Well, that was easy: Two-factor authentication hack feeds on phony e-mail

14 May 2018, by Nancy Owano

Credit: CC0 Public Domain

Two-factor authentication can be beat, as a hacker demo has shown. Lots of attention is being paid to a video posted where Kevin Mitnick, KnownBe4 chief hacking officer, revealed the two-factor exploit.

Two-factor authentication is "an extra layer of security that requires something an employee HAS and something they KNOW."

"The core of the attack comes in a phishing email, in this case, one purportedly sent by LinkedIn, to a member indicating someone is trying to connect with them on that social network," said Doug Olenick, *SC Magazine*.

The user gets a fake login page. The attack method is described in security parlance as a credentials phishing technique, which requires the use of a typo-squatting domain. The idea is to let the user give away his/her credentials. A white hat hacker friend of Kevin's developed the tool designed to bypass two-factor authentication.

In this kind of attack what is meant by a typo-squatting domain? It's a trick, and the "squatting" reflects how it cybersquats on another entity. Internet users who use the deliberately incorrect-lettered address with its typographical error plant may be led to a hacker-run alternative website.

Mitnick showed how this all works, in logging into his gmail account, via a phony Linked-In email.

Matthew Humphries, *PCMag*'s UK-based editor and news reporter, said in the attack, an email appears ok regarding the website being targeted, "so the recipient doesn't take the time to check the domain it was sent from."

In this instance, the email was from llnked.com rather than linkedin.com—easy to miss if you are not on the lookout for phony come-ons. Clicking the "Interested" button in the email takes the user to a website that looks just like the LinkedIn login page. All in all, Mitnick showed it was not that hard to just go ahead and nab a LinkedIn user's details, "simply by redirecting them to a website that looks like LinkedIn and using 2FA against them to steal their login credentials and site access," said Humphries.

The demo used LinkedIn as an example, but it could be used on Google, Facebook, and anything else carrying two-factor login; reports said the tool could be "weaponized" for just about any website.

Interestingly, it was last year when Russell Brandom said in *The Verge* that it was "time to be honest about its limits" in reference to two-factor authentication. Brandom gave an account of how the promise of two-factor began to unravel early on with mischief makers getting around it. He said, "it's become clear that most two-factor systems don't stand up against sophisticated users."

Nonetheless, he said, in most cases, the problem isn't two-factor itself. It's "everything around it. If you can break through anything next to that two-factor login—whether it's the account-recovery

process, trusted devices, or the underlying carrier account—then you're home free."

One obvious piece of advice, however, was offered and that is to be vigilant about links. Also, a perspective on what two-factor authentication is and isn't is helpful. It is a tighter solution than a basic password only mechanism. It is an extra layer of security. But as Stu Sjouwerman, CEO, KnowBe4, stated:. "Two-factor authentication is intended to be an extra layer of security, but in this instance, we clearly see that you can't rely on it alone to protect your organization."

More information:
www.knowbe4.com/press/knowbe4- … actor-authentication

APA citation: Well, that was easy: Two-factor authentication hack feeds on phony e-mail (2018, May 14) retrieved 26 January 2021 from https://techxplore.com/news/2018-05-easy-two-factor-authentication-hack-phony.html