

kiwicommons

How to use Twitter Safely

Developed by: Luke McKinney
June 24, 2009

How to Avoid Twitter Traps

Twitter is the latest of the social networking sites. Instead of all the options of Facebook or MySpace, Twitter is a high-tech haiku service. Users are limited to posting messages of one hundred and forty characters and reading the updates of others who do the same. It can be accessed online or by SMS text message, so it's perfectly adapted for the accelerated internet age.



But are its social strengths at the expense of security? Is it just teaching people to tell everyone exactly what they're doing at all times, without any delays, and encourages them to click on random links? It could be

worse, however, Twitter could use the Batsignal to broadcast your credit card number.

Part of the problem is the character limit: Twitter's whole strength is how it forces people to be fast, funny, or interesting in only a few characters. This means that people who want to forward links use services like TinyUrl, which compress the HTTP address into a few letters and incidentally make it impossible to see where you're going.

It's important to engage such scary factors intelligently. You can't just ban children from using the service, because then they'll use it without any adult advice. So like most things on the internet, it comes with its fair share of good and bad. With Twitter it can teach good security as well as bad, since two basic and widely applicable rules can protect every user:



1.) Only follow links from people you trust

As a mass-market social service most 'Tweeters' have two levels of trust: an inner circle of people they directly know and want to stay in touch with, and an outer layer of entertaining others they follow. Recognizing that they should only follow links from trusted sources is internet safety rule #1, and nowhere makes it more clear than Twitter.

2.) Keep your security software up-to-date

Unless you plan on hiding in a cave, you need to keep your computer protected. Recent studies show that unshielded systems end up infected within four minutes of being web-connected, no matter where you go. So not only do you need anti-virus and anti-malware software on your system, you need to remember to use it on a regular basis.

If you have time to use Twitter (tweet), you definitely have time to update your virus protection files and scan your system!

For more information go here (<http://help.twitter.com/portal>) to see Twitter's official support page, which includes how-to's on blocking users to general use information.

Sources: <http://blog.internetnews.com/skerner/2009/05/interop-is-twitter-making-us-l.html>
http://blogs.chron.com/techblog/archives/2008/07/average_time_to_infection_4_minutes_1.html