Lacera

ALERTA DE CIBERSEGURIDAD Covid19

En esta situación, ya de por sí difícil, los ciberdelincuentes representan una amenaza adicional para todas las empresas, pero también para las personas: explotan nuestra necesidad de información sobre el coronavirus para robar datos valiosos, contraseñas o información de tarjetas de crédito o para colocar *malware*, por ejemplo.

Desde **Lacera**, te pedimos que por favor **extremes la precaución** en este sentido. Para ayudarte, te contamos a continuación los 3 tipos de riesgos que estamos identificando:

1

En los últimos días, el número de correos suplantando identidades de grandes corporaciones se ha visto incrementado de manera drástica *(phising)*. Para este propósito, los ciberdelincuentes usan archivos adjuntos de correo electrónico cuya apertura puede desencadenar la descarga de *malware*. Una vez que se instala el *malware*, los atacantes pueden acceder no solo a tu equipo, sino a toda la red de la empresa.

2

Se están utilizando falsos sitios web de instituciones de renombre, como la Organización Mundial de la Salud (OMS) o los Centros para el Control y la Prevención de Enfermedades. Páginas que aparentemente son oficiales y a las que acudimos para consultar información sobre la situación actual y sin embargo, son páginas diseñadas para robar información sensible. Cuidado, este tipo de prácticas ha evolucionado rápidamente y no solo son páginas web, sino que también pueden ser apps para smartphones.

3

Otra variante es atraer al usuario a un sitio web falso, que puede ser aparentemente corporativo, y donde se te pide usuario y contraseña de tu cuenta de la empresa. Dado que hemos instaurado el teletrabajo, puede parecer una página corporativa para acceder a herramientas internas o de consulta. Aquí se harán con tu información de empresa para suplantar tu identidad.

¿Cómo puedes protegerte?

- Si has recibido un correo de un remitente no habitual, sospecha y revisa.
- Si recibes un correo de un compañero cuyo texto te resulta mínimamente extraño por su redacción o la petición que hace.
  - Revisa comprueba cuidadosamente el email remitente.
  - Ponte en contacto con esa persona por un método alternativo (llamada telefónica) para comprobar que realmente te está haciendo esa petición.
- Abre únicamente los archivos adjuntos de remitentes conocidos.
- Nunca hagas clic en un enlace de un correo si no conoces el remitente.
- Ten cuidado con las promociones "especiales de coronavirus", por ejemplo de (supuestos) proveedores de telecomunicaciones para ofrecer un mayor ancho de banda u ofertas especiales para dispositivos como ordenadores portátiles.
- No utilices ningún enlace que se te envíe en un correo; visita los sitios web de los ministerios, oficinas o universidades tú mismo.
- En tu casa, utiliza las mismas medidas de seguridad que aplicarías en la oficina (bloquea pantalla, no deje datos confidenciales...)

Tu precaución en estos momentos debe ser extrema. **¡Mantente alerta!**

Gracias por tu colaboración.

Lacera