Revista de Derecho Comunicaciones y Nuevas Tecnologías

Documento Gecti nro. 9

Los engaños en internet: de las cadenas, del correo no deseado, de la mensajería basura y otros demonios

Jeimy J. Cano

(Marzo de 2009)

Universidad de los Andes
Facultad de Derecho - GECTI
Revista N.º 4, junio de 2010. ISSN 1909-7786

Documento GECTI nro. 9

LOS ENGAÑOS EN INTERNET: DE LAS CADENAS, DEL CORREO NO DESEADO, DE LA MENSAJERÍA BASURA Y OTROS DEMONIOS

Jeimy J. Cano[1]

(Marzo de 2009)

Sumario

I. GECTI

El **G**rupo de **E**studios en internet, **C**omercio electrónico, **T**elecomunicaciones e **I**nformática (GECTI) fue creado el 5 de octubre de 2001 en la Facultad de Derecho de la Universidad de los Andes. Busca fomentar el trabajo multidisciplinario y establecer un puente entre la Universidad y la sociedad para procurar reflexiones y acciones en materia de la Internet, la Sociedad de la Información y temas convergentes.

1 Miembro investigador del Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática (Gecti) de la Facultad de Derecho y Profesor Distinguido de la misma Facultad. Universidad de los Andes. Colombia. Ingeniero de Sistemas y Computación, Universidad de los Andes. Magíster en Ingeniería de Sistemas y Computación, Universidad de los Andes. PH.D in Business Administration, Newport University. Profesional certificado como Certified Fraud Examiner (CFE) por la Association of Certified Fraud Examiners. Presidente de ACIS durante el periodo 2005-2007 Contacto: jjcano@yahoo.com

Las opiniones expresadas en este documento sólo comprometen a su autor y no a la Universidad de los Andes ni a los miembros del GECTI.

Introducción

Comenta Walter Riso en su libro *Cuestión de dignidad* que "la prudencia nos obliga a deliberar con nosotros mismos, es la que gobierna nuestros deseos y suaviza nuestros impulsos".[2] Si esto es correcto, nuestras actividades y acciones frente a un paseo por el mundo de Internet deberían tener la misma connotación. Es decir, nuestro criterio y atención activa debería ser la constante cada vez que navegamos en Internet.

La falta de prudencia, de sentido crítico y una sobre valoración de la información disponible en Internet nos hace presa de las iniciativas de los intrusos en Internet. Esta situación, reiterada una y otra vez en los niños, jóvenes y los adultos, presenta a Internet como una villa desprevenida y generosa en información y posibilidades, donde todos comparten y caminan sin preocupaciones.

Sin embargo, la verdad es otra. Internet es, como cualquier ciudad del mundo: con calles especiales y llenas de lujos, así como con vecindarios intransitables con desconocidos a la vuelta de la esquina a la espera de los incautos que se han atrevido a cruzar los límites del barrio. No es descabellado pensar que existan aún sitios inexplorados en Internet, dada la versatilidad de la red y todos sus complejos sistemas de interconexiones que no alcanzamos a dimensionar (Wells, J. 2009, p. xii).

En este contexto, los nuevos delincuentes informáticos, aquellos que aprovechándose de los sentimientos naturales de compasión, la inspiración filial propia del ser humano, el espíritu de superstición y magia que existe en cada persona, así como del desmesurado egoísmo por poseer, establecen estrategias para potenciar sus intenciones vinculando a más personas en su cruzada expansionista, que no es otra cosa que una forma de lucrarse, desestabilizar o invadir a un tercero con la excusa de una "causa buena", "denuncia justa" o "logro de lotería", que en la actualidad denominamos "cadenas", "correo no deseado" o sencillamente "mensajería basura".

El fenómeno de las cadenas es una realidad basada en el "sentimiento" de las personas, en su convicción frente a la vida, que busca un sentido de común unión, loable y necesario en una comunidad, pero que mal orientado es una forma devastadora que mina la confianza en los medios y servicios de Internet, lo que implica necesariamente un uso inadecuado que impacta tanto a los usuarios como a las tecnologías de información que los soportan.

En este documento revisaremos las implicaciones de las cadenas, desde las perspectivas psicológica, tecnológica y jurídica, que nos permitan avanzar en el desarrollo de un criterio más acertado para dar respuesta a una amenaza latente provocada por los atacantes,

2 Riso, W. (2008) *Cuestión de Dignidad*. Editorial Norma. p. 87.

que no es otra que comprometer la confianza y autorregulación de la red, con la falsa (pero creíble) necesidad de construir comunidad en un mundo interconectado y atento a los cambios propios de cada Estado-nación.

II. ASPECTOS PSICOLÓGICOS DEL ENGAÑO

Revisando lo que ocurre en el mundo real frente a los engaños de las personas, podemos observar algunas características interesantes que nos servirán de excusa para nuestro análisis en un contexto digital.

Cuando una persona es engañada se vulnera su confianza y la creencia de que quienes interactúan en la red lo hacen de buena fe. La confianza es ese valor que una persona da a otra, en la cual reconoce la confiabilidad de su interlocutor, la rectitud de sus acciones y la habilidad para ser consecuente entre sus pensamientos y acciones. En consecuencia, un engaño fisura la imagen del tercero y la valía de quien engaña, destruyendo la relación filial existente, la cual queda expuesta y mancillada, mientras no exista un proceso de reconstrucción basado en la revisión misma de los elementos que llevaron al artificio.

Cuando llevamos este tema al mundo de Internet, no existe una persona física que se impacte con nuestra censura, no hay un referente concreto que se afecte por nuestra inconformidad, lo que lleva a que no haya un impacto real y concreto en nuestro actuar, más allá de estar más prevenido ahora frente a lo ocurrido, prevención que perdura, lo que conlleve revisar y resolver la dificultad que se presenta, claro está, si es viable.

Frente al engaño en Internet, las personas tienen un sentimiento de desesperanza, pues evidencian que por más que se esmeren en denunciar o hacer sentir su voz de rechazo, no hay acciones efectivas que impacten a los posible infractores o estafadores, haciendo de su lucha, un clamor estéril que no es otra cosa que una voz más que se queja, dejando impotentes a otros como ellos y con una sensación de incapacidad que es aprovechada por el anonimato del delincuente en Internet.

Si bien esta situación psicológica de los internautas podría ser generalizada, es importante tomar acciones individuales para reconstruir nuestra perspectiva psicológica del engaño en Internet, manteniendo una actitud dinámica y preventiva que limite las acciones del intruso cuando intente vulnerar nuestra confianza personal o invocar nuestras conciencia colectiva en pro de un aparente beneficio. Dichas acciones no son otra cosa que mantener un deseo razonado, una anticipación responsable, que nos lleven a un juicio balanceado entre aquello que ocurre en la realidad frente a eso que se nos presenta a través de Internet y su servicios. (Adaptado de Riso, W. 2008, pág. 87)

Los engaños más frecuentes en Internet son las cadenas supersticiosas llenas de mensajes como:

> Ha llegado a tu vida el Tótem Electrónico Sagrado de la Prosperidad (TESP), un mítico mensaje que ha saltado del mundo físico al mundo virtual, consagrado en la Edad Media. Todo aquel que lo reciba estará lleno de bendiciones y realizaciones. Si intenta romper esta tradición milenaria, estará expuesto a las fuerzas oscuras que están destinadas para aquellos que no continúen esta cadena, mostrando el egoísmo de aquel que la rompe. Para que tu vida se llene de mayores logros y realizaciones, distribuye antes de la media noche cuidadosamente el mensaje adjunto, entre aquellos amigos cercanos de corazón noble y generoso, invocando el nombre de los maestros antiguos, con el mantra que sigue a continuación:
>
> Ven a mi vida prosperidad, ven a llenarme de tus dones y gracias. Haz de cada palabra y acción un canto a la esperanza y ayúdame a ser más con y por los otros, para que al encontrarme con la esencia misma de la Creación, pueda construir contigo, siendo la manos del arquitecto y la mente maestro.
>
> Recuerda que tienes hasta la media noche de hoy para que los poderes inherentes de esta invocación se materialicen en tu vida.

Un análisis psicológico de este mensaje muestra algunos aspectos antropológicos del ser humano que son utilizados por los atacantes para intimidar la estabilidad emocional de las personas desprevenidas y temerosas. Las palabras "tótem", "prosperidad", "consagrado", "tradición milenaria", "mantra" tienen una especial carga de valor que impregna la esfera de la persona que la lee; ve cómo es comprometido su espacio vital, su realidad externa, sólo por atender y leer estas frases. Recuerde, que *no* existe relación directa entre dichas palabras y la realidad circundante, sólo es una forma para manejar sus expectativas sobre la vida, pues finalmente son sus acciones y realidades las que hacen que las cosas pasen y no un mensaje diseñado por un "curioso o delincuente" para lograr impactar sistemas de mensajería por gusto o con ánimo de lucro.

A. Impactos tecnológicos de los engaños

Estamos expuestos a diario a una evolución de la criminalidad en medios tecnológicos, la cual nos advierte que los intrusos aprenden tan rápido como nuestros miedos y temores evolucionan con el fenómeno tecnológico. Las tecnologías de información que soportan los servicios de utilizamos a la fecha como son, entre otros, el correo electrónico, la navegación vía Internet, las redes sociales, los sistemas de conversaciones en línea, los mensajes instantáneos, registran cada uno de nuestros gustos, preferencias, sentires y deseos, cada vez que escribimos, navegamos, compartimos y enviamos comunicaciones a través de algunos de los medios previamente mencionados.

No obstante lo anterior, se nos olvida que compartir sin una convicción y sano análisis de la realidad implica abrir la puerta a una exposición personal más allá de lo que estamos dispuestos a revelar, dejando abierta la ventana para que un tercero se aproveche sin condiciones de lo que sentimos o creemos.

En este contexto, los atacantes saben que los jóvenes y algunos adultos, desconociendo lo que ocurre en las conexiones de la red, son objetivos relativamente fáciles para convencer y vincular en sus propósitos de afiliación para materializar acciones en contra de terceros o de ellos mismos, convencidos del argumento que pueden construir, basados en la información que hemos expuesto en la red.

En este sentido, cuando una cadena se crea, cuando una campaña de desprestigio se desarrolla o se arma un perfil en una red social, estamos asistiendo al mal uso de las tecnologías de información, lo que erosiona la estrategia para hacer de Internet una estrategia que desarrolle el comercio electrónico, la participación ciudadana incluyente y una herramienta para la conquista de la generación de valor con la investigación y el desarrollo.

Las tecnologías de información no son las únicas armas para luchar contra su mal uso; se hace necesario educar de manera consciente a los usuarios de éstas para fortalecer o crear buenos hábitos de higiene informática que erijan una barrera menos porosa para que al posible atacante le cueste más intentar vulnerar nuestra realidad digital o pierda interés en nuestros datos.

Al estar interconectados y compartiendo información todo el tiempo, la propagación de los engaños se vuelve exponencial y geométrica. Detenerla es prácticamente imposible, pues este sistema de conexiones virtuales replica y difunde la información, bien sea por acciones concretas de una persona o por registros y clasificación de los datos por máquinas de búsqueda que llevan un registro cercano de los cambios que sufren los sitios en Internet. Sólo basta mirar el proyecto Internet Achive[3] para ver la evolución de múltiples sitios en la red.

III. CONSIDERACIONES JURÍDICAS DE LOS ENGAÑOS EN INTERNET

Los "buenos intrusos" son aquellos que cuando realizan sus actividades vinculan a terceros para hacerlos "corresponsables" de sus acciones. No se han percatado que existe una necesidad implícita en cada atacante en no estar solo en lo que se hace, pues sabe que una culpabilidad compartida es más llevadera que ser el responsable único del hecho.

Si observamos en Internet, los engaños realizados requieren, por lo general, un apoyo de un tercero, bien sea consentido o no, y es allí donde está el tema de la responsabilidad y participación en los hechos delictivos, que tanto inquieta a muchos cuando se trata de establecer los alcances de las acciones legales en contra de un posible intruso (Soria Verde, M. y Sáiz Roca, D. 2006, cap. 2).

Consecuentemente con lo anterior, la utilización inadecuada[4] de los recursos de tecnolo-

3 Cfr. http://www.archive.org

4 Se entiende inadecuada como aquellas acciones que se ejecutan fueran del marco general definido del uso de la tecnología de información establecido por una organización.

gía, bien sea en un entorno abierto y público, como en uno cerrado y restringido (como una organización), conlleva un perjuicio inherente, que es causado por un tercero, cuyos intereses no conocemos, y que aun conociéndolos, son muchas veces confusos, dada la particularidad del entorno tecnológico y los elementos materiales probatorios asociados con los dispositivos tecnológicos utilizados.

Muchas preguntas surgen cuando se presentan los procesos administrativos, disciplinarios o penales que implican a una persona natural o jurídica en una conducta lesiva para un tercero, que vulneren sus principios fundamentales y que impliquen necesariamente una investigación profunda de los hechos en un contexto de ambientes con alta tecnología. Consideren una investigación donde se difame a una organización o persona realizada a través de redes sociales, correo electrónico, mensajes de texto o cualquier otro medio de difusión masiva, ¿qué implicaciones se pueden derivar de este hecho? Revisemos algunas reflexiones sobre esta situación (Marshall, A. 2008, cap. 7).

La primera reacción de la persona u organización es tratar de detener la difamación, para lo cual intenta por medios igualmente masivos desmentir los hechos o controvertir la evidencia que el mensaje sugiere. Esta estrategia, si bien quiere limitar el daño causado, puede ser recibida por el público como una estrategia de defensa o como una reacción de la organización de algo que puede ser cierto. Por tanto, se hace necesario diseñar con cuidado esta estrategia, para lo cual la colaboración y apoyo con las fuerzas de policía judicial y los prestadores de servicios de Internet son pieza fundamental.

Un segundo paso es establecer el origen del mensaje, con el fin de establecer los focos de difusión y tratar de establecer su fuente. En esta segunda fase, que se puede dar de manera paralela con la primera, hace falta el concurso de especialistas en informática forense para que descubran en los datos informáticos de los mensajes las pistas del recorrido que éstos han hecho desde su lugar de envío hasta el sitio donde han llegado. Es importante anotar que este especialista detallará de manera técnica sus hallazgos y soportará sus afirmaciones basado en la formalidad técnica asociada con la tecnología analizada.

Un tercer paso es, una vez entregado el informe del informático forense y revisadas las posibilidades de identificación de posibles infractores (que pueden ser tanto personas internas como externas a la organización), adelantar los procedimientos jurídicos requeridos para formalizar la denuncia del hecho, con el fin de formalizar los elementos materiales probatorios requeridos que fortalezcan las hipótesis planteadas en el informe pericial y así se profundice la investigación misma sobre los hechos presentados.

Si bien pueden existir otros pasos alrededor de la situación, es claro que al menos estos

Universidad de los Andes. Facultad de Derecho

tres deberán estar en su período y hora, para mostrar la diligencia y debido cuidado de la organización, los cuales son dos elementos claves en el momento de las investigaciones que se desarrollen, pues si adicional a lo ya indicado en el caso analizado, se vulneran derechos de un tercero, esta acción proactiva dará elementos a la organización para responder ante demandas en su contra por hechos semejantes.

IV. RECOMENDACIONES PRÁCTICAS PARA IDENTIFICAR Y CONFRONTAR LOS ENGAÑOS EN INTERNET

Como se ha revisado hasta el momento, los engaños en Internet no son ajenos a nuestra psique ni las consideraciones tecnológicas o jurídicas propias de ellos. En este sentido, un engaño lo es tanto en el mundo *offline* como en el *online*. Por tanto, debemos desarrollar una conciencia crítica, un sano criterio y una fortaleza psicológica para confrontar las estrategias de los atacantes para hacernos parte de su estrategia de engaño e intimidación, evitando ser cómplices de sus deseos y objetivos.

Para ello, a continuación presentamos algunas acciones concretas que nos invitan a cuestionarnos sobre lo que recibimos y enviamos mediante algunos de los servicios de Internet, como una forma de responder a la constante invasión de mensajes y actividades que remiten los atacantes a través de estos medios (Adaptado de Donovan, F. y Bernier, K. 2009, cap. 11).

1. Siempre que reciba un mensaje de una persona desconocida, no haga caso de éste y repórtelo, bien sea a la autoridad judicial pertinente o a la persona de la organización destinada para tal fin.

2. Si recibe un mensaje de una persona conocida, pero el contenido de la comunicación sugiere una estrategia de difamación en contra de un tercero, notifique a la entidad de la cual se habla, enfatizando en su labor de notificación, viendo el impacto que esto puede tener en la imagen de la firma. Asimismo, si se encuentra en un ambiente corporativo, notifique a la persona indicada el hecho.

3. Los mensajes sobre obras sociales o que se fundan en los sentimientos de bondad y afiliación de las persona deben ser revisados directamente con la firma que los envía. En caso de no poder contactarse con la firma que origina el mensaje, ignore el correo.

4. Cuando le anuncien que se ha ganado una lotería, que quieren compartir con usted una fortuna, piense: "¿usted haría lo mismo si tuviese esa oportunidad?". Recuerde que el atacante quiere jugar con sus sentimientos, y para ello usted debe razonar antes de darle vía libre a éstos, una vez ha leído el mensaje.

5. Los aspectos mágicos o esotéricos que se anuncien en mensajes a través de cualquier medio tecnológico son sólo eso, mensajes. Ellos no pueden materializar o generar acciones sobrenaturales. Es su mente la que crea los efectos en su entorno. No se deje sugestionar, pues cuando esto ocurre, el atacante logra su objetivo.

6. Cuando comparta información con un tercero, recuerde que ésta podrá estar expuesta en cualquier momento a través de Internet y sus servicios. Por tanto, cuando lo haga, sea consciente de los alcances que puede tener al estar disponible en máquinas de búsqueda en Internet.

7. Internet es uno de los logros más importantes de la humanidad y fue creado para abrir posibilidades y crear oportunidades para todos. De nosotros depende que este logro se mantenga y perdure en el tiempo. ¿Cómo? Haciéndole la vida más difícil a los desadaptados informáticos

V. REFLEXIONES FINALES

Hemos revisado algunas de las perspectivas de las implicaciones de los engaños en Internet y sus impactos en el contexto corporativo y social; sin embargo, aspectos como la privacidad, la cultura del menor esfuerzo y la inmediatez, la cultura del *cut and paste*, entre otros aspectos, se nos quedan fuera del alcance de este documento, con lo cual sabemos que abordar esta problemática requiere una mayor profundización de la realidad del ser humano frente a la tecnología y cómo su entendimiento de ésta lo hace un actor fundamental para la conquista del universo tecnológico que aún queda por descubrir.

Somos humanos y como tal estamos llenos de sentimientos y emociones, pero no podemos dejar que la emoción nos maneje, sino más bien someter a la razón nuestra reacción y sopesarla frente a la realidad evidente que nos aborda. En este sentido, los mensajes que transitan en Internet buscan poner a prueba al usuario en prudencia y sabiduría para hacer de ellos una forma para reírnos de las travesuras de los intrusos o una estrategia cómplice que "engancha" con los propósitos del atacante y seguir el juego del engaño que propone.

"La policía sólo puede entrar en tu casa con una orden de cateo, pero las leyes sobre el acceso de la policía a servidores remotos son menos estrictas", anota el ex asesor de privacidad del gobierno de Bill Clinton, Peter Swire (KREBS, B. 2009, pág. 60). Esta afirmación pone de manifiesto una de la implicaciones de compartir nuestra información con terceros: la información puede estar desprotegida y expuesta no sólo a una inspección autorizada de terceros, sino a una revelación no autorizada de ella por parte de personas inescrupulosas. Es un deber de cada uno de nosotros valorar la información que tenemos o publicamos, pues las implicaciones que se deriven de esta acción serán directamente proporcionales al nivel de sensibilidad de ésta.

Así pues, se hace necesario, "la filtración de información irrelevante y la condensación de información relevante"[5] para avanzar en una estrategia formal y conjunta entre todos los participantes de la red, con el fin de sorprender a los intrusos en su propio escenario, para que cuando su ex novia publique esas fotos comprometedoras, se expongan los datos de contacto de su celular y le lleguen mensajes cada vez más personalizados, recuerde que la información es un bien fundamental en una sociedad de la información y del conocimiento y un tesoro particular que muchos quisieran y pagarían por obtener.

Bibliografía

Ackoff, R., *Recreación de las corporaciones*. Oxford, Editorial Oxford Press, 2000.

Donovan, F. y Bernier, K., *Cybercrime fighters. Tales from the trenches*. Pearson Education Inc, 2009.

Krebs, B. ("Siguen tu huella", en *Popular Mechanics en Español, Núm. 62/03*. 2009, marzo.

Marshall, A. *Digital forensics. Digital evidence in criminal investigation*. John Wiley & Son – Blackwell.

Riso, W., *Cuestión de dignidad*. Editorial Norma, 2008.

Soria Verde, M. y Sáiz Roca, D. *Psicología criminal*. Pearson Prentice Hall, 2006.

Wells, J. *Computer fraud casebook. The bytes that bite*. John Wiley & Sons, 2009.

5 Ackoff, R., *Recreación de las corporaciones*, Oxford: Editorial Oxford Press, 2000.