Social networking has become huge. Facebook is now half a billion people. Twitter has 190 million tweeting 65 million times a day. The numbers for the social networking sites is not the focus of this article, but the security concerns those numbers bring along is. What's worse?-not even the best antivirus programs can fully protect users from the dangers.

While social networking sites do their best to stop threats, most of these threats can only be found once they have begun causing harm. Rogue applications, clickjacking (when one's account is hijacked by malicious code), and phishing are the most prevalent of attacks. Not sure what those names mean? Read on for some recent examples, what sites like Facebook and Twitter are doing to prevent them, and what steps you or your business can take to be safe while also being social online.

Rogue Applications

These applications can usually be spotted by asking the question "Is that too good to be true?" Knowing that your security can truly be at risk, it is best to be skeptical when choosing to add any third party application.

One example of a recent popular application (Profile Spy) offers to track who is really viewing a Facebook page. That sounds great, but if Facebook isn't the one offering, that should send off alarms. When setting up the application, the user is forced to click the like button and then forced to notify all contacts in order to activate the application. Basically, this application and others like it use Facebook colors and design to trick spam and collect personal information.

Clickjacking

Clickjacking is becoming one of the most serious problems on the internet because it focuses on exploiting how people use the internet rather than on specific software vulnerabilities. People surf the Web, and they click on things that are appealing to them. With clickjacking, however, users see only the exterior-that part which interests them-but there is a hidden button that then allows the attacker access to the user's account. Web cams and microphones can even be accessed to spy on the clicker. A recent clickjacking page on Facebook was called

Cheerleaders Gone Wild. This was a Facebook Page (now removed) that tricked users into clicking a link to a video, but while the video was showing distracting images of prancing cheerleaders, the software liked two other applications and published (spammed), this out to all friends.

Phishing

This is not a new tactic and because of its prevalence in e-mail, many people probably know a little about phishing already. But with half a billion people in one convenient place online, phishing has become a very popular sport amongst cyber criminals.

The bottom line--don't accept friend requests or give out any kind of personal information to strangers. I know the temptation. The face looks familiar from somewhere, and somehow it feels rude not to accept. But just don't do it.

To illustrate how much of a problem this desire to accept a friend request really is, the security software firm BitDefender released findings from an experiment last month. They took a sample size of 2000 users and sent them a friend request from an attractive young woman with blonde hair and a red dress. The result?-94 percent accepted this request. Only after half an hour conversation, 10 percent shared information used for password recovery questions, and after two hours, 73 percent were willing to send confidential information from their workplace.

Even more shocking is that 31 percent who became friends with the woman in the red dress work in IT security and were the most likely group to share personal data with this mystery beauty.

What are social media sites doing to help?

Twitter has finished its move to OAuth which allows authentication without requiring third parties to store user credentials. This eliminates the need to send user details over the Internet when the application is used.

Facebook is also adding a long needed security feature that will allow users to see what devices they have logged in, and log them out remotely. The feature will also show the browser and operating system on logged in devices. Facebook in particular has had problems keeping user data safe, so this new security feature should help users spot if his or her account has been hijacked. This new feature will be active by default.

Best Antivirus Programs

Obviously it is a must to have antivirus software from a trusted vendor installed, updated, and running on your computer, but threats on social networking sites are targeting people who are unaware of the dangers. Desktop security software will definitely help the clean up of any infections (as doing it manually is very time consuming), but will often do very little to prevent the infection itself. Therefore, the best antivirus when using one of these sites is simply *knowle dge* .
Know the dangers and how cyber criminals are exploiting habitual actions to cause harm.

So what are some simple steps to take for better security?

1. Do not accept any kind of friend request you are not 100 percent sure about.
2. Do not click on links or offers that you find, or that are sent to you from friends, that seem too good to be true. If you do click through, close out as soon as any other action is required (as in 'You must do X before you can get Y').
3. If your account has been used to spam others, or if you believe it has been hacked, change your password immediately.
4. Report any strange e-mails, notifications, or applications to the site administrators as soon as you spot them.
5. Do not reuse the same password for e-mail and social networking.