Have you been 'pwned' in a data breach? Troy Hunt can tell

December 5 2017, by Matt O'brien

Troy Hunt, information security author and instructor with Pluralsight testifies during the House Energy and Commerce Subcommittee on Oversight and Investigations hearing on Capitol Hill in Washington, Thursday, Nov. 30, 2017. (AP Photo/Carolyn Kaster)

Troy Hunt has collected a trove of 4.8 billion stolen identity records pulled from the darkest corners of the internet—but he isn't a hacker.

Instead, he uses that repository to help ordinary people navigate the growing scourge of the corporate data breach. All that personal information was originally taken from brand-name services such as LinkedIn, Kickstarter, Dropbox, MySpace and the cheating website Ashley Madison, and later assembled by Hunt.

Working barefoot and in beachwear from his home office on Australia's Gold Coast, the amiable security researcher set up his irreverent website, "Have I Been Pwned?" (POHND), in 2013. Millions of people have since used the free service to see if hackers have liberated their personal details from unwary companies and posted them online.

Along the way, Hunt has become a close student of data breaches and the slipshod security that makes many companies easy prey for attackers. He's exposed several such thefts himself, in some cases identifying them before the companies themselves did.

AN EPIDEMIC OF PWNAGE

"Pwned"—a deliberate misspelling of "owned"—is slang used by gamers to mean "utterly defeated." It's an apt description of what it's like to have criminals use your Social Security number, birthdate and other personal details to commit fraud in your name.

Hunt was invited to appear before Congress in late November to help lawmakers wrestle with this growing crisis of consumer data theft. In just the past two years, attackers have stolen sensitive information about hundreds of millions of people from the credit bureau Equifax, popular online services such as Uber and too many other companies to count.

Much of that stolen data flows directly into the black market. "Data breaches are another commodity, like heroin," Hunt testified Thursday before the House Energy and Commerce Committee.

UNLIKELY MESSENGER

Hunt's unlikely path from Queensland's Surfers Paradise Beach to what he describes as "fancy government things" on Capitol Hill has been a running joke since his invitation to testify was announced. Virginia Republican Rep. Morgan Griffith, introducing Hunt to lawmakers, noted that he "put on a suit and tie for us when he normally wears jeans and a black T-shirt."

Hunt said he splurged on the brand-new Hugo Boss suit and Australian outback-style boots because he didn't have anything else to wear. He also downloaded an app that instructed him on how to tie his necktie.

"Doing my best 'no really, I'm a professional' impersonation," he tweeted from the U.S. Capitol steps shortly before the hearing. "Did it work?"

Troy Hunt, information security author and instructor with Pluralsight, testifies

during the House Energy and Commerce Subcommittee on Oversight and Investigations hearing on Capitol Hill in Washington, Thursday, Nov. 30, 2017. (AP Photo/Carolyn Kaster)

ONCE MORE UNTO THE BREACH

Of course, this "new normal" of massive data breaches is no joke. So much personal data has been publicly exposed through both theft and voluntary sharing on social media that it's eroded traditional methods for verifying identity, such as usernames, passwords or knowledge-based questions about birthdays or family history.

In late November, Hunt helped discover a 2014 breach of the photo-sharing website Imgur after analyzing data from the hack passed along by one of his sources. Unlike Uber, which hid a recently-disclosed breach of more than 57 million stolen passenger and driver records for a year, Imgur took just 25 hours to go public after Hunt emailed the San Francisco company on Thanksgiving Day.

"Troy Hunt was extremely helpful in bringing the data breach to our attention and ensuring the sensitive data was passed to us in a secure manner," Roy Sehgal, Imgur's chief operating officer, said in an email.

PWN ALL THE THINGS

Hunt originally launched his site "as a bit of a curiosity," he said. At the time, he was a software architect at pharmaceutical giant Pfizer; a few years later, he quit to work as an independent information security consultant and instructor.

The researcher was analyzing data breaches floating around the web and

noticed that many people were turning up in multiple data breaches. "It struck me that this was something they probably didn't know," Hunt said in a phone interview.

People using his site can search on their email address to see whether and where their records have been exposed. Roughly 1.7 million people also subscribe to alerts that sound when their details pop up in newly discovered breaches. The website's user base has grown rapidly as bigger data breaches—some many years old—get attention.

WEARING THE WHITE HAT

Hunt "has credibility and integrity," said U.K.-based security researcher Ian Thornton-Trump, who has used Hunt's site to build a system that keeps customer credentials safe from attacks that re-use previously disclosed passwords. "He's resisted urges, and probably significant financial value, to sell out."

Thornton-Trump and other supporters say Hunt's usefulness has grown as more people confidentially share publicly exposed data with him, drawn by his reputation as an ethical gatekeeper of sensitive information.

"I hope they get a bit of a sense of doing the right thing," Hunt said. "I hope there's a sense of social good. They certainly don't get any money out of it."

Hunt warned Congress on Thursday that there's now a "perfect storm of data exposure" thanks to the growth in online services that are collecting more information than they really need. He also slipped in a suggestion that that the U.S. government, like some of its counterparts elsewhere, should do more to penalize companies that don't disclose their breaches properly.