Gobierno de Canarias

Consejería de Administraciones Públicas, Justicia y Seguridad

Dirección General de Telecomunicaciones y Nuevas Tecnologías

cibercentro

RECOMENDACIONES ANTE ATAQUES DE "PHISHING" PARA PERSONAL EN TELETRABAJO

Para hacer frente a la actual epidemia de coronavirus, en numerosas entidades se está generalizando el uso del teletrabajo como medida para evitar contagios. En este escenario, muchos usuarios no habituados a trabajar en remoto tienen que adaptar sus hábitos de trabajo a una nueva situación, en la que las relaciones con los sistemas de soporte y atención a usuarios tienen que realizarse por cauces no habituales.

Aprovechando estas circunstancias, los ciberdelincuentes pueden intentar realizar campañas de "phishing" en las que haciéndose pasar por personal del Gobierno de Canarias, o de empresas de soporte a usuarios, pretendan obtener credenciales de acceso a los sistemas.

Recomendaciones:

Si recibe llamadas, correos, mensajes, etc., aparentemente provenientes de personal del Gobierno de Canarias, centros de atención a usuarios, etc., recuerde que:

1. **Nunca debe facilitar información de medios de acceso** (usuario y contraseña, tokens, certificados, códigos recibidos por SMS, etc.).

   Ni siquiera tratándose realmente del personal de atención a usuarios debe realizarse esta práctica, ya que el personal de atención a usuarios debe tener mecanismos para corregir incidencias, resetear contraseñas, etc., sin requerir que el usuario final se lo facilite.
2. El personal de atención a usuarios del Gobierno de Canarias cuenta con medios de acceso a las infraestructuras que les deben permitir solventar los problemas sin requerir datos del acceso de los usuarios finales.
3. Si no está detectando ningún problema en su acceso remoto, no debería recibir llamadas o correos del centro de atención a usuarios.
4. **Si está detectando problemas en su acceso remoto, contacte directamente con CiberCentro** (Sirvete, 912, 922 922 912 - 928 117 912). **No confíe en llamadas o correos "proactivos" de un supuesto centro de atención a usuarios** si no puede confirmar que se trata realmente de CiberCentro o del departamento de informática de su Consejería u Organismo.

Cuando se encuentre haciendo uso de los medios de teletrabajo del Gobierno de Canarias, también recuerde que:

5. No debe realizar simultáneamente con el mismo equipo actividades ajenas a la actividad de trabajo, como por ejemplo:
   - acceder a páginas web no relacionadas con la actividad
   - ejecutar aplicaciones no corporativas
   - abrir documentos no corporativos o recibidos desde fuentes no confiables.
   - Permitir la ejecución de macros de documentos ofimáticos.
6. Recuerde que los medios de protección en un equipo fuera de las instalaciones y redes del Gobierno de Canarias pueden ser en algunos aspectos menores que cuando se está situado dentro del perímetro de seguridad del Gobierno de Canarias.

Si recibe algún tipo de llamada o correo sospechoso, o cree que su cuenta de usuario se ha visto comprometida, debe ponerlo lo antes posible en conocimiento de CiberCentro (Sírvete, 912, 922 922 912 - 928 117 912) para que se lleve a cabo el análisis del caso y aplicar las medidas de seguridad que se requieran.

Puede consultar más información sobre incidentes de seguridad en la web de CiberCentro.