Gawker hack underscores flaws with passwords

December 19 2010, By JORDAN ROBERTSON , AP Technology Writer

The fallout from a hacking attack on Gawker Media Inc. a week ago underscores a basic security risk of living more of our lives online: Using the same username and password for multiple sites is convenient, but costly.

After the attack on the publisher of such blogs as Gawker, Gizmodo and Jezebel exposed account information on as many as 1.4 million people, several unrelated companies had to freeze their accounts and force users to reset passwords.

Gawker Media itself didn't have all that much sensitive information about its users. But the usernames and passwords obtained there could open doors to more valuable accounts elsewhere, including e-mail and banking.

Twitter, Google Inc. and Yahoo Inc., among others, saw the potential damage and began resetting their passwords en masse, disrupting users as they tried to check their e-mail or post a tweet.

"It shows one of the fundamental problems with passwords - they get reused and shared across multiple sites," said Jeff Burstein, a senior product manager with the Symantec Corp. security firm.

Despite repeated warnings from security companies not to do so, users tend to reuse passwords anyway because they can be hard to remember

and manage. Users may have dozens, perhaps hundreds, of accounts - for e-mail, Facebook, Twitter, e-retailers, banks and the growing number of news websites and blogs requiring registration.

Although account information gets compromised all the time, the infiltration of Gawker's servers is noteworthy because the hacked data were posted online, for free. In most other breaches, the stolen data are never made public, but sold underground to criminals.

Because the databases were freely available, other sites were able to score the data and look for matches with their users.

Twitter acknowledged resetting some passwords for its 175 million users after hackers used the Gawker data to break into Twitter accounts and pump out links to a site selling acai berry drinks.

At least two of the biggest web e-mail providers, Yahoo and Google, also reset some passwords. Neither would say how many of its users were affected. Google described it as a "small subset" of its users.

Job-networking service LinkedIn also changed a small number of its 85 million users' passwords.

Some websites said the breach didn't affect them because they don't rely solely on passwords.

JPMorgan Chase & Co. said it didn't have to change any passwords because the bank has "multiple layers of security."

Banks typically require security questions and other challenges beyond just usernames and passwords to get into their sites, particularly when someone logs on from a specific computer for the first time.

So what can be done to better protect consumers? Security experts say the Gawker breach shows that it's time to move beyond passwords.

But people are used to needing only usernames and passwords to log onto accounts, and piling on more layers of security can be a hassle.

Many sites are trying to do the best with what they've got and what they think their users will accept. They require strong passwords that are tough to break with "brute force" attacks - using computers to keep trying commonly used passwords against an account until one works.

But those requirements have made it harder for people to remember their passwords, and that increases the likelihood that they'll be used across multiple sites.

Security tools that take advantage of smart phones can make it harder for strangers to break into your accounts. You're given a code through your phone to enter on the website with your password. That way, the website knows it's not a hacker, who wouldn't have access to your phone.

Burstein said imposing additional layers of security on users can backfire if the measures are too cumbersome, but added that the push for mobile phone security applications has been well received.