BRIEFING JÓVENES TALENTOS INSPIRATIONAL 2023

BRIEFING SOBRE CIBERSEGURIDAD PARA BBVA.

Creando Oportunidades

PATROCINADO POR NIELSEN.

Contexto

Actualmente, se ha incrementado el uso de los canales digitales, la tecnología, los móviles: compramos online, realizamos gestiones, contactamos por las RRSS…. Es un nuevo ecosistema de hábitos, contactos y formas de realizar gestiones que los ciberdelincuentes conocen: saben dónde pueden encontrarnos para realizar sus delitos de una manera mucho más “limpia”, eficiente, anónima y masiva.

Además, la pandemia contribuyó en gran medida a este impulso digital ya que muchas situaciones que no podíamos resolver presencialmente pasamos a realizarlas online. **En ese momento, los fraudes también se incrementaron** de manera exponencial.

La mayoría de estos fraudes se realizan en entornos ajenos a la seguridad que ofrecen las entidades financieras (en RRSS, mensajes…), pero cuando compartimos datos privados y confidenciales como claves, PIN o contraseñas, podemos permitir a extraños acceder a nuestras cuentas o tarjetas. Muchos fraudes pueden funcionar así:

1) Los delincuentes envían SMS, emails o realizan llamadas intentando engañar a los usuarios (todo esto se realiza fuera de los entornos seguros de las entidades financieras).
2) En estas acciones se pueden pedir claves y contraseñas, realizar ciertas operativas o que se instalen programas maliciosos en los dispositivos (malwares).
3) El ceder estos datos o claves, o realizar operativas, puede facilitar el acceso de los delincuentes a nuestras cuentas o tarjetas, o al control de nuestros dispositivos.

Aun así, las oleadas de fraudes se suceden y los delincuentes cada vez buscan nuevas estrategias y formatos que buscan poner a prueba lo que ya sabemos, sorprender y pillarnos desprevenidos, por ejemplo: Llamadas falsas (vishing) realizadas con números extraños (números largos tipo centralitas, desconocidos o extranjeros…). Ahora que el cliente lo conoce y lo evita, los delincuentes usan una técnica que consiste en poner una “máscara” a ese número largo, simulando ser el número real de la empresa/compañía (spoofing). Esto hace creer al usuario que realmente le llama su banco o su empresa de suministros, cuando realmente no es así.

Se podría pensar que los fraudes se suelen dirigir a los más mayores debido a la brecha digital que pueden sufrir, pero nada más lejos de la realidad. El fraude no

distingue entre generaciones, sino que afecta a todos por igual. Los más mayores no se sienten seguros en el manejo de nuevas tecnologías/dispositivos y por eso muchas veces simplifican y evitan su uso. Sin embargo, los más jóvenes precisamente por sentirse más seguros y familiarizados en el uso de dispositivos o tecnología, tienden a exponerse más (por ejemplo, robos de identidad en RRSS, estafas de criptomonedas, o falsos ecommerce...)

Por lo tanto, es importante insistir en la concienciación, e interiorizar la forma de actuar ante un mensaje raro o inusual:

- PARAR y PENSAR (¿Este mensaje tiene sentido?)
- SOSPECHAR (¿Soy un posible destinatario de este mensaje?)
- NO DAR DATOS (Y mucho menos privados o personales: claves, PIN, contraseñas...)

Cuando alguien llame haciéndose pasar por una entidad, u ofreciendo alguna oferta demasiado llamativa... Hay que aplicar el sentido común y ante la duda, es mejor colgar (o cortar la comunicación) y que uno mismo confirme, mediante los canales oficiales de la entidad/empresa/organización, que la comunicación o la oferta es veraz.

¿Qué enfoque de comunicación tenemos en BBVA?

En BBVA ofrecemos un entorno seguro de protección a los clientes en nuestros canales digitales (app, web), pero los fraudes se suelen dar fuera de este ámbito. Por eso, trabajamos la seguridad de nuestros clientes desde dos niveles de actuación:

- A través de la innovación, en productos y servicios que promueven la seguridad: Firma Biométrica, CVV dinámico, Apagar y Encender tarjetas desde la app...
- Concienciar y capacitar a nuestros clientes a través de consejos e información para que no bajen la guardia, puedan detectar un posible fraude y lo puedan evitar.

En BBVA podemos ofrecer a nuestros clientes herramientas (consejos, novedades, webinars, artículos) que refuercen la autoconfianza de los clientes (usuarios) para que puedan conocer mejor los fraudes y así puedan detectarlos y evitarlos.

Cuando tienes información y recursos para poder reaccionar, es más fácil poderse enfrentar a una situación de posible riesgo.

Por eso hemos trabajado en la plataforma de comunicación de CIBER*SENCILLO*, donde ponemos al cliente en el centro, nos alejamos de anglicismos y buscamos usar un tono más sencillo, cercano y desenfadado, para que nuestros clientes entiendan cómo son los fraudes y desde ahí puedan evitarlos y protegerse mejor. Porque cuando logramos explicarlo bien, evitar el fraude puede ser más fácil de lo que parece.

Site de BBVA.ES:
https://www.bbva.es/general/seguridad.html

Petición:

Objetivo

Impactar a los mayores usuarios de tecnología y dispositivos: los jóvenes. Es necesario que el segmento que puede estar más expuesto esté más protegido, y por ello, el objetivo es informar concienciando de los efectos que pueden tener nuestras propias acciones. Se pretende construir hábitos que refuercen la responsabilidad a la hora de usar los medios y dispositivos de manera segura y responsable (Al igual que se interioriza el uso del cinturón al montar en coche, se debe interiorizar que no se puede compartir cierto tipo de información, ni descargar apps o programas de los que se desconoce su origen).

Estrategia

Crear una acción de Marketing dentro de la plataforma de comunicación de Cibersencillo para lograr contactar de manera diferencial con el segmento joven. Despertar curiosidad en el segmento, llamar su atención sobre la ciberseguridad y la concienciación.

Colectivo

A jóvenes entre 18-30 años, con perfil digital (usuarios frecuentes de canales digitales: web y app). Principalmente dirigido a CLIENTES, pero podría ser utilizado para NO CLIENTES, ya que la concienciación es universal.

BRIEFING JÓVENES TALENTOS INSPIRATIONAL ‘23

Mensajes

Se debe deducir de los mensajes:

- Los canales digitales son seguros. No se debe generar dudas o alarma sobre ellos (son seguros y ayudan en las gestiones del día a día).
- Los datos como claves o contraseñas son privados y confidenciales: no se deben compartir, y nadie te los debe pedir (ni por teléfono, ni por SMS, ni por WhatsApp…).
- Es importante usar la tecnología de manera responsable.
- Sospecha cuando te pidan realizar alguna acción con urgencia o veas ofertas muy llamativas.
- Ante la duda, sé tú el que contacte con la empresa por sus canales oficiales y confirma lo que te han dicho o pedido.

Formato

- Video presentación de la dupla (Máximo 30 segundos)
- Concepto de campaña (PDF – Máximo 3 hojas)
- Estrategia y recomendación de plan de medios/estrategia de difusión. Deben incluir la estrategia que la dupla considere más adecuada para lograr los objetivos planteados. Puede recoger acciones online combinadas con offline. No hace falta hacer planificación económica. (PDF – Máximo 3 hojas)
- Cronograma de campaña (PDF – Máximo 3 hojas)
- Video-Case de la campaña (MP4 – Máximo 1 minuto)

Tono

- Mensajes diferenciales, creativos, directos, claros y llamativos.
- Usar un tono cercano (no paternalista) que empatice y conecte con el colectivo. Transmitir que BBVA te ayuda a que puedas evitar el fraude, pero no desde un prisma de superioridad o asumiendo que el cliente no sabe: Mi banco quiere echarme una mano y ayudarme a avanzar.
- El tono debe ser positivo: Debe conectar generando curiosidad y ganas de saber, pero evitando generar temor o desconfianza en los medios digitales.

Medios y canales

- Acción de marketing basada en los canales de RRSS que consideréis necesarios para difundir el mensaje de manera masiva y global.
- También se puede incluir el apoyo de los canales propios de BBVA (banners en web, etc.).
- Se puede considerar inversión en *medios pagados.*

Presupuesto

- No hay un presupuesto fijo para la campaña y las acciones, pero se pueden plantear propuestas, aunque tengan un coste económico, siempre y cuando no sean propuestas desorbitadas.