Universidad Nacional Abierta y a Distancia
ACREDITADA EN ALTA CALIDAD

Centro de Respuestas a Incidentes Informáticos
CIP - CSIRT Académico UNAD

Boletín Informativo
Número **DOS**

ECBπ
Escuela de Ciencias Básicas, Tecnología e Ingeniería

VIEM
Vicerrectoría de Innovación y Emprendimiento

Semillero de Investigación
Ceros y Unos

E-boletín Informativo CIP- 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 Dos
Febrero de 2022

Universidad Nacional Abierta y a Distancia (UNAD)
Vicerrectoría de Innovación y Emprendimiento (VIEM)
Escuela de Ciencias Básicas Tecnología Ingeniería (ECBTI)
CIP – 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
CIP – CSIRT Académico UNAD
Ing. Luis Fernando Zambrano Hernández – Director CIP CSIRT Académico UNAD

Responsable de la Edición
Ing. Luis Fernando Zambrano Hernández

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 2

Febrero 28 de 2022

Como Identificar Correos Electrónicos Con Contenido Malicioso

Autor: Luis Fernando Zambrano Hernández
ORCID: https://orcid.org/0000-0002-4690-3526

Introducción

En ocasiones, se ha evidenciado que a las cuentas de correo institucionales o personales llegan mensajes sugestivos con **asuntos** que al ser leídos generan nervios o inquietud por saber cuál es su información y en el momento de acceder al mensaje se presenta un incidente informático. La ciberseguridad reconoce estas acciones como un ciberataque denominado: **Ingeniería Social, usando técnicas como el Phishing, Vishing o Smishing.** Estas tienen como propósito que los usuarios revelen información personal o corporativa que pueda afectar su identidad física o digital[1] o, permitir al ciberdelincuente controlar sus dispositivos tecnológicos.[2]

Figura 1. Vector de Ordenador/ macrovector

https://www.freepik.es/vectores/ordenador

[1] *"es la versión en internet de la identidad física de una persona"* Identidad digital: ¿Qué es y cómo protegerla? [en línea]. Banco BBVA. Disponible en: Identidad digital: ¿Qué es y cómo protegerla? | BBVA

[2] Guía de Ciberataques. [en línea] Oficina de Seguridad del Internauta. Disponible en: https://www.osi.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf

Desarrollo

Mensajes con asuntos como los que se relacionan a continuación o como el que muestra la Figura 1, presentan un riesgo para la comunidad Unadista y en general para todas las personas que usen el servicio de **correo electrónico**, ya que, a partir del acceso o descargue del archivo adjunto, que por lo general son de tipo PDF o imagen, los dispositivos de cómputo pueden ser comprometidos con la instalación de un malware[3] (en próximos boletines se profundizará esta técnica de ataque). A continuación, se presentan algunos **asuntos** de correos identificados en la bandeja de entrada del servicio de correo de la UNAD[4]

- Atraso en obligaciones
- Noticia importante
- Requerimiento Judicial Fiscalía 04
- Ultimo llamado Requerimiento Fiscal
- Verificación de Tutela #9348293493
- Juzgado 05 Civil Primer Llamado
- Despacho 06 Civil Boleta de Citación
- Citación Juzgado Municipal
- Boleta de Citación Juzgado Municipal

Figura 2. Correo con indicadores de posible ataque informático

Fuente. Correo UNAD

[3] *"término general para referirse a cualquier tipo de "malicious software" (software malicioso) diseñado para infiltrarse en su dispositivo sin su conocimiento"* ¿Qué es el malware?. Avast. Disponible en: https://www.avast.com/es-es/c-malware

[4] Información reportada al correo: seguridad.informacion@unad.edu.co

La Figura 2, presenta características a considerar para identificar si un correo puede ser fraudulento:

1. El mensaje se envía a partir de un dominio no convencional o corporativo
2. El asunto se presentan errores de digitación
3. El atacante intenta orientar a la víctima para que descargue el archivo.
4. Al dar doble clic, descargar el archivo y abrirlo, el usuario final de forma **no deliberada** está ejecutando la intención del atacante, la cual es tomar el control del equipo de cómputo y extraer información.

Buenas Prácticas

Con el fin de reducir que este tipo de ataque se materialice, tenga presente las siguientes orientaciones[5]:

- No abra mensajes de remitentes desconocidos o conocidos con archivos adjuntos cuya extensión sea ejecutable (exe, com, bat, pdf). O extensiones extrañas.
- No responda mensajes que pidan información personal o financiera desde un formulario.
- No de clic a los enlaces de un correo electrónico que desconoce.

¿Cómo identificar correos sospechosos?

- Utilizan nombres y adoptan la imagen de empresas reales, que en algunas ocasiones presentan alteración.
- Llevan como remitente el nombre de la empresa o el de un empleado real de la empresa.
- Incluyen webs que visualmente son iguales a las de empresas reales.
- Algunos utilizan estrategias como ofrecer bonos de regalo o similar.
- Mantenga el sistema operativo y antivirus de su computador actualizado.

[5] Boletín Informativo por alerta de mensaje falso con virus troyano y suplantación de identidad [en línea]. Universidad Nacional Abierta y Distancia Disponible en: https://noticias.unad.edu.co/images/Boletin_Seguridad_UNAD_128_-_Mensaje_Falso_al_Correo_Institucional.pdf

¿Qué hacer en caso de haber accedido y descargado un archivo?

Si por algún motivo descargó y abrió el archivo adjunto realice los siguientes pasos:

- Avise a la persona encargada de las TI de la organización
- Si es su computador personal el que está comprometido, ejecute el antivirus con el fin de poder contener la intención del ataque

Nota: Pude usar portales web como https://www.virustotal.com, los cuales realizan análisis a los archivos sospechosos pasándolo por más de 30 bases de datos de antivirus e indicando si este presente alguna alerta de posible afectación para su dispositivo

- En cuentas de Gmail[6] o Microsoft[7], puede activar el doble factor de autenticación, este servicio es gratuito y eleva el nivel de seguridad del correo institucional.

Si ha presentado algún evento de este orden, notifique al correo seguridad.informacion@unad.edu.co

Canales de comunicación

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

- Correo: csirt@unad.edu.co
- Twitter: @csirtunad

[6] Como Activar la verificación en 2 pasos. [en línea]. Google. Disponible en: https://support.google.com/accounts/answer/185839?hl=es-419&co=GENIE.Platform%3DDesktop

[7] Activar o desactivar la verificación en dos pasos de una cuenta de Microsoft. [en línea]. Microsoft. Disponible en: https://support.microsoft.com/es-es/account-billing/activar-o-desactivar-la-verificaci%C3%B3n-en-dos-pasos-de-una-cuenta-de-microsoft-b1a56fc2-caf3-a5a1-f7e3-4309e99987ca

Recursos bibliográficos consultados

[1] *"es la versión en internet de la identidad física de una persona"* Identidad digital: ¿Qué es y cómo protegerla? [en línea]. Banco BBVA. Disponible en: Identidad digital: ¿Qué es y cómo protegerla? | BBVA

[2] Guía de Ciberataques. [en línea] Oficina de Seguridad del Internauta. Disponible en: https://www.osi.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf

[3] *"término general para referirse a cualquier tipo de "malicious software" (software malicioso) diseñado para infiltrarse en su dispositivo sin su conocimiento"* ¿Qué es el malware?. Avast. Disponible en: https://www.avast.com/es-es/c-malware

[4] Información reportada al correo: seguridad.informacion@unad.edu.co

[5] Boletín Informativo por alerta de mensaje falso con virus troyano y suplantación de identidad [en línea]. Universidad Nacional Abierta y Distancia Disponible en: https://noticias.unad.edu.co/images/Boletin_Seguridad_UNAD_128_-_Mensaje_Falso_al_Correo_Institucional.pdf

[6] Como Activar la verificación en 2 pasos. [en línea]. Google. Disponible en: https://support.google.com/accounts/answer/185839?hl=es-419&co=GENIE.Platform%3DDesktop

[7] Activar o desactivar la verificación en dos pasos de una cuenta de Microsoft. [en línea]. Microsoft. Disponible en: https://support.microsoft.com/es-es/account-billing/activar-o-desactivar-la-verificaci%C3%B3n-en-dos-pasos-de-una-cuenta-de-microsoft-b1a56fc2-caf3-a5a1-f7e3-4309e99987ca