Yahoo's mega breach shows how just how vulnerable data is

December 15 2016, by Bree Fowler

This Tuesday, July 19, 2016 photo shows a Yahoo sign at the company's headquarters in Sunnyvale, Calif. On Wednesday, Dec. 14, 2016, Yahoo said it believes hackers stole data from more than one billion user accounts in August 2013. (AP Photo/Marcio Jose Sanchez)

The revelation of Yahoo's latest hack underscores what many Americans have known for years: All those emails, photos and other personal files stored online can easily be stolen, and there's little anyone can do about

it.

The only saving grace is that the attackers apparently did not exploit the information for fraud. But their true motives remain a mystery.

While there are a number of straightforward measures all users should take to protect themselves, relatively few people actually do. And in this case, doing so wouldn't really have mattered. Even the most scrupulous individual countermeasures could only limit the damage.

"Yahoo users could have had immaculate computer security and still been the victim here," said Will Ackerly, chief technology officer at Virtru, a computer security firm he co-founded after working for eight years at the National Security Agency.

"Short of using encryption, there's no way to keep your email from being compromised in this kind of hack."

The mega breach disclosed Wednesday exposed more than a billion user accounts, the largest such attack in history. The company said the attack happened in August 2013, although Yahoo only discovered it recently. Worse, the company's announcement followed a similar announcement in September about a 2014 hack that Yahoo ascribed to an unnamed foreign government. That breach affected 500 million accounts.

Some experts believe the record-breaking amount of data stolen in the breach announced Wednesday also points to state-sponsored hackers in search of a specific target, which could be why three years later the data still hasn't been spotted for sale on the web. And neither Yahoo breach has yet been linked to online fraud or any specific repercussions for Yahoo users.

But their disclosure closely follows U.S. intelligence concerns about

Russian hacking of Democratic emails during the presidential campaign—not to mention recent attacks on a major health insurer, a medical lab-test company and the government office that manages millions of federal employees.

"The lesson is clear: No organization is immune to compromise," said Jeff Hill, director of product management for cybersecurity consultant Prevalent. And since most of us are dependent on big organizations that hold our digital lives in their hands, in a broad sense that means no one is safe.

The hacks represent yet another stumble for the struggling Sunnyvale, California, company as it tries to reinvent itself. The breaches occurred during the reign of Yahoo CEO Marissa Mayer, a once-lauded leader who has been unable to turn around the company in the four years since she arrived.

Earlier this year, Yahoo agreed to sell its digital operations to Verizon Communications for $4.8 billion—a deal that may now be jeopardized by the hacking revelations.

Meanwhile, it's clear that Yahoo didn't do enough to protect its users. For example, the company acknowledges using MD5, a password-storage method considered by many experts to be inadequate and inferior to others available at the time of the hack.

One of Yahoo's priorities will now need to be keeping its users updated as its investigation progresses, said Jeremiah Grossman, chief of security strategy for SentinelOne.

"I think that would go a long way to assuring users and everybody that they're doing the right things," said Grossman, who worked in security at Yahoo from 1999 to 2001. "The best peace of mind in cybersecurity is

transparency."

There's only so much a company like Yahoo can do to protect its users without damaging its business model, which involves selling advertising based on data gleaned from its users, Grossman noted.

As a result, it can't do things like encrypt user data, which would make the information useless to hackers. Other companies that don't sell advertising, such as Apple, are able to encrypt. And some, such as Google, do so too but not in a way that would have protected against this type of hack. They also hold the keys to that encryption, giving them the access they need for advertising sales.

"If you take a step back, the 1 billion people aren't Yahoo's customers, they're its product," Grossman said.

For Yahoo users, experts say, there's little to do except for changing their passwords if they haven't done so in the past three years. And it's tough to protect against future hacks at Yahoo or other companies that hold personal information.

Changing email providers is, at the very least, a pain for most people. Experts say picking a tough password is a must , though they are divided on exactly how important it is to change it frequently.

The same password should not be used for multiple sites, and the questions and answers needed to reset it should be unique as well.

While perfect security doesn't exist, no one wants to be an easy target either. Cybersecurity experts like to compare the hacker threat to running from a bear: You don't have to be the fastest runner—just not the slowest.

The Yahoo breach should serve as a lesson to users that they can't assume that companies, even large multi-national tech companies, are doing security right, said John Shier, senior security adviser at Sophos.

"Hopefully this is the one that wakes everybody up, although I doubt it will be," Shier said. "It's frustrating to see this happen over and over again when for many years we've known how to better protect systems."/author/bree-fowler .