



CYBER SECURITY

NEW YORK STATE DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES

17th Annual New York State
Cyber Security Conference

9th Annual Symposium
on Information Assurance

June 3 - 4, 2014
Empire State Plaza, Albany, NY



Social Media Considerations for Cyber Security and Crisis Response

Social Media Considerations for Cyber Security and Crisis Response

Social media allows for greater information sharing and engagement with citizens and stakeholders by government entities. Still, there is no such thing as a free lunch, pitfalls, conflicts of interest and of course security issues must be addressed so that optimal value can be achieved, and unintended consequences avoided or mitigated. Current problems and approaches to social media are presented for various scenarios



Joseph Treglia, PhD, Syracuse University

Melissa Delia, Syracuse University

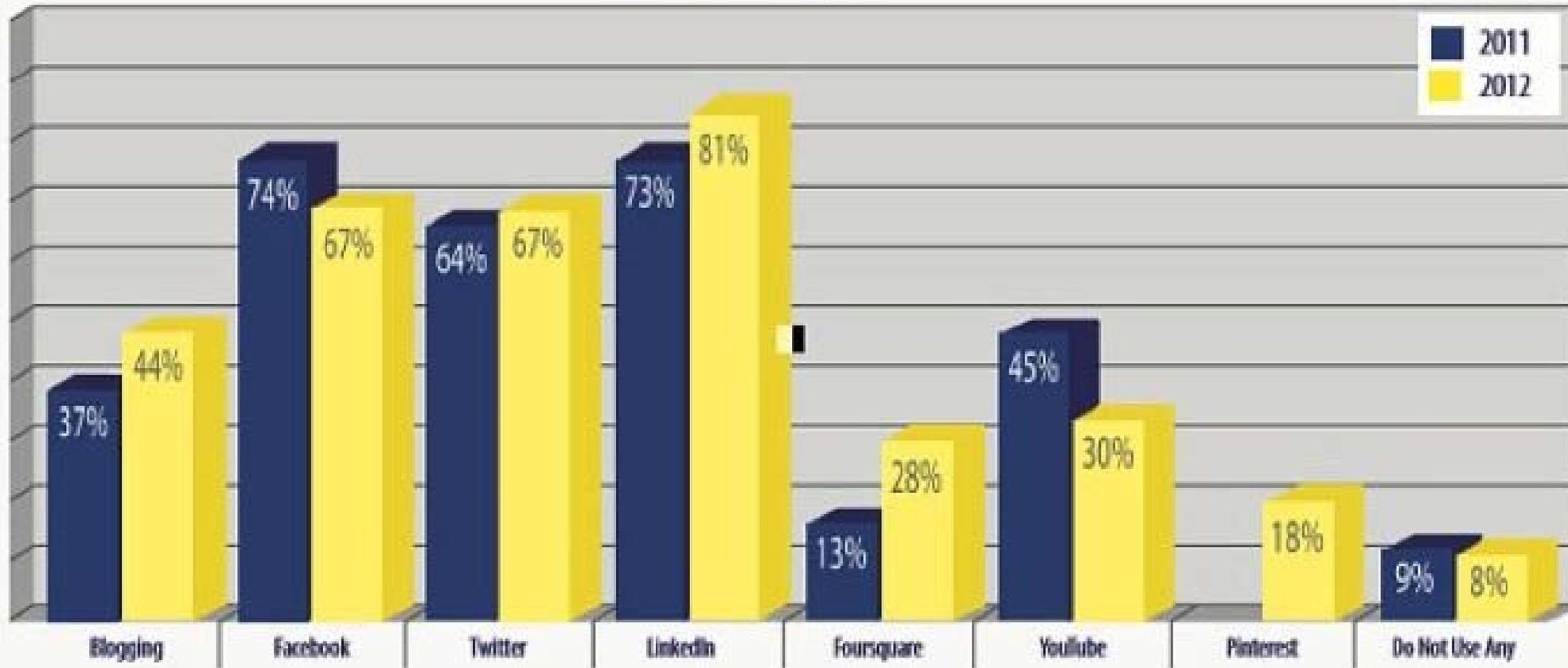
Gabriel Jansson, Syracuse University

- School of Information Studies

Conclusion (First)

- Social media is only as valuable as its authenticity, integrity, and availability
- Social media interactions are FOIL/FOIA discoverable
- Government sponsored websites can provide these necessary requirements
- .Gov , MIL, .EDU means something to users and employers
- Social media is an adjunct to other things

GROWTH IN SOCIAL MEDIA TOOLS 2011-2012



THE UNIVERSITY OF MASSACHUSETTS DARTMOUTH
CENTER FOR MARKETING RESEARCH

SOCIAL MEDIA AND THE 2012 INC. 500 STUDY



1 | Facebook
900,000,000 - Estimated Unique Monthly Visitors



2 | Twitter
310,000,000



3 | LinkedIn
255,000,000



4 | Pinterest
250,000,000



5 | Google Plus+
120,000,000



6 | Tumblr
110,000,000



7 | Instagram
100,000,000



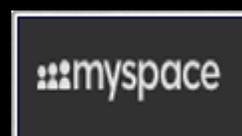
8 | VK
80,000,000



9 | Flickr
65,000,000



10 | MySpace
42,000,000



40,000,000



38,000,000



37,000,000



15,500,000



15,000,000



Friendster XING MySpace Bebo LinkedIn (Relationship) hi5 myYearbook Netlog MeetUp Welcome Skyrock

Global Messaging Ecosystem – Select Players, 2013



WhatsApp (USA), 4+ Years

MAUs = 400MM, +100% Y/Y
Messages / Day = 50B, +178% Y/Y



Tencent WeChat (China),
3+ Years

MAUs = 355MM, +125% Y/Y



Line (Japan), 2+ Years

MAUs = 280MM
Messages / Day = 10B
Revenue = \$388MM, +5x Y/Y (Q4:13)



KakaoTalk (Korea), 3+ Years

Messages / Day = 5.2B, +24% Y/Y
Revenue = \$203MM, +4xY/Y



Snapchat (USA), 2+ Years

Messages / Day = 1.2B



Viber (Israel), 3+ Years

MAUs = 100MM



Source: Publicly disclosed company data for 2013. Note: Snapchat messages / day comprises number of snaps sent per day and number of stories viewed per day.

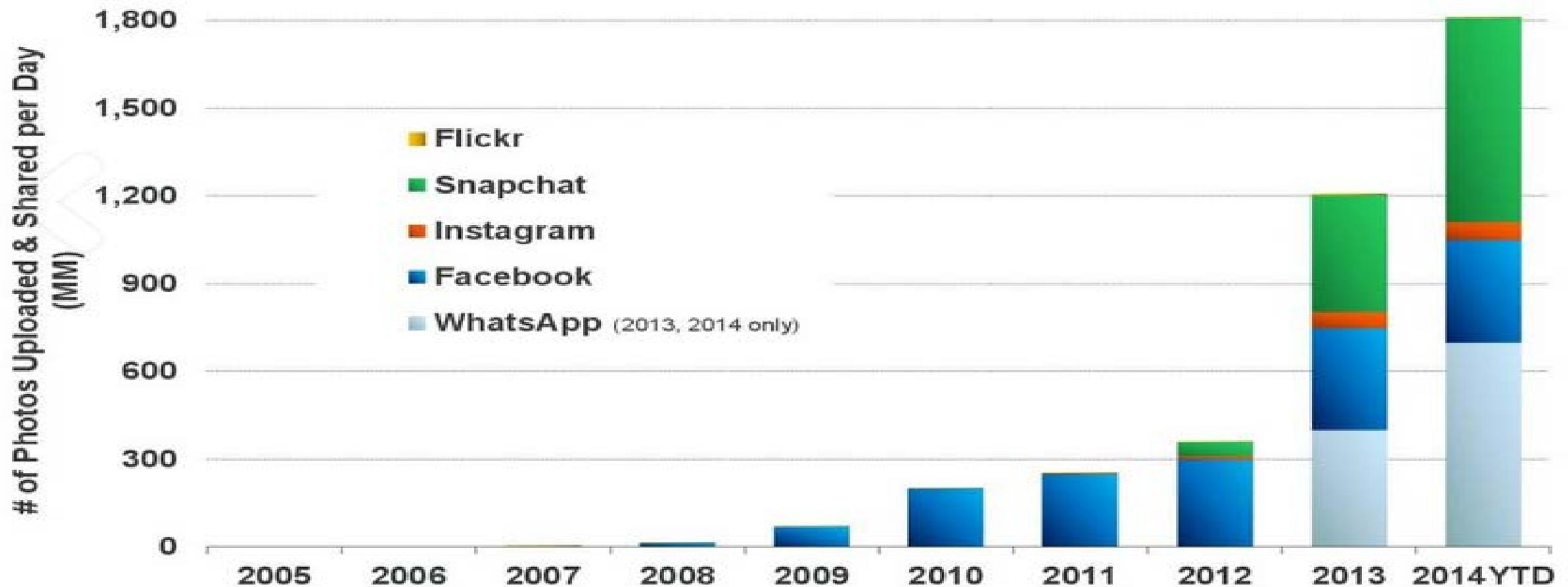
Social *Distribution* Leaders = Facebook / Pinterest / Twitter

- **Social Media Traffic Referral Leaders =** Facebook / Pinterest / Twitter with estimated 21%, 7%, 1% of global referrals, per Shareaholic, 3/14.
- **Social Distribution Happens Quickly =** Average article reaches *half* total social referrals in 6.5 hours on Twitter, 9 hours on Facebook, per SimpleReach, 5/14.

Photos Alone = 1.8B+ Uploaded & Shared Per Day

Growth Remains Robust as New Real-Time Platforms Emerge

Daily Number of Photos Uploaded & Shared on Select Platforms, 2005 – 2014YTD



SOCIAL MEDIA CHALLENGES

Freedom of Information Law

Records: Defined broadly as any information in any physical form that is kept, held, filed, produced, or reproduced, by, with or for a government agency. This can include:

- State
- City
- County
- Town
- Village
- Public Authorities
- School Districts

All of these Agencies are covered under FOIL

Freedom of Information Law (Continued)

Personhood: FOIL does not limit to just people, it is a broadly defined term to justify the response to **ANY** request for information.

- This could include robots, spam, spoofing attacks
- Potential to cause DoS attack

Requests to government agencies must be answered within 5 days

Social media should be used by government agencies with **caution**

- Any information captured from social media becomes FOIL-able, requiring that it be stored and maintained as official documentation
- Subject to the laws of FOIL / FOIA information requests and therefore must be reported on
- Origin can be unknown

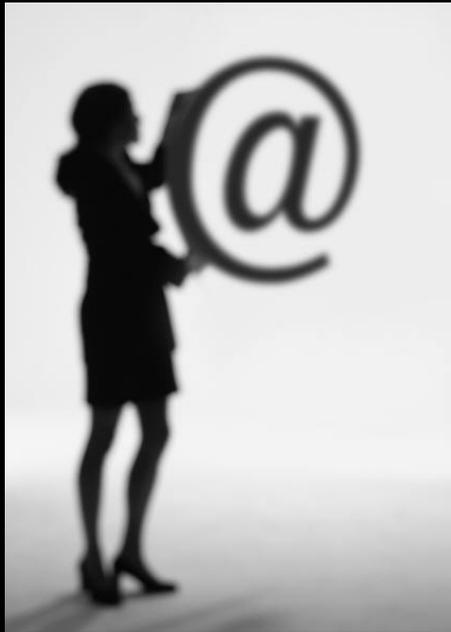
Freedom of Information Law (Continued)

Presumption of Access: All government agency records are accessible with the exception of some records, or portions of records within a series of exceptions.

- Social media requires additional reporting
- **Reasonable Disclosure**: Government agencies and employees have less privacy and more accountability than citizens, so any information within reason (excluding health information, social security numbers, etc.) is discoverable

TRUST ISSUES AND SOCIAL MEDIA

<http://YourAgencySite.ny.gov>



.GOV .MIL .EDU .ORG .US? .NET? .COM? .???

Government Trust: Establish Web Site using .gov .mil .edu

- Provides consistency
- Permits availability and legitimacy
- Facilitates user trust while removing the vulnerabilities common to private social media attacks
- Creates accountability (FOIL/FOIA)

User Trust

Trust – Trust as an element of information security on social media sites that is often let down.

Once a user establishes an account and relies on the information of the social networking site, finding value in what they find, their usage will increase³.

User Trust (Continued)

Trust and Uncertainty Reduction Theory (2011) states:

- “At this point, users have developed a belief that the information they find on the site is reliable and trustworthy, so they begin to trust the network itself, including servers, and hardware, and security measures.”

This relationship exists until a security breach is encountered, by then it is too late. Trust leads to confidence which is a downfall in social media itself due to security vulnerabilities.

Many Users cannot access Social Media

Many people work for others

Most employers **BLOCK** or **RESTRICT** Social Media access

Social Media sites are **PRIVATELY OWNED**

- Rules change
- Financial Interest
- Information Released
- Not trusted by many
- May require participation or other for access

Recommendations



MADISON COUNTY EMERGENCY MANAGEMENT AGENCY

1823

"TO SERVE AND PROTECT THE LIVES AND PROPERTY OF THE CITIZENS OF MADISON COUNTY FROM NATURAL, TECHNOLOGICAL, AND MANMADE DISASTERS."

HOME ABOUT US MASS NOTIFICATION SOCIAL MEDIA PRESS RELEASES WEATHER CLOSINGS TRAINING CALENDAR PHOTOS LINKS

MADISON COUNTY MASS NOTIFICATION SYSTEM

✉️ f t g+ 📺 📡 🌐

Madison County Mass Notification

EAS (Emergency Alert System) **EMERGENCY ASSEMBLY AREA** **mobile ALERTS**

[About Mass Notification](#)

[Frequently Asked Questions](#)

[Signup Instructions](#)

SIGN UP

The Madison County Emergency Management & Department of Homeland Security Agency is excited to announce we have partnered with Amatra to provide an electronic public alert and notification system in Madison County. On May 1, 2014 the Amatra system will go live for citizens, businesses, schools, government agencies and anyone else to enroll in this FREE emergency notification system. Amatra will be used to communicate information when emergency situations arise in Madison County.

How to get alerts:
#1 [CLICK HERE TO SIGN UP](#)
#2 Enter "MADISON" for Registration Code (Must be ALL CAPS)



Recommendations

National Terrorism Advisory System



NTAS
NO ACTIVE ALERTS
www.DHS.gov/alerts

Put this widget on your web page

No Active Alerts
AMBER ALERT



Sign up for alerts from the
Madison County Emergency Management & Homeland Security Agency
& other public safety agencies in your area.

Mobile #

Email

Zip Code

I accept the [Terms & Conditions](#) and [Privacy Policy](#)

Sign Up!

MCEMA SOCIAL CONNECTIONS

Tweets

[Follow](#)

 **Madison Co. EMA** @MadisonCoEMA 29 May
Interstate 69 is now open.
[Expand](#)

 **Madison Co. EMA** @MadisonCoEMA 29 May
Expect delays on I-69 at MM 217 for a severe accident. Unknown duration, please plan alternate route if possible. nixle.us/8ESTQ
[Expand](#)

 **Madison Co. EMA** @MadisonCoEMA 29 May
EMA is enroute to I-69 Northbound mile 217 for an accident. Plan an alternate route.
[Expand](#)

 **Madison Co. EMA** @MadisonCoEMA 26 May
TY to all of the veterans who have served or currently are serving in the military.
pic.twitter.com/8c6niVkg63
[Show Photo](#)

Tweet to @MadisonCoEMA

Find us on Facebook

 **Madison Co. Emergency Management & Homeland Security Agency**
[Like](#)

 13 hrs · 🌐

The June Jamboree is this coming week June 3 – June 7 at Falls Park in Pendleton. The Madison Co. LEPC and Madison Co. EMA will be setting up a booth at the event as part of our community outreach. The days and hours of the event are: T, W, TH, F 5PM – 10PM and Sat 1PM-11PM. Be sure to stop by our booth to learn about what our agency does.

7,761 people like Madison Co. Emergency Management & Homeland Security Agency





Recent messages from:
Madison County Emergency Management & Homeland Security Agency

Advisory  **Agency** causing delays.
[More >](#)
"Entered: 1 day, 19 hours ago"

Advisory Severe Weather Threat for Madison County this afternoon and evening. [More >](#)
"Entered: 1 week, 2 days ago"

Community I-69 Traffic Lane Shift Tonight At Main Street Bridge [More >](#)
"Entered: 1 week, 4 days ago"

Community State Road 128 Construction starting Monday [More >](#)
"Entered: 2 months, 3 weeks ago"

[View more messages from this agency >](#)

Receive messages by email & text

Sign Up!

message powered by: **nixle**

AS SOCIAL MEDIA
GROWS MORE ATTACKS
OCCUR

“Aol Mail Hacked With Spoofed Accounts Sending Spam” – techcrunch.com

“Target breach may have started with email phishing” – cbsnews.com

“Attack on Yahoo e-mail may spawn more phishing scams” – USA Today

“New York Times Hack Started With A Simple Email Scam” – buzzfeed.com

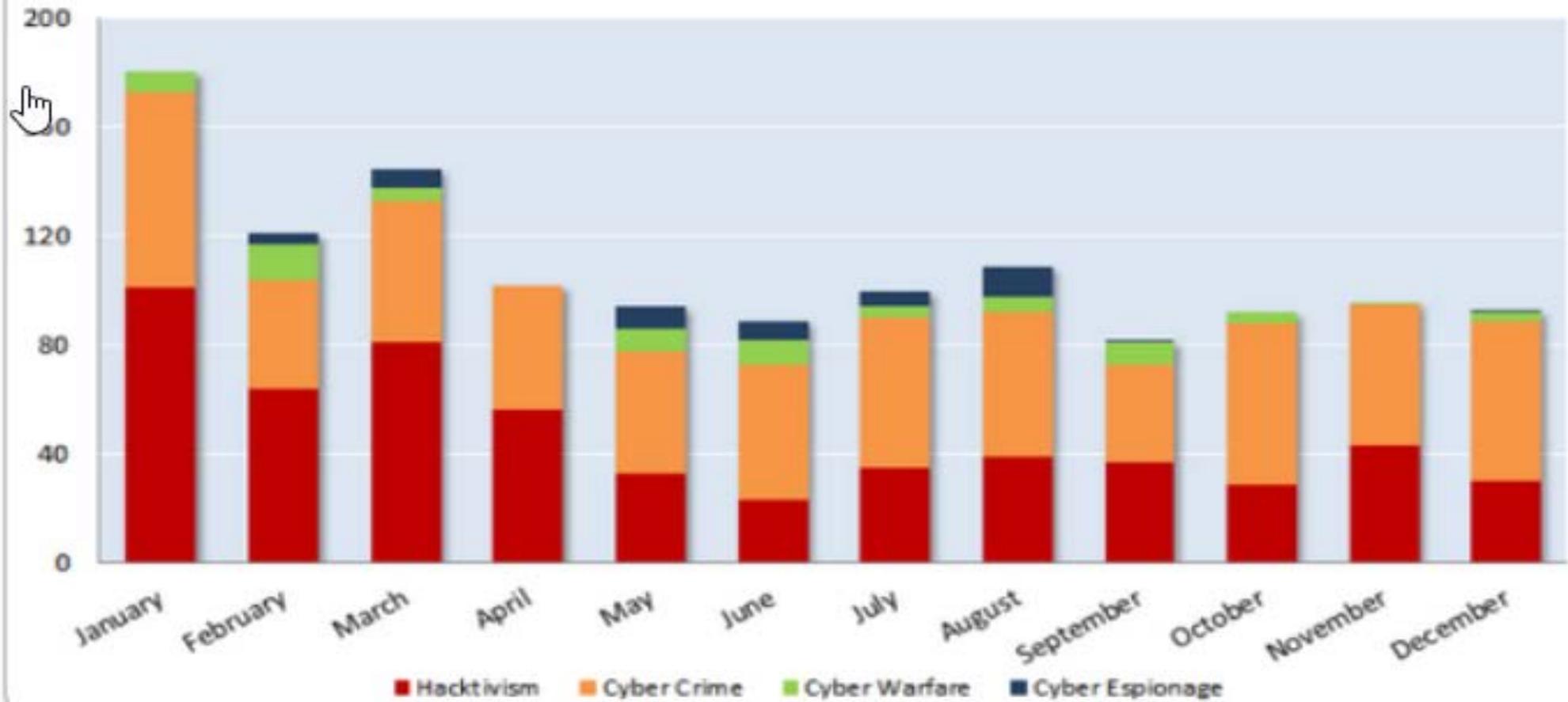
“Reports: Phishing attack hits Twitter”

“Email 'phishing' attacks by hackers growing in number, intensity”

“New Facebook Phishing Attack Steals Accounts, Financial Information” – PC Mag

“WARNING: Twitter Phishing Scam Spreads by Direct Messages”

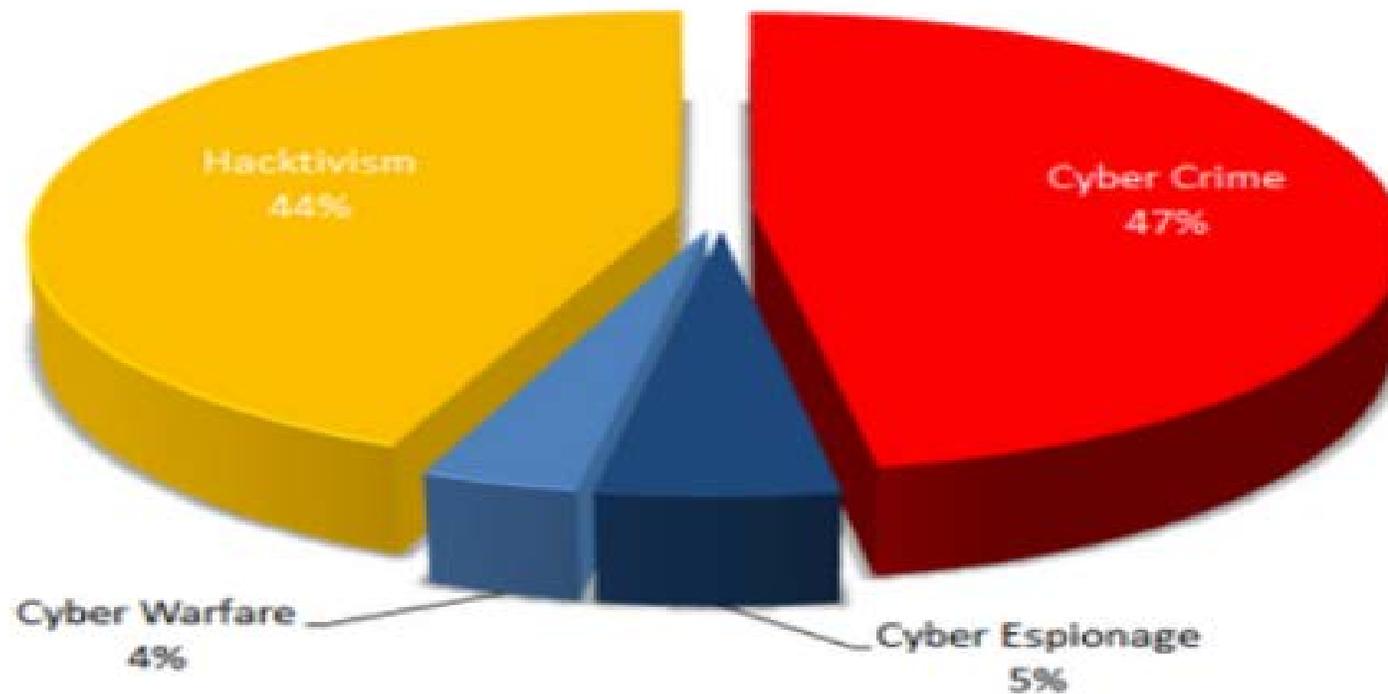
2013 Attack Trend (Drill down)



2013 Attack Trend with the Drill-down of Motivations

Exploring the motivations shows a slight advantage of Cyber Crime (47%) over Hacktivism (44%), well above Cyber Espionage (5%) and Cyber Warfare (4%).

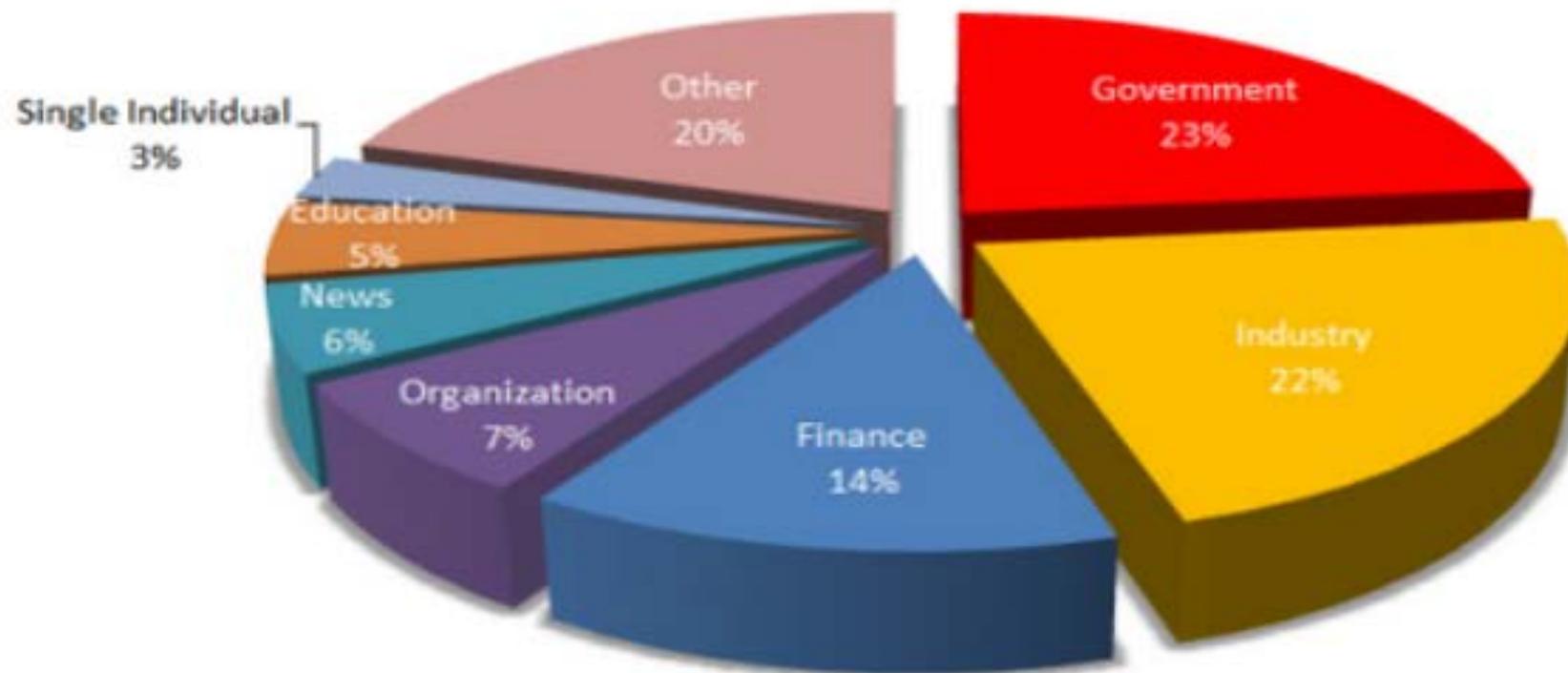
Motivations Behind Attacks (2013)



Motivations Behind Attacks (2013)

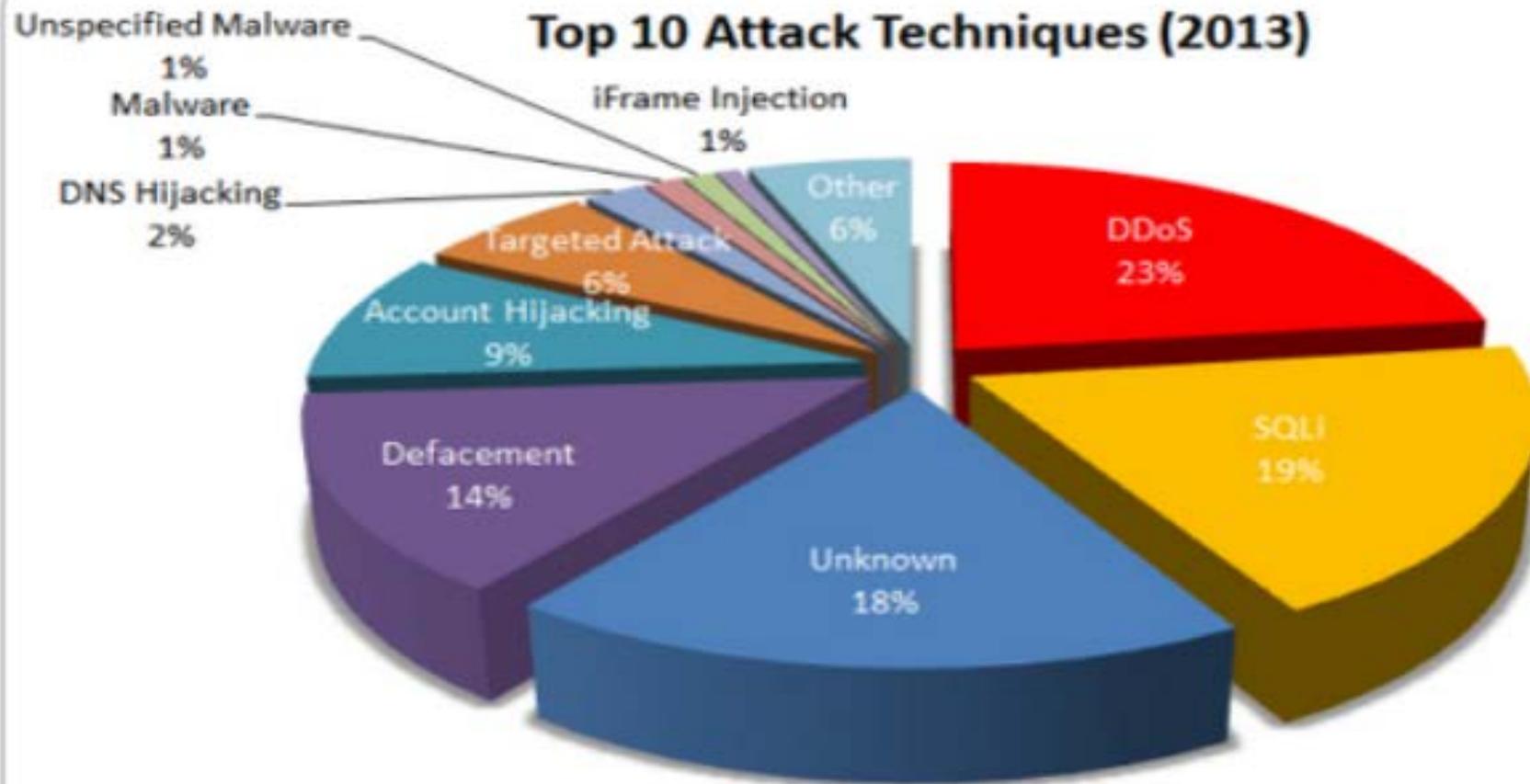
DDoS leads the chart of known Attack Techniques (23%) ahead of SQLi (19%) and Defacements (14%). It's also worth to mention the rank number five achieved by Account Hijacking (with 9%) and the growing influence of Targeted Attacks ranking at number six with 6%.

Top Targets (2013)



Top 10 Targets (2013)

And, last but not least, the Top 10 Countries chart is lead by US which suffered nearly 1 attack on 2, well ahead of UK (5%) and India (3%).



Top 10 Attack Techniques (2013)

Governments and Industries have been the most preferred targets for Cyber Attackers with similar values (respectively 23% and 22%). Targets belonging to finance rank at number three (7%), immediately ahead of News (6%) and Education (5%).

Spoofing

How to Spoof an Email

SQL Injection

Mysql.com Vulnerable To Blind Sql Injection:

- Vulnerability which involves spoofing tactics to gain access to information⁴.
- An error has occurred...

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near `"/contentPage.php?id=8"` at line 1

This means the website is vulnerable to SQL Injection.

Technical Flaws: SQL Injection

SQL Injection.

User-Id:

Password:

```
select * from Users where user_id= 'srinivas '
and password = 'mypassword '
```

User-Id:

Password:

```
select * from Users where user_id= '' OR 1 = 1; /* '
and password = '*/-- '
```

9lessons.blogspot.com



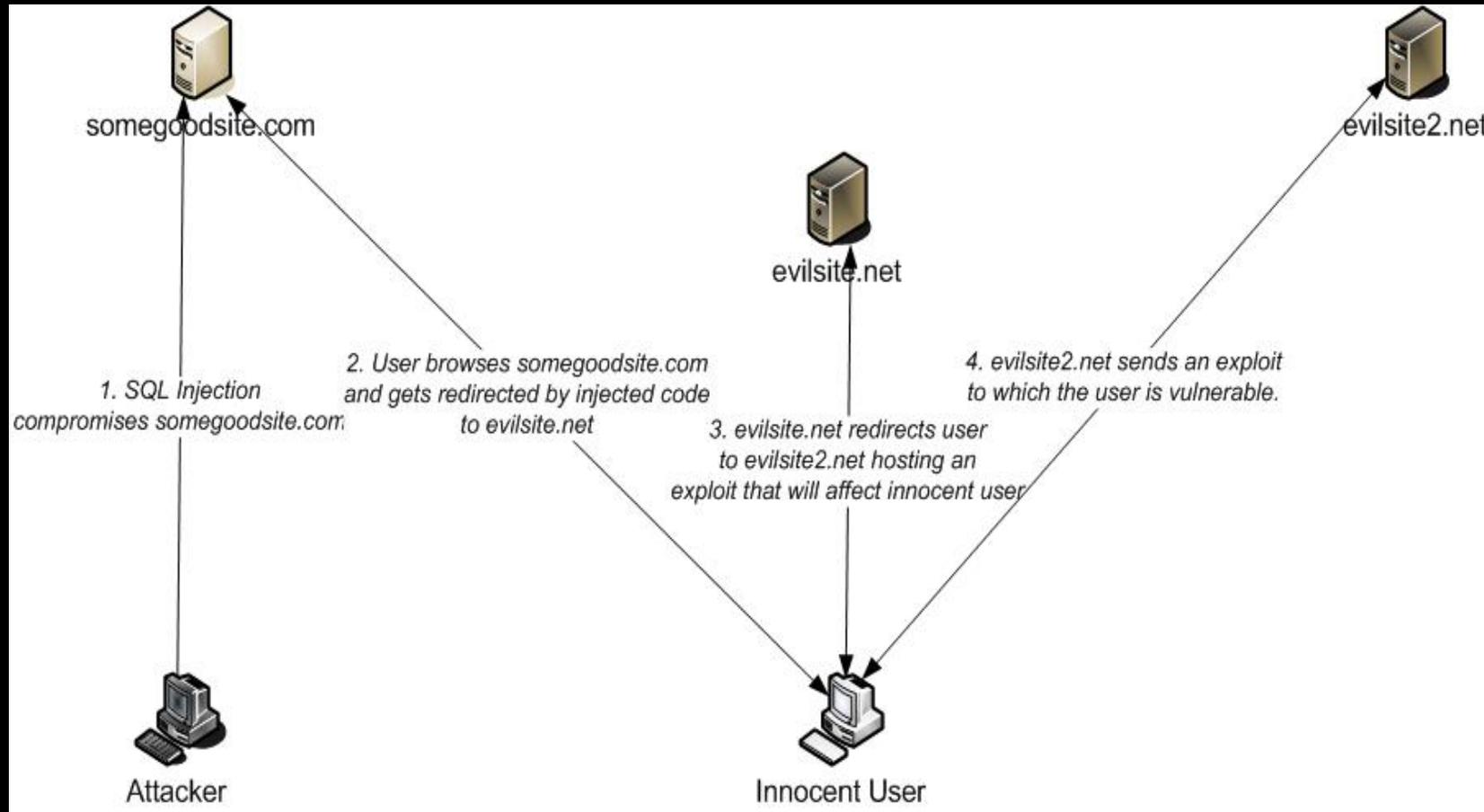
-: Administrator Login :-

Username:

Password:



Technical Flaws: SQL Injection⁵



Technical Flaws: SQL Injection

Mysql.com Vulnerable To Blind Sql Injection:

- Through a series of sending true/false MySql queries to the website, an attacker determines the answers/vulnerability through error messages received to gain access to the database.
- The attacker then uses this information to exploit the database information to insert malicious code, gaining access to user ID's and passwords, modify website content, even shut down the My Sql Server and bypass login.
- This is one of the most popular web application hacking methods. Can be done with free software and browser extensions/addons.

Technical Flaws: SQL Injection

SQL Injection Environment: Try it!

◦ You will need:

1. **SQL Map** - <http://sqlmap.org/>

Install Tutorial - <http://www.youtube.com/watch?v=LgfC8aTOkaY>

Testing SQL Injection - <http://www.youtube.com/watch?v=-KxgHgYiEcw>

2. **Backtrack 5** - <http://www.backtrack-linux.org/downloads/>

You can use in VM Virtual Box or Vmware

Install Walkthrough - http://www.backtracklinux.org/wiki/index.php/Install_BackTrack_to_Disk

Testing SQL Injection - <http://www.youtube.com/watch?v=OmkxZBSGx98>

MORE CASES/REAL
LIFE EXAMPLES

The Boston Marathon Bombings (A Real Life Incident)

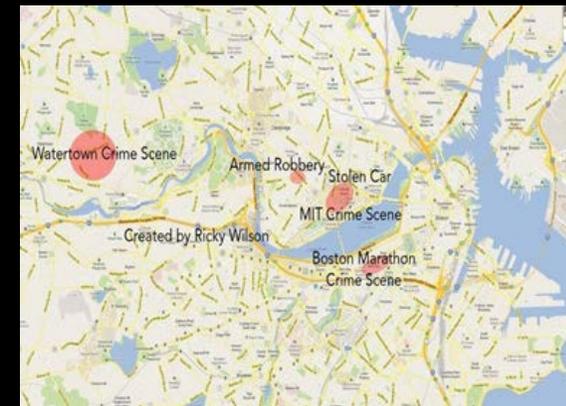
Authorities in Boston bombing helped, hindered by social media

Social media sites change how we send and receive information, real time, and allows responders and officials to communicate with the public to provide instruction and seek help.

How Social Media was used During the Boston Marathon Bombings

Social media sites change how we send and receive information, real time, and allows responders and officials to communicate with the public to provide instruction and seek help.

- Boston PD tweeted residents
- FBI released suspect images and tweeted “Bombing suspect may be driving ...plate 116GC7”.
- JFK Library tweeted “The fire in the building is out.”
- Massachusetts Senator Scott Brown posted statements on Facebook
- U.S. Attorney’s Office District of Massachusetts tweeted information about the case



How Social Media Hindered the Search for the Boston Marathon Bombers

As fake Twitter accounts using the name of the suspect popped up Friday and other tweeps began sharing updates of the pursuit gleaned from police scanners, the department **tweeted** this stern order:

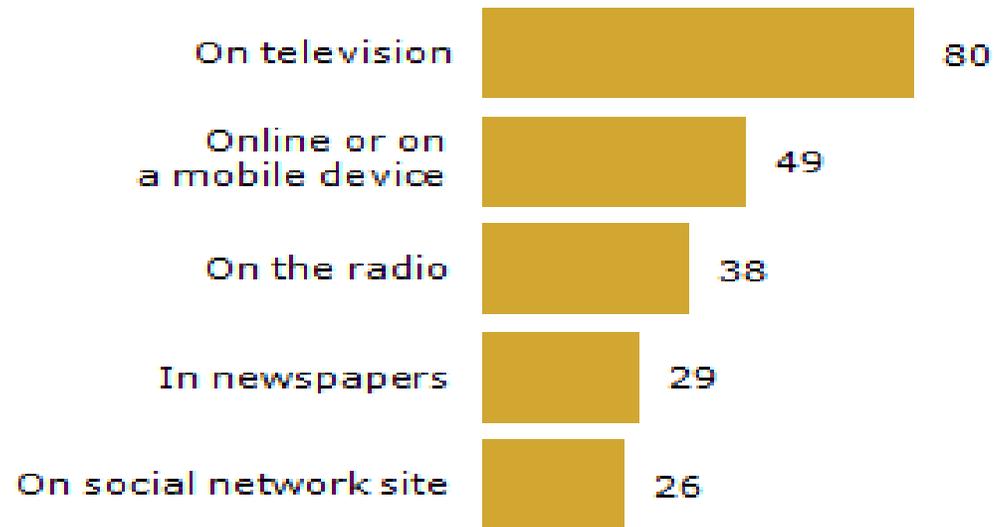
“

#MediaAlert: WARNING: Do Not Compromise Officer Safety by Broadcasting Tactical Positions of Homes Being Searched.

Social Media and the Boston Marathon Bombing

Following the Boston Bombings

Kept up with news and information about the bombings at the Boston Marathon...



PEW RESEARCH CENTER April 18-21, 2013.

*“Following the Boston Marathon bombings, **one quarter** of Americans reportedly looked to Facebook, Twitter and other social networking sites for information, according to The Pew Research Center...”*

-Dina Fine Maron (2013), *The Scientific American*

Privacy Concern



- Police Scanner
- False information that Police received from Twitter posted by Twitter users
- 2 people marked as Terrorists

Aftermath



Public Service Announcement

Prepared by the
Internet Crime Complaint Center (IC3)
April 25, 2013



BEWARE OF POSSIBLE FRAUD ASSOCIATED WITH THE BOSTON MARATHON EXPLOSIONS

The FBI reminds the public there is the potential for fraud in the aftermath of the Boston Marathon bombings. The FBI's Internet Crime Complaint Center has received indications that individuals may be using e-mail and social networking sites to facilitate fraudulent activities.

The FBI is aware of a spam e-mail with the subject line "Boston Marathon Explosion" and similarly themed messages being circulated to lure potential victims to malicious software and exploits. Spam e-mails and Web sites to which they are linked use a wide variety of deceptions to trick a user into taking actions that put the user's computer at risk for infection. Common techniques include links to compromised Web sites and pop-up messages prompting users to download software to view pictures, videos or other files.

Social media is another avenue criminals use to solicit donations. The FBI is aware that an account on a popular social media service using the Boston Marathon name and official logo was created soon after the explosions. Communications from the account represented that \$1 would be donated to the Boston Marathon victims for every communication other users sent to the account. Though the account was suspended by the social media service, others may use similar methods to commit fraud.

In Emergency Situations

- Emergency Requests
 - Companies are not legally required to comply with requests from Law Enforcement
 - Most companies have emergency hotlines to answer these requests
- Twitter
 - Anonymous Tweeter posted tweets threatening to open fire at a New York Theater
 - Tweets from Tweeter
 - “I got 600 people on my hit list and that’s gonna be a mass murder for real”
 - Emergency Request was submitted
 - Twitter rejected the request
 - Did not fall within threat parameters
 - Police subpoena forcing twitter to comply with request and turn over information

SOCIAL MEDIA IN GENERAL

Case Study: Engaging Social Media

Table 1. Overview of disasters in which social media was utilized

Disasters in which social media was used	Details on how social media was utilized in the disasters
The 7/7 Bombings in London	One of the first examples of social media use in a man-made disaster. Newly popular cell phone cameras were widely used. Flickr, a photo sharing site and Wikipedia were used to share news and information. This in turn popularized the ideas of the citizen reporter.
The 2007 San Diego Fires	Twitter was newly popular. Users in and outside the fire zones used Twitter through SMS. Information on safe locations and supplies was aggregated by outside users and used to make mashups with Google Maps. A large TV station relied on Twitter when its website crashed.
Typhoon Ondoy/Ketsana	Twitter was widely used. Online spreadsheets were used to share information on the disaster situation. PayPal was first used for online donations inspiring the Red Cross to adopt the practice. A crisis map was created with Google Maps and was described as "an invaluable resource" by relief workers.
The 2010 Haiti Earthquake	The Ushahidi crisis map platform was widely used, helping to create an ad-hoc 911 system. A total of 12,000 translators were recruited through Facebook, making for a 5 to 10 second turnaround time for incoming SMS messages. The map was used to track cholera outbreaks 6 months after the disaster. The system was widely used by relief organizations.
2010 Yushu Earthquake	A Twitter-clone site called Sina-Weibo was widely used to exchange information after the earthquake. Information is limited because of language limitations with Chinese.

Flickr →

Twitter,
Google
Maps →

Ushahidi
Facebook →

Sina-
Weibo →

Twitter →

Case Study: Engaging Social Media

Sina-Weibo →	2010 Yushu Earthquake	A Twitter-clone site called Sina-Weibo was widely used to exchange information after the earthquake. Information is limited because of language limitations with Chinese.
Twitter →	Super-typhoon Megi	The Philippine Atmospheric Geophysical and Astronomical Services (PAGASA) launched a Twitter account just before the typhoon. Their tweets were broadcasted by conventional mass media. After a month, the organization had 28,000 followers. There are 20 typhoons a year in the Philippines and the organization says it is the most cost-efficient way of making announcements to the public.
Twitter →	2010 Eruptions of Mount Merapi	A community radio station created to respond to an ongoing lava flow began using Twitter to organize. They were able to send 700 volunteers to places that were not reached by government aid. The organization had 35,000 followers and would make requests for help for driving and cooking and receive mass amounts of support from the community. It demonstrates the possibility of reducing dependency on foreign aid for communities.
Twitter →	2010 Canterbury (Christchurch) Earthquake and 2011 June Christchurch earthquake	The government used Twitter to send a coordinated flow of recovery information to residents. An official hashtag keyword was instituted. Misinformation was also spread using Twitter during the disaster. A symposium after the disaster about social media in the disaster discussed creating an "Emergency 2.0 Wiki."
SMS, Social Networks →	Hurricane Irene	The US Federal Emergency Management Association (FEMA) encouraged people to use SMS and social networks to keep in touch with family and friends instead of calling by phone so as not to jam networks.
Twitter →	2011 Virginia Earthquake	Twitter users in New York City and other locations saw tweets about the earthquake, which originated in Virginia state, up to 30 seconds before it was felt, showing that information moves faster through networks than the earthquakes themselves.

Case Study: Engaging Social Media

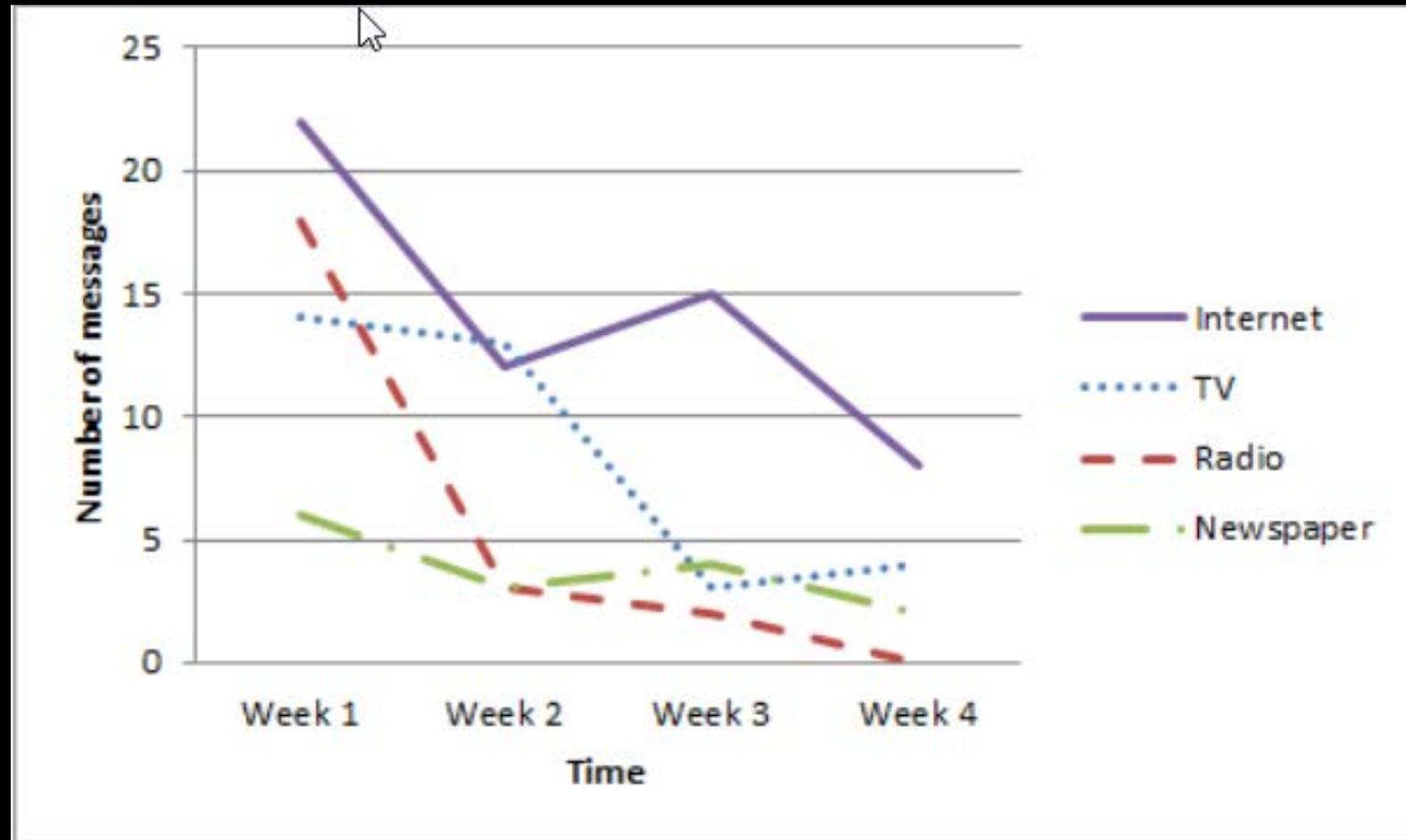
- Witnesses on the island hid, communicating via text messages

- Breivik wore a fake police badge and uniform in the attack – this data was texted out by some there

- People went to Twitter, [Google+](#) & live streaming for news on the story, many saying online news reports were faster than TV



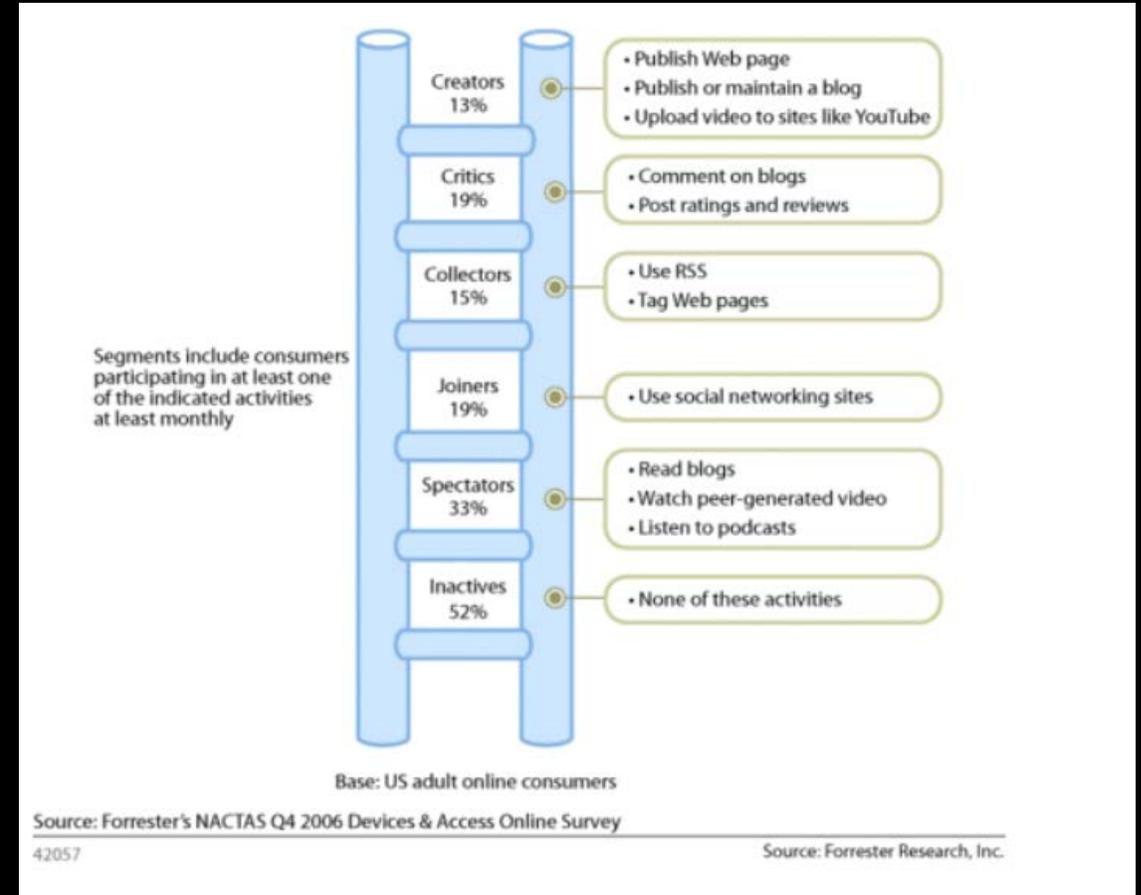
Media outlet utilization
by German participants
in the tracking of E-coli
(EHEC) outbreaks in
2011



SOCIAL MEDIA CHALLENGES

Social Media Challenges

- Government entities require government owned and operated websites that can be created and controlled to guarantee integrity and legitimacy.
- Privately owned social media sites create an environment easily exploited by one individual who may have 50 accounts, thus creating identity issues.
- Creators and Critics, at the top are not an accurate representation of the total population. Consequently, multiple accounts by the same individual can create the illusion that a topic is more widely accepted/represented than it really is.



Social Media Threats

Safe and Reliable Service?

- Social Media remains the top Phishing target.
- Social Media accounted for **36%** of Phishing attacks in 2013
- From 2011-2012 Symantec recorded an **81%** increase in malicious attacks
- **FACT:** YouTube hosts 100's of tutorials on conducting SQL Injection, XSS, Phishing and many other attacks



HOW DO WE
SOLVE THESE
CHALLENGES?

How do we protect
ourselves from these
attacks?

Recommendations: Social Engineering

Phishing Scams – beware social media links or emails asking for passwords claiming to be from the provider. Social media providers never ask for your password.

Impersonation – know your ‘Friends list’ to avoid account hacking and identity theft.

Recommendations: Social Engineering

Clone Phishing – make sure you are navigating to <https://www.facebook.com> and not <http://www.facebook.com> or <http://www.facelook.com>

Don't Be A Victim

Ensure that you see <https://www.facebook.com> and/or the padlock icon before the web address to ensure your connection is encrypted and the site is verified



 <https://www.facebook.com>

Subject: Facebook Account Update

facebook

Dear Facebook user,

In an effort to make your online experience safer and more enjoyable, Facebook will be implementing a new login system that will affect all Facebook users. These changes will offer new features and increased account security.

Before you are able to use the new login system, you will be required to update your account.

Click [here](#) to update your account online now.

If you have any questions, reference our [New User Guide](#).

Thanks,
The Facebook Team

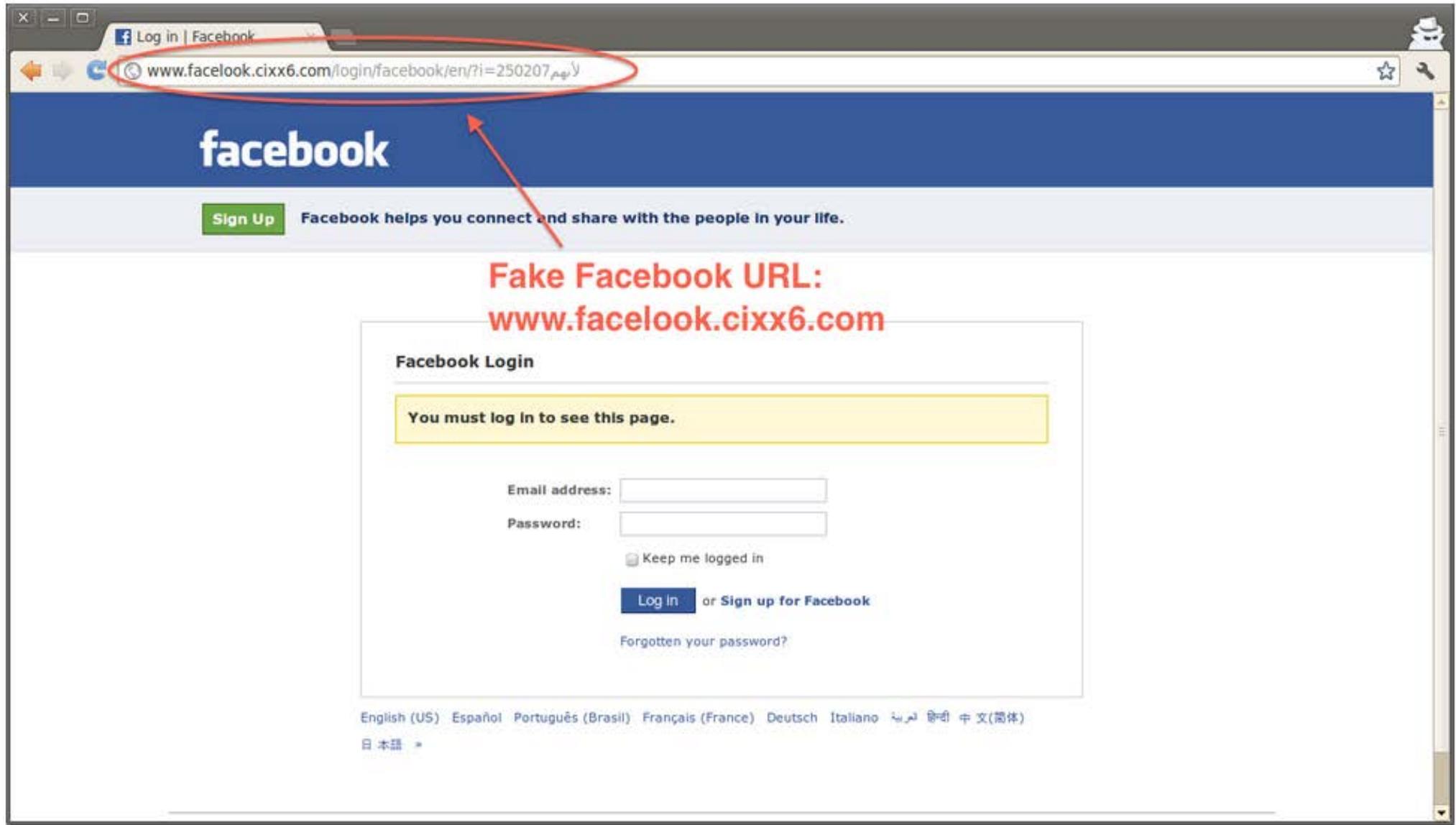
Facebook

Phishing Email

Update your Facebook account

Update

This message was intended for [brock@cs.cmu.edu](#)
Facebook's offices are located at 1601 S. California Ave., Palo Alto, CA 94304.



http://fbaction.net/

Services Writing Reads Facebook It Delicious It Reddit It Tumblr It Press This FriendFeed It Tumblr It bit.ly DiggBar Instapaper
TC TechCrunch TC TechCrunch + Add Ne... Google Reader (613) foursquare Login | Facebook

facebook

Sign Up

Facebook helps you connect and share with the people in your life.

Not
Facebook

Facebook Login

Email:

Password:

Remember me

Login or Sign up for Facebook

[Forgot your password?](#)

Social Media Best Practices (Individual)



- Create, manage Passwords⁶: Use strongest form of password which include very well mixed upper, lower and special characters along with numbers with minimum 12 characters (secure password ex. “Ka1t3\$JakX_8U0s@”).
 - Change passwords periodically.
 - Avoid dictionary-like words and use English characters for non-English language words to get best and hard to guess for hackers⁶.
- Ensure you are always on secured version of social media sites ([https](#)), even when redirected to third party websites, and specially when providing sensitive information to the site.

Social Media Best Practices



- Be wary of free or open Wifi networks where password sniffers could be located, even run from mobile phones.
- Stay proactive rather than reactive. If vendors or partners are asking for any confidential info like credit cards, research and find if they are following PCI-DSS compliances.
- Read social media privacy policies. Do not trust the default settings and adjust your privacy options as desired. Disabling all options and opening one by one as you use is the best way to go.
- Think carefully about who you allow to become your friend and what you share with him.

What are

companies doing to
prevent these
attacks?

Twitter

Fake Twitter emails

Some users may receive fake or suspicious emails that look like they were sent by Twitter. These emails might include malicious attachments or links to spam or phishing websites. Please know that Twitter will never send emails with attachments or request your Twitter password by email.

If you receive a fake email:

1. Forward the email to spoof@twitter.com.
2. Delete the email from your inbox. Don't download any attachments from these emails.

Find out more about Twitter Safety on our [account security page](#).

AOL

What is AOL Mail doing to prevent spoofing?

We updated our [DMARC](#) policy to tell DMARC-compliant email providers like Gmail, Yahoo! Mail, Outlook.com and others (including AOL Mail itself) to reject mail from AOL addresses that is sent from non-AOL servers.

Sending mail on behalf of AOL Mail users from non-AOL servers had been a common and legitimate practice for services like mailing lists and bulk senders. But it also provided the means for spammers to spoof addresses as described above. By switching AOL Mail's policy to "reject," we significantly thwart spammers' ability to spoof AOL addresses. You can read more about AOL Mail's move [here](#).

AOL Safety (From AOL Website)

Top 5 clues to spot an email scam:

- 1. Check the spelling
- 2. Check who signed it
- 3. **DOES THE EMAIL SCREAM AT YOU IN ALL CAPS or have lots of !!!!! at the end?**
- 4. The email has an executable attachment
- 5. The email has a link to a Web site
- **One final word of advice:** Never, ever respond to a spam email. By doing so, you confirm that your email account is active, and you'll likely be flooded with more spam.

Facebook

▼ **How do I report a phishing email?**

If you think you've received a phishing email, please forward this to phish@fb.com.

While we won't reply to every report, we'll use this information to investigate and take action where possible.

More info

[Get help for mobile apps and browsers](#) ▶

Last edited about 2 months ago

Facebook Safety (From Facebook Website)

Think before you click.

Watch out for fake Pages and apps/games.

Don't accept friend requests from people you don't know.

Pick a unique, strong password.

Never give out your login info (ex: email address and password)

Log in at www.facebook.com.

Update your browser.

Run anti-virus software



AMC on Social Media



AMC Headlines

- Tankers escort Thunderbirds to SkyFest
- Snapshot: Jeffrey Earnhardt stops in AFMES
- Snapshot: Jeffrey Earnhardt makes a pitstop at AFMAO
- McConnell medics host Guatemalan air force
- Reserve wing ready to assist with wildland fires
- WASP veteran shows off her flying skills
- Extending the reach: refueling the air-policing mission
- Herschel Walker visits McConnell
- SAPR down day focuses on Duty to Intervene
- Exercise Turbo Distribution: establishing a port in a storm

Air Mobility Command Top Stories

Air Mobility Command Top Stories 01 / 05 next >|



AMC Videos



Inside AMC

Search

search AMC

General Images Video

[View All RSS](#)

AMC Mission



AMC Travel Website

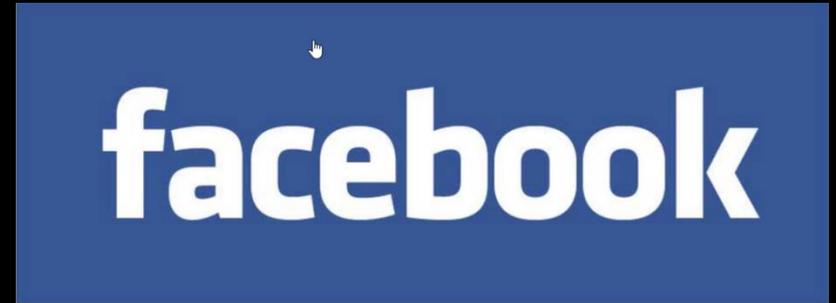


The Mobility Forum

Conclusion

- .Gov .MIL .EDU means something to users and employers
- Social media is only as valuable as its authenticity, integrity, and availability
- Social media interactions are FOIL/FOIA discoverable
- Government sponsored websites can provide these necessary requirements
- Social media is an adjunct to other things

Questions?



References

Enduser content: XSS. (n.d.). *Google+*. Retrieved May 25, 2014, from

- https://lh4.googleusercontent.com/-hSHkgJI2h7Y/UztNLulaW6I/AAAAAAAAAWo/rAVASUyF_C0/w640-h400-p-k/infographic%2B5.png

Freeman, R. (n.d.). New York State Committee on Open Government. *New York State Department of State*. Retrieved May 28, 2014, from <http://www.dos.ny.gov/video/coog.html>

Hellen, P. (2013, October 30). Halloween Edition: Security horror sequels - don't be a victim. *Rapid7*. Retrieved May 31, 2014, from <http://www.rapid7.com/resources/videos/horror-sequels-dont-be-a-victim.jsp>

Home. (n.d.). *Madison County Emergency Management Agency*. Retrieved May 25, 2014, from <http://www.madisoncounty.in.gov/EMA/mcema/Home.html>

Li, C. (2007, April 23). Forrester's new Social Technographics report. *Forrester: Empowered* . Retrieved May 31, 2014, from http://forrester.typepad.com/groundswell/2007/04/forresters_new.html

, M. M. (n.d.). CVE-2008-5711: Facebook Photo Uploader 4 ActiveX Control Buffer Overflow. *Rapid 7*. Retrieved May 31, 2014, from http://www.rapid7.com/db/modules/exploit/windows/browser/facebook_extractiptc

Passeri, P. (2014, January 19). 2013 Cyber Attacks Statistics (Summary). *Hackmageddon.com*. Retrieved May 25, 2014, from <http://hackmageddon.com/2014/01/19/2013-cyber-attacks-statistics-summary/>

References

- Passeri, P. (2014, May 29). 4 Years of Cyber Attacks. *Hackmageddon.com*. Retrieved May 25, 2014, from <http://hackmageddon.com/2014/05/29/4-years-of-cyber-attacks/>
- Peary, B., Shaw, R., & Takeuchi, Y. (2012). Utilization of Social Media in the East Japan earthquake and tsunami and its effectiveness. *Journal of Natural Disaster Science*, 34(1), 3-18. Retrieved May 30, 2014, from http://www.jsnds.org/contents/jnds/34_1_1
- Schimelpfenig, J. (2013, May 1). Social media security best practices . *Rapid7*. Retrieved May 31, 2014, from <http://www.rapid7.com/resources/videos/social-media-security-best-practices.jsp>
- Sreenivas, G. (2013, July 17). 3 Steps to mobile application risk management. *Rapid7*. Retrieved May 31, 2014, from <http://www.rapid7.com/resources/videos/3-steps-to-mobile-application-risk-management.jsp>
- Turla, J. (2012, October 30). Transforming your Android Phone into a Network Pentesting Device. *InfoSec Institute*. Retrieved May 31, 2014, from <http://resources.infosecinstitute.com/android-phone-pentesting/>
- Velsen, L. v., Gemert-Pijnen, J. v., Beaujean, D., Wentzel, J., & Steenberge, J. v. (2012). Should health organizations use Web 2.0 media in times of infectious disease crisis. *Journal of Medical Internet Research*, 14(6). Retrieved May 30, 2014, from <http://www.jmir.org/2012/6/e181/>
- What is Cross Site Scripting and how can you fix it?. (n.d.). *Acunetix*. Retrieved May 30, 2014, from <https://www.acunetix.com/websitesecurity/cross-site-scripting/>

In-Text Citations and External Links

1. [Cookie Vulnerability – XSS Vulnerability](#)
2. [Facebook cookie](#)
3. [Online Social Networks: enhancing user trust through effective controls and identity management](#)
4. [How to Hack Websites Using SQL Injection](#)
5. [SQL Injection Image](#)
6. [Phishing Email Image](#)
7. [Facebook Phishing Image Example](#)
8. [Facebook Phishing Image 2](#)

In-Text Citations and External Links

9. [Exploiting XSS on Facebook](#)
10. [Symantec Security Report](#)
11. [Cross Site Scripting](#)
12. [Top Phishing Targets](#)
13. [Future Proofing Web and Mobile Applications](#)
14. [What is XSS?](#)
15. [How to Fix XSS](#)
16. [Madison County Mass Notification System](#)

All logos are trademarks and property of their respective owners

Technical Flaws: Photo Uploader

Mobile smartphone devices are extremely vulnerable due to rooting and hacking applications available⁵

“dSploit” for rooted Android devices makes pen testing and network password sniffing easier on wireless networks.

Three Steps to Mobile Application Risk Management

- We are concerned with the last example in this video, about 1:50 into the talk.

