More than a micro-blogging service that lets users create and read other people’s “tweets” (text posts or updates that are up to 140 characters in length), Twitter fosters both real-life and online relationships. Tweets can range from the mundane to the life threatening. Some see Twitter as a productivity, lifestyle, or even work aid. Twitter profiles can be created for individuals, organizations, celebrities, athletes, companies, and movements—any conceivable entity that wants to establish a real-time feel to its online presence.

While incredibly useful and addictive for most, Twitter has had its share of attacks and history of abuse (see Figure 2). Restrictions in avenues that can be used to post updates (like free SMS and instant-messaging [IM] service) have not stopped the explosive growth of Twitter profiles all over the world (see Figure 3). Cybercriminals, however, are close on its heels.

**Spoofing, Hacking, and Other Authentication Issues**

In early 2007, Nitesh Dhanjani first reported via his blog a scenario that could instigate malicious activities related to Twitter’s services. By using an SMS application called FakeMyText, he was able to post a tweet on a target user’s profile without the owner’s knowledge. An attacker, however, needs to know a target’s phone number to post an unauthorized tweet.

While this was a valid and correctable oversight on the part of the application’s creators, the highly publicized hacking of over 30 popular Twitter accounts was largely more avoidable. Hackers simply guessed a Twitter administrator’s password.
(happiness) on January 5 and proceeded to post lewd and drug-related bogus posts on behalf of the personalities.

![Timeline of Major Twitter Attacks](image)

**Figure 2. Timeline of Twitter attacks.**

**Abuse of Services**

The two previous attacks rely mainly on weak passwords and easy access to information. However, users who have activated the personal identification number (PIN) requirement in mobile updates and who create strong passwords and change them frequently can still get in trouble. In mid-December 2008, Twitter users felt a surge in spammers who have set up bogus Twitter profiles to follow legitimate users. Users who follow spammer profiles (as it is common courtesy to follow a user who has requested to receive notification for updates) will then start receiving updates that contain links to advertisements. Spammers earn money in this classic click-fraud ploy.

In February, click-jacking attacks appeared on victim’s profiles, with the apt warning, “Don’t Click!” which of course tempted several users to click. This led users to a site where the click-jacking trick is hosted: pressing a button on the site actually posts the same “Don’t Click!” message on the users’ own profiles. The posting of the unwanted message was actually hidden from the user’s view by a specially crafted button.

A more sinister version of unwanted contact occurred about a month earlier when cybercriminals started exploiting the Direct Messages function by sending targets messages saying pictures of them were available on another website. The provided link, however, leads to a phishing page that looks very similar to the real Facebook login page. Phishers can gather users’ account information use them to blackmail or
hack *Facebook* accounts to impersonate the victim or to perform unauthorized financial transactions online.

**Application Vulnerabilities**

Unfortunately, users who avoid clicking links in *Twitter* notifications are not completely safe either. Application vulnerabilities, the same culprits that, in the larger landscape of threats, made drive-by (automatic and non-user-initiated) downloads possible, have been found in *Twitter*.

A 15-year-old code-writer created a script that exploited a cross-site scripting vulnerability in *Twitter*. Cross-site scripting is a blanket term for vulnerabilities in applications to unauthorized injection of code. In this relatively simple attack, users who simply view the profile of an already infected user gets infected as well. No additional clicks are necessary to launch the script. A mysterious post from the malware writer then appears on the victim’s profile appearing to come from the victim himself. The cycle continues when other users view the new victim’s profile.

This particular attack, fortunately, is benign, in that all the hacker chose to do was spread inane messages about himself and about how long *Twitter* was taking to fix the vulnerability. The exploit, however, was already available even prior to this in a proof-of-concept (POC) code by security researchers. *Twitter* has already solved this particular vulnerability and cleaned up the affected accounts.

However, cybercriminals, now working in teams and with various levels of expertise, can easily hunt down a new vulnerability and do more than just post harmless messages on user profiles. Add to this the fact that the character limit has made URL-shortening a necessary tool. URL shorteners mask actual URLs with shorter ones. Cybercriminals can thus launch attacks that spread links that download and execute malicious data-stealing or other destructive malware.
Nothing Micro about Micro-Blogging

Security Strategy: Don’t Wait for Malware Files

Web-based attacks start long before the actual download of a malicious binary—usually the one that does the major hauling of information or system modification on the user’s PC. Malicious links, if promptly classified as such, could be blocked by security software, protecting users from the entire remediation process of detecting and cleaning up an infected computer.

In the case of Twitter attacks, superior URL-blocking technology would have prompted an uninfected user that they are secretly being made to connect to a malicious remote location (the effect of a successful cross-site scripting attack). This prevents the user’s PC from running the script that will automatically post unwanted messages on his account, which in turn, can infect all the user’s contacts.

References: