Hacked on Christmas, DEphoto starts notifying customers, only to be attacked again - DataBreaches.Net

Published: 2025-01-01 · Archived: 2026-04-09 02:17:30 UTC

The threat actor known as 0mid16B contacted DataBreaches this morning to alert this site to a breach involving a U.K. photo business, DEphoto (DEphoto[.]biz). DEphoto is an established business for school, sports, club, and event photography.

According to 0mid16B, they attacked DEphoto on December 25, and acquired the personal information of 555,952 customers, 429,597 orders with detailed personal information of 240,307 orders, and 16,213 records with plain text credit card details (full card numbers, expiration dates, and CVV codes). All told, they claim to have exfiltrated hundreds of gigabytes of photos and other data, including the firm's library of photographs with customers' children and events photos.

0mid16B provided DataBreaches with a number of unredacted screenshots that appear to have been taken from DEphoto's network. One screenshot indicates that dephoto[.]bak and dephoto[.]mdf databases with more than 12 GB of data were among the accessed databases. Most screenshots related to customer orders and contained information with names, postal and email addresses, home and mobile telephone numbers, and in the case of people responding to franchise promotions, IP addresses.

Screenshot from database with full credit card numbers in plain text. Numbers and CVV codes redacted by DataBreaches.net

A Second Attack Follows Shortly After the First

According to 0mid16B, the first access was directly to the firm's backend MSSQl server.

0mid16B claims they informed DEphoto on December 25, and that the company allegedly “restored the system” but “did not protect or monitor it.” As a result of their failure to protect the system or to pay the demanded amount, 0mid16B hacked them for a second time on December 29. The second attack reportedly used the credentials from the DB user login to gain access to the front end.

When asked how much payment they demanded, 0mid16B stated that they managed to talk to the firm’s IT developer on WhatsApp on December 27, at which time, 0mid16B demanded 50,000 GBP ($62,741.16). There was no response.

Based on reviews on TrustPilot, it appears the firm quickly began sending out email notifications to affected customers. Entries dated December 28 for “date of experience” report people getting notified and being upset that DEPhoto had retained their information for so long. As one disgruntled person wrote:

> You took pictures at my sons football tournament 10 years ago, so why on earth are you still keeping (and now losing) my personal data?
>
> Your own Data Protection Policy states “Data retention:
> The company will retain personal data for no longer than is necessary.”
> How do you justify keeping my personal data for 10 years for the purchase of a couple of photos?

DEphoto’s privacy policy page was last updated in May, 2018, when GDPR officially took effect.

What’s Next?

0mid16B tells DataBreaches that they will be listing the 500k customer database for sale and will leak the rest of the data for free. Whether they follow through on that remains to be seen.

As of publication time, there is no notice or alert on DEphoto’s website about any incident.
