CIBERSEGURIDAD: CREDENCIALES

Si otra persona utiliza sus contraseñas o certificados, puede suplantarle y actuar en su nombre.

Si Las credenciales de acceso son los elementos, físicos o lógicos, que permiten identificar a las personas frente a los sistemas informáticos.

Las credenciales de acceso más habituales son las contraseñas y los certificados, pero existen otras posibles, como la huella, el iris o el uso de dispositivos especiales bajo custodia del usuario.

En nuestra Administración se utilizan, por el momento, contraseñas y, en ocasiones, certificados digitales.

Si las credenciales caen bajo el control de otra persona, todas las acciones que esta persona realice figurarán como hechas por usted y, a todos los efectos, usted será el responsable. Por eso es tan importante cumplir con la obligación de custodiarlas y nunca entregársela a ninguna otra persona.

También **es importante definir contraseñas que no sean fácil de adivinar y cambiar con cierta regularidad.**
En sus contraseñas emplee una combinación de mayúsculas, minúsculas, letras y símbolos especiales y no las ponga demasiado breves.

Evite usar la misma contraseña para varios servicios. Es especialmente importante no emplear las mismas contraseñas para aplicaciones de su trabajo que para servicios que utilice en su vida privada.

UT_TiC
GOBIERNO de CANTABRIA
CONSEJERÍA DE EDUCACIÓN, FORMACIÓN PROFESIONAL Y UNIVERSIDADES

CIBERSEGURIDAD: CORREOS FRAUDULENTOS

Los correos electrónicos son un medio usado muy frecuentemente para realizar fraudes o comenzar ataques informáticos.

Si recibe correos sobre premios, entrega de paquetes no esperados o incluso supuestas multas, es muy posible que sea un correo fraudulento.

También si recibe la petición de un cambio de número de cuenta para el pago de las facturas de un contrato o cualquier otra petición inusual o poco frecuente.

En estos casos fíjese bien en la dirección de origen del correo (suelen ser extrañas, con dominios nada habituales), esté atento a la calidad del texto empleado en el mensaje (un empleo pobre del español suele delatar a los malhechores) y trate de comprobar por un canal alternativo que la entidad remitente es real y que verdaderamente le ha realizado este envío (llámeles por teléfono o contacte por alguna otra vía). Muy importante: evite abrir los adjuntos y pinchar en los enlaces que contenga el correo antes de haber comprobado su autenticidad.

También tiene que tomar precauciones similares si recibe correos no previstos que en apariencia sean de sus contactos habituales, incluso compañeros de trabajo, pero que contengan adjuntos, enlaces o un estilo de redacción extraña, pues el remitente puede haber sido suplantado.

Si recibe alguno de estos correos, no lo toque ni lo borre y contacte con el Soporte Office 365, ellos pondrán el caso en manos de especialistas, que lo analizarán y si fuera fraudulento mejorarán los sistemas de protección para que no lleguen correos similares a otros usuarios.

Gracias por su colaboración.

Firma:
Unidad Técnica TIC

Información promovida por el Gobierno de Cantabria.

UT_TIC

GOBIERNO de CANTABRIA
CONSEJERÍA DE EDUCACIÓN, FORMACIÓN PROFESIONAL Y UNIVERSIDADES