# How Google Authenticator made one company’s network breach much, much worse

**reader comments**

122 with

A security company is calling out a feature in Google’s authenticator app that it says made a recent internal network breach much worse.

Retool, which helps customers secure their software development platforms, made the criticism on Wednesday in a post disclosing a compromise of its customer support system. The breach gave the attackers responsible access to the accounts of 27 customers, all in the cryptocurrency industry. The attack started when a Retool employee clicked a link in a text message purporting to come from a member of the company’s IT team.

## “Dark patterns”

It warned that the employee would be unable to participate in the company’s open enrollment for health care coverage until an account issue was fixed. The text arrived while Retool was in the process of moving its login platform to security company Okta. (Okta itself disclosed the breach of one of its third-party customer support engineers last year and the compromise of four of its customers’ Okta superuser accounts this month, but Wednesday’s notification made no mention of

either event.)

Most of the targeted Retool employees took no action, but one logged in to the linked site and, based on the wording of the poorly written disclosure, presumably provided both a password and a temporary one-time password, or TOTP, from Google authenticator.

Advertisement
Shortly afterward, the employee received a phone call from someone who claimed to be an IT team member and had familiarity with the "floor plan of the office, coworkers, and internal processes of our company." During the call, the employee provided an "additional multi-factor code." It was at this point, the disclosure contended, that a sync feature Google added to its authenticator in April magnified the severity of the breach because it allowed the attackers to compromise not just the employee's account but a host of other company accounts as well.

"The additional OTP token shared over the call was critical, because it allowed the attacker to add their own personal device to the employee's Okta account, which allowed them to produce their own Okta MFA from that point forward," Retool head of engineering Snir Kodesh wrote. "This enabled them to have an active GSuite session on that device. Google recently released the Google Authenticator synchronization feature that syncs MFA codes to the cloud. As Hacker News noted, this is highly insecure, since if your Google account is compromised, so now are your MFA codes."

The post is unclear on a variety of things. For instance, by "OTP token," did Kodesh mean a one-time password returned by Google authenticator, the long string of numbers that forms the cryptographic seed used to generate OTPs, or something else entirely? In an email seeking clarification, Kodesh declined to comment, citing an ongoing investigation by law enforcement.

https://arstechnica.com/?p=1968685