Universidad Veracruzana

Ciberamenazas

Información segura... ¡es cultura!®

Ciberamenazas

Hoy en día es cada vez más común escuchar, ver noticias de ciberataques, ciberamenazas y cibercrimen, pero ¿sabes qué es una ciberamenaza?

Una ciberamenaza es una acción maliciosa que se realiza en un entorno digital que tiene como objetivo perjudicar la seguridad de la información de una persona u organización y utilizarla con fines lucrativos y malintencionados.

Por lo que, si una ciberamenaza se materializa, puede tener un gran impacto negativo para una organización, una persona o incluso en la sociedad en general. De ahí que estas no solo pueden afectar a grandes empresas u organizaciones públicas, si no que hasta en los particulares existe un riesgo latente. Por ello la importancia de conocer las principales ciberamenazas que se han presentado más recientemente ya que éstas nos pueden afectar a todos.

Principales ciberamenazas

Ransomware

Esta es una de las ciberamenazas que se han incrementado más en el último año derivado de la pandemia que conllevó a muchas empresas a trabajar de forma remota. Y consiste en un código malicioso que cifra la información impidiendo su acceso a un equipo o dispositivo y que se propaga a otros dispositivos a los que tiene acceso, es decir, el ciberdelincuente "secuestra" la información de una persona u organización solicitando un rescate económico para que el propietario de la información pueda recuperarla.

Ingeniería social

Los ciberdelincuentes utilizan técnicas para manipular a los usuarios de una organización para conseguir mediante engaños datos confidenciales como usuarios, contraseñas, datos bancarios, etc. Los métodos más usados por los ciberdelincuentes de este tipo de ciberamenazas son:

- **Phishing:** Esta es la forma más común para que los ciberdelincuentes engañen a las personas ya sea particulares o empleados de una organización para que revelen información confidencial y consiste en el envío de un correo electrónico, haciéndose pasar por una organización o persona reconocida, con el fin de que el usuario ingrese a un enlace falso para que introduzca sus datos como usuarios, contraseñas, información bancaria y así cometer un fraude.

Ciberamenazas

Vishing: Técnica en la que el ciberdelincuente a través de una llamada telefónica engaña a una persona haciéndose pasar por una organización financiera, gubernamental o privada para solicitar información confidencial y realizar un fraude.
Smishing: El ciberdelicuente consigue engañar a las víctimas a través de un mensaje de texto falso con el fin de que ingrese a un sitio web malicioso.
Fraude Online: Los ciberdelincuentes utilizan sitios web falsos para engañar a las víctimas y que introduzcan sus datos confidenciales, como usuarios, contraseñas, números de cuenta.

Malware

Es una de las ciberamenazas más comunes y consiste en un software malicioso que tiene como objetivo infiltrarse en un dispositivo electrónico y dañarlo. Estos códigos pueden comprometer la seguridad, utilidad o preservación de un dispositivo. Entre algunos malware que hay son:

Troyanos: Código malicioso que aparenta ser legítimo.
Adware: Este malware muestra de forma automática y frecuente al usuario anuncios publicitarios en los dispositivos o navegador web y puede recabar información personal realizando un seguimiento de los sitios web que visita o registrando las teclas que pulsa.
Spyware: Tiene como objetivo instalarse en un dispositivo electrónico y funcionan como espías para robar información confidencial sin el consentimiento el usuario.

Recomendaciones para protegerte de las ciberamenazas

El trabajo remoto, clases en línea derivados del confinamiento conllevó a un incremento acelerado de personas conectadas a Internet, por lo que la protección contra las ciberamenazas debe ser prioridad para todas las organizaciones y usuarios. Así, #InformaciónSeguraEsCultura te brinda las siguientes recomendaciones:

- Instala y actualiza en los dispositivos de escritorio o móviles programas de protección de datos y antivirus para empresas.
- Actualiza constantemente aplicaciones y sistema operativo.
- Utiliza contraseñas seguras y diferentes para los dispositivos electrónicos y servicios.
- No abras correos electrónicos sospechosos y, en caso de hacerlo, no proporcionar datos confidenciales ni descargar archivos adjuntos.
- No compartir información confidencial fuera de los canales propios de la organización.

Ciberamenazas

Para cualquier duda o apoyo, puedes contactar al equipo de ciberseguridad de la Universidad veracruzana el UV-CSIRT en sus distintos medios de comunicación:

contactocsirt@uv.mx
www.uv.mx/csirt

Referencias:

https://seguroscibernéticos.es/que-son-las-ciberamenazas-principales-tipos/