

GEstrella-Venezuela (Aug 6, 2004 11:20:41 AM)

Buenos días, Agradezco a todos su participación, damos inicio al 2do Chat del 2004. 1. Cuales de los países miembros del CELAES tenían conocimiento de esta modalidad delictiva?

GPICHLING-Perú (Aug 6, 2004 11:22:47 AM)

El Perú sí tiene conocimiento de esta modalidad de fraude, la misma que se inicia con un SCAM (difusión masiva de correo electrónico a clientes y no clientes bancarios, que contiene una dirección URL que pretende orientar la navegación de los clientes a páginas similares a las que quiere afectar, a fin de obtener su información personal - Número de cuenta y Clave Secreta).

GEstrella-Venezuela (Aug 6, 2004 11:23:07 AM)

En Venezuela se tiene conocimiento motivado a que el Comité de Seguridad de la Asociación Bancaria de Venezuela, en un Comité de Seguridad ampliado se expuso el tema a todos los Jefes de Seguridad de los Bancos, pertenecientes al Sistema Financiero Venezolano.

GOrna - Ecuador (Aug 6, 2004 11:23:20 AM)

En Ecuador conocemos de este tipo de delito a través de los reportes que nos llegan de Internet (www.seguridadenlared.org), sin embargo no hemos tenido este problema.

Helena-Colombia (Aug 6, 2004 11:23:43 AM)

En Colombia también se conoce esta modalidad desde hace algún tiempo, aunque las entidades financieras reportan que no se han visto muy afectadas

GEstrella-Venezuela (Aug 6, 2004 11:25:24 AM)

2. Alguna de las instituciones presentes han sufrido esta nueva modalidad delictiva?

GPICHLING-Perú (Aug 6, 2004 11:25:59 AM)

Si, en El Perú se han presentado casos de Phishing.

GOrna - Ecuador (Aug 6, 2004 11:26:01 AM)

En Ecuador no hemos tenido este problema aun.

GEstrella-Venezuela (Aug 6, 2004 11:26:18 AM)

Ningún Banco en Venezuela a reportado casos.

Helena-Colombia (Aug 6, 2004 11:27:30 AM)

Sabemos en Colombia de por lo menos una entidad que ha sido víctima de este delito, aunque por factores de confidencialidad no podemos revelar su nombre

GEstrella-Venezuela (Aug 6, 2004 11:27:52 AM)

De acuerdo.

GEstrella-Venezuela (Aug 6, 2004 11:28:28 AM)

3. En caso de que la respuesta de la pregunta Nro. 2 sea afirmativa, indicar cuantos casos tienen registrados?

GPICHLING-Perú (Aug 6, 2004 11:29:11 AM)

Tenemos conocimiento que clientes de dos entidades bancarias que forman parte de nuestra Asociación han sufrido ataques utilizando esta modalidad de Fraude.

GEstrella-Venezuela (Aug 6, 2004 11:29:36 AM)

Ninguno

Helena-Colombia (Aug 6, 2004 11:29:58 AM)

En Colombia no tenemos registro del número de casos en que el cliente fue efectivamente víctima, porque la entidad detectó el fraude de forma temprana y lo controló

GEstrella-Venezuela (Aug 6, 2004 11:32:28 AM)

4. Sabían que existe un Organismo Internacional Anti Phishing?

GOrna - Ecuador (Aug 6, 2004 11:32:34 AM)

No.

GPICHLING-Perú (Aug 6, 2004 11:33:07 AM)

Si, tenemos conocimiento del Anti Phishing Working Group, organismo que registra las incidencias de esta modalidad de fraude, aunque las estadísticas no sean exactas debido a la falta de denuncia en la mayoría de casos y a que las entidades ocultan la información por un tema de imagen.

GEstrella-Venezuela (Aug 6, 2004 11:34:03 AM)

Tenemos conocimiento de la existencia de la Organización Anti Phishing, la cual tiene una página en Internet <http://www.ANTIPHISHING.ORG/> y se encarga de rastrear, interceptar y bloquear a dichas páginas de usurpación.

Danilo-Rep. Dominicana (Aug 6, 2004 11:35:04 AM)

Gabriel me perdí la pregunta, me la pueden repetir por favor, que presente inconvenientes para conectarme al Chat .

Helena-Colombia (Aug 6, 2004 11:36:27 AM)

En Colombia las entidades financieras también conocen de esta organización, aunque no se ha profundizado mucho en el estudio de casos

GEstrella-Venezuela (Aug 6, 2004 11:36:41 AM)

Danilo bienvenido te envío las 4 preguntas ya formuladas 1. Cuales de los países miembros del CELAES tenían conocimiento de esta modalidad delictiva? 2. Alguna de las instituciones presentes han sufrido esta nueva modalidad delictiva? 3. En caso de que la respuesta de la pregunta Nro. 2 sea afirmativa, indicar cuantos casos tienen registrados? 4. Sabían que existe un Organismo Internacional Anti Phishing?

Danilo-Rep. Dominicana (Aug 6, 2004 11:38:41 AM)

Tenemos conocimiento de la modalidad delictiva, no tenemos caso reportado, y tercero si conocemos del organismo internacional Anti Phishing

GEstrella-Venezuela (Aug 6, 2004 11:39:17 AM)

5. En caso de tener conocimiento de esta modalidad de fraude, la Asociación Bancaria de vuestro país ha divulgado esta información?

GPICHLING-Perú (Aug 6, 2004 11:39:59 AM)

Se ha tomado la decisión de no informar a los medios de comunicación debido a que no todos los clientes se ven afectados, solo aquellos que utilizan los servicios de Internet, acordándose en el Comité de Prevención de Estafas y Defraudaciones, que el procedimiento a emplear es la comunicación directa mediante un correo electrónico a aquellos usuarios que utilizan los servicios bancarios del portal financiero y la publicación en dicho medio de las medidas preventivas para evitar ser víctima de esta modalidad delictiva.

Helena-Colombia (Aug 6, 2004 11:40:33 AM)

En Colombia aún no se ha revelado información oficial sobre este fraude, pero sí se tiene programado el desarrollo de un documento de investigación sobre este que será elaborado por el Comité de Riesgo Informático de la Asobancaria

GOrna - Ecuador (Aug 6, 2004 11:41:00 AM)

Nosotros conocemos sobre el tema, pero recién estamos elaborando un documento para poderlo divulgar.

GEstrella-Venezuela (Aug 6, 2004 11:41:11 AM)

Si, la Asociación Bancaria de Venezuela ha emitido comunicados en los diferentes medios de comunicación escritos del país, alertando de este nuevo flagelo y exhortando a la población de la importancia de no suministrar la clave secreta a ninguna persona, el texto publicado fue el siguiente: A TODOS LOS CLIENTES DE LAS INSTITUCIONES FINANCIERAS VENEZOLANAS. ¡ALERTA! ¿Recibió un Correo Electrónico en nombre de su Banco, solicitando sus datos personales?. (Continua...)

Helena-Colombia (Aug 6, 2004 11:41:35 AM)

Este documento será inicialmente de uso privado de los bancos y de acuerdo con la recepción que se tenga, se espera tomar más medidas de cara a los clientes.

GEstrella-Venezuela (Aug 6, 2004 11:42:04 AM)

En la actualidad, están circulando correos electrónicos que simulen ser enviados por su Banco, en los cuales se les solicita información sobre sus datos personales, números de tarjetas y especialmente sus claves para acceso y transacciones electrónicas a sus cuentas bancarias. Por su seguridad, no responda ningún correo electrónico suministrando sus claves ni números de tarjetas, ya que se expone a posibles fraudes por terceros inescrupulosos. (continua..)

GEstrella-Venezuela (Aug 6, 2004 11:42:25 AM)

Le recordamos que sus datos pueden ser actualizados por su Institución Bancaria,

como una práctica regular que le garantice los servicios e información financiera, pero ninguna persona debe conocer el número de sus diferentes claves, esta información es personal, intransferible y confidencial.

Helena-Colombia (Aug 6, 2004 11:42:44 AM)

En Colombia se ha hecho algo similar a lo que desarrollaron en Venezuela, pero de forma general y alertando sobre cualquier tipo de fraude en canales electrónicos

Helena-Colombia (Aug 6, 2004 11:43:08 AM)

También se ha dado a conocer este documento o texto informativo a través de diferentes medios de publicidad

GEstrella-Venezuela (Aug 6, 2004 11:44:16 AM)

6. Consideran ustedes, que un mensaje en la página Web emitido por alguna Entidad Bancaria dando consejos de seguridad sería intimidatorio para los clientes?

Helena-Colombia (Aug 6, 2004 11:44:26 AM)

Gabriel, en Venezuela el texto del que nos hablas es el mismo para todos los bancos?

GOrna - Ecuador (Aug 6, 2004 11:44:49 AM)

No, pienso que hoy en día todos los usuarios de Internet o al menos su gran mayoría conocemos los riesgos de la tecnología, por lo que un mensaje de alerta sobre determinados temas, más bien contribuiría a la cultura de seguridad que deben tener los clientes de la Banca Virtual.

GEstrella-Venezuela (Aug 6, 2004 11:45:18 AM)

Si Helena ya que es el divulgado por la Asociación Bancaria de Venezuela en los medios de comunicación impresos

GPICHLING-Perú (Aug 6, 2004 11:45:50 AM)

La educación es uno de los pilares fundamentales en los que se soportan la seguridad y la confianza de los productos y servicios bancarios, por tanto consideramos que los temas de seguridad deben ser tratados directamente con los clientes (algunos productos bancarios presentan recomendaciones en la actualidad); esto permitirá que los usuarios utilicen con mayor confianza sus operaciones bancarias.

Helena-Colombia (Aug 6, 2004 11:46:10 AM)

Respondiendo a la pregunta 6, las entidades de hecho lo tienen implementado en varios casos, recomendando especialmente a los clientes que verifiquen que están realizando sus transacciones desde una página segura y que no están dando a conocer sus claves a nadie.

GEstrella-Venezuela (Aug 6, 2004 11:46:34 AM)

No, porque consideramos que el mantener informado a nuestros clientes no sería algo intimidatorio sino preventivo.

GEstrella-Venezuela (Aug 6, 2004 11:47:33 AM)

7. Que medios de difusión consideran deben ser utilizados para alertar a los clientes, sin tener que hacer inversiones considerables?

GPICHLING-Perú (Aug 6, 2004 11:47:59 AM)

El primer paso puede ser el envío de un correo electrónico personalizado a cada cliente que utilice los servicios de la banca por Internet, explicando claramente la modalidad y exponiendo las medidas preventivas para evitar ser víctima de fraude; y otra medida a ser considerada debe ser la inclusión en el portal del banco, la publicación de medidas de seguridad destinadas a contrarrestar las diversas modalidades de delito informático.

GOrna - Ecuador (Aug 6, 2004 11:48:26 AM)

- Mensajes en la Pág. Web

GEstrella-Venezuela (Aug 6, 2004 11:48:30 AM)

Consideramos que un sutil mensaje colocado en la correspondencia que se les envíe a los clientes y Banner (Imagen publicitaria en las páginas Web) colocados en las páginas de la Banca en línea, podrían ser algunos de los medios utilizados para llegar este tipo de información a nuestra clientela. Por ejemplo: No suministre su clave secreta por ningún motivo.

Helena-Colombia (Aug 6, 2004 11:48:44 AM)

A través de la misma página web es una alternativa. Otra es como insertos en los extractos que mensualmente se envían a los clientes e incluso en las pantallas de los cajeros automáticos. Estas tres opciones están siendo utilizadas por las entidades.

GEstrella-Venezuela (Aug 6, 2004 11:49:18 AM)

8. Considera que alertar a los clientes de un suceso antes de que este ocurra es contraproducente para la Institución Bancaria y da una imagen de vulnerabilidad en los sistemas?

GPICHLING-Perú (Aug 6, 2004 11:49:55 AM)

Los sistemas bancarios no son los directamente atacados por esta modalidad de fraude, es la información de los clientes en una página falsa la que se ve revelada, por tanto, no es la integridad del sistema informático del banco el que se ve afectado, como se ha podido apreciar en los casos producidos, sino que se resaltan las debilidades que existen en el lado del usuario y del software que utiliza.

GEstrella-Venezuela (Aug 6, 2004 11:50:42 AM)

En nuestro punto de vista consideramos, que nuestros clientes agradecerían que nosotros como Instituciones Financieras le avisáramos cualquier información referente a la Seguridad en sus productos bancarios, aunado a esto el nivel cultural de las personas que acceden a la Banca Online es de amplio conocimiento y nivel profesional, por lo que le da un grado de conciencia mayor sobre este tipo de información. Mucha gente pensará que lo que es vulnerable aquí no es la Institución bancaria sino los datos del cliente, pero hay que tener en

cuenta que el prestigio, confianza y confidencialidad de la Institución se ve inmiscuida en este tipo de fraude. (Continua...)

Helena-Colombia (Aug 6, 2004 11:50:43 AM)

Eso depende en gran medida de la forma como se de a conocer el mensaje. En Colombia por ejemplo, las entidades buscan siempre informar a los clientes de que tienen la infraestructura tecnológica necesaria que les permite garantizar un adecuado nivel de seguridad en las operaciones.

GEstrella-Venezuela (Aug 6, 2004 11:50:55 AM)

Nuestros portales cuando son accedidos, se les puede extraer sin restricción, los logos, así como los atacantes, pueden elaborar otro portal, muy similar al nuestro, por que se copian de toda la información disponible en la Web, colocando trampas para que nuestros clientes le suministren la información vital, esta situación debe ser puesta en conocimiento de las áreas de sistemas de nuestros Bancos, para que se tomen acciones restrictivas al respecto.

GOrna - Ecuador (Aug 6, 2004 11:51:58 AM)

Considero que al alertar a los clientes sobre sucesos que no han ocurrido no es el problema, el problema es la forma o el estilo como se comunica este tipo de información, por ello se debe ser muy sutil y preciso en el mensaje hacia los clientes

GEstrella-Venezuela (Aug 6, 2004 11:52:38 AM)

Danilo te envió la pregunta 8. Considera que alertar a los clientes de un suceso antes de que este ocurra es contraproducente para la Institución Bancaria y da una imagen de vulnerabilidad en los sistemas?

Helena-Colombia (Aug 6, 2004 11:52:44 AM)

Lo que dice Gabriel es cierto. Para esto, es muy importante estar de acuerdo entre las áreas de las entidades que se ven involucradas, con el fin de que el mensaje que se de al cliente sea lo más directo y sencillo

GEstrella-Venezuela (Aug 6, 2004 11:53:22 AM)

Es correcto Helena

GEstrella-Venezuela (Aug 6, 2004 11:54:07 AM)

9. En las páginas Web de sus Entidades Financieras existe algún lugar donde se coloquen Medidas de Seguridad de su Banco?

Danilo-Rep. Dominicana (Aug 6, 2004 11:54:15 AM)

Estoy de acuerdo con lo expuesto por Orna

GPICHLING-Perú (Aug 6, 2004 11:54:35 AM)

Si, en los portales bancarios de El Perú se publican medidas de seguridad a tener en consideración por parte de los usuarios de dichos servicios a fin de prevenirlos de un fraude o engaño, inclusive en algunos se publican, de forma preventiva, instrucciones de virus informáticos que podrían afectar a un portal de banco y que están operando en Internet.

GEstrella-Venezuela (Aug 6, 2004 11:54:58 AM)

Si, existen links en páginas financieras donde se puede obtener la información necesaria sobre los niveles de Seguridad que poseen dichas entidades con todos los productos que ellos disponen en la actualidad.

Helena-Colombia (Aug 6, 2004 11:55:55 AM)

En Colombia también varias de las entidades han publicado medidas preventivas de seguridad en sus páginas web, especialmente relacionadas con el cuidado en el uso de un PC seguro y el manejo de la clave.

GOrna - Ecuador (Aug 6, 2004 11:56:24 AM)

En nuestra institución hemos colocado algunos detalles de la Ley de Comercio Electrónico, pero en si medidas de seguridad aun no las hemos puesto, pero éstas están en desarrollo y se ejecutaran en los próximos días.

GEstrella-Venezuela (Aug 6, 2004 11:57:16 AM)

10. Tienen algún comentario o sugerencia adicional que emitir?

GPICHLING-Perú (Aug 6, 2004 11:57:47 AM)

La Asociación de Bancos del Perú viene realizando hace algunos meses, presentaciones relacionadas con modalidades de delitos informáticos vinculados a Internet en diversos Comités de ASBANC, entre ellos a los de Operaciones, Riesgo Operacional, Seguridad, CEAFOR y Prevención de Estafas y Defraudaciones, en los que inclusive se muestra en forma práctica, la forma en que los hackers utilizan software gratuito y disponible en Internet para obtener información confidencial de clientes; asimismo se les reitera la necesidad de educar a los clientes y usuarios, recomendándose además la implementación de software contra virus informáticos y software espías.

GEstrella-Venezuela (Aug 6, 2004 11:58:07 AM)

El personal de seguridad de nuestro Banco se encuentra dictando Charlas de Fraudes informáticos a todos los Entes Gubernamentales y Organismos Oficiales, sobre los nuevos modus operandi existentes en la actualidad, integrándolos de esta manera como entes multiplicadores de la seguridad, tanto personal como institucional.

GOrna - Ecuador (Aug 6, 2004 11:59:27 AM)

Es muy bueno que tengamos este intercambio de información entre todos los países miembros del CELAES, por lo cual propongo que lo hagamos una vez al mes abordando los diferentes tópicos que afectan a nuestras instituciones y a nuestros países.

Helena-Colombia (Aug 6, 2004 12:01:05 PM)

Quisiera saber cuál es el tema propuesto para el próximo Chat? Me gustaría poder intercambiar información sobre fraude por Internet; todos los tipos de fraude que se conozcan además del que hablamos hoy

Danilo-Rep. Dominicana (Aug 6, 2004 12:01:13 PM)

Gabriel respondiendo la pregunta nueve, si hacemos alerta de seguridad en la red.

GEstrella-Venezuela (Aug 6, 2004 12:02:20 PM)

Bueno Helena de una vez te nombramos coordinadora del 3er. Chat, ponte en contacto con Martha Lucía en FELABAN, para definir el tema y las preguntas.

GEstrella-Venezuela (Aug 6, 2004 12:03:06 PM)

Quiero agradecer a todos los colegas miembros del CELAES su participación activa en este Segundo Chat del 2004, el cual considero ha sido fructífero y beneficioso para todos los participantes, ya que nos ha permitido nutrirnos de las experiencias que en cada uno de nuestros países tenemos sobre el tema tratado. Adicionalmente, los invito a participar en el Tercer Chat que realizaremos el día Martes 24 de Agosto del presente año, a las 10:00 a.m. hora de Bogotá – Colombia.

GEstrella-Venezuela (Aug 6, 2004 12:05:01 PM)

Es propicia esta interacción para recordar que en base a lo acordado en República Dominicana los últimos Martes de cada mes será la fecha para la realización de nuestros Chat´s. Nuevamente gracias por su participación y con esto cerramos esta actividad.

GPICHLING-Perú (Aug 6, 2004 12:05:29 PM)

Muchas gracias, nos veremos el 24 de agosto.