Proyecto de Orden para combatir las estafas telefónicas y mediante sms por suplantación de identidad.

En los últimos años estamos asistiendo a un incremento exponencial de la cibercriminalidad y, en particular, de las estafas de suplantación de identidad que suelen comenzar con una llamada o un mensaje de texto en los que el emisor de la comunicación suplanta la identidad de una organización de confianza (entidad bancaria, administración pública, empresa de transporte, etc.) con la clara intención de defraudar, engañando al consumidor para que proporcione información personal y financiera confidencial, facilite sus claves personales o realice alguna acción como el acceso a una web, la llamada a un número telefónico, la realización de una trasferencia, o la contratación de un servicio, entre otros.

Durante este verano se ha dado trámite de audiencia pública para la implantación de medidas de protección a consumidores y empresas ante estafas telefónicas y mediante SMS por suplantación de identidad. Siendo así que el plazo para presentar alegaciones abarca desde el martes, 30 de julio de 2024 hasta el domingo, 15 de septiembre de 2024.

Se han sometido a consulta pública una serie de opciones técnicas y regulatorias destinadas a prevenir y combatir este tipo de estafas y prácticas fraudulentas que se canalizan a través de llamadas y mensajes de texto.

- Bloqueo por parte de los operadores de llamadas y SMS de numeración nacional, pero con origen internacional.

- Creación de una base de datos con los usuarios que utilizan alfanuméricos en sus mensajes (por ejemplo, el nombre de la compañía). Aquellos mensajes procedentes de entidades no incluidas en esta base de datos quedarán bloqueados.

- Prohibición de numeración móvil para llamadas comerciales, de forma que la ciudadanía pueda detectar que es un fraude si reciben una llamada desde una numeración de este tipo y habilitación de los números 800 y 900 para llamadas comerciales.

Las acciones fraudulentas suelen consistir en:

1) CLI Spoofing: manipulación del identificador de la llamada (CLI - Calling line identification), para que el número coincida con el número de una empresa u organismo público.

2) SMS Smishing: envío de SMS, ya sea con identificador numérico o alfanumérico, simulando ser una entidad legítima e invitando al receptor a acceder mediante un enlace a una web falsa que simula la verdadera.

Este tipo de fraudes se han incrementado en los últimos años, según los informes del Banco de España, el Ministerio del Interior o el Instituto Nacional de Ciberseguridad (INCIBE). Estas estafas son relevantes ya que hacen disminuir la confianza de la ciudadanía en la fiabilidad y seguridad del contenido transmitido a través de las comunicaciones electrónicas, perjudicando a aquellas empresas y organismos que hacen uso de llamadas y mensajes de texto legítimamente y, además, causan importantes daños financieros y económicos a todos los sectores de la sociedad, incluidos los consumidores, las empresas y los organismos públicos.

Algunos países europeos, como Finlandia, han puesto en marcha medidas similares a las incluidas en este plan, con una gran efectividad, ya que se han reducido las estafas por suplantación de identidad en casi un 90%.

Fuente: MINECO

https://avancedigital.mineco.gob.es/es-es/Participacion/Paginas/DetalleParticipacionPublica.aspx?k=441