How not to tell customers their data is at risk: The perils of the Optus approach

September 23 2022, by Edwina Luck and Nicholas Grech

Credit: Pixabay/CC0 Public Domain

Optus fears data on up to 9.8 million of its customers has been accessed in a sophisticated cyberattack—including, for some customers, passport and drivers license details, as well as phone numbers, dates of birth and

email addresses.

It made the announcement through the media, in the middle of Thursday's national day of mourning public holiday, and during the four-day long weekend in Melbourne in the lead-up to the AFL grand final.

At first, it didn't text or email its customers. Instead, it issued a press release in the belief this was "the quickest and most effective way to alert as many current and former customers as possible, so they could be vigilant and monitor for any suspicious activity."

Trust in the media is at an all-time low. Communications authority Edelman reports that globally, only 50% of people trust the media, down from 62% a decade ago. Far more people (61%) trust businesses.

Tweets rather than texts

It has been conventional wisdom that brands should take an integrated approach to marketing communications. Many channels are better than one, increasingly so as audiences for traditional channels continue to fragment.

An integrated marketing approach need not mean communicating through every available channel, but it should mean strategically selecting channels that are trusted and consumed by the brand's customers.

One of the best channels Optus has is its own phone network, and it is experienced in using it to contact its customers.

Customers are likely to expect this where Optus has something important to say, and they are likely to trust a direct message from Optus more than one filtered through the media.

They are even likely to spread it via word of mouth through friends who also use Optus, giving the company a continuing role in shaping the message.

Instead, Optus backed up its press release with tweets.

> Hi Marie, we issued a press release and proactively reached out to media as this is the quickest way to inform all our existing and former customers so they can be on high alert for anything suspicious. Kartik
>
> — Optus (@Optus) September 22, 2022

Optus has around 5.8 million active users, around 21% of the Australian population. They are a cross-section of the population, having little in common other than the fact they use Optus for communications.

Some of Optus' customers, especially those in Gen Z, might not use traditional news media. They wouldn't have received the message through that channel.

Former customers dating back to 2017 are also likely to be affected by the breach, taking the total affected to around 9.8 million, about one third of the population.

Twitter is used by about only about 18% of the population, and the overlap with Optus customers might not be large.

> We'll be contacting impacted customers soon with more information and details on how we'll support them. Optus will not be sending links in any emails or SMS messages. If you believe your account has been compromised, you can contact us on My Optus app (2/2) ^George

— Optus (@Optus) September 23, 2022

What can brands learn from Optus?

As marketing and branding experts, we've distilled three lessons, each well known before the data breach.

1. When you have news affecting your customers, tell them before anyone else, in a personalized, one-to-one approach.
2. Use channels that are trusted and consumed by your customers.
3. Encourage word of mouth through your relationships with your brand community and loyal customers.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation

Citation: How not to tell customers their data is at risk: The perils of the Optus approach (2022, September 23) retrieved 23 April 2024 from https://techxplore.com/news/2022-09-customers-perils-optus-approach.html