Computer/Internet Security Presentation

Social Networking (5)

<http://www.jeffbullas.com/2014/01/17/20-social-media-facts-and-statistics-you-should-know-in-2014/>

## Social web demographics

Social media is a blur of  tweets, shares and content. No longer is it just used by the young and the restless. It is global and embedded in every corner of the web.

So some questions. Which age groups are using social media, what countries are big Facebook users and what percentage are using mobile to access social media?

This is the who and the where of  social media users.

1. 72% of all internet users are now active on social media
2. 18-29 year olds have an 89% usage
3. The 30-49 bracket sits at 72%
4. 60 percent of 50 to 60 year olds are active on social media
5. In the 65 plus bracket, 43% are using social media
6. Time spent on Facebook per hour spent online by country. Here are the top three. USA citizens get the top gong at 16% followed by the Aussies at 14 minutes and the Brits at 13 minutes.
7. 71% of users access social media from a mobile device.

The paradigm of social media only being used by the younger generation should be put to rest now.

## Facebook

Facebook is still the biggest kid on the block, but there are some [pundits predicting](http://marketingland.com/study-google-will-overtake-facebooks-social-sharing-by-2016-49111) that by 2016 Google+ will surpass Facebook on “social sharing”.

Here are some of the latest figures to mull over.

1. There are now over 1.15 billion Facebook users
2. One million web pages are accessed using the “Login with Facebook”  feature
3. 23 percent of Facebook users login at least 5 times per day
4. 47% of Americans say Facebook is their #1 influencer of purchases
5. 70% of marketers used Facebook to gain new customers

See how***10 smart marketers***used Facebook to***double their email list***by[*clicking here*](http://www.jeffbullas.com/2014/06/20/10-facebook-contests-captured-10000-emails/). I’ll also show you how I used Facebook to grow my email list. It’s FREE,[*click here*](http://www.jeffbullas.com/2014/06/20/10-facebook-contests-captured-10000-emails/).

## Google+

Prying the numbers out of Google for Google+ has always been a challenge.  A bit like getting a date with the prettiest girl in the class. Not impossible but it doesn’t happen very often.

So what are the latest numbers?

1. There are now over 1 billion  with Google+ enabled accounts
2. It has reached 359 million monthly active users
3. Google+ is growing at 33% per annum.
4. The 45 to 54 year old bracket  increased its usage on Google+ by 56% since 2012

When you consider that Google+ has only been around for less than three years, then it is a success on many levels. So Google must be happy with with its investment, which is north of $500 million that it initially invested in Google+

## Twitter

Twitter has to be taken seriously. Last year it took off its short pants and become a public company. So what is happening in the Twittersphere?

1. There are now over 550 million registered users
2. 34% of marketers use Twitter to successfully generate leads
3. Twitter was the fastest growing network with a 44% growth from 2012-2013
4. 215 million monthly active users

Twitter has also made some changes in the last few months that has made it more visual and engaging. Business should no longer be ignoring the 140 character pip squeak.

## The others

We haven’t mentioned some important social media channels. These include. Pinterest, Instagram, LinkedIn, YouTube, Tumblr, Vine, Slideshare and many others.

This year expect the visual social media networks to hit more home runs.

Keep an eye on these two:

1. Pinterest with 20 million active monthly users
2. Instagram with 150 million active monthly users.

Social Networking is the usage of social media to interact with others online typically using texts, picture and videos.

<http://clearwebservices.com/social-media/how-does-social-media-work/>

Because Social Media is made up of so many elements, we tend to concentrate on the 3 big players in the field, which in terms of possible rewards and ROI would be:

* Facebook
* Twitter
* Youtube

Social Media works in many ways, but you have to look at it from the point of view of communication. Social Media is an instant communication tool to a potential audience of billions, because the moment you send a tweet, post a Facebook update or upload a video, anyone following, liking or subscribing to you will see it, something very few other forms of advertising can boast.

Social Media can be used by the majority of niches when it comes to business and although it can be undoubtedly time consuming, if you are willing to put the effort in and do things correctly then you will get rewards, as this has been proven time and time again.

Social Media not only acts as a sales tool and traffic increaser, it can also work to build up your brand or product exposure. We always look at the example of the pub chain Weatherspoons, because when you look at their menu, they say “Follow Us On Facebook”. The reason is simple. Very few people will actively go onto their website and check out their special offers, but if people follow them on Facebook, they can then get their special offers in front of people who want to know about them.

For a business, this makes perfect sense. We all use brands every day, like Tesco, B&Q and Countrywide etc, but how many of us actually go onto these websites to check out their offers regulary.

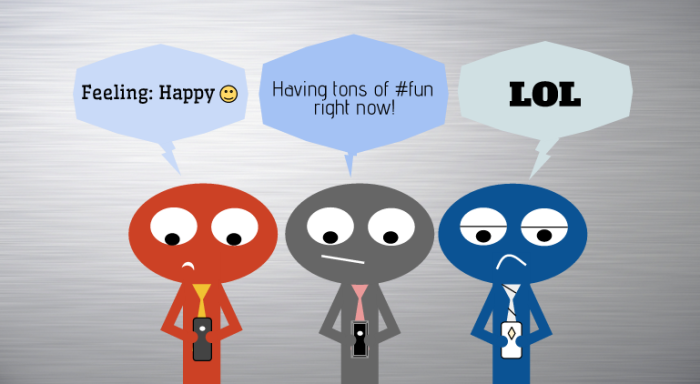
The answer is probably very few.

But, if these offers come onto our screens and are promoted to us, we will probably take more notice.

Social media works by building up people who actively want to know more about you and your business and then engaging with them. Having people who like you and never talking to them is like having a mailing list of 20,000 who you never email. You have to get your products, services and brand in front of people, and Social Media is an effective, in terms of costs and results, method of doing this.



<http://www.directtrafficmedia.co.uk/blog/how-social-media-can-help-or-hinder-home-security>



<http://jonnegroni.com/2013/05/24/social-media-is-making-us-more-insecure/>

Because students often post detailed and specific information on Facebook (including phone numbers, addresses, class schedules, social plans, etc.) you can be more easily stalked by strangers (or even acquaintances).   
  
Identity theft can also be a significant risk of social networking. Personal details like your full name, names of your family members, your phone number, birthday, address, and place of employment can all be used by identity thieves.  "Passport-style" profile photos also make it easier for identity thieves to replicate your online presence.

A social networking site can be a good way to make connections with people with similar interests and goals. They can be a way to connect with or "meet" people that a student may not have had the opportunity to before-including other students, staff, faculty and even alumni. Just as social media provides another avenue for making friends, it also makes it possible to renew old ones. Thus, meeting people and staying connected with classmates and friends is a major benefit of social networking sites.   
  
Social networking sites also offer event listings, group profiles and fan pages that can communicate the pulse of a campus culture. They can be a great way to understand and stay connected to your campus community as a whole.

Evaluate your social networking account and postings-how do you feel about your employers seeing what you have posted? How about your parents or grandparents?   
  
Do not post private information, including your cell phone number, home address, class schedule, social plans, etc. unless you are prepared for anyone to find you/track you down, any time of the day or night. Do not post anything that might be embarrassing to you in a potential employment situation. People have been denied work because of information found on social networking sites.   
  
Utilize the "Privacy" settings on your Facebook account-you can adjust your privacy settings so as to control who has access to your personal information. These settings change and evolve frequently, so check your privacy settings after any site updates to ensure that you are still protected.  
  
To minimize the risk of identity theft, carefully monitor the information you make publicly available on social media or make your profile private. Using different passwords for your social media sites, email accounts and any online commerce sites (banking, shopping, billing, etc.) can also make it more difficult for identity thieves to acquire information about you[[3]](http://www.pacific.edu/Campus-Life/Safety-and-Conduct/Online-Social-Networking-Dangers-and-Benefits-.html" \l "_ftn3" \o "). Using a group photo for your profile picture can also make it more difficult for thieves to replicate your identity online.

<http://www.pacific.edu/Campus-Life/Safety-and-Conduct/Online-Social-Networking-Dangers-and-Benefits-.html>

Social networking has changed the way we interact with friends and associates. While social networks, like Facebook, Twitter, YouTube, FourSquare, and Google+, play a significant role in our lives, they are also a high risk for security threats.

With hundreds of millions of users online, these tools not only attract friends and family wanting to stay in touch, but they also attract people wanting to know about you for the wrong reasons. Be aware of the top five security threats currently out there to help you stay safe online.

**1. Having Your Identity Stolen**

Identity thieves gather [personal information](http://resources.infosecinstitute.com/social-media-security-risk/) from social media sites. Even if you have your account on the highest security settings, there are still ways for an identity thief to get your information. Most social network sites have information that is required, such as email address or birthday. It’s common for an identity thief to hack an email account by using social information. For example, a common technique to get personal information is by clicking on “forgot password” and trying to recover the information through email. Once the thief has access to your email account, they then have access to all information on your social networking sites.

So what can you do to protect yourself? You don’t have to delete all your social profiles or hide from the real world; just take these precautions.

* **Have a strong password**. The stronger your password, the harder it is to guess. Use special characters like symbols and capital letters when creating your password. Also, don’t use “common” passwords, like your birthday or your child’s name.
* **Be careful with your status updates**. Often, we innocently post status updates that would give an identity thief information they need to steal our identity. For example, you may post “Happy birthday to my mother!” and then tag her in the post. Likely, your mother’s maiden name will be associated with that tag now. A popular security question is “What is your mother’s maiden name?” and if you share that online, you run the risks of identity thieves getting the answer to this commonly used question.
* **Don’t reveal your location.** You can use a fake location or make one up from another city and state. You may even be able to leave this information blank. Be cautious and never use a city and state where you live.

**2. Getting Your Computer Or Social Profile Hacked**

Hackers love social networking, going right to the source to interject malicious code. The codes[hackers](http://www.networkworld.com/news/2011/053111-social-media-security.html) use can steal your identity, inject viruses to your computer, and obstruct bank account information, to name a few. Shortened URLs, such as those created on bit.ly, are especially susceptible to hackers. Shortened URLs can trick users into visiting harmful sites where personal information can be compromised because the full URL is not seen.

The best advice is to never click on a link until you are sure of the source. To tell if a link is safe, you can:

* [**Hover over the link**](http://www.pcworld.com/article/248963/how_to_tell_if_a_link_is_safe_without_clicking_on_it.html)**.** If you hover over a link without clicking, you’ll see the full URL in the lower corner of your browser. If this is a website you recognize, go ahead and click.
* **Try a link scanner.** A link scanner is a website that lets you enter the URL of a link you suspect might be suspicious to check for safety. Try [URLVoid](http://www.urlvoid.com/) or [MyWOT](http://www.pcworld.com/article/231795/wot_web_of_trust.html) as possible options.
* **Check shortened links.** A shortened link is popular on sites like Twitter where character length matters. Some shortened link sites include bit.ly, Ow.ly, and TinyURL. Use a service like[Sucuri](http://sitecheck.sucuri.net/scanner/) to determine if the real link is secure.

**3. Inadvertently Letting Stalkers Find You**

When you use social networking sites, you are posting [personal information](http://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks). Once information is posted online, it’s no longer private and can fall into the wrong hands. The more you post, the more vulnerable you become to those who may wish to harm you. Even with the highest security settings, friends, associates, and even the brands you “like” on your networking sites, can inadvertently leak information about you. The websites you subscribe to, the apps you download, and the games you play on social networking sites all contain personal information about you. Every time you browse a website, companies can put invisible markers on your computer called cookies. In theory, no two cookies are alike. When you are online, these cookies track your activity as you move from site to site.

To keep sites from tracking your activity, click on the “Do Not Track” feature. Most websites have an option for you to opt out of tracking. You can also clear the cache and cookies on your browser regularly to help prevent any problems.

**4. Letting Burglars Know Your Whereabouts**

Telling the online world where you’re going and when you aren’t at home is inviting burglars to your house.  Did you know that a run-of-the-mill burglar can break into your home in less than 60 seconds and spend [less than 10 minutes](http://www.safewise.com/you-got-robbed) stealing your possessions? By telling the world you are on [vacation](http://daol.aol.com/articles/never-say-this-on-facebook-or-twitter/) in Europe, you’re letting potential thieves know where you are, how long you’ll be gone, and where you live. Burglars are fond of constant updates, especially about your travel plans. You wouldn’t stand up in the middle of a crowd and announce you’re going on vacation for a week, would you? Of course not, but that’s what you do when you post your vacation pictures and plans online.

When you go on vacation:

* Avoid posting specific travel plans. Never post when, where, or how long you’ll be gone.
* Wait until you are home to post pictures to a vacation album.
* Use highest privacy control. Only let certain groups, like a family group, view your photos.
* Be selective with the status updates. You can use an audience-selector dropdown menu on Facebook to choose certain groups to see your status updates.
* Stay offline. You’re on vacation, after all. Relax and forget about the online world for a few days.

**5. Becoming Overconfident**

One of the biggest threats to online security is overconfidence. Whether at home or at work, many users believe as long as they have a firewall and an antivirus installed, there is no threat to security. Many people also believe that they don’t have anything worth hacking so there’s no need to worry about security. With today’s technology, we are more connected to each other than ever before. When you neglect security, you not only put yourself at risk, but others are at risk as well.

To keep yourself and your information safe, pay careful attention to your online activity. Avoid posting information including:

* Travel plans (see point 4)
* Bank account information
* Your full address and birthdate
* Your children’s’ names, school, and birthdates
* Location information, such as the name of your work place
* Your daily schedule

You can still use social networks for all they were meant to accomplish, but you need to take extra precautions to make sure your personal information doesn’t get in the wrong hands. Know what threats you are most vulnerable to and take steps to protect yourself and your networks.

<http://www.mediabistro.com/alltwitter/5-social-media-threats_b51841>

### Using Third Party Apps

Part of the appeal of social media sites are all the various games and apps. Even though a significant number of them are safe, you do grant the app a certain level of permission concerning your information. Make sure you know what the app is viewing and sharing before agreeing to the terms.

<http://socialnetworking.lovetoknow.com/Security_Issues_With_Social_Networking_Sites>

SASKATOON – These days a simple online post could influence your future. Posting the wrong thing to social media could result in life-altering consequences, according to a professional in Saskatoon.

### RELATED

### [[Dalhousie dentistry](http://globalnews.ca/news/1755191/restorative-justice-will-it-work-in-the-dalhousie-facebook-scandal/)Restorative justice: Will it work in the Dalhousie Facebook scandal?](http://globalnews.ca/news/1755191/restorative-justice-will-it-work-in-the-dalhousie-facebook-scandal/)

### [[Ben Schmidt’s a word-a-day over 365 days video is racking up the views on YouTube.](http://globalnews.ca/news/1756337/1756337/)Saskatoon man’s YouTube video going viral](http://globalnews.ca/news/1756337/1756337/)

### [Biggest social media blunders of 2014](http://globalnews.ca/video/1746773/biggest-social-media-blunders-of-2014)

### [[One person is taken to hospital following a serious collision in north Edmonton, Monday, January 20, 2014.](http://globalnews.ca/news/1718751/twittertuesday-edmonton-police-using-social-media-to-battle-traffic-issues/)#TwitterTuesday: Edmonton police using social media to battle traffic issues](http://globalnews.ca/news/1718751/twittertuesday-edmonton-police-using-social-media-to-battle-traffic-issues/)

### [Social media expert walks through Facebook terms of use](http://globalnews.ca/video/1714537/social-media-expert-walks-through-facebook-terms-of-use)

“I think that people are not aware of actually how long or how far back that social media can be tracked,” said Essence Recruitment President Tracy Arno.

Facebook, Twitter and Pinterest accounts are just some of the social media platforms Arno goes through every day.

“We do our due diligence by screening candidates by Googling them and if their name comes up we will look at their profiles, so a lot of the times it’s a positive thing to show what their lifestyles are like and it shows kind of a good life balance but it could be negative,” said Arno.

Posting degrading comments about women on a Facebook group page has resulted in the suspension of 13 dentistry students at Dalhousie University in Halifax.

**READ MORE:** [Dalhousie refuses to release names of suspended students to dental boards](http://globalnews.ca/news/1757596/dalhousie-refuses-to-release-names-of-suspended-students-to-dental-boards/)

“I trust that the university is going to take some disciplinary and reparitive measures in this specific action but I also think that we need to focus on having a proactive approach on this, we need to make sure that people know this just isn’t OK in general,” said Jennifer Nowoselski, Dalhousie student union vice president.

While the intentions of a social media post may be innocent, it might not come off that way to others. Arno warns posters to be careful.

“When you do post, you are allowing the world to see you the way they want to see you, so you have no explanation, you cannot defend yourself and they can make any opinion they want on what you posted,” said Arno.

The bottom line is a seemingly harmless post or picture now, might make a devastating difference down the road.

http://globalnews.ca/news/1758706/all-it-takes-is-one-social-media-post-to-be-devastating/

<http://loopcayman.com/2014/11/17/police-math-teacher-pulled-knife-student/>