BOLETÍN ESPECIAL DE SEGURIDAD INFORMÁTICA N.- 2020-ESFORSE-TICS-003, SOBRE COMO DETECTAR Y DETENER ATAQUES DE INGENIERÍA SOCIAL

Ciberataques Ingeniería social

La mayoría de las personas tienen la idea errónea que los ciberatacantes utilizan herramientas altamente avanzadas y técnicas para comprometer las computadoras o cuentas de usuarios, esto no es cierto. Los atacantes han aprendido que a menudo la forma más fácil de robar su información es comprometer sus cuentas o infectar los sistemas engañándoles para que cometa un error.

¿Qué es ingeniería social?

La ingeniería social es un ataque psicológico a través del cual el delincuente engaña para realizar algo que no debería hacer. Lo que hace la tecnología actual más efectiva para realzar ciberataques es que físicamente no se puede ver, los atacantes pueden pretender ser cualquier cosa o persona y dirigirse a millones de personas alrededor del mundo, Además los atacantes de ingeniería social pueden evadir muchas tecnologías de seguridad. Tenga en cuenta que los ataques de ingeniería social no se limitan pueden ser llamadas telefónicas, mensajes de texto a su teléfono, mensajes a redes sociales o incluso en persona.

COMO DETECTAR Y DETENER ATAQUES DE INGENIERÍA SOCIAL:

Afortunadamente detener este tipo de ataque es más sencillo de lo que podría imaginar, el sentido común es la mejor defensa. Si ve algo sospechoso puede ser un ataque las pistas más comunes son:

- Alguien crea un tremendo sentido de urgencia, tratando de engañar para que cometa un error.
- Alguien pregunta por información a la cual no debería tener acceso o que ya debería saber, como los números de cuenta.
- Alguien le solicita su contraseña, ninguna organización legitima le pedirá eso.
- Alguien le presiona para que evada o ignore los procedimientos de seguridad o procedimientos que se espera siga en su trabajo.
- Algo es demasiado bueno para ser cierto. Por ejemplo, le notifican que ha ganado la lotería o un iPad sin siquiera haber concursado.
- Recibe un correo extraño de un amigo o colaborador de trabajo que contiene palabras que no utilizan comúnmente. Un ciberatacante puede haber entrado a su cuenta y trata de engañarle. Para proteger se debe verificar contactando a su compañero de trabajo por otros medios de comunicación, ya sea en persona o por teléfono.

Si sospecha que alguien intenta engañarle, no se comunique más con esa persona. Si el atacante está relacionado con el trabajo, asegúrese de informar inmediatamente de la situación a la mesa de ayuda o al equipo se seguridad informática. Recuerde, el sentido común es a menudo la mejor defensa.

REPORTE DE INCIDENTES:

Reporte el incidente al Departamento de TICS, a través de red telefónica interna mediante la ext. 194