Cómo lograr que la comunicación política interna sea confidencial

Tiempo de lectura: 6 min.

Daniel Eskibel

Mar, 18/06/2019 - 16:53

¿Te imaginas el desastre electoral que podría ocurrir si se filtraran los mensajes confidenciales que cruzan entre sí los integrantes de una campaña presidencial?

Pues no te lo imagines. Alcanza con recordar lo que le ocurrió a Hillary Clinton en 2016. La filtración de decenas de miles de correos electrónicos de su campaña electoral puso en conocimiento de la opinión pública las comunicaciones internas entre ella y su equipo así como los mensajes intercambiados entre sus colaboradores.

Aquello fue el comienzo del fin para sus aspiraciones presidenciales. Basta seguir las noticias de actualidad para comprender que no fue un caso aislado ni mucho menos. Lo cual me lleva a preguntarte: ¿estás realmente seguro de que tu comunicación política interna está a salvo de miradas indiscretas?

Me atrevo a suponer que no estás tan seguro como crees estar.

No tengo nada que esconder

Hay un error que se ha vuelto viral entre políticos, candidatos, gobernantes y consultores. Se puede resumir en la frase “yo no tengo nada que esconder”.

Como no hay nada oculto tampoco me tengo que preocupar demasiado. Y si no me preocupo demasiado me alcanza con usar las herramientas de comunicación que todos usan y que tienen detrás el respaldo de enormes compañías multinacionales.

Eso es lo que hacía John aquel sábado 19 de marzo de 2016. Aquel sábado John Podesta, por entonces jefe de la campaña presidencial de Hillary Clinton, trabajaba confiadamente en su computadora.

Era un hombre inteligente, culto y de gran experiencia política. Abogado y profesor de Derecho, había sido senador, jefe de gabinete del Presidente Bill Clinton y consejero del Presidente Barack Obama. Un verdadero peso pesado del Partido Demócrata y en general de la vida política de los Estados Unidos de América.

Estaba en su oficina. Trabajaba con tranquilidad. En un ambiente confiable y seguro. Con las herramientas habituales. En su pantalla tenía abierto su correo electrónico personal. El Gmail. El que siempre usaba.

Fue apenas un clic. Solo uno. Un simple clic en un enlace en un correo electrónico. Ese clic disparó una pesadilla electoral para su partido. Ese solo clic, tan inocente, abrió la puerta para un gigantesco hackeo de su cuenta y a través de ella del correo de Hillary y de otros muchos dirigentes demócratas.

Aquel clic de John fue el disparador. Decenas de miles de mensajes internos quedaron expuestos ante la opinión pública. Mensajes confidenciales. Pensados exclusivamente para el intercambio interno de la campaña y del partido.

Bastó un solo clic para precipitar la derrota de Hillary Clinton y el triunfo de Donald Trump. Podría decirse que aquel clic abrió un nuevo tiempo político en el mundo entero. Y marcó para siempre la carrera política de John Podesta.

La lección que nos deja el episodio es que la comunicación política digital presenta riesgos mucho más poderosos que los que vemos a simple vista. Y que la extendida idea de que no tenemos nada que esconder resulta un marco mental peligroso que generalmente nos conduce a graves errores.

El marco mental adecuado para campañas electorales, para gobiernos, para empresas consultoras y para partidos políticos es que la comunicación interna debe ser confidencial.

Ya sabes: confidencial, reservada, exclusiva para sus destinatarios y cerrada para el público general.

La confidencialidad de la comunicación interna es el equivalente colectivo a la privacidad de las comunicaciones personales. Para cualquier persona hay comunicaciones que son públicas y otras que son privadas. Y separar ambos campos es importante para el bienestar psicológico.

Del mismo modo deben diferenciarse las comunicaciones internas y externas de una organización política o empresarial. Unas son públicas, claro está. Pero las otras son privadas, confidenciales, reservadas.

Pero si quieres que la comunicación interna de tu organización sea confidencial, entonces deberás evaluar seriamente cuales son las herramientas que utilizas para ello.

¿De qué valdrían todos tus esfuerzos políticos si finalmente un hackeo o cualquier intrusión indebida diera por tierra con todo?

Canales de comunicación política interna

A principios de 2019 realicé una investigación entre los lectores de Maquiavelo & Freud. Es un público con formación universitaria y que ocupa lugares relevantes en partidos políticos, gobiernos y empresas consultoras.

811 personas respondieron online mis preguntas sobre herramientas de comunicación política. Los resultados son los siguientes:

El correo electrónico es para el 40 % de los encuestados el canal preferido para la comunicación política o profesional a distancia. En segundo lugar aparece el teléfono (33 %) y luego los mensajes (27 %).

El dato anterior tiene un matiz generacional: el 55 % de los Baby Boomers (nacidos entre 1943 y 1960) prefiere el email como principal canal de comunicación política o profesional, pero los más jóvenes (Millenials y Centenials) prefieren el teléfono como canal principal.

El 65 % utiliza Gmail para las comunicaciones importantes por correo electrónico, mientras el 19 % usa Hotmail / Outlook.

El 68 % prefiere WhatsApp para enviar y recibir importantes mensajes políticos o profesionales, al tiempo que el 11 % prefiere Telegram.

Cuando se trata de comunicaciones telefónicas el 64 % habla por la línea del móvil, el 11 % por la línea fija y otro 11 % por WhatsApp.

Para enviar y recibir archivos políticos o profesionales que sean importantes, el 37 % elige hacerlo por correo electrónico, el 20 % por Google Drive, el 16 % por WhatsApp y el 10 % por WeTransfer.

Las principales aplicaciones de comunicación que tienen instaladas los encuestados son WhatsApp (96 %), Facebook Messenger (77 %), Skype (44 %) y Telegram (31 %).

Si te ves reflejado en estos resultados, entonces no estás seguro. Porque todas las herramientas mencionadas como mayoritarias, todas, presentan debilidades de seguridad relativamente importantes.

8 recomendaciones para una comunicación política segura

No es necesario que te transformes en un hacker para mejorar de manera extraordinaria la seguridad de tus comunicaciones políticas confidenciales. Basta con seguir lo que recomiendan los expertos. En tal sentido te presento lo que yo mismo he recopilado estudiando a los principales investigadores.

Las recomendaciones principales en materia de comunicación política confidencial son las siguientes:

- Durante las reuniones los teléfonos móviles deben estar fuera de la habitación. Con apagarlos no basta: sácalos del lugar.
- Encripta el disco duro de tu ordenador. Seguramente hay un informático en tu equipo que te puede ayudar a hacerlo.
- Si te conectas a una red wifi pública (por ejemplo en hoteles, aeropuertos, bares o tiendas) utiliza siempre una red privada virtual (VPN). En mi caso uso ExpresVPN (veloz, segura y fácil de usar).
- Para hablar por teléfono utiliza Signal (es gratis y todas las llamadas de voz y las video llamadas son encriptadas e imposibles de interceptar).
- Usa Signal también para enviar y recibir mensajes instantáneos de texto, audio o vídeo, para compartir imágenes y documentos, y para grupos de comunicación. El cifrado es automático, es el más avanzado disponible actualmente y no puede ser quebrado ni siquiera por las más poderosas agencias de inteligencia.
- Para el correo electrónico usa ProtonMail (correo electrónico protegido con cifrado de extremo a extremo, regulado por las estrictas leyes suizas de privacidad, y con el centro de datos más seguro de Europa ubicado bajo mil metros de roca sólida).
- Si usas Telegram para mensajería, recuerda realizar las comunicaciones confidenciales a través de su chat secreto.

- Gestiona tus contraseñas con 1Password (una forma segura de guardar y gestionar tus passwords).

Son 8 recomendaciones. Hay otros servicios similares, claro está. Pero estos son los que te recomiendo porque yo mismo los uso y confío en ellos.

Una red segura para tu organización

Filtraciones, hackeos, noticias falsas, espionaje, manipulación de información, venta de datos, pérdida de privacidad, vigilancia, escándalos políticos…esa es nuestra realidad de hoy.

Tienes que prepararte para vivir, trabajar y hacer política en esa realidad compleja que nos toca vivir. Y para eso no puedes ser ingenuo y debes adoptar las herramientas necesarias. No lo dejes para después porque puede ser demasiado tarde. Hazlo ahora mismo.

Si eres consciente de todo esto deberías jugar un papel clave en tu organización. Informando a tus compañeros, persuadiendo, educando. Tienes que lograr la construcción de una red de comunicaciones confiables dentro de tu partido político, tu campaña electoral, tu empresa o tu gobierno.

Para eso nada mejor que compartir este artículo con las personas clave de tu organización. Que a nadie le pase lo mismo que al confiado John Podesta.

Maquiavelo&Freud

https://maquiaveloyfreud.com/comunicacion-politica-interna-confidencial/