Selva Orejón, de onBRANDING: «Cuidado con mostrar debilidades como una crisis sentimental en redes»

POR RUBÉN GUZMÁN 12 DE ENERO DE 2021 REDES SOCIALES TRANSFORMACIÓN

onBRANDING es una de las más destacas agencias españolas en el campo de la **reputación *online*** y la **ciberinvestigación**, y su fundadora y Directora Ejecutiva, **Selva Orejón**, un nombre clave cuando se trata de hablar sobre cómo podemos protegernos de los ciberataques o qué podemos hacer cuando somos víctimas de uno.

Después de haber hablado con **Mario Bonacho** de AVERUM Abogados, *partners* de **onBRANDING**, sobre cómo afrontar legalmente los ciberataques, hoy Selva nos cuenta cómo su agencia ayuda a prevenirlos y minimizar sus consecuencias, y nos da algunas claves para no dar facilidades a los criminales profesionales, los acosadores o aquellos que tratan de dañar la **reputación online** de una persona u organización.

P: En onBRANDING protegéis la identidad digital. ¿Qué tipo de servicios ofrecéis para conseguirlo?

Los servicios que ofrecemos son los siguientes:

RepControl, ideado para la gestión y el control de la reputación online. En él realizamos tareas de vigilancia, monitorización y realización de informes periciales de cálculo de pérdida de reputación *online* (de inmensa ayuda para los procesos judiciales), para que así se inicien las acciones de mejora de imagen, identidad y reputación.

También identificamos riesgos, situaciones hostiles y todo aquello que pueda afectar a la reputación tanto de personajes públicos como de organizaciones. La reputación *online* es su credibilidad en Internet: nosotros la protegemos desde situaciones preventivas hasta reactivas y judiciales.

En este tipo de procesos de identificación y control reputacional, realizamos monitorización activa mediante escucha activa, identificamos riesgos, los valoramos, planificamos acciones de defensa y monitorizamos activamente todos los registros que afecten a su reputación *online*. Las amenazas en las redes sociales son cada vez más rápidas y amplias, con posibles efectos sobre los trabajadores, sobre la identidad y sobre la credibilidad. Pueden causar graves daños reputacionales. Preparamos la defensa *online* de los clientes y monitorizamos su marca para protegerlos de forma eficaz.

«HAY AGENCIAS DE COMUNICACIÓN QUE, DE FORMA INCONSCIENTE, ESTÁN FILTRANDO DATOS DE LOS CLIENTES POR UNA FALTA DE SEGURIDAD EN LAS COMUNICACIONES»

P: Una vez desatada un crisis *online*, ¿qué se puede hacer para atajarla?

R: Parte de nuestra especialización es la creación de equipos de respuesta rápida en casos de crisis *online* para atenderlas en el menor tiempo posible. Contamos con profesionales en diversos ámbitos que se enfrentan a las crisis de forma eficaz y rápida, atajando los ataques, realizando acciones y controlando los efectos colaterales, buscando siempre la capacidad de resiliencia. Atendemos sus crisis en el menor tiempo posible para acabar con el problema.

Cuando además una situación de crisis requiere de una respuesta urgente activamos el servicio SOC reputacional. Nuestro equipo está formado en respuesta rápida ante incidentes críticos reputacionales para atenderlos en el menor tiempo posible y de forma eficiente. Analizamos, evaluamos y reaccionamos de forma activa o pasiva, buscando siempre la capacidad de resiliencia ante ataques de tipo 1) golpe mortal, tipo 2) golpe recuperable o tipo 3) caso de mejora.

Algunos de estos casos son para el desmentido de *fake news*, bulos, falsas acusaciones, injurias, calumnias, filtración de documentos, baja de dominios perjudiciales que se han dado de alta a nombre del cliente, eliminación de contenido, desindexación de videos e imágenes dañinas de urgente necesidad de respuesta.

En cualquier crisis, la necesidad de respuesta debe ser inmediata pero también segura, por eso tenemos el servicio SegCom: Seguridad Comunicativa. Es un clásico encontrarnos con situaciones en las que agencia de comunicación de forma totalmente inconsciente está filtrando datos de los clientes por una falta de seguridad en las comunicaciones de sus trabajadores o colaboradores.

P: ¿Qué papel juega la ciberinvestigación en el trabajo con vuestros clientes?

R: Todo proceso de acompañamiento *online* requiere de algunas incursiones en ciberinvestigación.

Realizamos informes exhaustivos de ciberinvestigación liderados por nuestros detectives colegiados de confianza. Ante cualquier problema nos ayudan apoyándonos con el servicio *onTRACKERS* para discernir qué identidad técnica se encuentra tras los ataques recibidos y qué nivel de peligro se esconde detrás de la Red. Por ello, disponemos de un servicio de ciberinvestigación para analizar las amenazas, dar una respuesta y realizar exámenes forenses digitales.

Una de las situaciones que más se repiten son las acciones contra el *hacktivismo*. Si por los mensajes recibidos o el ataque técnico no se sabe de dónde proviene la amenaza, la ciberinvestigación puede dar con la fuente.

«CUANDO UN CLIENTE SUFRE CIBERACOSO, NOSOTROS ESTAMOS SIEMPRE, DESDE EL INICIO DEL PROCESO LEGAL AL APOYO PSICOLÓGICO»

P: ¿Ayudáis también a las víctimas de ciberacoso?

R: Fuera del ámbito empresarial y en algunos casos dentro de él, pero generalmente contra personajes públicos pero también contra ciudadanos anónimos, se dan casos de ciberacoso: acoso, acecho, amenazas, coacciones… y bullying (especialmente en menores de edad).

Somos especialistas en identificación de ataques, análisis de eventos de ciberataques y acecho. Contamos con profesionales especialmente formados para enfrentarse al ciberacoso y proteger a los clientes de él. Apoyamos a los clientes con informes que pueden adjuntar a la denuncia.

No es justo que el ciberacoso condiciones la vida de una persona y/o de su familia. En onBRANDING, acompañamos al cliente con el servicio **onBULLYING**: *stop* acoso, *stop* bullying.

La idea que queremos transmitir es que nosotros estaremos siempre. Cuando la víctima decida poner el *STOP* al acoso que sufre y cuando necesite iniciar el proceso legal con la denuncia o no. Cuando necesite un psicólogo especialista en cyberbullying le pondremos en contacto con el equipo del Instituto Carl Rogers. Cuando necesite de abogados, peritos especializados en identidad digital o peritos informáticos, psicológicos, perfiladores criminales, peritos lingüistas, y ciberinvestigadores, aquí estaremos, siempre. Para poder poner freno al acoso de forma profesional.

Una vez el cliente se enfrenta a una situación de acoso, o cuando quiere actuar de forma preventiva, ponemos en marcha el servicio de **Protección de la Identidad digital**.

Entre otras amenazas, las que se centran en la identidad digital son las que más posibilidades tiene de afectar a un cliente, por el mal uso intensivo de las redes sociales e Internet.

P: Mirando tu currículum, tu formación es multidisciplinar y abarca la comunicación, el desarrollo de negocio y el peritaje judicial. ¿Qué tipo de perfiles profesionales buscáis para trabajar en onBRANDING?

R: En onBRANDING trabajamos con casos que necesitan de distintos perfiles para su resolución. Contamos con especialistas en ciberseguridad, expertos en tecnología, criminalistas, analistas técnicos, expertos en *profiling* de criminales, atención al cliente…

Además, contamos con la colaboración de psicólogos y terapeutas de familia, adolescencia e infancia para los casos más serios de *bullying* o acoso.

«NUESTROS CLIENTES SUELEN ACUDIR A NOSOTROS CUANDO EL DAÑO YA ESTÁ CAUSADO, NO HAY CONCIENCIA DE PREVENCIÓN»

P: Vuestros clientes ¿suelen acudir a vosotros tras haber recibido ya algún ciberataque o ya hay cierta conciencia de prevención de la identidad digital? Como nos olemos un poco la respuesta a esta segunda pregunta, te vamos a formular también la inversa: ¿os ha llegado algún cliente del que hayáis dicho "vaya, lo han estado haciendo bastante bien en temas de ciberseguridad"?

R: Tenemos clientes de todo tipo, desde empresas preocupadas por su reputación a famosos y *celebrities* que están sufriendo *hackeo* de redes sociales, acoso y extorsión; también familias y adolescentes con problemas derivados de redes sociales.

Por normal general, acuden a nosotros cuando el daño ya está causado. Cuando se dan cuenta que están siendo víctimas de algún ciberdelito o de situaciones críticas. No suele haber una concienciación en prevención y mucho menos una solicitud de actuación temprana.

No solemos encontrarnos casos con una cobertura en ciberseguridad realmente adecuada. En ese caso, suelen ser empresas o *celebrities* que acuden a nuestros servicios de prevención o asesoramiento. Generalmente, son los menos.

Nosotros hemos creado onBRANDING Academy: contamos en nuestro haber con numerosos cursos y clases de concienciación que han formado a diferentes colectivos, desde fuerzas de la ley a personas de alta relevancia, así como a organizaciones.

P: Hacéis hincapié en que la monitorización y la prevención son fundamentales para evitar cibermales mayores. ¿Cómo realiza onBRANDING estas funciones para sus clientes?

R: A través de herramientas especializadas, y sobre todo, a través de la experiencia y conocimientos de nuestro equipo. Esto forma parte de nuestro modo de operar y de lo que nos diferencia del resto de competidores, por lo que no te puedo dar muchos más detalles.

Sí que tengo que matizar que el contacto directo con la víctima/cliente y la voluntad real de ayudarles a restablecer la normalidad es fundamental para que el caso funcione.

P: Una de vuestras especialidades es la protección de la reputación digital. Es un tema amplísimo, claro, pero ¿podrías enumerarnos cuáles son las actuaciones más habituales para atajar una crisis en este aspecto?

R: Una crisis de reputación puede tomar muchos rumbos y puede tener orígenes muy distintos. Pero de forma general, es necesario monitorizar y analizar la situación; prevenir y proteger en materia de ciberseguridad; trazar una estrategia de comunicación.

«TODOS PODEMOS SER VÍCTIMAS DE CIBERESTAFAS Y *HACKEOS*, Y NO SOLO LOS PERSONAJES PÚBLICOS»

P: Empresas y figuras públicas como los *influencers* parece que pueden ser el principal objetivo de los ciberataques, pero ¿hasta qué punto somos todos posibles víctimas? ¿Deberíamos todos los ciudadanos tomar ciertas precauciones en este aspecto?

R: En los últimos meses los casos de *celebrities* que están siendo víctimas de *hackeo* y extorsión han aumentado considerablemente. El fin principal de estos ciberataques es la obtención de un rédito económico. Los pagos que las víctimas puedan efectuar se utilizan para financiar más acciones ilegales, e incluso el terrorismo. Este es el motivo por el que todos podemos ser víctimas de ciberestafas y *hackeos*, y no solo los personajes públicos. Si consideran que un usuario es lo suficientemente vulnerable para obtener la compensación que buscan lo intentarán.

P: ¿Es nuestro móvil nuestro punto débil?

R: Por supuesto. Utilizamos aplicaciones de banca, mensajería, correo electrónico, y cada vez abrimos más enlaces que podrían tener un origen fraudulento, que pueden terminar en *phishing* o secuestro del dispositivo. Si un ciberdelincuente controla nuestro teléfono, podría tener acceso a contraseñas y contactos y causar graves daños personales y profesionales.

P: Te pedimos un consejo: ¿qué crees que nunca deberíamos exponer en nuestras redes sociales?

R: Nuestra ubicación en tiempo real, la identidad de menores ni su ubicación en tiempo real. Debemos tener especial cuidado con exponer nuestros puestos de trabajo o mostrar debilidades como, por ejemplo, una crisis sentimental o una posible depresión. Esto podría ser un motivo para que suplantadores de identidad intenten aprovecharse de la situación para llevar a cabo estafas, o generar confianza en nosotros.

«RECOMENDAMOS A LOS PADRES QUE ABRAN PERFILES EN LAS REDES QUE SUS HIJOS UTILIZAN PARA CONOCER CÓMO FUNCIONAN Y EL CONTENIDO QUE SE GENERA»

P: La exposición de los jóvenes a la tecnología es total y, como tú muy bien has dicho en otras entrevistas, no han tenido "maestros digitales" en sus padres, porque son las primeras generaciones que han crecido con las redes sociales. ¿Qué podemos hacer para protegerlos?

R: Siempre recomendamos a los padres de menores que abran perfiles en las redes sociales que sus hijos utilizan. No con el fin de espiarles o controlarles, sino para conocer cómo funcionan y el contenido que se genera.

Es importante formarnos en las nuevas tecnologías y en redes sociales, estar al día y poder mantener conversaciones con nuestros hijos sobre contenidos, riesgos y prevención.

P: Vuestra relación con los clientes tiene un carácter muy especial. Manejáis información muy sensible que exige una confianza total en vosotros. Y, en ocasiones, llegarán a onBRANDING personas que están sufriendo crisis personales producidas por los ciberataques. Personalmente, ¿cómo llevas la implicación emocional en estos casos? ¿Llega a ser un trabajo 24/7 y es difícil no llevarse las emociones a casa?

R: Es un trabajo que necesita de una implicación total y la atención es imprescindible. Las víctimas están pasando por situaciones muy difíciles, que en ocasiones pueden llegar a arruinar su vida por completo, y necesitan la mayor rapidez y eficacia en la actuación para devolverles la normalidad; pero también apoyo psicológico y acompañamiento.

Es complicado gestionar las emociones de nuestro equipo, ya que a veces vemos cosas muy duras. Al final, no debemos perder la empatía y tenemos que saber ponernos en el lugar del otro, no ver solamente "clientes". Creo que ahí reside la eficacia de nuestro método de trabajo.

P: Vuestro trabajo os plantea dilemas éticos, sobre todo en casos como las crisis de reputación digital. ¿Lo afrontáis como un abogado? ¿Todo ciudadano tiene derecho a la defensa de la reputación digital, incluso ante la posibilidad de que esa crisis se desate por actitudes o hechos ciertos y con connotaciones negativas?

R: Procuramos seleccionar los casos con los que sentimos conexión y que consideramos que necesitan nuestra ayuda. Es cierto que una "víctima" puede haber sido el primero en cometer el error o el "delito", y posteriormente está siendo víctima como repercusión al daño que ha causado; en estos casos se nos plantean problemas éticos. Debemos valorar si nos sentimos cómodos con el caso o si entra dentro de nuestros valores éticos. Sin duda, en muchas ocasiones enfrentamos situaciones que no son fáciles de afrontar, y eso también pertenece a nuestro día a día.