Universidad Veracruzana

Inducción a la seguridad de la información

Información segura... ¡es cultura!®

Inducción a la seguridad de la información

¡Bienvenido a la Universidad Veracruzana!

Ahora que eres parte de nuestra comunidad universitaria, podrás tener acceso a diversos servicios tecnológicos como son:

- Correo electrónico Institucional
- Red de telecomunicaciones RIUV (wifi) y red cableada
- Portal de acceso MiUV
- Sistemas académicos y administrativos (EMINUS, SIIU)
- Entre otras plataformas

Para que puedas aprovechar al máximo sus beneficios, es importante que sepas que la seguridad de la información es muy importante para nosotros. Te invitamos a revisar detenidamente la siguiente información que te ayudará a prevenir riesgos.

¡Información Segura es Cultura!

La seguridad de la información

La seguridad de la información la hacemos todos, y nosotros como usuarios somos la primera línea de defensa contra los actores mal intencionados que buscan hacer mal uso de tu información personal, por esta razón a continuación te daremos una descripción de las amenazas más comunes a las que estamos expuestos, así como algunos consejos para prevenirlas:

Malware:

El código malicioso o malware es un programa informático desarrollado con la intención de robar información confidencial como números de tarjetas de crédito, tu información personal como usuarios y contraseñas, archivos de texto o multimedia etc., para realizar fraudes o afectar tu reputación y la de las organizaciones a las que perteneces.

En los últimos años se ha popularizado un tipo de software malicioso que bloquea tu información dejándote incapacitado para usarla, y después pedirte una suma de dinero como rescate para liberar tus datos “secuestrados”, este tipo de malware se conoce como ransomware. Además de este, existen otros, como son los gusanos, caballos de Troya, spyware por mencionar algunos.

Por lo general estos códigos utilizan vulnerabilidades en los sistemas operativos y los programas instalados en ellos y se activan cuando haces clic en algún enlace peligroso de una página no segura, cuando instalas algún software sospechoso, al abrir algún archivo adjunto malicioso de un correo electrónico o cuando insertas algún dispositivo de almacenamiento como las memorias y discos duros externos USB.

Para evitar ser víctima de esta amenaza sigue las siguientes recomendaciones:

- Utiliza algún programa o aplicación antivirus y mantenla actualizada;
- Mantén actualizado tu sistema operativo y programas instalados;
- Visita páginas seguras (https) y también puedes usar algunos complementos en tu navegador que advierten sobre sitios riesgosos;
- Instala únicamente software legítimo y descargado de fuentes confiables;
- Asegúrate de conocer al remitente del correo electrónico, no abras enlaces ni descargues archivos adjuntos de desconocidos;
- Analiza con un programa antivirus tus dispositivos de almacenamiento externos antes de empezar a trabajar con ellos.

Phishing

Esta amenaza cuyo nombre hace alusión a la palabra en ingles fishing (pesca) es una técnica que se conoce como ingeniería social, en donde el ciberdelincuente trata de obtener tu información haciéndose pasar por alguna fuente confiable, por lo general se hace a través de correo electrónico dónde te pide información confidencial.

Este tipo de mensajes pretenden generarte inquietud y demandan una respuesta rápida solicitándote contestes el mismo correo, descargar un archivo adjunto o te invitan a entrar a un enlace dónde llenarás un formulario.

Algunos ejemplos de estos casos serían:

- Correos fraudulentos de remitentes desconocidos o haciéndose pasar por algún miembro de la comunidad universitaria solicitando información de usuarios y contraseñas de correo.
- Correos de remitentes desconocidos incitando a descargar y abrir algún archivo que puede ser malicioso.
- Recibir algún correo de alguna institución bancaria solicitando que actualices tus datos.
- Correos intimidatorios haciéndote creer que tienen información privada tuya, obligándote a pagar cierta cantidad de dinero a cambio de no divulgarla.

Con la información antes mencionada es importante que sepas que por ningún motivo la Universidad Veracruzana te solicitará datos de acceso como usuario y contraseña por algún medio.

Es importante que sigas las siguientes recomendaciones para estar prevenidos contra algún intento de phishing:

- No respondas ningún correo electrónico que te solicite información personal o financiera, los bancos, así como nuestra universidad no te pedirán datos personales ni de acceso por este medio.
- No ingreses a sitios solicitados por correo electrónico dónde te pidan datos.
- Pon atención al remitente de los correos que la dirección corresponda a la institución mencionada, desconfía de cualquier cuenta cuyo dominio sea público como Gmail ejemplo: tubanco@gmail.com.
- Revisa los indicadores de seguridad cuando entres a algún sitio web, por lo general lo puedes hacer en el candado pequeño junto a la barra de direcciones del navegador.
- Si recibes algún tipo de correo con las características antes mencionadas repórtalo a la cuenta de reportaspam@uv.mx

UV-CSIRT – Infosegura

Para poder dar atención a estos incidentes de seguridad, la Universidad Veracruzana cuenta con un área de denominada UV-CSIRT, dónde puedes solicitar información en temas de ciberseguridad relacionados a los servicios la UV te ofrece, para ello, el área cuenta con un sitio web en donde puedes obtener información, así como reportar algún incidente.

UV-CSIRT también publica continuamente boletines de ciberseguridad alertando a la comunidad sobre amenazas recientes, no olvides visitar su sitio web y seguir sus redes sociales para mantenerte al tanto de las noticas más relevantes en ciberseguridad.

www.uv.mx/csirt
Facebook: /uvcsirt
Twitter: @uvcsirt

Inducción a la seguridad de la información

Infosegura es un servicio que gestiona el equipo de respuesta a incidentes de ciberseguridad (UV-CSIRT) de la Universidad Veracruzana el cual tiene la finalidad de establecer una cultura de seguridad de la información para proteger los activos de información y mantener su confidencialidad, integridad y disponibilidad, así como hacer conciencia en la comunidad universitaria para que actúen de forma responsable en su manejo.

Para ello pone a disposición de todos, una serie de recursos digitales en el que se comparten consejos de ciberseguridad, infografías, videos, entre otros, visita su sitio web y sigue sus redes sociales.

www.uv.mx/infosegura
Facebook: /seginfouv
Twitter: @infoseguraUV
Instagram: @infosegurauv

Normativa institucional

Si bien la Universidad Veracruzana cuenta con medidas de seguridad implementadas para los servicios tecnológicos, es de suma importancia que tú como usuario de las plataformas conozcas los mecanismos de seguridad implementados, mismos que son descritos en el reglamento vigente de la seguridad de la información el cual tiene como objetivo principal, establecer el marco normativo para el uso de los activos de información, al mismo tiempo persigue los propósitos siguientes:

- Sensibilizar a los integrantes de la comunidad universitaria y usuarios externos en el cuidado, protección y responsabilidades asociadas al tratamiento de la información que no es pública;
- Mantener la confidencialidad, disponibilidad e integridad de la información personal e institucional; y
- Dar cumplimiento a las disposiciones legales en la materia.

Te invitamos a hacer lectura de este reglamento en el siguiente enlace:

https://www.uv.mx/legislacion/files/2017/07/Seguridad-de-la-informacion-Universidad-Veracruzana.pdf