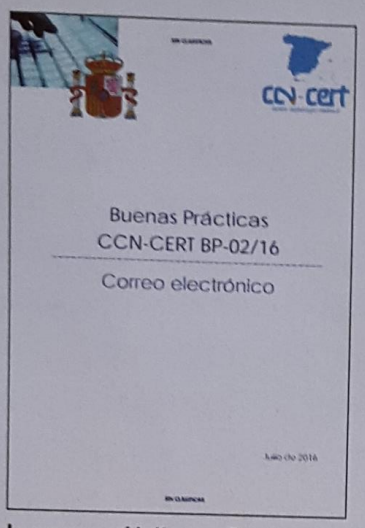
Revista SIC

El CNI inicia la publicación de una serie de informes destinados a promover el uso seguro de las TIC



Dar a conocer las técnicas más habituales de ingeniería social, así como los recursos más utilizados por los atacantes para conseguir infectar un equipo u obtener información personal de un usuario, son algunos de los objetivos del primer Informe de Buenas Prácticas CCN-CERT BP-02/16, que el **Centro Criptológico Nacional (CNI)** acaba de hacer público. Se trata del primero de una serie de documentos destinados a un público general que busca concienciar y facilitar el uso seguro de las TIC, que el Organismo irá publicando periódicamente en su portal web bajo el epígrafe "Informes de Buenas Prácticas".

El primer informe publicado dedica así sus páginas al análisis del 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 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 de forma eficaz los correos-e dañinos mediante patrones anómalos, la verificación del remitente, la comprobación de los ficheros descargados o de las actualizaciones del sistema operativo.