Nest users now covered by Google’s ultra-secure Advanced Protection Program

reader comments

60 with 38 posters participating, including story author

Share this story

Accounts for Google’s Nest line of smart home devices are now covered by the company’s Advanced Protection Program, which traditionally has provided enhanced security for journalists, politicians, elections workers, and other people who are frequently targeted by hackers.

Google rolled out APP in 2017. It requires users to have at least two physical security keys, such as those available from Yubico, Google’s Titan brand, or other providers. Typically, keys connect through USB slots or Near-field Communication or Bluetooth interfaces. Once registered, the keys provide cryptographic secrets that are unphishable and, at least theoretically, impossible to intercept through malware attacks or other types of hacking. APP also limits the apps that can connect to protected accounts, although registering Thunderbird to connect to Gmail is relatively easy.

Pulling up your account by the bootstraps

Once an account is enrolled and each device (including a

phone) is authenticated through the physical-key process Google calls bootstrapping, people can use their iOS or Android devices as a security key. That's usually easier, faster, and more convenient than using physical security keys. Typically, users must bootstrap only rarely after the bootstrapping process, such as when Google detects suspicious behavior. APP also pushes alerts to users' devices and registered email accounts each time a new device connects.

Authenticator apps, which use temporary one-time passwords to provide a second factor of authentication, don't work with APP accounts. Google imposes this restriction because the temporary passcodes are susceptible to phishing and attacks that compromise the app.

Since implementing APP for Gmail, GSuite, and Google Cloud accounts, Google has beefed up APP with other enhancements, such as increased safeguards against phishing, malware, and fraudulent access to users' data. Once users have ownership of two or more (non-phone) physical security keys, enrolling in APP takes five to 10 minutes, most of which is taken up with the one-time enrollment of keys and the logging out and subsequent logging in of each computer or handheld device during the bootstrapping process.

On Monday, Google said that it's extending APP to Nest, a line of devices that allow users to remotely control thermostats, locks, surveillance cameras, home entertainment systems, and other household devices. Nest devices have periodically been subject to malicious hacks, in some or most cases as a result of users choosing passwords that can be guessed or are reused from other sites the experience breaches.

Google in February said it would mandate two-factor authentication (2FA) to protect Nest users within the next few months. Ring, a line of competing products from Amazon, has also begun requiring user accounts to use an additional factor of authentication. Also known as multi-factor authentication,

2FA makes account compromises much harder, because in addition to a valid password, attackers must either take physical control of a target’s authentication device (i.e., something the user has) or the target’s fingerprint, iris scan, or other biometric (i.e., something the target is).

Bringing APP to Nest provides a level of security that makes sense for accounts that have access to some of a household’s most intimate moments, not to mention locks, thermostats, and other critical systems. Enrolling involves transferring Nest accounts to Google accounts (if that hasn’t been done already). Users then go through the normal enrollment procedure. Once a phone is added, people use it to bootstrap each smart home device connected to the account. Google has more details here.

https://arstechnica.com/?p=1680415