Google says Nest security camera terror warning from North Korea was hoax, not a hack

January 25 2019, by Edward C. Baig, Usa Today

For one Northern California family it was a terrifying experience: an emergency warning that came through a Nest surveillance camera of three intercontinental ballistic missiles, apparently from North Korea, headed straight to Los Angeles, Chicago and Ohio.

Laura Lyons told the East Bay Times that the warning, "sounded completely legit, and it was loud and got our attention right off the bat....It was five minutes of sheer terror and another 30 minutes trying to figure out what was going on."

The warning proved to be a hoax, and according to Nest's parent Google, it wasn't a hack at all but rather the result of a compromised password.

"Nest was not breached," Google said in a statement emailed to USA TODAY. "These recent reports are based on customers using compromised passwords (exposed through breaches on other websites). In nearly all cases, two-factor verification eliminates this type of security risk."

"We take security in the home extremely seriously," wrote Google, "and we're actively introducing features that will reject compromised passwords, allow customers to monitor access to their accounts and track external entities that abuse credentials."

The Lyons' incident was just the latest example of a scary scenario in which an intruder with your password can hack into a Nest. Last month, for example, a Houston couple heard a male voice tell them through their Nest that he was in their baby's room and was going to kidnap the child. That, too, was a frightening hoax.

The unfortunate reality is that data breaches have become all-too-common. A security site Have I Been Pawnd uncovered a breach of 773 million emails and 21 million passwords. You can check the site to see if your account was compromised.

Back in December, Nest said it reset all the accounts where customers reused passwords previously exposed through breaches on other websites and published publicly.

If you have a Nest security camera, you can help protect yourself by turning on the two-step verification optional security feature.

After you enter your Nest password, Nest will send a temporary verification code to your phone that ensures that you are really you. You'll need this code whenever you sign into the Nest app with a password, change or reset your password, remove your phone number, or turn off 2-step verification.

To enable the feature, tap Settings in the Nest app on your phone, tap Account and then tap Manage Account. From there, tap Account Security and tap the switch to toggle to 2-step verification.

Nest does not recommend sharing a user name and password with others, and to give family members their own accounts before turning 2-step verification on.

Two-step verification may strike some of you as a bit of a hassle. But if

it protects you from a truly terrifying hacker intrusion it will be well worth it.