Student X

Social Media and Privacy

Thesis Statement

How concerned are we about privacy and security when we are using our favorite social

media sites.

How often do we ask ourselves that question? With all the data breaches, identity theft

and sharing of personal information by service providers on the rise, privacy and security

should be our 1st priority. Guess what its not. We focus more on sharing pictures of outings and

clicking on articles we find interesting not thinking about it could be actually be a virus or spam.

We are living our lives more and more on social media. True enough social media has

Brought us together enriched our personal lives, business relationships, and even made us

more productive and some of us has even become face book famous. On the other hand social

media has ruined lives, broken up marriages, and put some of us in financial debt. The reason

for is where computers users go so does the bad guys.

Cyber criminals have flocked to social media like white on rice, seeking whom they may

devour. They will use any opportunity to steal personal information or spread malware

for future attacks and to defraud unsuspecting users.

These are some of the tricks Facebook users are confronted with on a daily basis:

Facebook Likejacking: using intriguing posts often referencing current events to trick users into

clicking on malicious or phishing link.

Rogue apps: Which could lead to spam, phishing or malware via facebook.

Facebook chat attacks: Can spread malware via unsolicited links and promote phishing apps.

Now despite the pitfalls and dangerous of using the social media has this caused users

to be worried about their privacy. Well according to Ponemon institute research there has been

an increase in “Privacy sensitive” users, from 55% five years ago to 61% today.

The ironic thing about social media privacy is users actually think they are safe and

rarely change their online behavior even if they are hit by a major cyber incident.

What we fail to realize everytime we search online for restaurants, share good or bad

news with our facebook family and friends or tweet to our followers the audience is bigger than

you could ever imagine. The reasoning for that is every move you make leaves cyber foot prints

in the sand and hackers are following them.

What is really scary is the fact that teenage social media users careless about privacy.

A teens whole world is on social media. They share all kinds of personal information about

themselves. Yes, these sites are designed to encourage the sharing of our personal life to

others. When we share your life we forget that friends of friends can also see the post.

According to stastics 60% of teen facebookers post private and most report high levels

of confidence in their ability to manage settings. That’s not the major concern for teenage

users. Their concern is how to shape their reputation on facebook and become facebook

famous. They don’t think about or concern themselves about third-party access to their data.

Social media is not just where criminals steal information, it is also where they trade

data. Everyone once in a while we will see a picture shared by a friend out to dinner but we are

hesitant to click on it because we are not quite sure they posted it.

Interconnectivity of social media means it is a perfect hunting ground for illegal activity

and more and more people are realizing that their “friend” may not actually be their friend.

“The problem with social media is that people have an inherent trust,” explains Mark

James, security specialist with IT security firm ESET. “And that is what is being tapped into by

those cyber criminals,” “People still believe that you have to click on something and download a

file to be infected,” he says. “This really isn’t the case anymore there are things like drive-by

downloads that can very easily infect and compromise your machine.

Setting up a fake page to avoid detection only takes a matter of minutes, and social

media sites have the inherent interest in keeping access simple. After, all they want to attract

as many users as possible.

Hackers never sleep. Just when you think you have done everything right in protecting

your computer along comes a new exploit to keep you up at night. It might be an SMS text

message with a malevolent payload or a stalker who dogs your every step online. Or maybe its

an emerging technology like in-car Wi-Fi that suddenly creates a whole new attack vector.

Whether you are in IT manager protecting employees and corporate systems or you’re simply

trying to keep your own personal data safe, these personal threats some rapidly growing.

We all know social media can be fun but remember there are bad guys out there looking

to steal, kill, and destroy our personal information. So always have a virus protector on your

computer and remember to change your password every three months. Of course that will not

prevent hackers from trying but lets not make it easy for them.

References:

Blog.trendmicro.com

[www.usatoday.com](http://www.usatoday.com)

[www.pewinternet.com](http://www.pewinternet.com)

[www.bbc.com](http://www.bbc.com)

www.darkreading.com