

Recomendaciones ciberseguridad frente al COVID-19

En este contexto en el que nos encontramos, además del virus (coronavirus - COVID-19) que monopoliza las noticias, están igualmente proliferando otros "virus" (los creados por los ciberdelincuentes) tratando de aprovecharse de la intensidad con la que todos estamos siguiendo de cerca la actualidad y las noticias. Muchas personas están trabajando desde sus casas y es posible que nos relajemos en la atención y cuidado que habitualmente debemos tener y que periódicamente os recordamos. También es posible que no configuremos adecuadamente nuestros equipos.

Debemos ser especialmente cuidadosos cuando accedemos a los recursos del trabajo desde nuestra casa.

Os damos un conjunto de recomendaciones y recordatorios en materia de seguridad (ciberseguridad) que son aplicables tanto a nivel laboral como personal:

- * Se han creado páginas web maliciosas que ofrecen información sobre el COVID-19, con el fin de infectar los equipos de los usuarios que acceden a las mismas desde el domicilio propio; nuestra seguridad depende fundamentalmente de la atención y cuidado que podamos prestar.

- * Evitad abrir documentos y archivos adjuntos que nos lleguen por correo, WhatsApp y otros medios que contengan supuesta información sobre el COVID-19. Toda la información relevante que debemos conocer nos llegará por canales oficiales, televisión,... y también por los medios habituales de la Universidad de Zaragoza.

- * No descargues aplicaciones no oficiales para conocer el alcance y evolución del COVID-19. Muchas de ellas están creadas con el objetivo de infectar el equipo (PC, móvil, tablet) en el que sean instaladas y ejecutadas.

- * Evitad colaborar con la desinformación. No reenviéis información que no provenga de fuentes y orígenes legítimos.

- * Ante cualquier sospecha, o ante la simple duda, es preferible que contactéis con el servicio de informática en <https://ayudica.unizar.es> indicando como servicio 5.-Otros Incidencia de seguridad y privacidad, donde se sigue atendiendo a todos los usuarios y redoblando esfuerzos para tratar de mantener el nivel de servicio requerido en estas circunstancias excepcionales en las que nos encontramos. Ellos revisarán con los medios humanos o técnicos adecuados lo que sea preciso y resolverán las dudas que podáis tener.

- * Recomendamos inhabilitar la ejecución de macros en los documentos ofimáticos (Word, Excel, etc.) ya que son una fuente muy importante de infección de equipos.

- * Debemos mantener actualizado el sistema operativo, antivirus y aplicaciones de nuestros equipos.

* Todas las infecciones mencionadas suelen ser en muchos casos silenciosas, por lo que el ordenador infectado queda comprometido sin que seamos conscientes de ello; es posible que el atacante pueda tener acceso a información confidencial sin nuestro conocimiento (contraseñas, claves de acceso a bancos, números de tarjeta de crédito o de cuentas bancarias, etc.), con las consecuencias que ello puede tener.

Salud para todos y quédate en casa