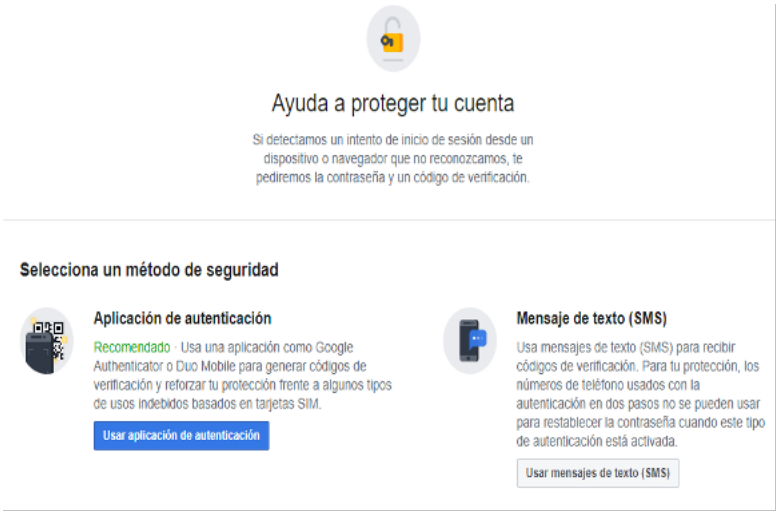


Figura 2.12. Ejemplo de métodos de seguridad

3. Escogemos nuestro prefijo del país y ponemos nuestro móvil de uso personal.

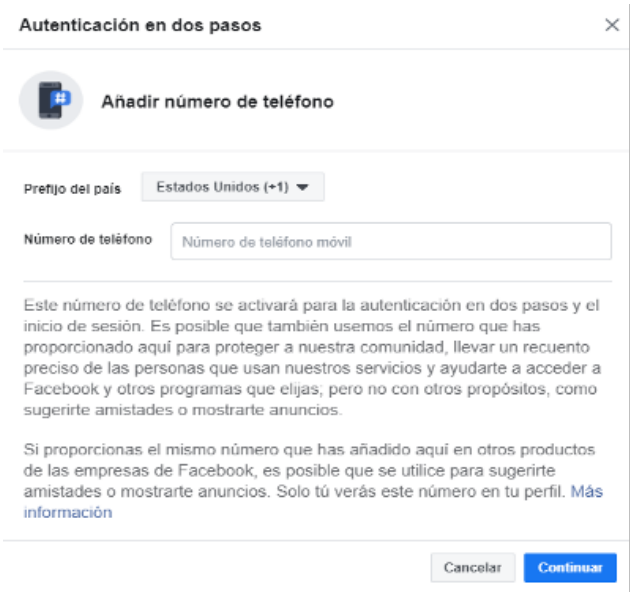


Figura 2.13. Añadir número de teléfono

4. Ahora se nos solicitara digital el código que llega a nuestro smartphone como mensaje de texto

Figura 2.14. Solicitud de código para activar la autenticación

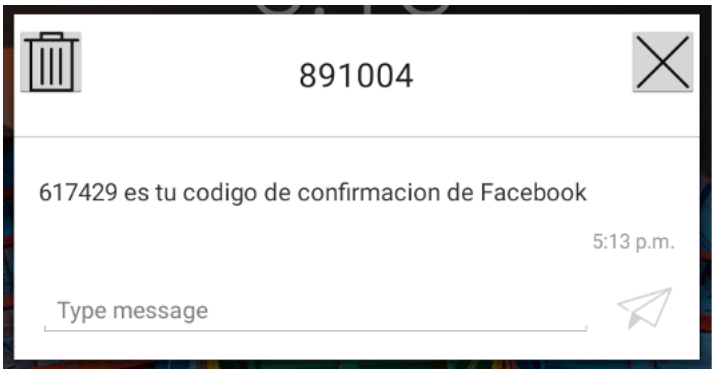


Figura 2.15. Ejemplo de celular Android de código de confirmación

5. La autenticación en dos pasos estará activada.

Figura 2.16. Mensaje de autenticación activada

Ahora imaginemos el escenario donde un hacker consigue nuestra contraseña y va a intentar entrar a nuestra cuenta de Facebook.

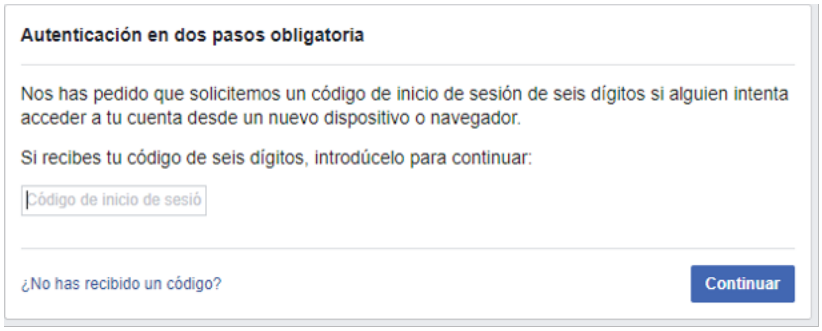


Figura 2.17. Autenticación de dos pasos requerida

Automáticamente lo va a detener la autenticación de dos pasos y nos va a llegar un mensaje al móvil que alguien ha intentado acceder a nuestra cuenta, si somos nosotros debemos ingresar el código del mensaje de texto y podremos entrar, si no somos nosotros significa que alguien intento entrar y debemos cambiar nuestra contraseña.

Figura 2.18. Código de autenticación

2.3. SEGURIDAD EN REDES SOCIALES

Las redes sociales abrieron puertas a una infinidad de posibilidades, desde una mejor forma de comunicación, incluso abrió ideas a empresas para aprovecharse

de estas herramientas. Ahora una empresa que no se encuentre en Internet y en redes sociales, prácticamente no existe ni vende. Aunque no todo sea tan bueno.

2.3.1. Cuentas privadas y suplantación de identidad

La mejor forma de evitar una suplantación de identidad es tener nuestra cuenta privada, si no somos una figura pública, seguro has visto como una persona dice que hay una cuenta falsa por ahí de él o ella, esto pasa normalmente por tener un perfil para todas las personas, generando que desconocidos puedan ver nuestras fotos, estados e intereses, así somos una víctima muy fácil de la suplantación de identidad. También procurar no agregar a personas que no conocemos, ya que incluso, pueden ser cuentas falsas con el fin de conseguir datos de nuestro perfil.

Ahora como ejemplo, tomaremos la red social Instagram, que ha tenido un crecimiento muy alto en estos tiempos.

1. En la configuración de nuestro perfil, seleccionamos la opción de "Privacidad"

Figura 2.19. Configuración en Instagram

2. Seleccionamos el apartado de "privacidad de la cuenta"

Figura 2.20. Botón de privacidad

3. La cambiamos a "Cuenta privada"

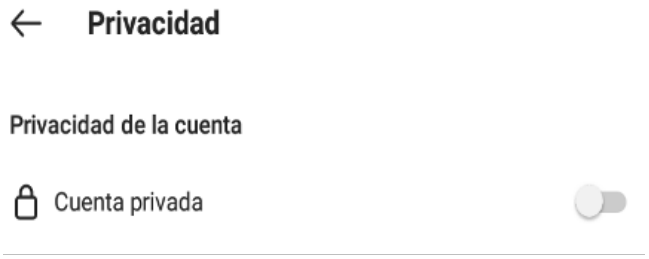


Figura 2.21. Cuenta privada en Instagram

2.3.2. Ubicaciones

Las ubicaciones es un tema delicado, casi todas las redes sociales permiten la opción de compartir con ubicación ya sea fotos o vídeos, el hecho es que al tu compartir tu ubicación dices a todo el mundo que lugares frecuentas, peor aún, si tú compartes la ubicación exacta de tu casa, algunas personas comparten toda su data y peor aún tienen la cuenta pública, cualquier desconocido con intenciones maliciosas puede acceder a toda la información de la víctima y aprovecharse de ella, **desaconsejo todo el uso de ubicaciones** a no ser que sea de algún viaje o lugar de poca frecuencia que visites.

2.3.3. Marketing dirigido al comportamiento

La famosa publicidad que nos sigue a cualquier lugar que naveguemos, se le denomina **Marketing dirigido al comportamiento**, si buscamos en Mercado libre o Amazon algún artículo, no es de sorprender que en Facebook nos invadan de publicidad de ese artículo o artículos parecidos, por eso su nombre, según como nos comportemos en Internet, así mismo nos aparece publicidad de lo que hagamos. Con este modelo de negocio las redes sociales y en especial Alphabet que es la dueña de Google, pueden generar grandes ganancias y la empresa que hizo la publicidad también obtiene un nuevo cliente o compra, así que es una ganancia para ambos y el cliente encuentra algo que le gusta.

Aunque en otro sentido el marketing dirigido al comportamiento va en contra de la privacidad de las personas, ya que no tenemos total libertad de que buscar o hacer en Internet porque siempre estaremos vigilados.

Una forma de evitar este tipo de publicidad y que no nos puedan rastrear, es usar navegadores y buscadores anónimos, asi conseguimos garantizar la privacidad en Internet, para que no se guarden las Cookies que son un pequeño archivo que se almacena en el navegador de un usuario cada vez que entramos a una página, sirve para conocer la actividad de dicho usuario y mostrar cierto comportamiento diferente para cada uno de estos, por ejemplo, el inicio de sesión se almacena en una Cookie y cuando entramos a una página automáticamente ingresamos a ella sin tener que poner nuestro usuario, ni contraseña, de esta manera nos identifica cada página a la que entremos.

2.3.4. Tor y DuckDuck Go

Tor (The onion router) en español el enrutador de cebolla, su nombre se debe a que son varias capas de cifrado que protegen tu tráfico de red, todo el tráfico que pasa por la "Red Tor" es encriptado. Es un navegador anónimo que puedes descargar buscándolo en Google, en pocas palabras **Tor se usa para garantizar el anonimato de una persona que navega por Internet**, algunas personas usan Tor para entrar a algo llamado la Dark Web y Deep Web, varios de estos sitios se usan para hacer compras ilegales, comprar órganos en mercado negro, armas, drogas, comunicación de bandas criminales, espionaje y un fin de cosas que puedes ver en estos sitios; en verdad Tor no se creó con este fin, lo malo del anonimato es que las personas siempre lo usan para el mal. The Tor Project que es la organización que soporta a Tor, no tiene la culpa de cómo se usa su proyecto, eso va más en cada usuario.

DuckDuck Go en cambio es un Buscador anónimo, puedes usar DuckDuck Go entrando a duckduckgo.com es una alternativa a Google que no recopila tu información cuando realices una búsqueda, así que no se personalizan resultados, dependiendo de tus anteriores búsquedas o preferencias,

simplificando, Tor sería un Google Chrome o un Firefox y DuckDuck Go sería Google o un Bing, la diferencia con relación a la seguridad informática es que Tor y DuckDuck Go no recopilan datos sobre ti.

2.4. POSIBLES ATAQUES

Si vimos cómo defendernos en caso de posibles ataques, ¿Por qué no saber de qué manera nos pueden atacar nuestras cuentas y contraseñas.

2.4.1. Ataque de fuerza bruta

Un ataque de fuerza bruta no es más que ir probando muchas combinaciones posibles de contraseña, los programas para hacer este tipo de ataque usan algo llamado diccionario, que es una lista de combinaciones muy larga y cuando se prueba trata con todas las posibles opciones y probablemente alguna sea tu contraseña, por eso contraseñas como:

1234
abc
qwerty

Son tan fáciles de hackear, porque seguramente estén en cualquier lista de palabras para hacer un ataque de fuerza bruta.

2.4.2. Ataque de diccionario

La diferencia de un ataque de diccionario a un ataque por fuerza bruta, radica en que el ataque de diccionario prueba palabras reales que se encuentran en un diccionario y el de fuerza bruta combinaciones, algunas veces sin sentido, pero este es más peligroso porque muchas personas usan contraseñas como:

mariposa123
celular30

15comida

En una lista de ataque por diccionario, se pueden encontrar estas contraseñas, aunque algunas plataformas cuando detectan que se está probando tantas contraseñas diferentes en un corto periodo bloquea estas peticiones.

2.4.3. Phishing

El phishing es una técnica de engaño, donde se hacen pasar por una entidad o persona, requiriendo contraseñas, un ejemplo sería que Google solicita por correo cambiar nuestra contraseña porque fue comprometida, pero en verdad es una página falsa con un nombre muy diferente al de Google, si llegamos a digitar nuestras contraseñas automáticamente se comprometerá nuestra contraseña y si tenemos las mismas contraseñas en todos los sitios, pues un hackeo a todas tus cuentas procederá.

2.4.4. Keylogger

Los keylogger son programas informáticos capaces de detectar pulsaciones del teclado, pueden ser por Hardware o Software, por esto no es recomendable usar computadores en lugares desconocidos, tomar memorias USB tiradas en la calle, porque si la otra persona tiene un Keylogger instalado, cuando escribamos nuestras contraseñas, quedaran guardadas en un archivo de texto, después el atacante podrá usar las contraseñas y comprometer nuestra información.

Existen muchos más ataques para cuentas y a contraseñas, las que mostré son unas de las más usadas, aunque existen técnicas más sofisticadas y peligrosas.

3. COMPRAS ONLINE SEGURAS

Durante la pandemia del COVID-19, el comercio electrónico creció exponencialmente en países donde muchas personas no se adaptaban a estas prácticas, ya sea por miedo a ser estafado o a lo desconocido, porque no es lo mismo interactuar con una computadora o celular a una persona en una tienda. Según ESET, una multinacional especializada en la seguridad cibernética reveló en una encuesta que sólo el 29% de los usuarios de Internet se sienten completamente seguros a la hora de hacer compras en línea y el 61% utiliza el comercio electrónico con una mayor frecuencia antes de la pandemia. El mundo cambió y las personas seguirán usando Internet para hacer sus compras, pero es asombrosa la baja cantidad de usuarios que se sienten completamente seguros al comprar por Internet.

3.1. PRINCIPALES MIEDOS A COMPRAR EN LÍNEA.

- Los datos de mi cuenta bancaria o tarjeta serán robados si la registro en línea.
- Mejor comprar en físico, así pruebo el producto.
- El producto nunca va a llegar.
- Sin tarjeta de crédito no puedo comprar en línea.
- Me pueden suplantar la identidad.
- No sé nada de tecnología.
- A mi amigo lo estafaron comprando en línea.
- El precio es muy bajo, será malo.
- No sé dónde está mi pedido y lo compre hace un buen tiempo.

Todos estos miedos son normales, pero combatibles, con ese fin escribí este libro, para que puedas usar Internet de una manera segura y tranquila, ya que todos necesitamos los conocimientos básicos de seguridad informática, pues

consumimos la tecnología, así que te voy a mostrar cómo combatir todos estos miedos.

3.2. COMBATIR EL MIEDO DE COMPRAR ONLINE

Para combatir el miedo de comprar en línea, lo primero que hay que hacer es comprar cualquier artículo de muy bajo costo, así sabrás cuál es tu propia experiencia, cómpralo en páginas muy conocidas como Mercado libre o Amazon, para que tengas una mayor tranquilidad a la hora de hacer una compra en el comercio electrónico.

3.3. CUIDADO CON LOS SITIOS NO SEGUROS

Los sitios no seguros se encuentran por todo Internet, queriendo conseguir tus datos bancarios, para posteriormente comprar o vender tus datos, para ello cada vez que visitemos una página Web debemos asegurarnos de que traiga certificado SSL, comprobando que toda la información que pase por esa página se cifre, la manera en que podemos hacerlo es mirar si tiene un candado en la parte de arriba del sitio web.

Figura 3.1. Certificado SSL en Amazon.com

En cambio, a la hora de navegar en un sitio no seguro sin certificado SSL automáticamente el navegador lo detecta e informa al usuario que está navegando por un sitio que no es seguro.

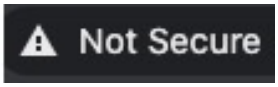


Figura 3.2. Sitio no seguro detectado por el navegador

Las personas que ingresen sus credenciales en sitios no seguros, la información que se manda navega en texto plano y cualquier persona que se encuentre en la red puede leer esa información y sacar nuestras tarjetas de crédito o contraseñas, por eso es fundamental a la hora de comprar o ingresar contraseñas en cualquier sitio verificar esto primero.

3.4. CUIDADO CON LOS NOMBRES DE DOMINIO

Algunas personas se dedican a comprar dominios y convertirlos en páginas de phishing por ejemplo Amazon.com puede ser Amazoncom.com o incluso de tu página de banco de vez de tener el nombre habitual, incluye algunas letras o números, cuando entramos a esta página se ve exactamente igual a la de nuestro banco, pero en verdad es una página maliciosa esperando a que ingresemos nuestros datos, por eso siempre debemos verificar el nombre de la página sea el correcto.

3.5. PHISHING POR CORREO ELECTRÓNICO

Complementado con los nombres de dominio, cuando entras a tu correo electrónico, aparecen correos insinuando ser nuestra entidad bancaria, alguna red social, mencionando que nuestra cuenta está comprometida y que debemos restablecer la contraseña. Esto puede ser cierto, pero muchos de los mensajes intentan llevarnos a una página falsa como hablamos en la anterior sección y a la hora de "restablecer nuestra contraseña e ingresar los datos" no va a suceder nada, dejándonos salir de la página tranquilamente, pero lo que acabamos de hacer es dar nuestras credenciales a una persona con intenciones maliciosas.

En estos casos, rápidamente debemos cambiar nuestra contraseña o cancelar nuestra tarjeta de crédito. Para confirmar que un correo electrónico es verídico debemos ver quien fue el que envió el mensaje por ejemplo uno de MercadoLibre tiene que aparecer algo así usuario@mercadolibre.com especificando el nombre de dominio al final, este debe estar copiado

exactamente como en la página web, no debe ser Gmail ni cambiando ciertos caracteres un ejemplo de una página que quiera estafar sería casdj@mercadooolibre.com como vemos hay varias o de más.

Figura 3.3. Correo verídico de mercadolibre.com

3.6. NÚMERO DE SEGUIMIENTO

Al realizar una compra en páginas confiables, dan un número de seguimiento y como su nombre lo indica es un número con el que podemos rastrear en donde esta nuestro pedido, así asegurar que el pedido no se retrase y poder estar tranquilos si el pedido va a llegar o no; el número lo podemos ingresar en páginas como 17track.net y automáticamente nos da detalles de nuestro pedido.

Figura 3.4. Ejemplo de un número de seguimiento

3.7. COMPRAS EN TIENDAS DE INSTAGRAM

Instagram abrió un mercado muy grande, pues el comercio electrónico funciona muy bien en esta plataforma, el problema es que, para comprar algún artículo, la mayor parte de negocios en Instagram no tienen página web, normalmente el pago se efectúa depositando en alguna cuenta bancaria ya que no manejan transacciones por tarjeta de crédito o PayPal que es más seguro. En estos casos

nos podemos fiar de los comentarios de otras personas en la misma red social, que se vean cuentas verídicas y no bots, para ello simplemente debemos pasar por los comentarios para ver qué opina la gente de la tienda y meternos en algunos perfiles para comprobar que no se vean como cuentas sin sentido. No confíes en seguidores y "me gusta" de una tienda, ya que hoy en día es muy fácil comprar seguidores o likes en sitios donde llenamos la página de bots, estos simplemente son cuentas que no existen y hacen acciones automáticas. Aunque confía más en las tiendas que tienen página web, si tienen página web es que en verdad les importa el crecimiento de su negocio y saben que genera una mejor credibilidad y confianza por parte de los usuarios.

3.8. ¿POR QUÉ LOS PRECIOS SON MÁS BAJOS?

La razón de que los precios sean bajos no se debe a que son de mala calidad, tal vez lo que compras, anteriormente lo compró una empresa a un distribuidor por Internet, esa es la razón, algunas tiendas locales compran al por mayor en Internet para vender a personas que no compran en línea, o vender en tiendas de Instagram, sería mejor buscar directamente al vendedor y comprar incluso más económico, aunque esto puede sacrificar tiempos de envío.

3.9. POSIBLES ATAQUES

Los ataques más comunes en prácticas de comercio electrónico son los siguientes:

3.9.1. Troyanos

Un troyano es un malware que parece un software inofensivo, pero al ejecutarlo y darles permisos, brinda a cualquier atacante acceso remoto a nuestro dispositivo. El troyano ZeuS, también llamado ZeuS o zbot se usa para robar cuentas bancarias mediante el registro de teclas de navegador, el troyano se introduce por descargas, vía ventanas emergentes, correos electrónicos y muchos más formatos.

3.9.2. Spyware

Un Spyware es un tipo de programa maligno que infecta un dispositivo y su función es recopilar información sobre el propietario del dispositivo. Un spyware por lo general viene como troyano que al darle permisos empieza a rastrearnos y a recopilar toda información de la víctima. El marketing dirigido al comportamiento no es un Spyware, si Google o Facebook puede rastrear ciertas cosas de nuestra actividad, incluso fuera de sus propias plataformas, pero nosotros aceptamos los términos de condiciones, **un malware deja de ser malware cuando el usuario le da autorización y privilegios porque él quiere**.

3.9.3. Phishing

El Phishing lo hemos mencionado a lo largo de este libro para conseguir cuentas bancarias o tarjetas de crédito, los atacantes envían correos masivos para hacerse pasar por entidades oficiales o algunos pagan publicidad en páginas poco confiables para redirigirlos a sus páginas de Phishing.

3.9.4. Keylogger remoto

La diferencia de un Keylogger ordinario a un Keylogger remoto, es que el atacante sólo tiene que esperar que la victima instale el malware deseado, posteriormente las pulsaciones de teclado se envían por correo electronico al atacante sin que la victima se de cuenta de que pasa internamente, robandole tarjetas de credito y contraseñas importantes.

4. SEGURIDAD EN REDES LOCALES E INALÁMBRICAS

Piensa en cuantos dispositivos tienes conectado en estos momentos a Internet, ¿smartphone, computador, neveras, parlantes, audífonos, Amazon echo, luces inteligentes, interruptores? Hoy en día hemos pasado la brecha de cuantos dispositivos tenemos conectados gracias al Internet de las cosas (IoT) la mayoría de nuestros dispositivos tiene el hardware necesario para interactuar con otros equipos.

Imagina que compras una cámara inteligente la cual vigila tu casa cuando no hay nadie, ahora imagina que alguien también tiene acceso a las imágenes de la cámara, es algo que ninguno quisiera ¿cierto? En este capítulo veremos la forma de cuidarnos navegando por Internet en nuestras redes LAN o WAN.

4.1. REDES LAN Y WAN

Local Área Network (Red de área local) LAN: se limita a un espacio reducido en el cual varios computadores están conectados en una misma red, está es la red de tu casa, tienes un Router y varios dispositivos están conectados a esa misma red, pueden compartirse recursos entre ellos, pero un dispositivo que esté fuera de esta red no va a poder conectarse a alguno de los dispositivos. También esta red son las que manejan tanto empresas pequeñas como empresas grandes.

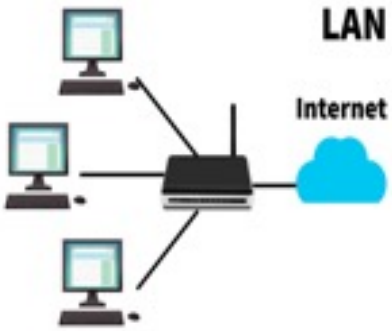


Figura 4.1. Ilustración red LAN

Wide Area Network (Red de área amplia) WAN: una definición rápida de una WAN es el propio Internet la red de redes, donde una red de computadores se extiende en un gran territorio, como una ciudad, país o el planeta, es una extensión más grande de la LAN, se puede pensar que una WAN es varias redes LAN interconectadas.

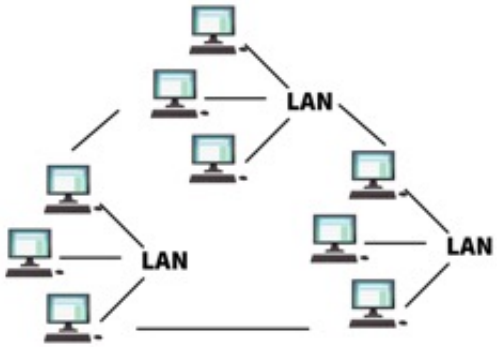


Figura 4.2. Ilustración red WAN

4.2. NAVEGACIÓN SEGURA

Siempre hay que identificar si un sitio web sea seguro, fijarse que una web esté usando el protocolo HTTPS y no HTTP, esto debido a que en el sitio HTTPS la información viaja cifrada y no en formato de texto plano como en HTTP. Hay herramientas para realizar un ataque conocido como **"Man in the middle"** u **"hombre en el medio".**

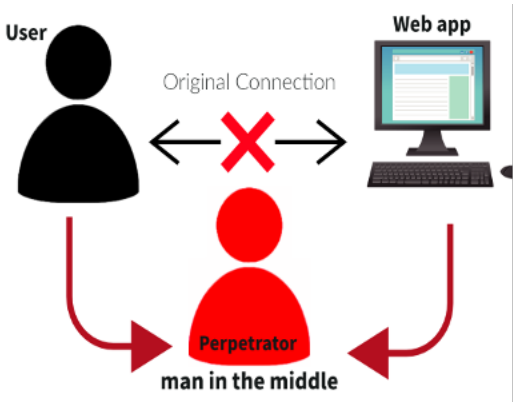


Figura 4.3. Ataque de hombre en el medio "man in the middle"

No se refiere que exista un hacker en el medio de nuestra computadora con un cable invisible tratando de obtener nuestras credenciales, se refiere a interceptar una comunicación entre dos dispositivos el atacante manipula el tráfico y se puede hacer pasar por un dispositivo y obtener la comunicación o información sensible, aquí es donde te menciono que si la información no viaja cifrada el atacante podrá interceptar el tráfico de una manera fácil, herramientas como Wireshark para analizar paquetes, o Ettercap ayudan al hacker a este propósito.

4.3. REDES INALÁMBRICAS

¿Sabías que cambiar la contraseña del Wi-Fi periódicamente es una gran medida de seguridad?, incluso si el atacante no tiene acceso a tu red local no podrá llevar a cabo el ataque de **hombre en el medio**, por esa razón es super importante saber quien tiene acceso a nuestra red Wi-Fi, cada proveedor tiene diferentes formas para cambiar la contraseña, por lo que puedes llamar a tu proveedor de Internet y preguntar de qué manera puedes cambiarla con tu proveedor o solicitarle que la cambie cada cierto tiempo.

Las redes inalámbricas transmiten datos a través de ondas de radio, donde una onda se puede interceptar de una manera rápida por cualquier persona, razón por la que se tomaron las medidas de seguridad necesarias para poder cifrar la información que viaja por ondas, se usan diferentes protocolos, WEP, WPA, WPA2, WPA3, veremos que significa cada uno y cual te recomiendo usar.

4.4. PROTOCOLOS WI-FI

WEB: el protocolo WEP fue el primer intento de una protección inalámbrica. WEP hace un cifrado con una clave hexadecimal de 64 o 128 bits, siendo una clave estática. Si alguien conoce la clave podrá acceder a la señal, se creó para

prevenir ataques de un intermediario. Sin embargo, falló con este propósito ya que se ha descubierto múltiples vulnerabilidades de este protocolo.

El protocolo reveló su debilidad en **2001 catalogando a WEP como un protocolo inseguro que no se debería usar en ninguna red**.

WPA: Posteriormente a WEP aparece WPA o Wi-Fi Protected Access. Este protocolo sucesor, aparece en 2003 debido a las debilidades de WEP, comparte algunas similitudes con WEP, pero tiene mejoras en la forma en que se manejan las claves de seguridad, mientras WEP usa la misma clave para cualquier sistema, WPA utiliza el protocolo de integridad con una clave temporal, que cambia las claves utilizadas por un sistema, esto evita que los atacantes creen sus propias claves de cifrado que coincidan con la red, como pasaba en WEP, adicionalmente las claves que utiliza WPA son de 128 Bits. También incluye controles para saber que los mensajes no tienen modificaciones, desgraciadamente también existe vulnerabilidades para este protocolo.

WPA2: El WPA2 llego en 2004 que es una versión mejorada del WPA, funciona con dos modos usa una clave previamente compartida, de código de acceso compartido, para usos domésticos y un modo empresarial, usa el protocolo de código de autenticación de mensajes de encadenamiento, proporciona una verificación de autenticidad para los mensajes y es el más seguro comparándolo con WPA o WEP, es vulnerable a ataques de reinstalación de claves, que permite a los ataques hacerse pasar por una red clonada y obliga a la víctima a conectarse a esa red, esto permite al hacker descifrar una pequeña parte de los datos, pero recordemos que el usuario es el eslabón más débil de la seguridad informática con este libro te estas volviendo una persona hábil en conocimientos de seguridad para que no te logren hackear si tienes precaución podrás usar WPA2.

WPA3: fue anunciado en enero de 2018 llega a reemplazar a WPA2, que no se puede considerar absolutamente segura, dispositivos que usen WPA2 no pueden conectarse en puntos de acceso WPA3, este deshabilita los protocolos

anteriores, maneja un cifrado individualizado así que el atacante no podrá desencriptar el tráfico que se haya realizado antes de la intrusión. Sin duda alguna la mejor opción es WPA3.

4.4.1. Saber cuál es la seguridad de mi red Wi-Fi

Aunque sepamos que WPA3 es el más seguro, muchos dispositivos siguen usando WPA, incluso se pueden encontrar varios dispositivos con WEP que literalmente realizar un ataque en una herramienta como aircrack-ng no tarda mucho tiempo y es super fácil, le debes evitar si o si en caso de tener el protocolo WEP, veamos cual es mi protocolo.

Pasos prácticos con Windows:

1) Hacer clic en Icono de Wi-Fi y abrir configuración de red e Internet

2) Hacer clic en Propiedades
3) Valida que por lo mínimo sea WPA2

Figura 4.4 Ilustración panel de control Windows WPA2

Como se evidencia, tengo WPA2 así que puedo estar tranquilo que algún atacante le tomará más tiempo acceder a mi red.

4.5. PERSONAS CONECTADAS A MI RED

La cantidad de personas que tienen acceso a nuestra red local, familiares, amigos que nos visitan, personas que le damos acceso en fiestas, esa es la principal razón de cambiar la contraseña del Wi-Fi periódicamente, pero ahora analicemos cuantas personas estén conectadas a nuestra Red.

Pasos prácticos con celular:

1) En la App Store o Play Store instalaras la aplicación "Fing"

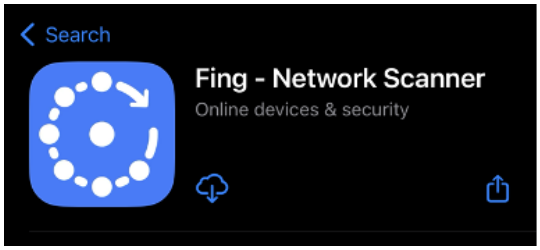


Figura 4.5 Aplicación Fing

2) Abres la aplicación

3) Seleccionar Buscar dispositivos

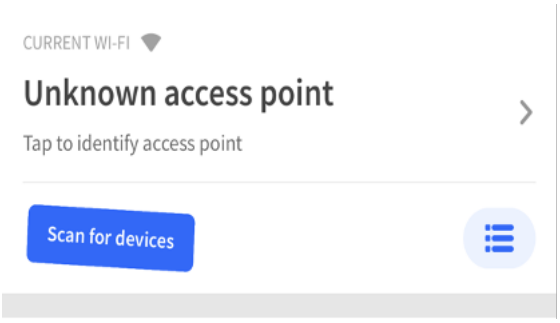


Figura 4.6 Encontrar dispositivos

4) Aparecerán todos los dispositivos conectados

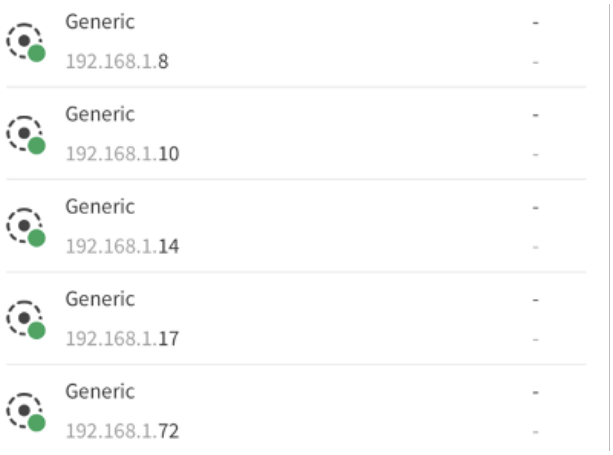


Figura 4.7 Dispositivos conectados

5) Identifica al dispositivo que no reconozcas y bórralo

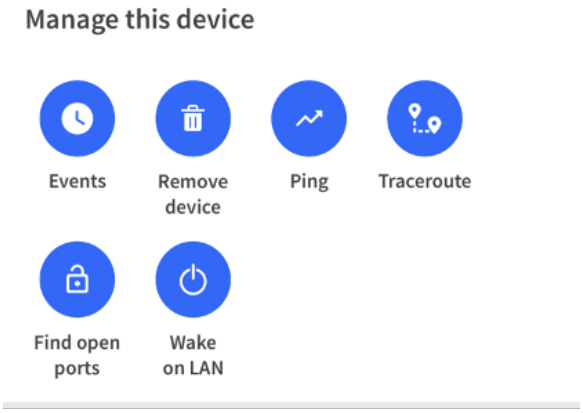
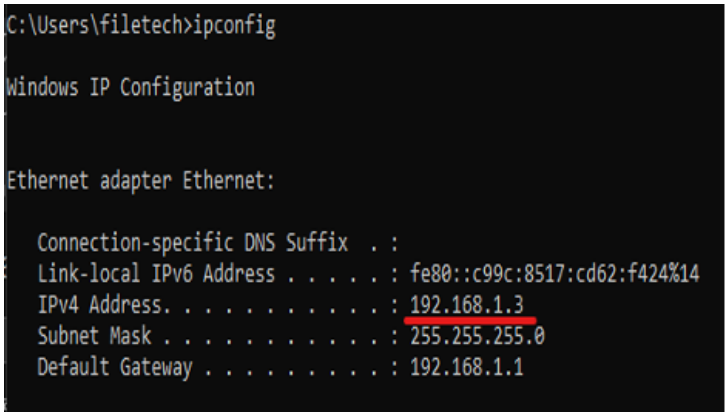


Figura 4.8 Eliminar dispositivos

6) Si tienes dudas de cuáles son tus IP puedes usar ipconfig en el CMD de



Windows o con la aplicación FING instalada puede darte información de tu IP para que no borres el dispositivo incorrecto.

Figura 4.9 IP por medio del comando ipconfig

7) Si encuentras dispositivos que no reconoces lo mejor es que llames a tu proveedor de Internet para el cambio de contraseña o que te indiquen de qué manera puedes cambiarla, normalmente cada proveedor tiene su aplicación móvil para hacer el cambio de contraseña

4.6. POSIBLES ATAQUES

Los ataques más comunes en redes LAN o WAN

4.6.1. ARP Spoofing

Permite atacar equipos que se encuentren en la misma red LAN, el atacante se hace pasar por nuestro router, con este logra que todo el tráfico de la red pase por él, permitiéndole realizar cualquier acción sobre él, este es el primer paso para realizar un ataque de hombre en el medio.

4.6.2. Ataque de hombre en el medio

El man in the middle o el hombre en el medio es de los ataques más fáciles de realizar, puede hacerlo un hacker con experiencia o sin experiencia, se logra

realizar al entrar a webs insegura usar protocolos inseguros, el atacante debe tener acceso a tu red.

4.6.3. Ataque de denegación de servicio

También llamado DOS o **Deny of service**, este ataque logra que un recurso sea inaccesible debido a múltiples peticiones que hacen colapsar el servicio. Es normal que un sitio se caiga cuando la demanda por los usuarios es más de lo común, el problema es cuando un atacante "simula" esa demanda y hace colapsar algún recurso como una página web, provoca la pérdida de conectividad de la red al sobrecargar los recursos.

4.6.4. Escaneo de puertos

Al estar en nuestra red, el atacante puede escanear nuestros puertos para saber si tenemos alguno abierto el cual se pueda vulnerar, escanear puertos puede ser una actividad ilegal. En las empresas sólo administradores de redes y sistemas puede realizar esta labor.

4.6.5. OS Finger Printing

Si sigues usando Windows 7, Windows XP, o sistemas operativos desactualizados, esta técnica sirve para saber cuál sistema operativo tienes, herramientas como nmap la cual puedes descargar de la página oficial https://nmap.org/ y ejecutar el comando nmap -O "ip", nos dirá el sistema operativo de la víctima una manera muy sencilla para saber si tiene un sistema desactualizado.

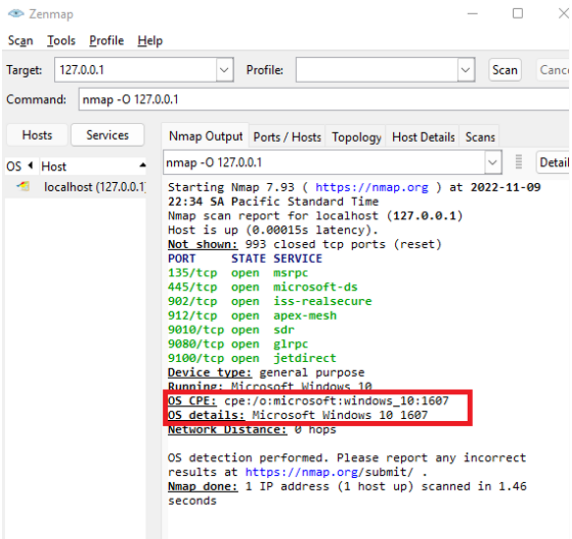


Figura 4.10 Escaneo del sistema operativo víctima

5. INGENIERIA SOCIAL

El momento que todo el mundo sin habilidades técnicas puede ser un verdadero hacker, imagina que una persona te diga su contraseña sin tener que realizar algún tipo de ataque a nivel técnico, sólo con tu manera de socializar puede conseguir el PIN de una tarjeta de débito o incluso acceder a una clave Wi-Fi, pareciendo una "buena persona". Lograr entrar a una zona restringida por el simple hecho de hablar con el guarda de seguridad, en esto consiste el arte de la ingeniería social, hackear a las personas, conseguir que hagan algo de forma voluntaria y que beneficie al atacante.

Este capítulo radica en saber protegerte de las habilidades sociales de un individuo, mas no en proteger nuestros dispositivos o redes, ya que los ataques más efectivos son cuando vulneran a una persona. El eslabón más débil en la seguridad informática, un correo de phishing engañándote en dar tus credenciales también es un ataque de ingeniería social ya que trata de convencerte de que descargues un programa, ingreses alguna credencial en un sitio web que no es el oficial y robar así tus credenciales.

5.1. VULNERABILIDADES HUMANAS

Cuando una persona nos interesa o le tenemos algún tipo de aprecio, somos más abiertos a realizar algo que nos solicite esa persona, es la naturaleza humana, nos sentimos bien con lo que nos resulta familiar. Cuando vivíamos en tribus y llegaba algún extranjero, normalmente resultaba en guerra, apreciamos más si una persona es como nosotros, viste como nosotros o tiene pensamientos similares.

La ingeniería social se basa en la programación neurolingüística (PNL) que se refiere a como interpretamos la realidad a través de los sentidos, los ingenieros sociales estudian mucho estos temas ya que aprenden a leer el lenguaje corporal

o comportarse de una forma que la otra persona se sienta bien. Existe una serie de neuronas denominadas **"neuronas espejo"** que funcionan cuando una persona realiza acciones y la otra persona imita las acciones, estas neuronas también son llamadas neuronas de empatía, cuando una persona toma postura corporal similar a la nuestra, esto puede generar confianza, puede ser una reacción natural del ser humano, pero el ingeniero social se aprovecha de esto ya sea en una entrevista de trabajo o al tratar de ganarse la confianza de una persona

5.2. POSIBLES ATAQUES DE INGENIERÍA SOCIAL

5.2.1. Dumpster diving o trashing

Esta técnica consiste en buscar en la basura alguna información relevante para ser utilizada por el ingeniero social, si la empresa o el individuo tiene papeles importantes y los arroja a la basura, debe tener en cuenta que cualquiera que se arriesgue a recoger esa basura va a encontrar esa información.

La manera de prevenir este tipo de ataque es **triturar los papeles** con información sensible para que el individuo le cueste encontrar toda la información que necesita.

Figura 5.1 Dumpster

5.2.2. Eavesdropping

Si escuchas una información sin el consentimiento de los involucrados, estás haciendo eavesdropping, las señales de radio no viajan encriptadas eso significa que es muy fácil que cualquier persona escuche conversaciones de policías o vigilantes hablando por este tipo de señales, sólo encontrando la frecuencia correcta puedes escuchar las conversaciones.

La manera en que recomiendo evitar este tipo de ataque es usar aplicaciones que usen cifrado de extremo a extremo como WhatsApp, Telegram o Signal, para que las conversaciones no se puedan interceptar, también no hablar de cosas sensibles en un espacio público ya que cualquiera podría escuchar.

Figura 5.2 Eavesdropping

5.2.3. Phishing

Ya hemos hablado del phishing varias veces durante el libro, este es un ataque de ingeniería social, la manera de evitarse es ver el destinatario del correo electrónico, validar que las páginas web tengan el dominio verdadero y no uno alterado.

Figura 5.3 Phishing

5.2.4. Pïggybacking y tailgating

Hay una persona con altos privilegios de entrar a un área restringida y tú vas detrás de él, logrando tener acceso al área, te estarías "colando". En esto consiste este tipo de ataque, como entrar a una empresa en la cual no trabajamos vistiendo de manera elegante para parecer más inadvertido.

La manera de evitar este tipo de ataques es pedir siempre las credenciales, implementar controles de reconocimiento fácil o dactilar.

Figura 5.4 Pïggybacking y tailgating

5.2.5. Llamadas y mensajes falsos

Entra un mensaje de un familiar al cual le tienes mucho aprecio, en el mensaje te dice "estoy en un problema ¿me podrías prestar algo de dinero? Te lo devuelvo apenas me paguen, pero lo necesito el día de hoy", en ese caso al tratarse de un familiar tu confías y se lo das, pero la realidad es que a tu familiar lo han acabado de hackear.

Llega una llamada de tu banco, parece una llamada real de dicha empresa o también te llaman diciendo que fuiste el ganador de una rifa entre todos los clientes y lo único que debes dar para efectuar tu premio es mencionar los números tarjeta de crédito o si no pierdes el regalo, ¿Qué harías? De la emoción muchas personas caen en estas técnicas, pues como hemos hablado alteran los

sentimientos de las personas, la parte humana de cada uno de nosotros, por ende, se logra ejecutar el ataque con una simple llamada.

La manera de evitar esto con mensajes falsos es insistir en verse o realizar una video llamada para estar seguros de que, si se trata de una emergencia y a nuestro familiar no lo han hackeado, con las llamadas es un poco más difícil, pero puedes asegurarte de que ninguna entidad bancaria te va pedir datos sensibles o personales por llamada, por ende no estas obligados a darlos.

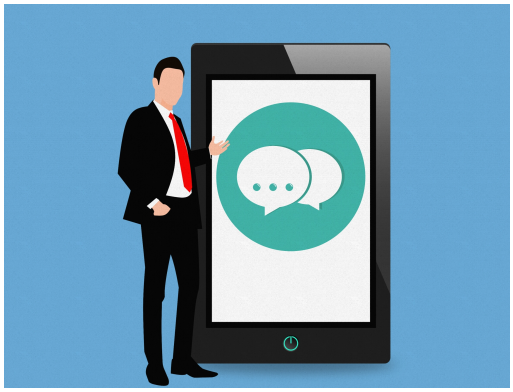


Figura 5.5 Llamadas y mensajes falsos

5.2.6. Deepfake

Las llamadas falsas no son mucho problema para ti, una vez leído lo anterior no será mucho problema para ti, pero ahora imaginemos una llamada de un número desconocido y que la voz sea igual a la de tu jefe pidiendo que hagas algo de manera urgente, o te llaman y vez a un familiar secuestrado y te piden que vayas a una ubicación a rescatarlo, probablemente sea un deepfake, son archivos de video, imagen o voz manipulados mediante inteligencia artificial para que parezca una obra de la persona real.

¿Como detectar un Deepfake? sé que en esa posición cualquiera podría caer, pero lo que debes hacer es prestar mucha atención en los videos, normalmente tienen incoherencias visuales en cabello, ropa, aunque hay unos muy bien elaborados es difícil que lleguen a la perfección, observa esos pequeños detalles. Cuando es con voz, pregunta cosas que sólo tú y la persona saben, si es un

hacker no sabrá que responder al menos que te haya investigado muy bien y si es una voz pregrabada, no podrá contestar la pregunta, así podrías detectar que la que está detrás del teléfono sea la persona que dice ser, fíjate que sea el celular de tu familiar.

5.2.7. Baiting

Te encuentras en la calle, hay una USB tirada en el suelo, la USB tiene un mensaje como "Fotos viaje", "Confidencial", tú no puedes aguantar el saber que hay en la USB así que la conectas a tu computador y no hay nada, tales fotos no existen y la desconectas, pues probablemente te acabaron de insertar un **troyano** u otro tipo de **malware**, en esto consiste el ataque despertar la curiosidad y que tu insertes un dispositivo en tu computador.

La manera de evitar este tipo de ataque creo que es de las más lógicas, no insertes nada en tus dispositivos de lo que encuentres en las calles.

Figura 5.7 Baiting

5.2.8. Bribing

A un empleado le ofrecen cierta cantidad de dinero que sería su salario de 5 años, le dicen que lo único que deberá hacer es conectar una USB a un equipo especial de la empresa, el empleado al ver tal tentación en poco tiempo acepta, afectando toda la red de su compañía, así que es demandado por la empresa y multado a la vez.

El soborno es un ataque de ingeniería social de los más usados, lamento decirte que para esto no hay manera de cómo defenderse. Si el empleado tiene altos niveles de acceso y es tentado a un soborno, vulnerará la empresa si quiere, normalmente las empresas trabajan mucho el tema de reflexionar sobre soborno, ya que es una práctica ilegal, pero después de que alguien acepte, es difícil defenderse, para algunas personas lo único que va a importar es el dinero y esa es nuestra vulnerabilidad.

Figura 5.8 Bribing

5.2.9. Office snooping

Un compañero de trabajo el día de hoy no asiste a laborar debido a una incapacidad, automáticamente otra persona aprovecha para husmear en sus terminales para encontrar información a la cual solamente tiene acceso el compañero inactivo, puede hacerse pasar por el compañero y si ejecuta un ataque, un informático forense determinara que el ataque provino desde el computador del compañero inactivo.

La manera de evitar este tipo de ataques es asegurando nuestros dispositivos con clave, si es un portátil traerlo a nuestra casa y no dejarlo en la compañía, también serviría instalar cámaras en el lugar de trabajo.

Figura 5.9 Office snooping 5.9

5.2.10. Shoulder surfing

La estrategia milenaria de saber cuál es la contraseña de alguien, pin de tarjeta de crédito u otros, es simplemente hacerse atrás y mirar como pone su contraseña en el cajero o en su computadora, o el pin en su celular, algunas personas acostumbran a dejar su contraseña pegada en una etiqueta, este tipo de ataques también consiste en dejar cámaras, o usar telescopios y drones.

La manera de protegerse es ser cuidadoso y como se mencionó en el primer capítulo sería tapar siempre que digites tu contraseña, teclado o cajero, estas prácticas de seguridad las enseñan mucho, pero aun así las personas las ignoran.

Figura 5.10 Shoulder surfing

5.2.11. Suplantación

La suplantación radica en hacernos pasar por alguna persona o entidad con el objetivo de engañar a una persona o máquina para obtener algo en especial.

Existe la seguridad física, lógica y digital, la física es la que consiste suplantar alguna identidad sin algún dispositivo electrónico, crear alguna personificación de la persona a suplantar u obtener sus tarjetas de identificación. También por llamadas telefónicas, mensajes, al requerir un equipo de cómputo es una suplantación lógica y la digital es la creación de cuentas de redes sociales falsas suplantando la identidad de una persona.

Existen varias maneras de evitar la **suplantación**, todo dependerá el tipo de suplantación; si te clonan una red social como Facebook, puedes usar el reporte de cuentas y suplantación para que la cuentan la bloqueen e informar a tu circulo social sobre esto, de la lógica la hemos mencionado varias veces de cómo cuidar tus contraseñas, ataques contra phishing o telefónicas y la con la física asegúrate de si se te pierde un papel realiza la denuncia por si suplantan tu identidad.

Figura 5.11 Suplantación

5.2.12. Extorsión

Las peores técnicas de ingeniería social, aquí aplica la **sextorsión**, donde un individuo asegura tener videos íntimos de la otra persona y le pide que haga algo o si no divulga ese contenido, o Honey trap donde este tipo de ataque trata de vulnerar a la persona por medio de su deseo sexual. Puede ser un atacante que simule ser un perfil femenino y se gana su confianza, si la persona tiene algún contenido con él cual amenace para divulgar y pida alguna recompensa a cambio.

Si ya la persona tiene dicho contenido y se comprueba que, si lo posee, piensa ¿Si hago lo que me pide me dejara de molestar? Lo más probable es que no sea así, habla con personas de confianza en este caso, pídeles que no vean este material si lo llegan a ver en Internet por respeto, tristemente en la seguridad informática sólo hay una oportunidad para defenderse, si no ha pasado aún, hay muchas maneras como todo lo enseñado en este libro y asegurar tus dispositivos móviles o pc para que no sean vulnerables a ataques, que es lo que vamos a ver en el siguiente capitulo.

Figura 5.12 Extorsión

5.3. INGENIERÍA SOCIAL CON UNA MIRADA POSITIVA

En este capítulo nos faltó mostrar mucho contenido, el área de la ingeniería social es enorme y se podría hacer un libro completo de esta área, se mostraron los principales peligros de la ingeniería social, aunque se habla de los usos de la ingeniería social de forma negativa, se puede usar de manera muy positiva, como en marketing para mejorar las ventas por medio de persuadir a los clientes, mejorar la comunicación y atraer nuevos clientes a nuestras empresas, entender el funcionamiento humano es una gran habilidad y te puede hacer lograr alcanzar grandes cosas. Si puedes explora más esta área que es de las más interesantes en seguridad informática.

6. SEGURIDAD EN DISPOSITIVOS

El celular es el dispositivo con el que te comunicas, compartes fotos, grabas vídeos, haces compras, accedes a tus cuentas bancarias, retiras dinero, hoy al pensar en un smartphone hablamos de toda tú información en un pequeño dispositivo, ¿qué pasaría si se filtrara toda la información de tu teléfono? ¿pagarías una extorsión a cambio de no divulgar tu información privada? En este capítulo veremos los principales riesgos a la hora de usar los dispositivos con los que trabajas día a día.

Las personas que descargan aplicaciones piratas o crackeadas tienen altísimo riesgo de contraer un malware ya sea un **spyware** como hablamos en el capítulo 1, es un software cuya función es recopilar información sobre el propietario del dispositivo, o varios tipos de malware que hablaremos adelante.

Las personas buscan la manera de tener aplicaciones famosas de pago como Spotify, Netflix, Adobe Photoshop, Office, incluso algunos creen que Windows es gratis y no es así, Windows tiene una licencia la cual es de pago, cuando usas los famosos "cracks" para poder tener el software de manera pirata probablemente sea un virus encubierto "troyano" que se haga pasar por una solución, pero en verdad te quiere robar tu información y datos personales, le das permiso al software para poder crackear el programa, efectivamente tienes tu programa gratis, pero te llega un virus adicional. También las páginas de ver películas o series de manera gratuita contienen anuncios que son adware y pueden instalar, ejecutar o tomar datos de ti y tus dispositivos, tienes que saber que si es un producto es gratis, algo debe obtener de ti para que ese producto pueda serlo, en este caso quiere tu información, tus datos o inyectarte un virus.

6.1. PROTECCIÓN DE MALWARE

Es muy fácil protegerte, lo que debes hacer es usar software legal y descargado directamente de las tiendas de aplicaciones App Store, Play Store o Microsoft Store, en caso de que no esté el aplicativo en las tiendas buscar las páginas del propietario del software y verificar que sean verídicas como el nombre de dominio o si tiene https.

En caso de que no tengas o no quieras pagar por usar estas herramientas, sería usar software gratuito open source que nos da un software que puede realizar la misma tarea sin coste, por ejemplo la alternativa a Windows es usar Linux, con un simple tutorial bastará para que puedas instalar Linux como sistema operativo, Photoshop existe Gimp, Office usa LibreOffice, el software open source no pide nada a cambio esto se logra porque un desarrollador público el código de su aplicación y más desarrolladores apoyaron esta iniciativa, esto hace que el software sea seguro ya que todos pueden ver cómo está construido internamente ese programa, normalmente sobreviven por donaciones, por ende no va tratar de robar tu información.

Los **antivirus** es un adición a la seguridad anteriormente implementada, de nada nos sirve tener un antivirus si le damos permiso al virus de ejecutarse, pero cuando ya nos protegemos de manera consciente, no instalando programas piratas, no entrando a páginas web inseguras revisando que siempre tenga protocolo https, controlando nuestra red Wi-Fi, el antivirus si nos podría salvar, porque si nos envían un link que posiblemente es un malware y sin querer lo abrimos, es donde el antivirus puede reaccionar y bloquearte el virus o la web insegura antes de entrar a ella. Los antivirus almacenan los códigos maliciosos por medio de hashes y existen en una base de datos enorme el cual tiene clasificados una gran cantidad de virus; un hacker de sombrero negro muy bueno tratara de que el malware no lo pueda detectar un antivirus.

Como antivirus el propio Windows (ojala lo tengas de manera legal) trae **Windows defender** el cual es un excelente antivirus para lo que necesitas, en Android hay antivirus gratuitos pero si se trata de antivirus lo mejor es tener

uno de pago, trata de buscar algunas opciones económicas o si lo usas gratis, recuerda que tal vez te pida acceso algunos datos para mejorar el servicio, en el sistema de los iPhone iOS o Mac Os los computadores de Apple también pueden tener virus, sólo que como el iPhone o las Mac tiene una menor cantidad de usuarios, los hackers no le ponen tanta atención atacar un equipo Apple, se van por Android o Windows ya que es el más usado, añadiendo que iPhone actualiza constantemente sus dispositivos haciendo que sea muy seguro, pero en caso tal, puedes también mirar las opciones de antivirus. Recuerda que, aunque en el iPhone no existan tantos virus, si un hacker logra entrar a tu iCloud por medio de otros ataques hablados en capítulos anteriores no importara que tengas un equipo de estos, no importa que el dispositivo sea seguro, cuando el usuario no tiene las bases de seguridad.

En caso de que usas una cámara en tu computador una buena práctica de seguridad es taparla, ya que si hay un malware en tu equipo el hacker podrá ver la cámara de tu ordenador o celular, tomar capturas de pantalla, tapar la cámara nos garantiza que no nos vayan a estar grabando y si tienes micrófono físico desconéctalo cuando no lo estes usando, un malware tratara de elevar privilegios para poder hacer más cosas dentro del equipo.

6.2. TIPOS DE MALWARE

En esta sesión trataremos de evitar los malware que hemos mencionado con anterioridad, ya que hemos hablado de spyware o keylogger y troyanos, así que pasaremos de ellos

6.2.1. RootKit

La finalidad de un Rootkit es poder ejecutar permisos de super usuario, para poder realizar acciones que una vez instalado no tiene, escalando los privilegios, tener más control sobre la maquina infectada, además con los privilegios evita dejar rastros dentro de los dispositivos.

6.2.2. Ransomware

El Ransomware infecta un dispositivo y posterior a eso procede a encriptar el disco, sólo el hacker tiene la contraseña para poder desencriptar el disco, el hacker procede a pedir una recompensar ya sea en bitcoins o consignaciones, normalmente en bitcoins gracias a su anonimato y la victima deberá pagar si quiere la contraseña.

6.2.3. Adware

Si tienes iPhone probablemente alguna vez hayas sido infectado por el virus del calendario, o en un Android y Windows cuando aparece una pestaña cargada sin tu consentimiento de un aviso que muestra un mensaje de "tu dispositivo ha sido infectado, por favor instalar este software para arreglarlo" en realidad tu dispositivo no está infectado, la única infección es el adware, puedes probar borrando el navegador y reinstalarlo.

6.2.4. Gusanos

Los gusanos son virus que tienen el poder de replicarse en la red, ocasionando que haya consumos altos en la red, fallos y lentitud de la red, no es de los virus que más daño haga a tu dispositivo o a tu vida personal, pero si suele ser muy molesto ya que baja la capacidad de tu red.

6.2.5. Botnet

Existe lo que se conoce como un computador zombie, no es nada parecido a series y películas famosas de zombie, más bien tu computador queda esclavo a una red grande de ordenadores que pueden ejecutar comandos sin que el propietario lo haga, se usa para hacer ataques de denegación de servicio distribuido (DDoS) que son ataques que tratan de hacer caer alguna página web o servicio, un computador sólo no puede hacer caer una página como Amazon, pero una red de millones de computadores si puede, ahí el fin de convertir tu dispositivo en un Bot.

6.2.6. Virus informático

Las personas tienen la creencia que el malware en si son los virus, pero los virus hacen parte de la categoría de malware, un virus está diseñado con la condición de que realice acciones que perjudiquen el dispositivo, como dañarlo, alterar el software o sus funciones principales, es muy molesto debido a que no podemos usar nuestro dispositivo con regularidad gracias a la intervención del virus.

7. ATAQUES QUE NO PUEDES EVITAR

Existe una clase de vulnerabilidades, hackeos que no pueden ser evitados, por más conocimientos en seguridad que tengas, por más que seas Microsoft, Google, Amazon, o empresas tecnológicas que tengan controles de seguridad grandes, pueden lograr salir ilesos de este tipo de ataques, la vulnerabilidad que aprovechan los atacantes es conocida como vulnerabilidad Zero Day (Vulnerabilidad de día cero) y aprovecharse de la vulnerabilidad se conoce como un Zero Day Exploit.

7.1. EXPLOITS

No hemos tocado este término alrededor del libro, pero es muy importante conocerlo en el ámbito de seguridad informática, un exploit es una pieza de software con el fin de aprovecharse de una vulnerabilidad, los hackers construyen software con el fin de aprovechar las vulnerabilidades de algún sistema y con ello conseguir accesos remotos a la máquina, inyectar código malicioso u obtener credenciales.

7.2. ZERO DAY

Los Zero Day o vulnerabilidad de día cero es una vulnerabilidad que acaba de ser descubierta y que todavía no existe una actualización que solucione el problema, puede ser de algún aplicativo, sistema operativo, navegador, dispositivos electrónicos básicamente cualquier componente de hardware o software

Figura 7.1 Zero Day línea de tiempo

7.3. VULNERABILIDADES MÁS PELIGROSAS

Un hacker explora vulnerabilidades a diario, tanto hackers éticos como no éticos de sombrero negro, si un hacker ético encuentra una vulnerabilidad que puede afectar mundialmente un sistema operativo como sería Windows, normalmente el hacker va a alertar sobre esa vulnerabilidad a la entidad, las empresas pagan a los hackers por descubrir vulnerabilidades en sus sistemas dependiendo de que tan crítica es, si el hacker advierte sobre la vulnerabilidad es un gran acierto porque alerta a todas las personas que estén usando el software donde reside la vulnerabilidad puede ser un sistema operativo como Windows y a la empresa para que la pueda corregir, en este caso sería Microsoft, si la vulnerabilidad consiste en poder tomar control remoto de otro sistema operativo Windows desde un equipo sin que la persona se dé cuenta, La empresa va priorizar al máximo corregir dicha vulnerabilidad, logrando que en tiempo récord se pueda solventar y los usuarios puedan estar tranquilos, ya que empresas, personas naturales y gobierno usan los sistemas de Microsoft, pero el tiempo que esa vulnerabilidad esta sin corregir pueden explotarla y aprovecharse de ella y eso que este es el caso más optimista.

Un hacker de sombrero negro encuentra una vulnerabilidad día cero la cual permite acceder a muchos servidores por medio de una aplicación si se encuentra instalada en la maquina objetivo y ejecutar comandos de administrador sin las credenciales de acceso, el hacker no va reportar a la empresa creadora de la aplicación, haciendo que solamente el hacker conozca dicha vulnerabilidad, el hacker tiene 2 caminos, vende la vulnerabilidad al mercado negro o explota la vulnerabilidad por cuenta de él, si la vende a una organización que realiza actos criminales para obtener beneficios económicos, esta organización empezara a atacar a los objetivos de mayor importancia, una vez empiece a realizar los hackeos a las empresas, las empresa aplicaran técnicas de informática forense para saber cómo fue hackeado el servidor, ocasionando que la vulnerabilidad sea detectada, anunciada y corregida, todo esto una vez

dañando la reputación de la compañía, servicios de empresas o personas, a parte que la vulnerabilidad habrá existido hasta que alguien la explota o se descubra por otro hacker, peor sería si varios hackers encuentran la vulnerabilidad pero nadie la reporta.

7.4. CIBERGUERRA

Las vulnerabilidades de día cero también son aprovechadas por los gobiernos mundiales, afectar la economía de un país por medio de hackeos y no por medio de armas es un gran punto de ataque. En una guerra, comenzarían hackers de un gobierno a realizar ataques a páginas web, servidores del otro y viceversa, la mejor manera de lograr que estos ataques sean efectivos es por medio de vulnerabilidad de día cero, ya que el otro va tener medidas de seguridad y control ante los ataques conocidos o vulnerabilidades conocidas, si un hacker de un gobierno encuentra alguna vulnerabilidad se deberá trasmitir ese conocimiento y no reportarlo como haría un hacker ético, probablemente muchos gobiernos tengan guardado grandes cantidades de vulnerabilidades de día cero, esperando poder usarlas en algún momento.

7.5. EJEMPLO DE ZERO DAY

Un día estás hablando con una aplicación de mensajería muy común, como lo es al día de hoy WhatsApp, la persona te envía un video y se proyecta un video de manera habitual, la abres, no pasa absolutamente nada en el momento, pero por dentro el video en verdad era un archivo ejecutando código malicioso dentro de tu dispositivo, una persona tiene acceso a WhatsApp de manera remota, el encuentra chats comprometedores el cual usa para extorsionarte y pedirte dinero en cantidades por no relevar la información a tu pareja, este caso fue el que le paso a Jeff Bezos todo por un Zero Day que existía en WhatsApp el cual se pudo explotar por medio de un archivo de video que ejecutaba código malicioso dentro del dispositivo.

7.6. CONTRAMEDIDAS

Es la primera vez que no te puedo dar una solución a este tipo de hackeos, pero puedes estar aliviado si no eres una empresa, gobierno, persona famosa o de mucho dinero, ya que los Zero Day se explotan primero por este tipo de personas o entidades y posteriormente que una de estas personas fue atacada, se releva la vulnerabilidad y es corregida rápidamente, lo que tú debes hacer en ese caso es instalar la actualización para corregir la vulnerabilidad. El problema es que muchas veces aprovechan estos Zero Day automatizados y atacan a muchísima gente, lo ideal es siempre tener la última versión, no usar sistemas operativos antiguos y esperar que las actualizaciones de los sistemas sean validadas por otros usuarios, ya que una actualización nueva de iOS puede tener un Zero Day, lo ideal es actualizar un día después de que se haya publicado la actualización al menos que tu versión actual este comprometida por una vulnerabilidad de este tipo.

Se han visto muchos casos de ataques, malware y contramedidas en este libro, espero que hayas aprendido que la seguridad informática es para todos y no sólo para personas técnicas, todos usamos la tecnología y todos debemos aprender a usarla correctamente, lo ideal es que si cuidas tus cuentas bancarias así mismo cuides tus accesos a tus redes sociales u otro tipo de cuentas en Internet y recuerda “si es humano, es hackeable.

BIBLIOGRAFÍA

- Santos, J. C. (2023). seguridad informatica. cfgm. incluye cd-rom. editorial ra-ma.
- Varon, A. A. R. (2023). Hacking Con Ingenieria Social. Tecnicas Para Hackear Humanos. Mundo Hacker (informatica General). Ra-ma Editorial.
- Varon, A. A. R. (2023). Hacking Con Ingenieria Social. Tecnicas Para Hackear Humanos. Mundo Hacker (informatica General). Ra-ma Editorial.
- B, A. K. (2016b). Hacking Etico 101 - Cómo hackear profesionalmente en 21 días o menos!: 2da Edición. Revisada y Actualizada a Kali 2.0. (2.). Createspace Independent Publishing Platform.
- Wise, D. (2022). Psicología Oscura: La Guía Definitiva de la Psicología Oscura, Un Nuevo Enfoque de la Persuasión y la Manipulación a Través de las Mejores Técnicas . . . PNL y Lenguaje Corporal (Spanish Edition). Independently published.
- B, A. K. (2017). Hacking Wireless 101: ¡Cómo hackear redes inalámbricas fácilmente!: 2 (1.). Createspace Independent Publishing Platform.
- Ghimiray, D. (2022, 7 enero). What are Wi-Fi security protocols and are they encryption tools? https://www.avast.com.
- Platzi. (2020, 25 noviembre). Ataques hacker casi imposibles de detener: 0-day exploits [Vídeo]. YouTube. https://www.youtube.com/watch?v=gjV6wbEipW4
- Rogers, M. (2022, 18 febrero). What the Jeff Bezos WhatsApp Hack Means for App Security. Okta, Inc. https://www.okta.com/blog/2020/04/what-the-jeff-bezos-whatsapp-hack-means-for-app-security/
- Mumford, A. (2022, 18 marzo). A LAN, abbreviated from Local Area Network, is a network that covers a small geographical area such as homes, offices, and groups of buildings. Whereas a WAN, abbreviated from Wide Area Network, is a network that covers larger geographical areas that can span the globe. An example of a widely. . .. Purple.

https://purple.ai/blogs/whats-the-difference-between-a-lan-and-a-wan/

- Allen, S. (2018). Técnicas prohibidas de Persuasión, manipulación e influencia usando patrones de lenguaje y técnicas de PNL (2a Edición): Cómo persuadir, influenciar y manipular usando patrones de lenguaje y PNL. Createspace Independent Publishing Platform.
- El comercio electrónico está en auge pero ¿Es seguro para los consumidores? (s. f.). ESET. https://www.eset.com/sk/blog/skodlivy-kod-digitalne-hrozby/el-comercio-electronico-esta-en-auge-pero-es-seguro-para-los-consumidores/
- Red LAN - Concepto, tipos, topologías y qué es Internet. (s. f.). Concepto. https://concepto.de/red-lan/