Zoom is leaking some user information because of an issue with how the app groups contacts

Zoom is apparently leaking some email addresses, user photos, and allowing some users to initiate a video call with strangers because of an issue with how the app handles contacts that it perceives work for the same organization, according to a report by *Vice*.

Typically, Zoom will group contacts with the same email domain into a "Company Directory" so you can, for example, search for a specific person, see their photo and email, and start a video call with that person. That makes sense for a company with employees on Zoom, but the app has also been grouping some people together who signed up for the service with a personal email, reports *Vice*. That means an affected user might be able to see the personal email addresses and photos of people with their same domain in their Company Directory, even if none of those people are actually colleagues.

It's unclear how widespread this issue is or how many domains may be affected. An affected user shared a screenshot with *Vice* showing 995 accounts in his Company Directory. This user also said he ran into the issue with the domains xs4all.nl, dds.nl, and quicknet.nl, which are all email domains from Dutch ISPs. Zoom said it blacklisted those domains after *Vice* brought them to the company's attention.

"Zoom maintains a blacklist of domains and regularly proactively identifies domains to be added"

“Zoom maintains a blacklist of domains and regularly proactively identifies domains to be added,” a Zoom spokesperson said to *Vice* in a statement. Zoom also directed *Vice* to a support page where users can request to have domains blacklisted. Zoom doesn’t group “publicly used domains including gmail.com, yahoo.com, hotmail.com, etc,” according to a support doc. Zoom was not immediately available for comment.

Zoom has a spotty track record with security. Last July, a security researcher discovered that a malicious website could open a Zoom video call on Macs without a user’s permission. The company quickly patched its software and uninstalled a local web server that created the vulnerability. Check Point Research published a report in January about a flaw that would have let hackers eavesdrop on calls. And Zoom confirmed today that its video calls aren’t actually end-to-end encrypted, despite what its .

https://www.theverge.com/2020/3/31/21201956/zoom-leak-user-information-email-addresses-photos-contacts-directory