Instituto Tecnológico De Aguascalientes.

Sistemas y computación

Ingeniería en tecnologías de la información y comunicaciones.

SEGURIDAD EN LAS APLICACIONES DE SOFTWARE TC2 2024B

Unidad 2.

Actividad 2.2 – Caso de estada y Top Ten de antivirus.

Docente: Lic. Ricardo Luna Carlos.

Alumnos:

Ramos Sánchez Axel Gael – 20151630.

Flores Rodríguez Agustín Quetzal – 20151633.

García Betts Gabriel Sebastián – 20151621.

Jiménez Herrera Cristian – 20151639.

Diego Alejandro Campos Delgado – 20151718

02 de octubre del 2024.

Aguascalientes, Ags

Tabla de contenido

Introducción.

La Estafa del Espejo Retrovisor es una modalidad de fraude digital que ha ganado popularidad en los últimos años, aprovechándose de la vulnerabilidad psicológica de las personas mediante técnicas de ingeniería social. En esta estafa, los atacantes suelen utilizar tácticas de phishing y simulación de incidentes para generar situaciones de pánico en la víctima, lo que los lleva a actuar de manera impulsiva y a compartir información personal o realizar pagos indebidos. Este tipo de actividad delictiva refleja la creciente sofisticación de los cibercriminales, quienes emplean métodos más complejos y personalizados para lograr sus objetivos.

En este contexto, la protección mediante un antivirus adecuado juega un papel crucial para detectar y prevenir estas amenazas. En la investigación se analiza el Top Ten de los antivirus más recomendados por los expertos, así como una comparativa con el software de protección instalado en casa, para determinar la eficacia de los diferentes productos en la lucha contra estafas como la del espejo retrovisor.

Estafa del espejo retrovisor.

La **Estafa del Espejo Retrovisor** es una modalidad de estafa digital que se ha vuelto popular, involucrando técnicas de ingeniería social, phishing y manipulación psicológica. Aunque es menos conocida que otros tipos de estafas cibernéticas, está ganando notoriedad debido a su efectividad. Vamos a desglosar esta estafa y los puntos clave relacionados con la materia de ciberseguridad.

Desarrollo de la Estafa del Espejo Retrovisor.

1. **Descripción de la Estafa**:
    - **Ingeniería Social**: Los delincuentes se aprovechan de la confianza o el desconocimiento de las víctimas para obtener información personal o acceso a sus cuentas. En el caso de la estafa del espejo retrovisor, los estafadores crean situaciones de pánico o urgencia para manipular a la víctima.
    - **Phishing**: Uno de los métodos más utilizados en este tipo de estafa es el phishing, donde los atacantes envían correos electrónicos o mensajes de texto fraudulentos que aparentan ser legítimos. Estos mensajes suelen contener enlaces maliciosos que, al ser abiertos, permiten a los delincuentes robar información sensible.
    - **Manipulación psicológica**: Se apela a emociones como el miedo, la urgencia o el alivio para que las víctimas actúen rápidamente y sin pensar, como proporcionar información personal o realizar pagos.
2. **Técnicas utilizadas**:
    - **Suplantación de identidad**: Los estafadores pueden hacerse pasar por empresas confiables o autoridades, utilizando nombres de marcas, correos electrónicos que parecen legítimos o sitios web falsos.
    - **Simulación de accidentes**: El término "espejo retrovisor" hace referencia a incidentes relacionados con supuestos accidentes

automovilísticos en los que los estafadores contactan a la víctima alegando que ha estado involucrada en un incidente. Les piden que realicen pagos o proporcionen información para "resolver" el problema.

3. **Temas específicos**:
    - **Phishing**: Las víctimas reciben correos electrónicos o mensajes con enlaces que llevan a sitios fraudulentos donde se les solicita información personal o financiera.
    - **Software malicioso (malware)**: Al abrir los enlaces o archivos adjuntos, la víctima puede descargar malware que los estafadores usan para espiar, robar datos o secuestrar dispositivos.
    - **Fraude financiero**: Muchas de estas estafas tienen como objetivo final el robo de dinero, ya sea directamente a través de transferencias bancarias fraudulentas o al obtener acceso a cuentas financieras de la víctima.

Análisis de Antivirus: Protección contra la Estafa del Espejo Retrovisor.

Para combatir estas amenazas, es esencial contar con una protección adecuada en el hogar. Realizaremos una comparación entre los antivirus más populares según los expertos y el antivirus instalado en casa.

Top Ten de los Antivirus (2024)

1. **Bitdefender**

   Ventajas:

- Excelente protección contra malware y phishing.
- Ofrece navegación segura y un gestor de contraseñas. Desventajas:
- Puede ralentizar el sistema en ciertos dispositivos.

2. **Norton 360**

   Ventajas:

   - Protección en tiempo real contra amenazas.
   - Monitoreo de la dark web para proteger información personal. Desventajas:
   - Precio más alto en comparación con otros antivirus.

3. **McAfee Total Protection**

   Ventajas:

   - Fuerte protección contra amenazas y ataques de phishing.
   - Red de protección en múltiples dispositivos. Desventajas:
   - La interfaz puede ser confusa para usuarios principiantes.

4. **Kaspersky Total Security**

   Ventajas:

   - Gran capacidad de detección de phishing y malware.
   - Filtro de protección para pagos en línea. Desventajas:
   - Relación controversial con gobiernos, lo que puede generar desconfianza.

5. **Avast Premium Security**

   Ventajas:

   - Excelente protección contra phishing y vulnerabilidades de red.
   - Protección para varios dispositivos. Desventajas:

- Reportes recientes sobre la venta de datos de usuarios han dañado su reputación.

6. **ESET NOD32**

   Ventajas:

   - Ligero y rápido, ideal para usuarios con computadoras menos potentes.
   - Alta precisión en la detección de malware. Desventajas:
   - Pocas funciones adicionales más allá de la protección básica.

7. **Webroot SecureAnywhere**

   Ventajas:

   - Sistema muy ligero y rápido.
   - Protección en tiempo real contra malware. Desventajas:
   - Menos funciones de protección adicional en comparación con otros antivirus.

8. **Trend Micro Maximum Security**

   Ventajas:

   - Protección efectiva contra phishing.
   - Seguridad para transacciones bancarias en línea. Desventajas:
   - Impacto en el rendimiento del sistema en algunos dispositivos.

9. **Sophos Home**

   Ventajas:

   - Gran opción para familias, permite proteger múltiples dispositivos.
   - Funciones de control parental. Desventajas:
   - Falta de algunas funciones avanzadas que ofrecen otros competidores.

10. **Panda Dome**

    Ventajas:

    - Protección contra amenazas emergentes y phishing.
    - Interfaz amigable y fácil de usar. Desventajas:
    - Poca protección adicional más allá de antivirus y antiphishing.

Comparativa del Antivirus en Casa Vs. Los Populares.

Antivirus en casa.

CCleaner:

CCleaner es una herramienta de optimización para sistemas Windows, macOS y Android, diseñada para mejorar el rendimiento del equipo al limpiar archivos innecesarios y gestionar la configuración del sistema. Aquí están sus características principales:

Características de CCleaner:

1. **Limpieza de archivos temporales**:
    - Elimina archivos temporales, cachés del sistema y del navegador, cookies, historial de navegación y otros datos que ocupan espacio en el disco.
    - Compatible con varios navegadores como Chrome, Firefox, Edge, entre otros.
2. **Optimización del rendimiento**:
    - Libera espacio en el disco al borrar archivos innecesarios.
    - Reduce la carga del sistema al desactivar programas que se inician automáticamente con el sistema operativo.
3. **Limpieza del Registro de Windows**:
    - Corrige errores y entradas obsoletas en el registro, lo que ayuda a mejorar la estabilidad y el rendimiento del sistema.
4. **Desinstalador de programas**:
    - Permite desinstalar programas de manera sencilla, eliminando archivos residuales que otros desinstaladores pueden dejar atrás.
5. **Gestión de programas en el inicio del sistema**:

    - Facilita la desactivación o activación de programas que se ejecutan al iniciar el sistema, reduciendo el tiempo de arranque.

6. **Borrado seguro de archivos**:
    - Permite eliminar archivos de manera permanente y segura para evitar su recuperación.
7. **Actualizador de software (Pro)**:
    - Detecta programas desactualizados en el equipo y facilita la actualización de los mismos para mantener el sistema seguro.
8. **Monitoreo en tiempo real (Pro)**:
    - La versión Pro ofrece un monitoreo continuo del sistema para detectar problemas de rendimiento o acumulación de archivos no deseados en tiempo real.
9. **Gestión de complementos y extensiones del navegador**:
    - Permite deshabilitar o eliminar complementos y extensiones no deseadas de los navegadores.
10. **Análisis y reparación de discos duros**:
    - Incluye herramientas para verificar y optimizar el estado de los discos duros.
11. **Programador de limpiezas automáticas (Pro)**:
    - La versión Pro permite programar limpiezas automáticas del sistema en intervalos regulares.

Versiones de CCleaner:

- **CCleaner Free**: Incluye las funciones básicas de limpieza de archivos, optimización del sistema y eliminación de programas.
- **CCleaner Professional**: Añade características como monitoreo en tiempo real, actualizaciones automáticas de software y programación de limpiezas.
- **CCleaner Professional Plus**: Ofrece funciones adicionales como la optimización de discos y herramientas avanzadas de análisis de hardware.

Ventajas:

- Mejora la velocidad y rendimiento del sistema.
- Fácil de usar, con una interfaz intuitiva.
- Herramienta todo en uno para limpieza y optimización del sistema.

Desventajas:

- En su versión gratuita, no ofrece protección en tiempo real ni automatización.
- En algunos casos, la limpieza excesiva del registro puede causar problemas si no se utiliza con precaución.

Seguridad de Windows (Windows Defender):

Windows Defender (ahora conocido como **Microsoft Defender Antivirus**) es la solución de seguridad integrada en los sistemas operativos Windows. Ofrece protección en tiempo real contra amenazas como virus, malware, spyware y ataques de phishing, con el objetivo de proteger los equipos de usuarios y empresas.

Características de Windows Defender:

1. **Protección en tiempo real**:
    - Monitorea el sistema constantemente para detectar y bloquear virus, malware, ransomware y otras amenazas.
    - Actualizaciones automáticas de las bases de datos de virus a través de Windows Update.
2. **Análisis de seguridad**:
    - Ofrece escaneos rápidos, completos o personalizados del sistema para identificar posibles amenazas.
    - Escaneo automático de archivos y programas al abrirlos o descargarlos.
3. **Protección basada en la nube**:
    - Utiliza inteligencia artificial en la nube para detectar amenazas emergentes y proteger el sistema en tiempo real.
    - Recibe información sobre amenazas de otros dispositivos protegidos por Microsoft para mejorar la detección.
4. **Protección contra phishing**:

- Integrado con Microsoft Edge, Defender detecta y bloquea sitios web fraudulentos que intentan robar datos personales.
- Puede bloquear sitios peligrosos en otros navegadores si se configura con los complementos adecuados.

5. **Control de aplicaciones**:
   - Supervisa aplicaciones y archivos ejecutables, permitiendo solo aquellos que sean confiables o estén debidamente firmados.
6. **Protección contra ransomware**:
   - Incluye la función **"Control de acceso a carpetas"**, que protege archivos y carpetas específicas contra accesos no autorizados por malware o ransomware.
   - Permite hacer una lista de aplicaciones de confianza que pueden acceder a estas carpetas protegidas.
7. **Firewall de Windows**:
   - Defender incluye un firewall integrado que monitorea y controla el tráfico de red, bloqueando conexiones no autorizadas.
   - Protege tanto redes públicas como privadas.
8. **Desempeño**:
   - Consume pocos recursos del sistema, lo que lo hace eficiente sin ralentizar demasiado el equipo.
   - Está completamente integrado en Windows, lo que garantiza su compatibilidad sin necesidad de instalación adicional.
9. **Protección en la nube empresarial** (Microsoft Defender para empresas):
   - Ofrece administración avanzada de amenazas, informes centralizados y herramientas de análisis para entornos empresariales.

Ventajas:

- Gratuito y preinstalado en todos los sistemas Windows, sin costo adicional.
- Actualizaciones automáticas y protección en tiempo real sin interrupciones.
- No requiere configuraciones avanzadas, es ideal para usuarios promedio.

Desventajas:

- Menos funciones adicionales en comparación con antivirus pagos (como gestores de contraseñas o VPN).
- Protege principalmente en entornos de Windows, sin soporte nativo para otras plataformas como macOS.

CleanMyMac X:

CleanMyMac X es una aplicación desarrollada por MacPaw que ofrece una solución integral para mantener tu Mac limpio, optimizado y protegido contra amenazas de seguridad. Aquí tienes una descripción detallada de sus características y funcionalidades:

Características Principales:

1. **Protección Antivirus:**
    - **Moonlock Engine:** Esta tecnología antimalware analiza tu Mac carpeta por carpeta para detectar y eliminar adware, ransomware, mineros de criptomonedas y otras amenazas específicas de macOS.
    - **Protección en Tiempo Real:** CleanMyMac X ofrece protección continua contra troyanos, secuestradores del navegador y otros tipos de malware.
2. **Limpieza y Optimización:**
    - **Limpieza de Archivos Basura:** Elimina archivos temporales, cachés y otros archivos innecesarios para liberar espacio en tu disco duro.

- **Desinstalador Completo:** Ayuda a desinstalar aplicaciones de manera completa, eliminando todos los archivos asociados.
- **Mantenimiento del Sistema:** Incluye herramientas para optimizar el rendimiento del sistema, como la reparación de permisos de disco y la ejecución de scripts de mantenimiento.

3. **Monitoreo del Sistema:**
   - **Control de Salud del Mac:** Monitorea el estado de tu Mac, incluyendo el uso de la CPU, la memoria y la temperatura del hardware.
   - **Alertas de Rendimiento:** Te notifica sobre problemas potenciales y te ofrece soluciones para mantener tu Mac funcionando sin problemas.

Ventajas:

- **Interfaz Intuitiva:** CleanMyMac X tiene una interfaz fácil de usar que facilita la navegación y el uso de todas sus funciones.
- **Actualizaciones Regulares:** MacPaw proporciona actualizaciones frecuentes para mejorar la funcionalidad y la seguridad de la aplicación.
- **Certificación de Seguridad:** CleanMyMac X ha recibido la distinción oficial “Gold” por su capacidad de detectar y eliminar virus en macOS.

Desventajas:

- **Costo:** Aunque ofrece una versión gratuita, muchas de las funciones avanzadas requieren una suscripción de pago.
- **Consumo de Recursos:** Algunas funciones pueden consumir una cantidad significativa de recursos del sistema durante su ejecución.

Comparativa con los Antivirus Populares (Top Ten)

1. **Bitdefender**:
   - **Protección en tiempo real avanzada** con múltiples capas de seguridad, protección contra ransomware y un rendimiento ligero.

- **Ventajas**: Protección completa contra amenazas cibernéticas con firewall, VPN y controles parentales.
- **Desventajas**: Pago, aunque ofrece versiones gratuitas con características limitadas.

2. **Norton 360**:
   - Antivirus altamente confiable con protección avanzada, incluido un **firewall inteligente**, **protección contra ransomware** y **VPN**.
   - **Ventajas**: Protección multiplataforma (Windows, macOS, iOS, Android), control parental, gestión de contraseñas.
   - **Desventajas**: Suscripción costosa en comparación con otros antivirus.
3. **McAfee Total Protection**:
   - Proporciona **protección en tiempo real**, controles parentales, **VPN ilimitada** y administración de identidad.
   - **Ventajas**: Excelente protección en múltiples dispositivos y plataformas.
   - **Desventajas**: El impacto en el rendimiento del sistema puede ser mayor que el de otros competidores.
4. **Kaspersky Total Security**:
   - Antivirus con excelente detección de amenazas y protección contra **malware, phishing y ransomware**.
   - **Ventajas**: Fácil de usar, con **múltiples capas de seguridad**.
   - **Desventajas**: Pago y con opciones de características avanzadas limitadas en la versión gratuita.
5. **Avast Premium Security**:
   - Antivirus freemium con una buena protección básica, aunque **la versión gratuita muestra muchos anuncios** para actualizar a la versión Pro.
   - **Ventajas**: Protección sólida con buenas características en la versión de pago (VPN, firewall, etc.).

- **Desventajas**: La versión gratuita carece de características importantes como la protección contra ransomware.

6. **ESET NOD32**:
   - Antivirus ligero que ofrece una **gran protección contra malware** con un impacto mínimo en el sistema.
   - **Ventajas**: Protección completa con enfoque en usuarios avanzados y empresas.
   - **Desventajas**: Menos características adicionales en comparación con otros antivirus.
7. **Webroot SecureAnywhere**:
   - Un antivirus ligero con detección basada en la nube, ideal para **usuarios con dispositivos de bajo rendimiento**.
   - **Ventajas**: Rápido y eficiente, con un enfoque en **protección online**.
   - **Desventajas**: Puede tener dificultades al detectar amenazas más avanzadas en comparación con los líderes del mercado.
8. **Trend Micro Maximum**:
   - Antivirus especializado en **protección contra ransomware** y ataques avanzados.
   - **Ventajas**: Protección sólida con controles parentales y gestión de privacidad.
   - **Desventajas**: Impacto en el rendimiento durante escaneos.
9. **Panda**:
   - Ofrece protección **en tiempo real** con **VPN incluida en su versión completa**.
   - **Ventajas**: Muy fácil de usar, especialmente para principiantes.
   - **Desventajas**: Las funciones avanzadas requieren una suscripción paga.
10. **Sophos**:
    - Solución de seguridad orientada a **protección familiar**, con controles parentales y **protección multiplataforma**.

- **Ventajas**: Excelente protección para toda la familia, incluye versiones gratuitas con funciones básicas.
- **Desventajas**: Menos características en la versión gratuita en comparación con otros antivirus.

Conclusión.

Se comprendió con claridad la actividad y algo que se gustaría recalcar es que la “estafa del espejo” es una manera de estafar con mucha facilidad ya que personas que no conocen de estafas pueden caer sumamente fácil ya que, crean un ambiente de confianza al momento de pasar el contacto después de ocasionar el accidente y el primer error que comete la gente es acceder a la información que el estafador les manda y sin verificar. Es muy importante nunca llenar datos personales ya que con esto ocasionamos que hayamos caído completamente en la estafa.

Con respecto al antivirus nos podemos dar cuenta que existen muchas opciones para adquirir un antivirus, al tener este servicio podemos evitar entrar a una página maliciosa y obviamente evitar virus que puedan entrar a nuestra computadora. También nos podemos dar cuenta de todos los beneficios que tienen los antivirus de paga, por esa razón no tenemos que descartar la idea de contratar uno de esos antivirus en vez de utilizar los de casa. Además, es importante contar con un antivirus ya que nos pueden evitar muchos problemas en un futuro y evitar perder información valiosa que se encuentra dentro de nuestra computadora.

Referencias.

[1]. Collins, B. (2022, marzo 8). The best antivirus software in 2024 for PC. TechRadar. https://www.techradar.com/best/best-antivirus

[2]. Rubenking, N. J. (2024, septiembre 24). The best antivirus software for 2024. PCMAG. https://www.pcmag.com/picks/the-best-antivirus-protection

[3]. Spadafora, A. (2022, octubre 4). The best antivirus software 2024: Free and paid options. Tom's Guide. https://www.tomsguide.com/us/best-antivirus,review-2588.html

[4]. Test antivirus software for Windows 10 - August 2024. (s/f). Av-test.org. Recuperado el 2 de octubre de 2024, de https://www.av-test.org/en/antivirus/home-windows/

[5]. TikTok - make your day. (s/f). Tiktok.com. Recuperado el 2 de octubre de 2024, de https://vm.tiktok.com/ZMhhUm56H/