Crossing the Digital Divide (v63)

“Google Hack”

By Joseph Feigon for the Observer

Content Contribution: Nathaniel Mott

The attack worked by tricking people into giving a malicious app permission to access their Google accounts. How? By sending emails that appeared to come from Google Docs, the collaborative productivity suite, which bore a link to a Google sign-in page. Once there, an app called "Google Docs" requested permission to access the victim's Google account. If those permissions were granted, the attacker had almost total access to the account, which meant they could "read, send, delete, and manage your email" and "manage your contacts" without alerting Google's security features.

That entire process--from receiving the spoofed email to giving the attacker total access to your account--could take just a few seconds. Many people send files to each other via Google Docs, and because the spoofed emails appeared to come from someone the victim knew, most probably didn't think twice before clicking the malicious link. From there, why wouldn't you let Google Docs access your account? Both are offered by Google, after all, and it's not hard to imagine a less technically savvy individual just assuming that Google had changed something in its services to require new permissions.

***

Roughly 1 million people fell victim to a phishing attack that offered total access to Gmail accounts. Google initially responded to the attack with a series of tweets, and now that the dust has started to settle, it's also published a blog post explaining how its systems protect you from phishing attempts. Yet questions still remain about how the company plans to prevent attacks similar to this one from reoccurring.

This attack worked by tricking people into clicking on what appeared to be a link to a Google Doc. The link opened a malicious app instead, and that app in turn requested permission to "read, send, delete, and manage your email" and "manage your contacts." But the request came from an app called "Google Docs," so combined with the email seeming to originate from the service, everything seemed to be above board.

That wasn't the case. Google Docs won't request permission to access your Gmail account--yet the sheer number of services that request access to Google, Facebook, and Twitter accounts has trained people to automatically grant those permissions without a second thought. Google said in its blog post that it stopped the phishing attack in one hour, but in that time it managed to affect 0.1 percent of its users, or roughly 1 million people.

Google has since been criticized for allowing this to attack to happen in the first place, especially since it was warned of this possibility all the way back in 2011. Thus, this blog post is less about Google bragging about how well it stopped this attack and more about making sure people still trust it. The company shared the following list of protections it uses to stop phishing attacks (and spam) from affecting those who use its products:

- Using machine learning-based detection of spam and phishing messages, which has contributed to 99.9% accuracy in spam detection
- Providing Safe Browsing warnings about dangerous links, within Gmail and across more than 2 billion browsers
- Preventing suspicious account sign-ins through dynamic, risk-based challenges
- Scanning email attachments for malware and other dangerous payloads

Those protections weren't enough in this case, though. Google still managed to halt the attack in its tracks, and the company said it's "taken steps to re-secure affected accounts," but the fact that a malicious app tricked people into offering access to their accounts via Google's OAuth system using an email claiming to come from Google Docs that was sent to Gmail users still raises questions about how those services are safeguarded.

Google acknowledged those concerns and said it plans to prevent similar attacks in the future:

> In addition, we're taking multiple steps to combat this type of attack in the future, including updating our policies and enforcement on OAuth applications, updating our anti-spam systems to help prevent campaigns like this one, and augmenting monitoring of suspicious third-party apps that request information from our users.

The company also advised users to take a Security Checkup to make sure the only apps and devices allowed to access their accounts are legitimate, heed warnings and alerts

shown in its products, and to report suspicious messages. Business admins were also told to turn on two-factor authentication for their employees, limit what information those employees are allowed to share, and running OAuth audit log reports.