Recomendaciones de seguridad informática COVID-19

A nivel mundial se están detectando numerosos incidentes de seguridad que intentan aprovechar la crisis del COVID-19 para suplantar a organismos oficiales con el fin de acceder a equipos y sistemas y obtener información, ya sea personal (claves de acceso, datos bancarios, etc.) o corporativa.

A nivel institucional, recuerde que cualquier medida que adopte la Universidad de Jaén respecto al COVID-19 será comunicada a través de la página "Información sobre el coronavirus COVID-19" de la UJA.

Por otra parte, el Servicio de Informática está aplicando las medidas de seguridad recomendadas por el Centro Criptológico Nacional (CCN) en relación a este tema.

A continuación, le trasladamos las recomendaciones básicas de seguridad informática que, como miembro de la comunidad universitaria, deberá seguir:

- ¡Cuidado con los bulos!
    - No difunda información que no provenga de medios y fuentes oficiales.
    - No contribuya a la difusión de contenido no contrastado.
    - No comparta mensajes que puedan generar alarma en la población.
- No descargue aplicaciones no oficiales para conocer el alcance y evolución del COVID-19. Muchas de ellas están creadas al objeto de infectar el equipo en el que sean instaladas.
- No responda a mensajes que soliciten claves de usuario, datos personales o bancarios. El Servicio de Informática nunca le solicitará, por ningún medio, las claves de su cuenta TIC de la UJA.
- No abra ficheros adjuntos ni enlaces contenidos en correos sospechosos o procedentes de remitentes desconocidos. Incluso si alguien aparentemente conocido le solicita información inusual, contacte con él mediante una llamada telefónica a fin de corroborar la legitimidad de su correo. Puede consultar al Servicio de Informática los correos sospechoso a través de la dirección *abuse@ujaen.es* o mediante la plataforma Murphy.
- Tenga precaución con las llamadas de teléfono suplantando a un servicio técnico. Se están utilizando para engañar a los usuarios, obteniendo información confidencial o solicitando suscripción a números de tarificación especial.

- Utilice contraseñas robustas y renuévelas de forma periódica. No reutilice la contraseña de su cuenta TIC de la UJA en otros servicios o aplicaciones. Asimismo, en general, guardar las contraseñas en el navegador no es una buena práctica.
- Tenga siempre instalado en su equipo windows la última versión de antivirus corporativo (actualmente, Panda Dome). Recuerde que ningún antivirus le proporciona una seguridad contra virus/malware al 100%. Por ello, debe seguir siempre todas las recomendaciones de seguridad que aquí le indicamos.
- Mantenga actualizado su sistema operativo y navegador instalando los parches de seguridad que proporciona de forma automática y periódica el fabricante.
- Si utiliza un equipo portátil propiedad de la UJA, recuerde que debe utilizarlo exclusivamente para fines laborales. Asimismo, si utiliza su equipo particular para acceder a aplicaciones corporativas de la UJA, extreme las precauciones siguiendo todas las recomendaciones aquí indicadas y procure realizar siempre una navegación segura por Internet.
- Para velar por la seguridad de la información corporativa, desde el Servicio de Informática se están monitorizando los accesos remotos (VPN, escritorio remoto, etc.) a los servicios y sistemas y, si fuera necesario, se activarán controles adicionales a los actuales.
- Realice una copia de seguridad de forma periódica. Recuerde que si sus ficheros son eliminados o cifrados por algún virus o software malicioso (malware), la única solución para recuperar su información es a partir de una copia de seguridad.

Información adicional interesante:

- UJA
  - Recomendaciones de seguridad informática
  - Guía para evitar el Phising
  - Uso seguro de la web
  - Guía para realizar una copia de seguridad
- OSI (Oficina de Seguridad del Internauta)
  - Coronavirus, ¿cómo podemos ayudarte a trabajar desde casa de manera segura?
  - Ponle freno a las noticias falsas
- CCN (Centro Criptológico Nacional)
  - Ciberconsejos - Phising
  - Ciberconsejos - Bulos
- Bulos sobre coronavirus
  - OMS (Organización Mundial de la Salud)
  - Maldita.es