May 3, 2017 SCAM ALERT from the PC Club Board

A widespread phishing scheme is targeting people across the web.
The sophisticated attack looks like it is coming from a trusted source asking you to open a Google Document. If you click, it takes you to a page to open the "Google Docs" app with your Google (GOOG) account. This grants access to your email account and contacts.

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. https://myaccount.google.com/permissions

It's unclear how widespread the attack is, but reporters at publications including BuzzFeed, CNN, and Motherboard tweeted that they'd receiving the phishing email, as had many of their sources.

On Wednesday afternoon, "Google Docs" was a global trending topic on Twitter, meaning a lot of people were talking about the attacks.
It's not clear who is behind the phishing attempts. This attack can spread quickly -- the fake Google Docs app can read your contacts and send more phishing attempts to your 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.

Google said it is investigating the phishing scam. The company advises people not to click on the link and report any phishing attempts to the company.

"We have taken action to protect users against an email impersonating Google Docs, and have disabled offending accounts," Google said in a statement. "We've removed the fake pages, pushed updates through Safe Browsing, and our abuse team is working to prevent this kind of spoofing from happening again.