CSIRT-CV
Centre Seguretat TIC de la Comunitat Valenciana

Concienciación en Ciberseguridad

Hola:

Los intentos de estafa de **suplantación de identidad de la Generalitat Valenciana** son cada vez más frecuentes y sofisticados. Desde el Centro de Seguridad TIC de la Comunitat Valenciana (CSIRT-CV), adscrito a la Conselleria de Hacienda y Economía, le enviamos este comunicado para alertarle de los peligros de esta técnica, a través de la cual un atacante finge ser otra persona/entidad para engañar a otros con fines maliciosos, así como proporcionarle algunas **recomendaciones para saber identificar estas acciones y actuar ante este tipo de ataques cibernéticos**.

En las últimas semanas, el centro de ciberseguridad ha identificado varios **correos electrónicos falsos haciéndose pasar por la Generalitat o por alguno de sus organismos** con el objetivo de obtener información confidencial o realizar acciones fraudulentas engañando previamente a los destinatarios.

Ante un correo electrónico sospechoso o fuera de la normalidad, le pedimos:

• **Extremar la precaución, sobre todo si se tratan contratos, facturación, solicitud de información, cambios de domiciliación o de cuentas y pago de los anuncios de licitación**, entre otros.

• **Difundir entre el personal a su cargo o compañeros** esta comunicación para evitar ser víctimas de posibles estafas digitales o robos de información.

Recomendaciones

En caso de recibir algún correo que, simulando pertenecer a algún organismo o dominio dependiente de GVA, les solicite el envío de datos y/o documentación o cambios en la facturación, **se recomienda** seguir las siguientes medidas:

- **Verificar la identidad** de las cuentas de correos y de las cuentas bancarias.
- **NO responder ni enviar información alguna.**
- **NO abrir enlaces o archivos sospechosos**.
- **Informar al organismo supuestamente suplantado** si tiene dudas sobre la legitimidad del mensaje.
- Si duda sobre la legitimidad de un correo, **reportar** al CAU o Departamento de Seguridad Informática correspondiente.
- Si se considera haber sido **estafado**, ponerlo en conocimiento de las Fuerzas y Cuerpos de Seguridad del Estado e interponer la denuncia correspondiente.

¿Qué consiguen los ciberdelincuentes con la suplantación de identidad?

Los ciberdelincuentes, suplantando la identidad de la Generalitat Valenciana o de algún organismo dependiente de ella, consiguen:

- Obtener información (DNI, información bancaria, direcciones...) que puede ser utilizada para cometer fraudes financieros o venderse en el mercado negro a cambio de dinero.
- Redirigir a los usuarios a páginas falsas para que ingresen sus credenciales bancarias o realicen pagos que, en realidad, se ingresan en las cuentas de los atacantes.
- A través de enlaces o archivos adjuntos disfrazados en mensajes oficiales, los ciberdelincuentes pueden instalar malware en los dispositivos de las víctimas. Asimismo, pueden secuestrar el dispositivo para pedir un rescate (ransomware), espiar la actividad del usuario o extraer información sensible.
- Suplantar a un organismo como la Generalitat puede tener como objetivo infiltrarse en sus redes o sistemas informáticos, lo que permitiría a los atacantes robar grandes volúmenes de datos, alterar registros oficiales o llevar a cabo otras actividades maliciosas a nivel interno.

Por último, recordar que CSIRT-CV ofrece **cursos gratuitos online** sobre ciberseguridad, entre los que se encuentran el **Curso de Delitos Tecnológicos** y el de **Seguridad en el Correo Electrónico**.

Agradecemos su colaboración.

Un saludo,

Equipo CSIRT-CV

GENERALITAT VALENCIANA
Conselleria d'Hisenda i Economia

CSIRT-CV
Centre Seguretat TIC de la Comunitat Valenciana
