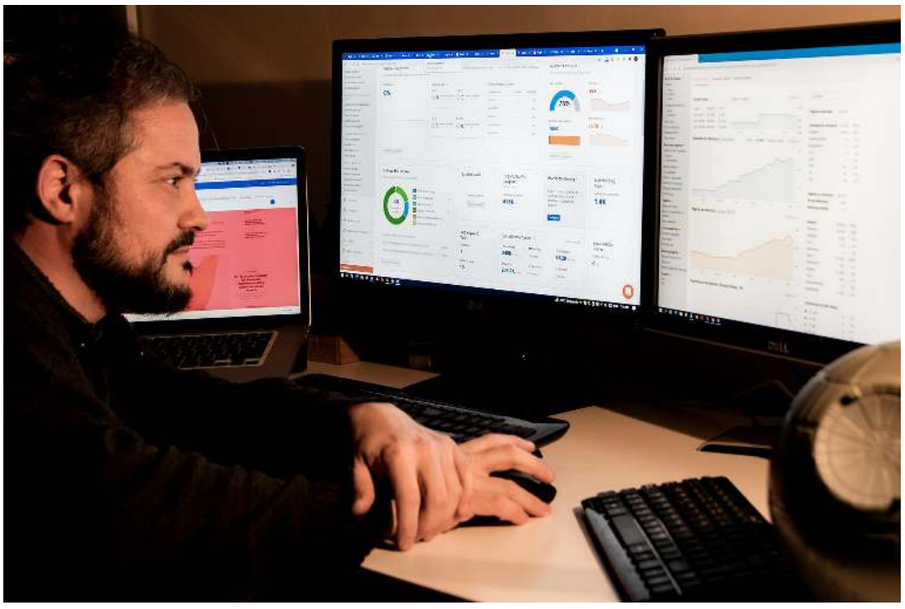
COMUNICACIÓN DE CRISIS

SEO: por qué ya hoy es la clave en la defensa de la reputación corporativa



Coppari, experto en SEO: “La gente que ataca es ingeniosa”

Por Christian Atance

Durante la pandemia se multiplicaron las prácticas maliciosas que buscan sabotear los resultados de búsqueda de sitios webs de competidores en motores como Google o Bing. El trabajo de las consultoras SEOs se reconfiguró por completo con este cambio de escenario. Cómo blindarse de los ataques y proteger la reputación online.

Un ejemplo fue la entrada en Wikipedia que hizo el kirchnerismo contra el vocero presidencial argentino, Juan Pablo Biondi, durante la crisis de gobierno desatada por el kirchnerismo tras la dura derrota electoral en las primarias de septiembre.

El cambio se hizo evidente con la explosión del trabajo remoto que generó la llegada del coronavirus a nivel global. Antes las agencias de relaciones públicas trabajaban a la par con consultoras SEOs para generar contenidos positivos para viralizar y escalar a las primeras páginas de los motores de búsqueda.

Hoy, por el contrario, la tarea es diametralmente opuesta. Se enfocan en la limpieza de links tóxicos, una forma cada vez más común utilizada para generar SEO negativo. "El negocio empezó a virar por completo desde la llegada de la pandemia", explica Gastón Coppari, consultor especializado en el tema.

El SEO negativo se engloba dentro del denominado Black Hat, un conjunto de prácticas poco éticas que viola las directrices de los motores de búsqueda para posicionar una determinada web. Principalmente tratan de manipular los algoritmos de sitios como Google o Bing para incrementar los rankings de un sitio propio. En su versión inversa, el foco se pone en la web de un competidor para relegar sus apariciones.

Existen varias tácticas de SEO negativo. Una de las más difundidas y económicas es la creación de backlinks tóxicos y spam en páginas de baja calidad que se apuntan a la web que se desea perjudicar. Para ello, se utilizan a modo de anchors términos penalizados o delicados. "Las granjas de enlaces, el software automatizado y las PBNs (redes de blogs públicos) son ampliamente utilizados para generar este tipo de enlaces malignos", explica Ricardo Mendoza Castro, International Lead para España y América Latina en Semrush.

En la práctica, lo que se busca es direccionar un gran número de enlaces no naturales al dominio de otra persona con el objetivo de que este sea penalizado. En este sentido, Coppari apunta que "hoy se puede comprar en la red un paquete de 100.000 links tóxicos por unos 200 dólares".

Si bien Google está mejorando la forma en la que identifica y descarta los enlaces de este tipo de ataques, el riesgo aún es alto. Para el especialista, es necesario "concentrar recursos para evitar estrategias maliciosas deliberadas que buscan bajar la autoridad de dominio de determinados sitios".

Coppari recomienda analizar regularmente los perfiles de enlaces y chequear el valor y la tendencia de puntuación de autoridad de las webs a través de sitios como Moz o Ahrefs. Una caída en los indicadores puede indicar algún problema con los perfiles de backlinks.

el mercado de habla hispana más desarrollado en términos de protección. Tienen muchos know how y nos llevan varios años de ventaja", apunta Coppari.

Para Aldo Leporati, managing director de Porter Novelli Argentina, la "administración de backlinks es una de las herramientas más poderosas de reputación online. Detectar información errónea y negativa es esencial para entender si te están pegando o no".

Otra técnica de SEO negativo utilizada es el hackeo de webs, considerada una de las más eficaces porque los atacantes pueden afectar su rendimiento como deseen e incluso pedir el pago de rescates. Aquí se suelen crear links salientes a otros sitios o redirecciones a páginas de baja reputación.

La creación de duplicados de sitios o partes de ellos es otra táctica empleada. En este caso, la estrategia es enlazarlos y difundir las copias falsas en webs penalizadas o de mala calificación. Ello puede provocar que sitios o páginas específicos dejen de aparecer en los resultados de búsqueda. Algunas herramientas como Copyscape permiten auditar regularmente la web en busca de clones no deseados.

Para socavar la reputación de una marca o web se suele recurrir también a reseñas negativas, que en muchos casos generan caídas de tráfico. Generalmente se llevan a cabo a través de la creación de cuentas de correo y perfiles sociales falsos. Otro camino es la generación de solicitudes de eliminación falsas de los mejores backlinks que apuntan al sitio web de la organización.

"La gente que hace ataques es ingeniosa", dice Coppari. Pero la buena noticia es que la tecnología también ofrece armas con las que defenderse basadas en IA, robots y sistemas de software sofisticados, entre otros, que ya están utilizando consultoras SEOs y agencias de PR.

"Términos como blindaje o cleaning digital -sacar enlaces negativos de la primera página del buscador- llegaron para quedarse", señala Leporati. "Es algo que todo profesional debe incorporar", dice. El concepto parte de la base de que, según numerosos estudios, son pocas las personas que pasan a la segunda página de resultados cuando llevan a cabo una búsqueda en Internet. Por ello, es clave reaccionar a tiempo y con las herramientas necesarias.

"La desinformación, los rumores y las fake news se viralizan y ponen en jaque a las organizaciones. Los stakeholders son cada vez menos leales y más exigentes. Pocos entienden que la ORM genera credibilidad y buena reputación", dice el CEO de Porter Novelli.

más frecuentes. Probablemente el más recordado en lo que va del año es el que vivió la estadounidense Colonial Pipeline entre el 6 y el de mayo. El incidente detuvo todas las operaciones de su red de oleoductos y provocó el desabastecimiento de combustibles en varios estados.

A mediados de agosto de 2020, en pleno verano europeo, el grupo asegurador español MAPFRE sufrió un ciberataque, del tipo ransomware, que ralentizó sus sistemas. A poco de declarado el incidente, la empresa decidió tomar el toro por las astas desde el punto de vista comunicacional y pidió disculpas públicamente a sus clientes por no poder brindar atención con su calidad habitual.

Para muchos especialistas, se trató de un ejemplo de transparencia a imitar. Principalmente porque las empresas afectadas habitualmente suelen ocultar las crisis de ciberseguridad a sus clientes y la opinión pública o comunicarlas con un retraso significativo.

“Muchas empresas no toman conciencia del daño reputacional y la pérdida de confianza que puede generar un ciberataque”, dice Leporati. “Normalmente se preguntan quién debe resolver una situación así. ¿Los abogados? ¿El equipo de IT?. Pero lo cierto es que con ellos solos no alcanza”.

Para el director de Porter Novelli, el creciente riesgo al que están expuestas las empresas obliga a repensar manuales y procedimientos de comunicación de crisis. “El equipo de PR tiene que estar involucrado desde el minuto uno”, resalta.

septiembre 20th, 2021 | Categorías: COMUNICACION DE CRISIS | Etiquetas: COMUNICACIÓN DE CRISIS | Comentarios desactivados

También podría interesarte...