



Will Facebook Get You Hired or Fired?

Kevin Prince
Chief Technology Officer
Perimeter E-Security

A friend of mine told me a story about his mother who would always know when he got into the candy jar without asking. As a small child he couldn't figure out how his mom could be omniscient. He thought that was reserved for Deities and Santa Claus. When he got a bit older, he asked his mom how she did it. With a smile she told him that his fingers would be various colors from the candy coating and his mouth would have chocolate smears.

Facebook is like that candy jar and our employers or perspective employers are like my friend's mom. Companies look at social networking sites such as Facebook, MySpace, Twitter, LinkedIn, Bebo, Friendster and others with mixed emotions. On one hand, permitted use attracts younger employees, a friendly culture, creative sharing of ideas, and encourages friendships between co-workers. On the other hand, it can have implications with information security, liability, productivity, bandwidth consumption and more.

Are social networking sites making an impact? Well, governments are considering monitoring them, human resource departments are using them to screen applicants, authority figures have been known to infiltrate them in cyber disguise, and worms and Trojan horse software have been written specifically for them. I think it is safe to say that, yes, social networking sites are impacting our lives.

As of 2/12/09, Facebook is over 200 million members strong. With the viral and addictive qualities it has, employers have become concerned. About half of all companies use web content filtering or black lists to block access to social networking sites. Do they have a right to be concerned? Look at these statistics from the March 2, 2009 issue of Fortune Magazine.

- The typical Facebook user spends an average of 169 minutes a month on the site, where Google News gets 13 minutes and the New York Times website gets ten minutes.
- Facebook total daily minutes went from 1.1 billion to more than 3 billion in the last 12 months.
- Facebook users who update their status daily went from 4 million to 15 million in the last year.
- The Facebook user base doubled in that same time.
- It took 14 years for cell phone usage to reach 150 million units sold while Facebook members reached that in a mere 5 years. This is one of the fastest adoption rates in history.

Whether you are an avid user of social networking sites, know someone who is, or are concerned about our companies exposure to the risks of them, you need to stay safe. Criminals and those with less than honorable intentions are using these sites in ways we do not expect...and do not want!

BE AWARE

Users should be aware that 30% of companies are using social networking sites to learn about applicants as they interview for jobs. Even a photo or brief description of a user can offer insight into an applicant that is valuable for companies.

Be cautious of who you add as friends. There are known cases when someone takes on the identity of others, becomes an online friend, and then gathers other information about you, your contacts, associations, interests, group affiliations, etc. This information can be used for fraud, social engineering and other criminal activity.

Be conscious of what you post - assume that the entire world can view your comments, videos, and pictures. Ask yourself if you would want your boss, mother, priest, and spouse to see what you put out there...because they just might. Don't trust any site to keep your content private and remember, THE INTERNET NEVER FORGETS. All it takes is one night of partying and ending up with less than fully clothed pictures on the Internet that spread like wildfire.

Phishing is a common method cyber criminals use to lure individuals into giving up their personal information. *Spear phishing* is where the criminals target a specific group of users, for example all customers of a particular bank or credit union. *Whaling* is an even more directed attack at one particular person. Although these attacks are often directed towards high net-worth individuals, cyber-criminals use social networking sites and other online databases to obtain the majority of the information which allows them to commit these crimes.

Many companies have or are imposing Internet use policies. Be sure you understand what it says because your HR department will probably want you to sign and tie your employment to it. If Internet abuse is going on (based on whatever their definition is, which could include reduced productivity) you could lose your job. This could be Facebook, day trading, sports sites, and a myriad of other places on the net.

An Internet use policy could outline surfing as something that negatively impacts business processes. You might not know it but if your Facebook friend sends you a link to the latest High Definition movie and you download it, that could saturate the Internet bandwidth for the company and bring legitimate business communications to a halt.

There are cases where someone was viewing inappropriate adult material on their computer and a co-worker walked by and saw it. This leads to lawsuits against the company and often the termination of the offending employee. Offenses that may lead to termination can also include slandering a coworker on a social networking site.

BE SAFE

People are generally more cautious about messages in email than they are when they get a link, chat, text, post, or something else within a social networking website. For some reason we turn off our defenses once we are logged in. In fact, people are ten times more likely to click on a link sent to them in a social networking site than in regular email. Cyber criminals use this to their advantage. In the last year there has been a huge upswing in the variety and frequency of these types of attacks. Phishing attacks, Trojan horse programs, and malicious software can be used to compromise your identity.

Facebook has already experienced its fair share of worms. One of which is Koobface, which sends you an email that appears to be from one of your friends and directs you to a YouTube video where you are directed to download some new software which is in fact a Trojan horse program that infects your system.

These methods can also be used to compromise your computer, which can lead to bank account compromise, and if you are at work, spread and infect other systems. This can lead to the total

compromise of the company you work for resulting in millions of dollars in damages, lawsuits, lost business, fines, and more. The average cost of a data security breach for a company is 6.6 million dollars.

Remember that if you are infected with malware or a Trojan horse program, you likely would never know it. Your system would simply be under the control of a hacker and be used to capture your usernames and passwords, gain access to your online bank accounts, launch attacks against other systems, relay SPAM, or take full remote control.

Social networking sites are here to stay. Use these sites as tools. Be sure they don't keep you from your dream job or put you in the unemployment line.

Kevin Prince
Chief Technology Officer
Perimeter E-Security
KPrince@perimeterusa.com

ABOUT THE AUTHOR

Named Chief Technology Officer of Perimeter in 2009, Kevin Prince spearheads the company's technology strategy and leads the technical team in working closely with its customers to manage all of the complexity and compliance requirements of securing information across the enterprise.

With more than 19 years of expertise in Information Technology and 11 years focused on Internet security, Mr. Prince is an evangelist on Internet security topics, including network security threats, fraud, identity theft, cyber terrorism and data breaches. Through regular speaking engagements, webinars, whitepapers and blog postings, Mr. Prince is dedicated to educating organizations on how to manage information complexity, meet increasingly stringent compliance and security requirements, and mitigate risk. Mr. Prince has trained federal examiners for several years.

ABOUT PERIMETER E-SECURITY

Perimeter is the trusted market leader of information security services that delivers enterprise-class protection and compliance for businesses of any size. Through its cost-effective security-as-a-software platform, Perimeter offers the most comprehensive compliance, security and messaging services that include but aren't limited to: hosted email, encrypted email, firewall management and monitoring, vulnerability scanning, host intrusion and prevention, email antivirus and spam, remote data backup and email archiving.

As companies struggle with the increasing cost, complexity and stringent compliance requirements associated with their information intensive businesses, Perimeter is the only provider that can simultaneously reduce the cost, manage all of the complexity and meet all of the compliance requirements from a single platform.

Headquartered in Milford, CT, with seven geographically distributed technical operations centers and three redundant datacenters, Perimeter's on demand services, which are offered both on a Network (in-the-cloud) and CPE (customer-provided equipment) basis, are validated by TruSecure and guaranteed for current and future regulatory compliance. If you would like to speak with us or view a product demo, please don't hesitate to call at 800.234.2175 Option #2 or visit our web site at www.PerimeterUSA.com.