**RECOMENDACIONES DE LA SECRETARÍA GENERAL DE ADMINISTRACIÓN DIGITAL PARA SALVAGUARDAR LA SEGURIDAD DE LA ORGANIZACIÓN DURANTE EL TELETRABAJO DE LOS EMPLEADOS PÚBLICOS, ESPECIALMENTE PARA EVITAR EL ROBO DE CREDENCIALES Y CONTRASEÑAS**

En el actual escenario de confinamiento domiciliario por la situación de crisis sanitaria que ha motivado la declaración del estado de alarma, muchos empleados no acostumbrados 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*". Se trata de actuaciones delictivas en las que un tercero, haciéndose pasar por personal de la organización, muy frecuentemente por miembros de los servicios técnicos de atención a usuarios, pretenden obtener credenciales de acceso a los sistemas.

Para evitar, en lo posible, la filtración a terceros ajenos a la organización de información que comprometa la seguridad o los intereses de nuestro centro de trabajo, la Secretaría General de Administración Digital, dependiente del Ministerio de Asuntos Económicos y Transformación Digital, ha publicado las siguientes

**Recomendaciones**

Si recibe llamadas, correos, mensajes, etc., aparentemente provenientes de personal de la organización, centros de atención a usuarios, etc., **recuerde que:**

1. **Nunca debe facilitar información** de medios de acceso *(usuario y contraseña, tokens, 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 de los organismos 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.

Si está detectando problemas en su acceso remoto, **contacte directamente** con los medios de atención a usuarios que su organismo haya puesto a su disposición. No confíe en llamadas o correos "proactivos" de un supuesto centro de atención a usuarios si no puede confirmar que se trata realmente del centro de atención a usuarios del organismo.

**Cuando se encuentre haciendo uso de los medios de teletrabajo del organismo, también recuerde que:**

- 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.

- Los **medios de protección** en un equipo fuera de las instalaciones del organismo pueden ser en algunos aspectos **menores** que cuando se está situado dentro del perímetro de seguridad del organismo.

Murcia, 13 de abril de 2020.

El Servicio de Asesoramiento a Entidades Locales.