centro criptológico nacional

#CiberCOVID19

Ante las campañas de malware y de desinformación que se están generando a raíz de la pandemia del coronavirus, te aconsejamos seguir las siguientes recomendaciones.

Phishing

- Presta especial atención a los emails que recibes. La cura del coronavirus no la recibirás por correo electrónico.
- Evita abrir documentos y archivos adjuntos sobre el COVID-19 en los correos electrónicos que recibas.
- No descargues aplicaciones no oficiales para conocer el alcance internacional del COVID-19.

Desinformación

- No difundas información que no provenga de medios y fuentes oficiales.
- No contribuyas a la difusión de contenido no contrastado.
- No compartas mensajes que puedan generar alarma en la población.

centro criptológico nacional

#CiberCOVID19 | #NoTeInfectesConElMail

Los ciberdelincuentes se están aprovechando de la pandemia del coronavirus para infectar sistemas informáticos mediante técnicas de phishing. Presta atención a los emails que recibes y a los links a los que accedes.

En el mes de marzo, el número de incidentes de phishing en organismos públicos ha aumentado un **70%** con respecto al mes anterior.

Identidades suplantadas:

Temáticas del phishing:

- Buenas prácticas para prevenir el virus
- Informes actualizados sobre la situación (número de infectados y fallecidos, alcance internacional, etc.)
- Análisis del impacto del coronavirus en diferentes sectores
- Ofertas para invertir en vacunas y productos sanitarios
- Falsas alertas sanitarias

Contenidos que se adjuntan en correos electrónicos dañinos:

- Archivos infectados (PDF, Word, etc.)
- Links a páginas web dañinas
- Links a páginas web que simulan ser la página oficial de un organismo o institución