Alerta Seguridad Informática: Consejos para teletrabajo y COVID-19

Jue, 19/03/2020

Teletrabajo Estudiantado#UGREnCasa

Consejos útiles de fácil aplicación para facilitar la seguridad informática mientras se teletrabaja

Phishing:

1. Sea muy cuidadoso con los correos recibidos con información sobre el COVID-19.
2. No pulse enlaces ni abra archivos adjuntos en correos electrónicos, mensajes de texto, WhatsApp, etc.
3. Desconfíe de correos que soliciten donaciones a supuestas víctimas.
4. Ignore enlaces a páginas web donde ofrezcan vacunas o tratamientos para superar la enfermedad.
5. Sospeche de posibles oportunidades de inversión en compañías que afirman poder detectar, prevenir o incluso curar los efectos del virus.
6. Nunca conteste al remitente. Uno de sus objetivos es simplemente confirmar direcciones de e-mail.
7.

Y por supuesto si se el piden claves en pagina ajenas a dominio ugr.es no les haga caso.

Teletrabajo. Cuidado con el soporte técnico:

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 est práctica, ya que el personal de atención a usuarios debe tener mecanismos para corregi 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 correos del centro de atención a usuarios.

4. 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, en nuestro caso el 36000 o 958241010 opcion 3. 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

Recuerda que cualquier información oficial se hará a través de los canales definidos por la Universidad de Granada en https://covid19.ugr.es y el email @email.

Compartir en