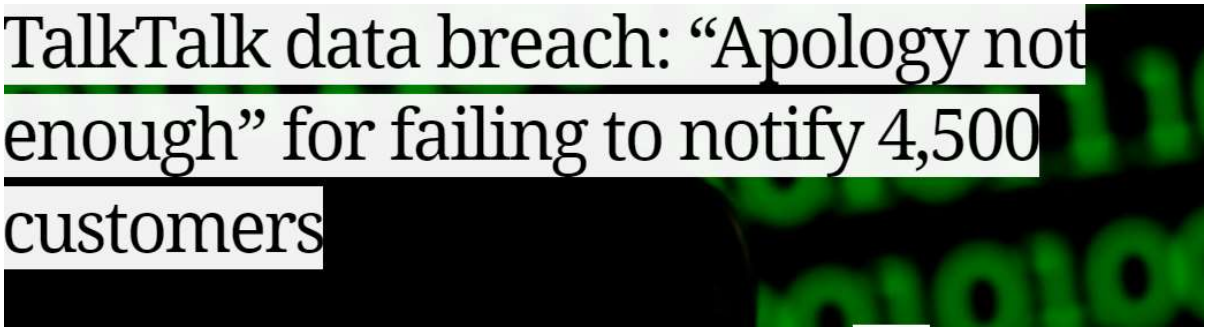
VERDICT



Telecommunications firm TalkTalk has been slammed by cybersecurity experts for failing to notify around 4,500 of its customers that their personal information was stolen during the 2015 TalkTalk data breach.

Breached personal details including full names, addresses, dates of birth, email address and bank details were all searchable on Google.

In 2015 a 17-year-old boy was found guilty of being behind the TalkTalk data breach, in which the personal details of nearly 157,000 TalkTalk customers were compromised.

The Information Commissioner’s Office (ICO) fined TalkTalk £400,000 for the breach. At the time this was the record fine handed out by the data regulator – £100,000 less than the then maximum penalty.

The latest development follows an investigation by BBC Watchdog, initiated after viewers got in touch with concerns that their details had been exposed by the TalkTalk data breach without their knowledge.

One victim told the BBC that his phone, email and bank account had been "bombarded" with fraudulent attacks.

When presented with the BBC's findings, TalkTalk said it was a "genuine error" and that only a small number of affected customers hadn't been notified. TalkTalk said it has since written to those customers to apologise.

However, Anjola Adeniyi, technical leader at cyber threat analytics and operations firm Securonix said that in this case "an apology is not enough".

He added that TalkTalk should "offer identity theft and fraud protection to the affected customers."

TalkTalk data breach: Phishing dangers

Jake Moore, security specialist at cybersecurity firm ESET, said that "failure to let customers know of a data breach is similar to being kicked while you are down."

"The first thing companies should do as soon as they are made aware of any cyber threat or breach of their customers' data is to hold their hands up and make them aware," he continued.

"They should also include advice on next steps for customers. It is becoming a given that companies could get hacked, whatever the company size."

Moore recommended that customers that have been with TalkTalk since before the 2015 breach should look out for fraudulent activity on their cards and be wary of phishing attempts.

"Never click on links in emails you are not expecting – even if they look genuine and personalised," he said.

"The unfortunate reality is that if the data was accessible for this long on the dark web, the chances are it has already been accessed by unintended parties," added Adeniyi.

Since the 2015 breach, tougher data protection laws known as the General Data Protection Regulation (GDPR) have come into effect, further outlining the importance of being open with customers about how their data is being used.

"The GDPR requires organisations to be clear, open and honest with people from the start about how they will use their personal data (the Principle of lawfulness, fairness and transparency, Article 5 GDPR)," said Robert Wassall,

a leading data protection lawyer and head of legal services at cybersecurity firm ThinkMarble.

“In any event, in my opinion, regardless of what the law requires, organisations should always be honest and open with their clients as otherwise there will be a loss of trust.”