GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA

centro nacional de inteligencia
centro criptológico nacional

CCN-CERT
centro criptológico nacional

El informe de Buenas Prácticas CCN-CERT BP-02/16 incluye un decálogo de seguridad con los principales puntos a tener en cuenta

Cómo identificar correos electrónicos dañinos y utilizarlos de forma segura

- **El CCN-CERT ha hecho público el primero de una serie de informes destinados a un público general que busca concienciar y facilitar el uso seguro de las tecnologías de la información y las comunicaciones.**

- **Este primer informe se centra en el correo electrónico, una de las herramientas más utilizadas en la comunicación e intercambio de archivos, tanto por empresas como por usuarios y, por tanto una de las preferidas por los atacantes para infectar y comprometer equipos.**

Madrid, 20 de julio de 2016.- Dar a conocer las técnicas más habituales de ingeniería social, así como los recursos utilizados por los atacantes para conseguir infectar un equipo u obtener información personal de un usuario, a través del correo electrónico, son algunos de los objetivos del primer **Informe de Buenas Prácticas**, que el **CCN-CERT** acaba de hacer público. El documento ofrece también un conjunto de pautas y recomendaciones para mitigar las acciones realizadas a través de esta herramienta, al tiempo que se ayuda a los usuarios finales a identificar los correos electrónicos dañinos.

La concienciación, el sentido común y las buenas prácticas en el uso del correo electrónico son las mejores defensas para prevenir y detectar este tipo de incidentes

El **CCN-CERT BP-02/16** incluye un primer apartado sobre el correo electrónico como vía de infección a través de ficheros ejecutables con iconos o ficheros ofimáticos con macros, así como el uso de espacios para ocultar la extensión, la usurpación del remitente o los enlaces dañinos (caso del phishing bancario, enlaces de descarga de ficheros dañinos o web exploit kits).

El informe cuenta además con una guía de buenas prácticas en el uso del correo electrónico, junto con el modo de identificar los correos dañinos mediante patrones anómalos, verificación del remitente, comprobación de los ficheros descargados o actualizaciones del sistema operativo.

Informes de Buenas Prácticas

Con este documento, el CCN-CERT ha iniciado una serie de Informes destinados a un público general que busca concienciar y facilitar el uso seguro de las tecnologías de la información y las comunicaciones. Estos documentos se irán publicando periódicamente en su portal bajo el nombre de Informes de Buenas Prácticas.

20 de julio de 2016

	Decálogo de seguridad del correo electrónico
1	No abra ningún enlace ni descargue ningún fichero adjunto procedente de un correo electrónico que presente cualquier síntoma o patrón fuera de lo considerado normal o habitual.
2	No confíe únicamente en el nombre del remitente. El usuario deberá comprobar que el propio dominio del correo recibido es de confianza. Si un correo procedente de un contacto conocido solicita información inusual contacte con el mismo por teléfono u otra vía de comunicación para corroborar la legitimidad del mismo.
3	Antes de abrir cualquier fichero descargado desde el correo asegúrese de la extensión y no se fíe por el icono asociado al mismo.
4	No habilite las macros de los documentos ofimáticos incluso si el propio fichero así lo solicita.
5	No debe hacerse clic en ningún enlace que solicite datos personales ni bancarios.
6	Tenga siempre actualizado el sistema operativo, las aplicaciones ofimáticas y el navegador (incluyendo los plugins/extensiones instalados).
7	Utilice herramientas de seguridad para mitigar *exploits* de manera complementaria al software antivirus.
8	Evite hacer clic directamente en cualquier enlace desde el propio cliente de correo. Si el enlace es desconocido es recomendable buscar información del mismo en motores de búsqueda como Google o Bing.
9	Utilice contraseñas robustas para el acceso al correo electrónico. Las contraseñas deberán ser periódicamente renovadas. Si es posible utilice doble autenticación.
10	Cifre los mensajes de correo que contengan información sensible.

Figura 6-1. Decálogo de seguridad

Sobre CCN-CERT, CERT Gubernamental Nacional

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN (www.ccn.cni.es). Este servicio se creó en el año 2006 como el **CERT Gubernamental/Nacional** español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 regulador del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

De acuerdo a todas ellas, es competencia del CCN-CERT la gestión de ciberincidentes que afecten a **sistemas clasificados**, de las **Administraciones Públicas** y de **empresas y organizaciones de interés estratégico** para el país. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

MÁS INFORMACIÓN

CCN-CERT
eventos@ccn-cert.cni.es
+34 670 29 20 05

Síguenos en
www.ccn-cert.cni.es/

@CCNCERT

http://youtu.be/5XxS9mZZfKs

20 de julio de 2016