Castilla-La Mancha

Recomendaciones ante ataques de “phishing”

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 de la organización, en especial de atención a usuarios, pretendan obtener credenciales de acceso a los sistemas.

Recomendaciones

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

- **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.

- El personal de atención a usuarios cuenta con medios de acceso a las infraestructuras que les deben permitir solventar los problemas sin requerir datos del acceso de los usuarios finales.

- 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, preferentemente mediante el sistema CRU** (https://cru.jccm.es). **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 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.

- Recuerde que 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.