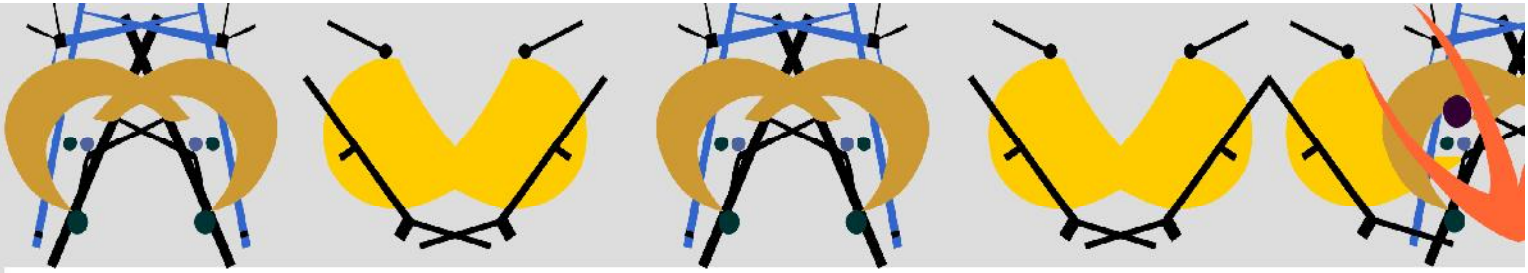


El riesgo de la Ingeniería Social

En la Seguridad de la Información

Reina Camacho
reina.camacho@ucv.ve

¿A cuántas personas no has escuchado que le "hackearon" su cuenta de correo, facebook, twitter; o que realizaron operaciones fraudulentas en su cuenta bancaria? Una forma muy frecuente de cometer estos delitos es solicitando información confidencial a los propios usuarios. Revisemos el siguiente correo:

> Estimado titular de la cuenta Web- Mail de la Universidad Central de Venezuela (UCV), como consecuencia del cambio de servidores/plataforma, en estos momentos estamos actualizando nuestra plataforma, base de datos y centro de cuentas de correo electrónico, eliminando de este modo toda vieja cuenta de correo electrónico Web, para reutilizar el espacio para las nuevas cuentas.
>
> Para evitar que su cuenta de correo sea eliminada, requerimos que la actualice, así podremos determinar que es una cuenta actualmente activa. Para completar la actualización, debe hacer clic en http://www.ucv.com.ve/ y entrar en la opción: "Detalles de su Cuenta" o enviar inmediatamente a este correo electrónico (serviciosdtic@ucv.com.ve), la información que se solicita a continuación.
>
> Confirmar Email: .....
> Dirección de correo electrónico: .....
> EMAIL Contraseña: .....
> Confirme Contraseña: .....
> Fecha de nacimiento: .....
>
> Pedimos disculpas por las molestias ocasionadas.
> Atentamente,
> DTIC - UCV
> e-mail: serviciosdtic@ucv.com.ve

Tiempo atrás, se utilizaba el teléfono simulando ser un empleado, bien sea de un banco o una empresa, con el propósito de obtener información valiosa o confidencial, como contraseñas de acceso al correo, número de tarjetas de créditos, entre otras. Con Internet la obtención de información ha pasado a ser más sofisticada.

La manipulación o engaño hacia los usuarios para obtener información sensible de forma voluntaria es lo que se conoce como Ingeniería Social. Christopher Hadnagy[1] la define como:

> El acto de manipular a una persona para que lleve a cabo una acción que –puede ser o no- [sic] lo más conveniente para cumplir con cierto objetivo. Este puede ser la obtención de información, conseguir algún tipo de acceso o lograr que se realice una determinada acción.

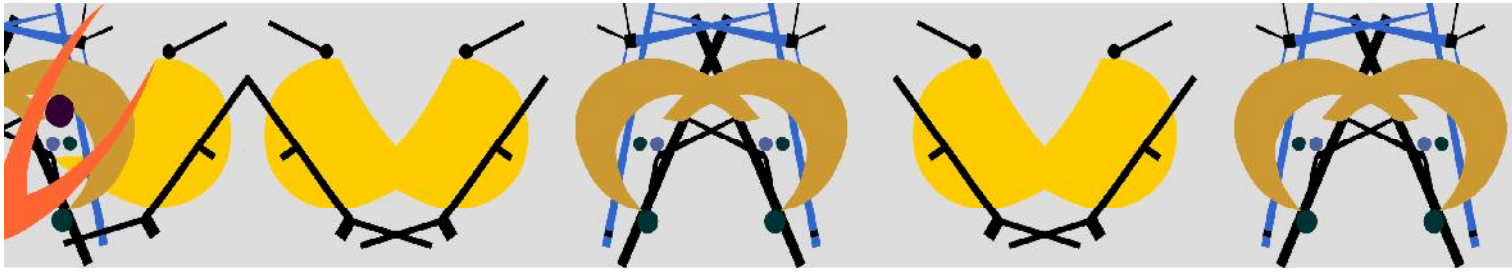
La Ingeniería social se aplica en todos los contextos de la vida cotidiana y en especial en las Tecnologías de Información.

Según Kevin Mitnick[2] uno de los más famosos hackers, crackers del mundo, los principios básicos y comunes a todas las personas en que se basa la Ingeniería social viene dado a que todos queremos ayudar, no nos gusta decir NO, el primer movimiento es siempre de confianza hacia el otro. A todos nos gusta que nos alaben, también existe el miedo y la codicia, la inocencia y la credulidad.

Existen diferentes formas de hacer Ingeniería Social, entre las más comunes tenemos:

- **Phishing (suplantación de identidad):** se obtiene información confidencial empleando el correo electrónico o algún sistema de mensajería instantánea para cometer el fraude o la estafa.
- **Envío de adjunto a un correo electrónico:** se obtiene información confidencial enviando un troyano adjunto o un capturador de teclas, entre otros, al correo electrónico para tener control de la computadora.
- **Vishing:** se obtiene información confidencial empleando una llamada telefónica para cometer el fraude o la estafa.

La encuesta realizada por Check Point® Software Technologies[3] en el año 2011, la cual entrevistó a más de 850 profesionales en Tecnologías de Información y Seguridad, ubicados en EEUU, Canadá, Reino Unido, Alemania, Australia y Nueva Zelanda; y a organizaciones de todos los tamaños y renglones (financiera, industrial, defensa, ventas, salud y educación), arrojó como resultado que aproximadamente el 48% de las empresas encuestadas admitieron que han sido víctimas de la Ingeniería Social, más de 25 veces en los últimos dos años. Esta encuesta también mostró que los correos de phishing son clasificados como la fuente más común de técnicas



Mateo manaure (1951)

de ingeniería social (47%), seguido por sitios de redes sociales, que pueden exponer datos profesionales y personales (39%) y dispositivos móviles inseguros (12%). Además, indicó que las ganancias financieras son citadas como la razón más frecuente para los ataques de ingeniería social, seguido de acceso a datos propios (46%), ventajas competitivas (40%) y venganza (14%).

La UCV no escapa de estas estadísticas, en los últimos cinco años la comunidad universitaria ha sido víctima de todas estas formas de fraude o engaño, produciendo consecuencias graves tanto para la persona en sí como para la red de la UCV, la cual se ha visto seriamente comprometida. En este año (2014), un ataque phishing ocurrió en una facultad, debido a la ingeniería social realizada de forma exitosa a uno de sus usuarios a través del correo electrónico (correo como el descrito anteriormente), provocando la suspensión de dicho servicio por más de 48 horas a toda la facultad.

Los usuarios son parte primordial para la seguridad de la institución, existen muchas técnicas de violación que se sustentan en las personas y no el software o hardware de la empresa.

A pesar de que la UCV maneje equipos de última generación para la protección a la red y de la información, herramientas de detección y prevención de intrusos (IPS/IDS), antivirus actualizados, sistemas para el control de acceso, en fin, que utilice las herramientas más sofisticadas en lo que a seguridad informática se refiere, basta con contar con desconocimiento, curiosidad, descuido o negligencia por parte de un usuario y "buum", se filtra la información sensible necesaria para el delito.

La principal defensa contra la Ingeniería Social es educar a toda la comunidad universitaria (obreros, estudiantes, vigilantes, técnicos, docentes, profesionales) en el uso de las políticas de seguridad[4] y dar capacitación que alerte a los usuarios de los peligros que existen en la vida diaria cuando hacemos uso de las tecnologías de información. ■

Fuentes Electrónicas:

1. http://www.bscconsultores.cl/descargas/B.1%20La%20 Ingeniera%20Social.pdf
2. http://es.wikipedia.org/wiki/Kevin_Mitnick
3. http://exo-community.com/articulos/estadisticas/81-seguridad-informatica/4611-check-point-revela-que-casi-la-mitad-de-las-empresas-son-victimas-de-la-ingenieria-social.html
4. http://www.ucv.ve/filecadmin/user_upload/dtic/Documentacion_y_Normativa/Manual_Politicas_DTIC_FINAL_2009_Aprobado__2_.pdf

Algunas recomendaciones para los usuarios:

- Averigüe y verifique la identidad de la persona que solicita información precisa.
- Pregúntese qué importancia tiene la información requerida.
- Antes de realizar cualquier operación a través de una web verifica la legitimidad de la página.
- Jamás responda preguntas que involucre datos personales o sensibles.
- Evita hacer click a todo lo que le hace click.
- No anotar las contraseñas en lugares donde puedan ser fácilmente visibles o encontradas por otros.
- Evite brindar información que pueda comprometer la seguridad de su sistema y la suya personal.
- No se deje intimidar o adular para terminar ofreciendo información.
- Recuerden que los bancos jamás envían correos ni realizan llamadas telefónicas solicitando números de tarjeta, ni confirmación o actualización de datos.

"…el eslabón más débil de la cadena de seguridad: la gente que usa y administra los ordenadores".

Kevin Mitnick