Yahoo email account passwords stolen (Update 2)

30 January 2014

Yahoo alerted users of its free email service Thursday that hackers slipped into accounts to loot information using stolen passwords

Usernames and passwords of some of Yahoo's email customers have been stolen and used to gather personal information about people those Yahoo mail users have recently corresponded with, the company said Thursday.

Yahoo didn't say how many accounts have been affected. Yahoo is the second-largest email service worldwide, after Google's Gmail, according to the research firm comScore. There are 273 million Yahoo mail accounts worldwide, including 81 million in the United States.

It's the latest in a string of security breaches that have allowed hackers to nab personal information using software that analysts say is ever more sophisticated. Up to 70 million customers of Target stores had their personal information and credit and debit card numbers compromised late last year, and Neiman Marcus was the victim of a similar breach in December.

"It's an old trend, but it's much more exaggerated now because the programs the bad guys use are much more sophisticated now," says Avivah Litan, a security analyst at the technology research firm Gartner. "We're clearly under attack."

Yahoo Inc. said in a blog post on its breach that "The information sought in the attack seems to be names and email addresses from the affected accounts' most recent sent emails."

That could mean hackers were looking for additional email addresses to send spam or scam messages. By grabbing real names from those sent folders, hackers could try to make bogus messages appear more legitimate to recipients.

"It's much more likely that I'd click on something from you if we email all the time," says Richard Mogull, analyst and CEO of Securois, a security research and advisory firm.

The bigger danger: access to email accounts could lead to more serious breaches involving banking and shopping sites. That's because many people reuse passwords across many sites, and also because many sites use email to reset passwords. Hackers could try logging in to such a site with the Yahoo email address, for instance, and ask that a password reminder be sent by email.

Litan said hackers appear to be "trying to collect as much information as they can on people. Putting all this stuff together makes it easier to steal somebody's identity."

Yahoo said the usernames and passwords weren't collected from its own systems, but from a third-party database.

Because so many people use the same passwords across multiple sites, it's possible hackers broke in to some service that lets people use email addresses as their usernames. The hackers could

have grabbed passwords stored at that service, filtered out the accounts with Yahoo addresses and used that information to log in to Yahoo's mail systems, said Johannes Ullrich, dean of research at the SANS Institute, a group devoted to security research and education.

The breach is the second mishap for Yahoo's mail service in two months. In December, the service suffered a multi-day outage that prompted Yahoo CEO Marissa Mayer to issue an apology.

Yahoo said it is resetting passwords on affected accounts and has "implemented additional measures" to block further attacks. The company would not comment beyond the information in its blog post. It said it is working with federal law enforcement.