Twitter hacked by old technique -- again

July 15 2009, By JORDAN ROBERTSON , AP Technology Writer

(AP) -- Breaking into someone's e-mail can be child's play for a determined hacker, as Twitter Inc. employees have learned the hard way - again.

For the third time this year, the San Francisco-based company was the victim of a security breach stemming from a simple end-run around its defenses: A hacker guessed the password for an employee's personal e-mail account and worked from there to steal confidential company documents.

The techniques used by the attackers highlight the dangers of a broader trend promoted by Google Inc. and others toward storing more data online, instead of on computers under your control.

The shift toward doing more over the Web - a practice known as "cloud

computing" - means that mistakes employees make in their private lives can do serious damage to their employers, because a single e-mail account can tie the two worlds together.

Stealing the password for someone's Gmail account, for example, not only gives the hacker access to that person's personal e-mail, but also to any other Google applications they might use for work, like those used to create spreadsheets or presentations.

That's apparently what happened to Twitter, which shares confidential data within the company through the Google Apps package that incorporates e-mail, word processing, spreadsheet, calendar and other Google services for $50 per user per year.

Co-founder Biz Stone wrote in a blog posting Wednesday that the personal e-mail of an unnamed Twitter administrative employee was hacked about a month ago, and through that the attacker got access to the employee's Google Apps account.

Separately, the wife of co-founder Evan Williams also had her personal e-mail hacked around the same time, Stone wrote. Through that, the attacker got access to Williams' personal Amazon and PayPal accounts.

Stone said the attacks are "about Twitter being in enough of a spotlight that folks who work here can become targets."

Some of the material the hacker posted online from the Google Apps documents was more embarrassing than damaging, like floor plans for new office space and a pitch for a TV show about the increasingly popular online messaging service.

Twitter says only one user account was potentially compromised because a screenshot of the account was included among the stolen documents.

The value in hijacking a user's account is limited, as those attacks are mainly used to post fake messages and try to trick the victim's friends into clicking on links that will infect their computers.

Sensitive Twitter documents were filched, though.

The hacker claims to have employee salaries and credit card numbers, resumes from job applicants, internal meeting reports and growth projections.

Stone said the stolen documents "are not polished or ready for prime time and they're certainly not revealing some big, secret plan for taking over the world," but said they are sensitive enough that their public release could jeopardize relationships with Twitter's partners.

What the attacks on Twitter show is that Web sites don't need to get compromised in the traditional sense to put its users and employees at risk.

Hackers don't need to find a vulnerability in the site itself, or plant a virus on an employee's computer, to sneak inside.

The easier approach is much more low-tech: All they need to find is an employee who uses weak passwords for his or her e-mail accounts, or has security questions that are easy to answer with a little information about the person.

It's an old strategy that's becoming more and more valuable as people's personal and work lives merge online.

It can be trivial to guess someone's passwords, as former vice presidential candidate Sarah Palin found out during the election, when her personal e-mail was hacked and screenshots were posted online. The

attacker sneaked in by accurately guessing the answer's to Palin's security questions, based on information about her and her family that was already online.

Password-guessing programs are also a common hacking tool. An attacker runs the program against an account, and if it's allowed to try lots of times and the password isn't very complicated, the hacker's in.

Twitter was hit twice before this year in similar incidents.

In an attack against Twitter in January, a Twitter support staffer's account was compromised using a password-guessing-program. The hacker got administrative access to the site. The Twitter feeds for Barack Obama, Britney Spears and other celebrities were used to send out bogus messages. A similar attack happened in May.

The attacks on Twitter serve as a reminder of why many corporations are reluctant to jump on the cloud computing bandwagon. Outsourcing sensitive jobs can save money but also open up companies to more risk, because their data aren't entirely under their control.

Another trend online is for Web-based services to streamline access by letting users log into each others' sites with the same usernames and passwords. Facebook and other services have begun to do this, raising possible security risks.

The lesson from Twitter's latest security troubles is an old one: Use strong passwords, which include some combination of letters and numbers, and for companies, be careful about how many accounts are linked to the same username and password combination.