# Phishing attack

**https://www.cnn.com/2022/03/23/tech/okta-breach-acknowledgment/index.htm**

**A widespread phishing scheme targeted people across the web on Wednesday.**

The sophisticated attack appeared to come from a trusted source asking you to open a Google Document. If you clicked, it took you to a page to open the "Google Docs" app with your Google ( GOOG ) account. This granted access to your email account and contacts.

Google said it stopped the attacks in one hour.

Eva Galperin, director of cybersecurity at the Electronic Frontier Foundation, says anyone who clicked on the link should check their Google App permissions and remove the one called "Google Docs." You can do that by clicking this link It's unclear how widespread the attack was, but reporters at publications including BuzzFeed, CNN and Motherboard tweeted that they'd receiving the phishing email, as had many of their sources.

According to threat intelligence firm Cisco ( CSCO ) Talos, at the peak of the attack its customer base saw around 150 messages sent per minute. The firm said the impact to the general population was likely much larger. (Talos declined to share its customer base figures.) On Wednesday afternoon, "Google Docs" was a global trending topic on Twitter, meaning a lot of people were talking about the attacks.

In a statement to CNNTech, a Google spokesperson said the attack affected fewer than 0.1% of Gmail users. (Gmail has over one billion monthly active users, and 0.1% of that total would be at least one million accounts.) Google said contact information was accessed and used in the attack, but no other information was exposed.

"We protected users from this attack through a combination of automatic and manual actions, including removing the fake pages and applications, and pushing updates through Safe Browsing, Gmail, and other anti-abuse systems," the company said in a statement.

It's not clear who was behind the phishing attempts. This attack spread quickly -- the fake Google Docs app read users' contacts and sent more phishing attempts to their contacts.

A phishing attack is a popular method of stealing credentials and hacking into people's emails, bank accounts or other private accounts. A hacker poses as a trusted source and sends you a malicious link.

Experts say the phish was convincing and sophisticated.

Here's what happened: Hackers created a malicious app and named it "Google Docs," which looked trustworthy. Google uses an authorization system called OAuth, which uses security tokens instead of

passwords to connect your Google account with third party apps. Because the malicious app looked legit, it essentially tricked users into trusting it with their security token -- which is all that was needed to access the accounts.

This is a popular phishing method -- security firm Trend Micro reported earlier this year that Russian hackers were using it.

"As we have seen repeatedly, these kinds of schemes are usually the precursor to larger nefarious activities, like money transfers, planting ransomware, etc.," said Frances Zelazny, VP of cybersecurity startup BioCatch.