

ALARMA DEL FRAUDE

NATIONAL CREDIT UNION ADMINISTRATION
1775 DUKE STREET, ALEXANDRIA, VA 22314

DATE: Octubre de 2010 **NO. de la ALARMA del fraude:** 10-Fraud-01

FECHA: Uniones de crédito de los
Federal-Asegurados

SUBJ: Tentativa de Phishing - solicitud del E-mail usando la
dirección de NCUA

Estimada junta directive:

El propósito de esta alarma del fraude es informar a todas las uniones de crédito de los federal-asegurados alrededor a tentativa phishing reciente de obtener los números de cuenta de la tarjeta de crédito del miembro, fechas de vencimiento y firmas electrónicas. En los casos divulgados a NCUA, los autores enviados E-mails fraudulentos, representando para ser del NCUA, a los miembros de unión de crédito y el público en general. Los email indican que el NCUA agregará \$50.00 al miembro explica el participar en un examen. El acoplamiento encajado en el mensaje dirige a miembros a a versión falsificada del Web site de NCUA con un examen ilícito que solicita la tarjeta de crédito números de cuenta e información personal confidencial.

Nos referimos altamente sobre el riesgo de imitar el Web site de NCUA y el uso de la insignia oficial de NCUA potencialmente para hacer que el scam aparece más auténtico a miembros unsuspecting. NCUA nunca preguntará los miembros de unión de crédito o a general público para la cuenta personal o personalmente la información identificable como parte de un examen. Cualquier E-mail que alegue para ser de NCUA y pide la información de la cuenta es fraudulento y debe ser tratado como sospechoso. Hemos tomado medidas para cerrar este sitio abajo, pero los miembros de unión de crédito deben seguir siendo alertas a las variaciones posibles de este E-mail fraudulento.

La gerencia de la unión de crédito debe seguir siendo vigilante y mandar a empleados supervisar y identifique cualquier actividad fraudulenta debido a esta tentativa phishing. Personal de la unión de crédito debe continuar educando a miembros con respecto a las muestras de cualquier actividad fraudulenta. Los usuarios finales que chascaron encendido acoplamientos uces de los del E-mail deben consultar con una computadora seguridad o especialista del contra-virus para determinar la necesidad de reinstalar una imagen limpia del sistema informático. Las uniones de crédito deben también animar a miembros que tomen el siguiente precauciones adicionales:

- Computadoras afectadas de la exploración usando software actualizado del del contra-virus.
- Permita las actualizaciones automáticas para el software del contra-virus y el funcionamiento de la computadora sistemas.
- Instale los remiendos de la seguridad para los usos comunes del software puntualmente.
- Esté enterado que los E-maices phishing tienen con frecuencia acoplamiento a los Web pages que reciben código y software malévolos.
- No abra los accesorios no solicitados o inesperados del E-mail.
- No siga los acoplamiento del Web en E-maices no solicitados de actividades bancarias federales evidentes las agencias, en lugar, bookmark o mecanografía la dirección del Web de la agencia.
- Llame la agencia usando haber sabido y apropíese del número de teléfono para verificar legitimidad del mensaje y del archivo unido.

Los miembros afectados por este scam, y las variantes de este scam, deben ser aconsejados para remitir el mensaje entero del E-mail a Phishing@ncua.gov. Además, demandas oficiales referente a cualquier E-mail fraudulento sospechado puede ser archivado con el fraude del Internet Centro de la queja (IFCC) en www.ic3.gov. El IFCC es una sociedad entre Oficina federal de la investigación y del centro blanco nacional del crimen del collar.

Las reglas y las regulaciones de NCUA pieza aberturas de 748, de las direcciones del apéndice B de la unión de crédito o sistemas del abastecedor de servicio de la unión de crédito que comprometen la información del miembro. Crédito la gerencia de la unión debe determinar el potencial para que el incidente cause daño o inconveniencia substancial al miembro. De acuerdo con el análisis riesgo-basado de la gerencia del incidente, las acciones siguientes pueden ser necesarias:

- Contenga y controle el incidente (el monitor, congela, o las cuentas afectadas cercanas mientras que preserva los expedientes y la otra evidencia).
- Notifique a miembros del incidente según lo contorneado específicamente en el apéndice B. de la parte 748.
- Archive un informe de actividad sospechoso del acuerdo con la regulación establecida.
- Notifique el director regional apropiado de NCUA (o la autoridad de supervisión del estado).
- Entre en contacto con y archive un informe con autoridades locales de la aplicación de ley.

NCUA continuará siguiendo esta edición y proveyendo de usted la información adicional como autorizado. En el medio tiempo, si usted tiene cualesquiera preguntas, entre en contacto con por favor su distrito Examinador, oficina regional, o autoridad de supervisión del estado.

Sinceramente,

/s/

Melinda A. Love
Director de la examinación y del seguro