SERVICIOS INFORMÁTICOS
Edificio Torre de Control
Campus Universitario
28871 Alcalá de Henares (Madrid)
Teléfonos: 91 885 47 00
Fax: 91 885 47 47

Recomendaciones de Seguridad (COVID-19)

En el contexto de la adopción de medidas técnicas y organizativas necesarias para compatibilizar la prestación del servicio con la no presencia en el puesto de trabajo derivadas de la alerta sanitaria del COVID-19, y con el fin de evitar que elementos indeseables se aprovechen de esta situación para realizar campañas maliciosas que puedan poner en grave riesgo la información y los sistemas de la UAH, sugerimos encarecidamente que se tengan en cuenta las siguientes recomendaciones:

- Desconfía de los correos electrónicos y mensajes recibidos relacionados con campañas que supuestamente informan sobre temas de salud pública (*phising*). Estos correos se están utilizando para incluir enlaces maliciosos, robar credenciales de acceso, etc. No se deben abrir adjuntos ni reenviar correos sospechosos.
- Comprueba la dirección de correo electrónico remitente del mensaje y también el enlace web al que te remite el mensaje. A veces, es evidente que la dirección web es falsa, pero otras veces los ciberdelincuentes son capaces de crear enlaces que se parecen mucho a las direcciones legítimas.
- Presta especial atención a los correos, mensajes y llamadas procedentes de departamentos de Informática, RRHH o Comunicación en los que se especifican instrucciones acerca del uso de conexiones remotas, operaciones financieras, etc. En algunos casos, los atacantes intentan suplantar a dichos departamentos con fines maliciosos. Se debe comprobar que el origen sea realmente quien dice ser. Sospecha mucho más si además el contenido del mensaje te urge a realizar cualquier tipo de acción cuanto antes, con una urgencia injustificada.
- Utiliza siempre los mecanismos oficiales de comunicación de la UAH (Comunic@, página web institucional, etc.), que facilitan información actualizada acerca de las acciones que se deben tomar, evitando posibles suplantaciones.
- No hagas copias de los datos de trabajo en equipos de casa. Utiliza preferentemente herramientas de trabajo en grupo y compartición de ficheros con licencia corporativa en la UAH (Microsoft Teams, Onedrive, Office 365, etc.).
- No te registres en sitios de uso personal con la cuenta de la UAH y en ningún caso utilices la misma contraseña.
- Nunca des a nadie tus contraseñas. Nadie debería pedírtelas.
- Ten siempre actualizados tus equipos y tu antivirus.
- Ante una situación de riesgo es más importante que nunca guardar la tranquilidad y reflexionar antes de actuar o tomar decisiones precipitadas.
- Dado lo excepcional de la situación, no podemos descartar que algunos servicios tanto propios de la UAH como externos se vean saturados por la sobrecarga de estos días. Recomendamos paciencia y comprensión.

Recuerda que la ciberseguridad de nuestra Universidad empieza por ti y la construimos entre tod@s.