Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD

Boletín Informativo

Dieciséis

Junio: ¿Cómo Mantener Seguros sus Dispositivos Móviles?

VIEM
Vicerrectoría de Innovación y Emprendimiento

ECBTI
Escuela de Ciencias Básicas, Tecnología e Ingeniería

Semillero de Investigación
Ceros y Unos

Boletín de Ciberseguridad

Medio de Divulgación del Centro de Respuestas a Incidentes Informáticos: CSIRT Académico UNAD

E-boletín Informativo CSIRT Académico UNAD

Edición electrónica, financiada por la Universidad Nacional Abierta y a Distancia (UNAD)

Medio de divulgación: Correo Electrónico, Sitio Web

Incluye: Noticias, alertas o informes relacionados con la disciplina de la ciberseguridad

Número Dieciséis
Junio de 2023

Universidad Nacional Abierta y a Distancia (UNAD)
Vicerrectoría de Innovación y Emprendimiento (VIEM)
Escuela de Ciencias Básicas Tecnología Ingeniería (ECBTI)
CSIRT Académico UNAD

Vicerrectoría de Innovación y Emprendimiento (VIEM)
Ing. Andrés Ernesto Salinas - Vicerrector

Escuela de Ciencias Básicas Tecnología e Ingeniería (ECBTI)
Ing. Claudio Camilo González Clavijo – Decano

Especialización en Seguridad Informática (ECBTI)
Ing. Sonia Ximena Moreno Molano – Líder Programa de Especialización en Seguridad Informática

Semillero de Investigación Ceros y Unos, adscrito al Grupo de Byte InDesign

Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD
Ing. Luis Fernando Zambrano Hernández – Director
CSIRT Académico UNAD

Responsable de la Edición
Ing. Luis Fernando Zambrano Hernández

Revisó
Ing. Diego Fernando Medina Soto
Director CCAV Facatativá

Estado legal:
Periodicidad: Quincenal
ISSN: 2806-0164

Universidad Nacional Abierta y a Distancia
Calle 14 sur No. 14-23 |Bogotá D.C
Correo electrónico: csirt@unad.edu.co
Página web: https://csirt.unad.edu.co

Tabla de Contenido

Boletín informativo Número 16

Junio 25 de 2023

¿Cómo Mantener Seguros sus Dispositivos Móviles?

Autores:

Fernando Zambrano Hernández
CSIRT Académico UNAD
https://orcid.org/0000-0002-4690-3526

Hernando José Peña Hidalgo
CSIRT Académico UNAD
https://orcid.org/0000-0002-3477-2645

Yenny Stella Nuñez Álvarez
ORCID: https://orcid.org/0000-0003-0128-1214

Néstor Raúl Cárdenas Corral
CSIRT Académico UNAD
https://orcid.org/0000-0003-3691-0148

Introducción

Nota.1: [Fotografía] Recuperado de https://www.freepik.es/

En la actualidad, los dispositivos se han convertido en un apoyo tecnológico para el desarrollo de nuestras actividades diarias. En estos, se almacena gran cantidad de información personal que pasa de datos de contacto hasta contraseñas y datos de orden financiero y de salud. Mantener seguros estos dispositivos que cada día están más presentes en nuestra vida cotidiana es una prioridad. Por consiguiente, es necesario conocer un poco sobre los riesgos a los que nos enfrentarnos y cómo hacer uso de herramientas que protejan nuestra privacidad y que prevenga posibles ciberataques.

El presente boletín muestra recomendaciones que contribuyen en optimizar la seguridad de nuestros dispositivos móviles

Desarrollo

¿Qué se considera como dispositivos móviles?

Se considera como dispositivo móvil a cualquier medio electrónico portátil el cual permita realizar tareas y acceder a servicios y aplicaciones de forma práctica y en cualquier momento. Siendo altamente funcionales ya que están diseñados para ser transportados por el usuario de forma ágil y fácil.

Algunos dispositivos móviles con los que interactuamos en el día a día son:

- Teléfonos inteligentes (Smartphone)
- Tabletas
- Computadores portátiles
- Smartwatches (relojes inteligentes)
- Dispositivos de internet de las cosas[1]
- Consolas de juegos portátiles

Ilustración 1: Evolución de los dispositivos móviles

Fuente: https://www.brainvire.com/wp/wp-content/uploads/2017/01/The-Future-of-Mobile-Computing-Is-Bright-Set-To-Take-Major-Business-Sectors-by-Storm-image-03-1024x563-1.png

La imagen anterior, presenta una línea de evolución de la tecnología en los últimos treinta años donde los factores de diferencia en la evolución giran en torno a: el tamaño y la portabilidad, el acceso a internet, el uso de pantallas táctiles e interfaces intuitivas y la potencia y rendimiento respecto al procesamiento y almacenamiento de los datos.

[1] Proceso que permite conectar los elementos físicos cotidianos al Internet: desde los objetos domésticos comunes, como las bombillas de luz, hasta los recursos para la atención de la salud, como los dispositivos médicos; las prendas y los accesorios personales inteligentes; e incluso los sistemas de las ciudades inteligentes. Recuperado de: ¿Qué es el Internet de las cosas (IoT) y cómo funciona? (redhat.com)

¿Cuáles son los riesgos que más se presentan en dispositivos móviles?

Al ser un dispositivo el cual puede ser transportado y conectado a en diferentes medios o redes de comunicación, estos dispositivos, presentan los siguientes riesgos:

- La falta de actualizaciones regulares del sistema operativo[2] y sus aplicaciones.
- La descarga de archivos (documentos, imágenes, audio, video) de fuentes no confiables
- El ser engañado a través de mensajes y correos electrónicos (phishing, vishing, smishing[3]) los cuales tiene como objetivo robar credenciales y datos personales. Entre otros datos.
- El conectarse a redes Wi-Fi públicas o abiertas, facilita al ciberdelincuente el interceptar datos transmitidos a través de estas redes y de esta forma poder acceder a la información personal del usuario
- Los dispositivos móviles son susceptibles a la pérdida o el robo, lo que puede llevar a la exposición de información sensible.
- La aceptación de parte del usuario en la autorización de solicitudes de permisos excesivos de aplicaciones maliciosas, permite al ciberdelincuente acceder a datos y funciones del dispositivo que no son necesarias para el funcionamiento

Nota.1: [Fotografía] Recuperado de https://www.freepik.es/

¿Qué hacer para mejorar la seguridad de un dispositivo móvil?

En dispositivos móviles de tipo smartphone con sistema operativo Android o iOS (Iphone), se recomienda:

Mantenga el sistema operativo actualizado, asegurándose de tener siempre la última versión del sistema operativo Android instalada con versiones oficiales, ya que las actualizaciones suelen incluir parches de seguridad que corrigen vulnerabilidades.

Descargue aplicaciones solo de fuentes confiables (Google Play para sistema operativo Android o App store para sistema operativo iOS) con el fin de evitar el uso de aplicaciones (apps) de fuentes desconocidas, puesto que estas pueden contener malware o virus informáticos.

Habilite el bloqueo de pantalla con alguno de los métodos proporcionados por el dispositivo como: un PIN, una contraseña o un patrón de seguridad. Esto protegerá el dispositivo en caso de pérdida o robo.

Active el cifrado[4] del dispositivo, esto protegerá sus datos en caso de que alguien intente acceder físicamente al dispositivo.

Utilice una solución de seguridad móvil confiable que incluya características como escaneo de malware, protección contra sitios web maliciosos y antirrobo.

Habilite la autenticación de dos o más factores para las cuentas de usuario que puedan ser configuradas en el dispositivo con este control. Esto proporciona un paso adicional de seguridad al requerir un segundo o tercer método de verificación. Eje. Un código enviado al teléfono o al correo electrónico.

Los siguientes enlaces pueden ser de ayuda para activar el factor de doble autenticación en cuentas
Outlook o Gmail.
Para las cuentas de la Universidad Nacional Abierta y a Distancia lo puede consultar aquí.

Revise los permisos de las aplicaciones antes de ser instaladas. Si la tienda donde está realizando la descarga cuenta con comentarios de usuarios, téngalos presente en el momento de tomar la decisión de hacer uso de la aplicación. Así mismo verifique que la aplicación que esté intentando instalar proceda de fuentes confiables (Hacer una consulta en Internet es válido)

En lo posible, hacer uso de una aplicación VNP[5] si está conectado a una red pública. Aunque este tipo de conexiones no es recomendable, el uso de una VPN reduce el riesgo de exponer su información.

Realice copias de seguridad periódicas y ubíquelas en un espacio de confianza

Habilite la función de "Encontrar mi dispositivo. Esto le permitirá localizar, bloquear y borrar el dispositivo de forma remota en caso de pérdida o robo. Los siguientes enlaces sirven de apoyo para esta configuración:
Android o iOS

En dispositivos móviles como computadores portátiles con sistema operativo Windows:

Mantenga Windows actualizado, asegurándose de tener las actualizaciones automáticas habilitadas para recibir los últimos parches de seguridad y actualizaciones del sistema operativo. El siguiente enlace puede servir de apoyo:

Windows Update

Instale un software antivirus y antimalware confiable que incluya protección contra virus, malware y otras amenazas en tiempo real, garantizando mantener este software actualizado con el fin de obtener una protección óptima. El siguiente artículo del periódico el tiempo ilustra un poco más cuales son los activos de mayor confianza para el 2023:

"Cómo elegir los mejores antivirus para Windows 2023 en Colombia"

[2] Definición de Sistema Operativo (uaeh.edu.mx)
[3] Phishing, Vishing, Smishing, ¿qué son y cómo protegerse? | BBVA
[4] ¿Qué es el cifrado? Definición de cifrado de datos | IBM
[5] ¿Qué es una VPN? - Explicación de las redes privadas virtuales - AWS (amazon.com)

Active el Firewall[6] de Windows para proteger el computador contra accesos no autorizados desde internet. El siguiente enlace ilustra la forma de identificar si el Firewall de Windows se encuentra activo:

"Activar o desactivar el Firewall de Microsoft Defender"

Utilice contraseñas seguras robustas y únicas para sus cuentas y asegúrese de no reutilizarlas en otras cuentas. Existen programas que permiten gestionar contraseñas. Le invitamos a dar lectura al siguiente articulo:

"Los 16 mejores gestores contraseñas para proteger y recordar todas las que tengas"

Si cuenta con un sistema operativo Windows versión Pro o Enterprise puede habilitar el cifrado de disco, esto permite proteger los datos en caso de pérdida o robo del dispositivo portátil. Le invitamos a dar lectura al siguiente articulo:

"Activar el cifrado de dispositivo"

Revise y deshabilite servicios y características que no sean necesarias. Esto podrían ser puntos vulnerables para posibles ataques.

Configure cuentas de usuario con privilegios limitados. Una buena práctica es hacer uso de una cuenta estándar para el uso diario y una cuenta de administrador solo cuando sea necesario realizar cambios en el sistema. El siguiente enlace puede ser de apoyo para configurar cuentas con o sin privilegios:

"Crear una cuenta de administrador o de usuario local en Windows"

Habilite BitLocker To Go para unidades USB

"Preguntas más frecuentes sobre BitLocker"

Realice copias de seguridad periódicas de los datos importantes de forma regular en un dispositivo externo o en la nube para evitar pérdidas de datos en caso de un problema de seguridad o un fallo del sistema.

No abra correos electrónicos o enlaces de fuentes desconocidas o sospechosas.

[6] ¿Qué es un firewall? - Soporte técnico de Microsoft

Canales de comunicación

El CSIRT Académico UNAD, actualmente cuenta con los siguientes canales de comunicación:


Correo: csirt@unad.edu.co


Twitter: @csirtunad


Página web: https://csirt.unad.edu.co