



Prueba Inicial – Correo electrónico

1. Introducción

Una de las principales fuentes de infección de código malicioso en las organizaciones y los hogares, es a través de archivos adjuntos en los correos electrónicos recibidos por los usuarios, tanto al correo electrónico de la organización como al personal, consultados desde Internet.

Por esta razón, es muy importante concientizar a los usuarios de las consecuencias que puede tener, el descargar y ejecutar en su equipo un archivo adjunto infectado.

La presente prueba consiste en el envío de un correo electrónico a través de una cuenta de correo falsa, simulando ser un usuario interno de la institución. Para ello se creará una cuenta ficticia que puede ser personal o que englobe un asunto a tratar, por ejemplo auditoria@institucion.mx.

De una forma sencilla, se redactará el cuerpo de un correo el cual convenza al usuario de que descargue y ejecute un archivo adjunto infectado.

Para ello se ha diseñado un archivo que, al ser ejecutado, abre automáticamente un navegador en el equipo del usuario y lo redirige a la página web.

En ésta página, diseñada especialmente para la prueba, se advierte al usuario del peligro que puede haber causado para la institución la descarga y ejecución de un archivo adjunto en un correo. Además, se indican una serie de medidas preventivas para evitar posibles infecciones, concientizando al usuario a mantener la seguridad de la red institucional.

Es importante mencionar que no será identificado ni utilizado ningún dato personal de los participantes en la prueba.

2. Descripción

Esta prueba está basada en el envío de un correo electrónico con un archivo adjunto, el cual, al ser ejecutado, abre al usuario una página web, advirtiéndole del peligro que conlleva la acción que acaba de realizar. Para ello deben de seguirse los siguientes pasos:

a. El correo

En primer lugar, es necesario contar con el apoyo de los administradores o responsables de la creación de cuentas de correo institucionales, ya que, con su ayuda, se creará una cuenta de correo falsa para la prueba. Esta puede ser de carácter personal, haciendo uso del mismo patrón





que tenga la institución para las cuentas de correo (inicial del nombre y primer apellido, nombre y apellido separados por un punto, primer apellido y nombre...). Otra opción es el uso de una cuenta de correo genérica, con el nombre de un departamento de la institución (real o ficticio) como pueden ser: informatica@institucion.mx, sistemas@ies.edu o rrhh@anuies.mx

En el caso de que no se disponga del servicio de correo en la propia institución, se deberá solicitar una nueva cuenta de correo a quien gestione este servicio.

Después se redacta el cuerpo del correo y se envía utilizando la cuenta recién creada:

-  Se añaden como destinatarios las cuentas de correo que van a formar parte de la prueba.
-  Para dar credibilidad al correo, es recomendable que éste lleve en el campo de CC (con copia) a personal con cargo importante de la institución, de quien debe de obtenerse el permiso explícito para incluirlo en la prueba y explicarle la finalidad.
-  El asunto o subject es el título con el que se desea llegue el correo, por lo que debe de ser atractivo, claro y creíble.
-  A continuación, escribir el cuerpo del correo. Para cumplir con el contexto en el que se basa esta prueba, es recomendable generar un correo remitido por un área técnica de la institución o alguno de sus miembros, de esta forma se aporta una confianza al usuario, para que éste descargue y ejecute el archivo adjunto.
-  Un ejemplo de correo electrónico podría ser el siguiente.

Asunto: Auditoría de Seguridad Interna.

Buenos días

Desde el Departamento de Informática se hace llegar este correo informándole que en días posteriores se llevará a cabo una Auditoría de Seguridad en la institución. Uno de los procedimientos exige que se realicen ciertas comprobaciones en su equipo de cómputo.

Derivado de lo anterior, se ha adjuntado a este correo un archivo que debe ser ejecutado en cada uno de sus equipos de trabajo, con el fin de obtener el estado de las actualizaciones de seguridad del sistema operativo y de las aplicaciones.

Gracias por su colaboración.

Departamento de Informática
Nombre de la institución





 Finalmente, es indispensable no olvidar adjuntar el archivo ejecutable al correo a enviar.

 Una vez concluida la prueba y el periodo de despliegue, será necesario eliminar la cuenta falsa de correo creada. Además, se recomienda explicar los motivos de la prueba a los usuarios implicados en la misma.

b. El archivo

Se ha realizado un archivo ejecutable, el objetivo de este archivo es abrir el navegador del usuario o, en el caso de que esté abierto, abrir una pestaña nueva, que dirija a la página web de http://anuies-tic.anuies.mx/web/wp-content/uploads/2018/05/Imagen_Prueba_inicial.jpg donde se describen los peligros a los que se ha expuesto el usuario al haber ejecutado el archivo, así como las medidas que debe de tomar para no provocar una posible infección de código malicioso en la red.

El archivo debe de ser renombrado acorde al cuerpo del correo. En el caso del ejemplo anterior el nombre podría ser: *Audit.exe*, *auditoria_seguridad.exe* o *audit->nombre institución>-año.exe*

Este archivo NO es identificado por los antivirus como código malicioso. Sin embargo, al tratarse de un archivo ejecutable, es probable que el sistema operativo solicite la confirmación de que se desea ejecutar. Una de las razones de esta prueba es observar que decide hacer el usuario en este punto.

Una vez finalizada la prueba, se solicitará a los usuarios involucrados que eliminen el archivo de su equipo, en caso de haber sido descargado.

