Social Networks: Minimizing the risks of the new frontier

Parag Deodhar, CA, CISA, CFE

Chief Risk Officer – Bharti AXA General Insurance

AGENDA

Weighing the value of social networking with its risks

How spam, application vulnerabilities and malware are being used to infiltrate social networking sites

Specific vulnerabilities to watch out for with social networking

User education, policies and enforcement

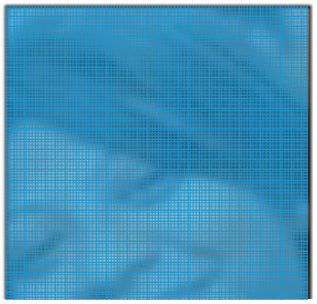
The ease of phishing and what to do about it

Value @ Risk

Dumped on FB, IIM-B student hangs herself

TIMES NEWS NETWORK

Bangalore: An MBA student hanged herself in her hostel room in the Indian Institute of Management, Bangalore, on Monday evening. Mali-



THE TIMES OF INDIA, BANGALORE
TUESDAY, SEPTEMBER 20, 2011

Investigation officers said she found out from FB that her boyfriend had dumped her.

Police said the couple had had an argument, which resulted in the breakup.

Later, her boyfriend had left a post on FB saying, "Feeling super cool today. Dumped my new ex-girlfriend. Happy independence day."

Evolution of communication on internet

- Bulletin Boards
- Web based e-mails
- Instant Messaging
- P2P
- Blogs & Forums
- Social Networking
- Instant Status Updates
- Status Updates with Geo Tagging

Social networking is something that is in absolute harmony with the principles of internet – Connecting People

Social Network Accounts Outnumber People On Earth

In-Stat SILICON - Apr 3 - There are now more social-networking accounts than there are people in the world, according to figures from In-Stat. The market analyst reports that there were ~10 billion social-networking and online-world accounts in 2010 and that ~4.5 billion of these are active.

Only way to communicate

"You don't blog, you don't Twitter, you have no RSS feed, you're not on Facebook...and you wonder why you can't communicate?!"

Status update: Social Networks

- Whether you 

or not social networks have taken over our lives – both professional and personal.
  - Corporates use it for marketing and communication
  - Schools and Colleges use it to communicate with students and parents
  - Individuals use it for professional networking
  - Personal use – sharing photos and videos, opinions, status updates, games, chat…

22 Jan 2010, Astronaut T. J. Creamer posted the first unassisted update to his Twitter account from the International Space Station marking the extension of the Internet into space

Importance to business

- Sales and Marketing of products & services
- Brand building
- Reach out to large customer base. Very high conversion of prospects to customers.
- Immediate feedback and comments, helping the business to make quick adjustments
- Connected to the customer
- Employee hiring

Of the Fortune 100, 65% have active Twitter accounts, 54% have Facebook fan pages, 50% have YouTube video channels and 33% have corporate blogs

Weighing the value of social networking with its risks

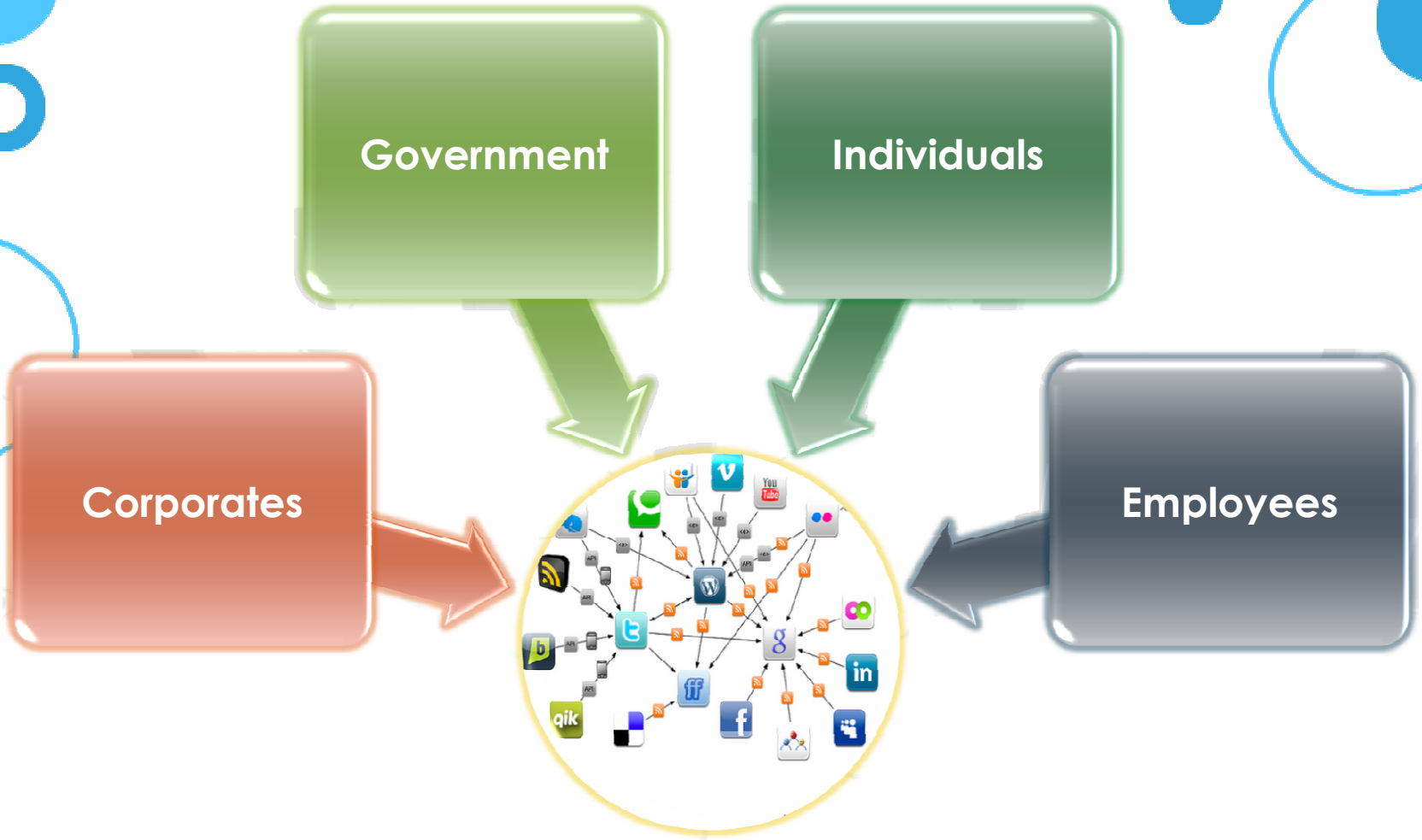
BENEFITS

- ✓ Always connected
- ✓ Great way to find new contacts.
- ✓ Database of prospective clients
- ✓ Accessibility to a wide range of information
- ✓ Service industry – Means to connect with customers

RISKS

- × Spam
- × Application flaws leading to loss of your information
- × Inappropriate usage – posting objectionable content
- × Hate Crime
- × Identity Theft

Who is @ Risk



Government @ Risk

LIVE BBC NEWS CHANNEL

Israeli military 'unfriends' soldier after Facebook leak

The Israeli military cancelled a planned raid on a Palestinian village after one of its soldiers posted details of the operation on Facebook.

The unnamed soldier revealed the time and place of the raid and the name of his unit on the social networking site.

He said on his status update that his unit planned a "clean up" raid.

An IDF poster warns against loose talk on social networking sites

The soldier was court-martialled and sentenced to 10 days in prison. He was also ousted from his battalion and relieved of combat duties.

"On Wednesday we clean up Qatanah, and on Thursday, God willing, we come home," the soldier wrote on his Facebook page. Qatanah is a village in the West Bank near Ramallah.

FROM OTHER NEWS SITES

- Reuters UK Cosmopolitan Dubai was perfect spot for Hamas killing - 7 hr
- New Zealand Herald Israel raid calle after soldier's Facebook slip - 11 hr
- Telegraph Israeli raid details on Facebook - 27 hrs ago
- MSNBC via MSN Money Israeli raid c off after Facebook slip - 37 hrs ago
- France24 Israel aborts raid after so posts details on Facebook - 40 hrs
- About these results

TOP MIDDLE EAST STORIES

Government @ Risk

UK riots: Arrests over Facebook 'incitement' to more violence

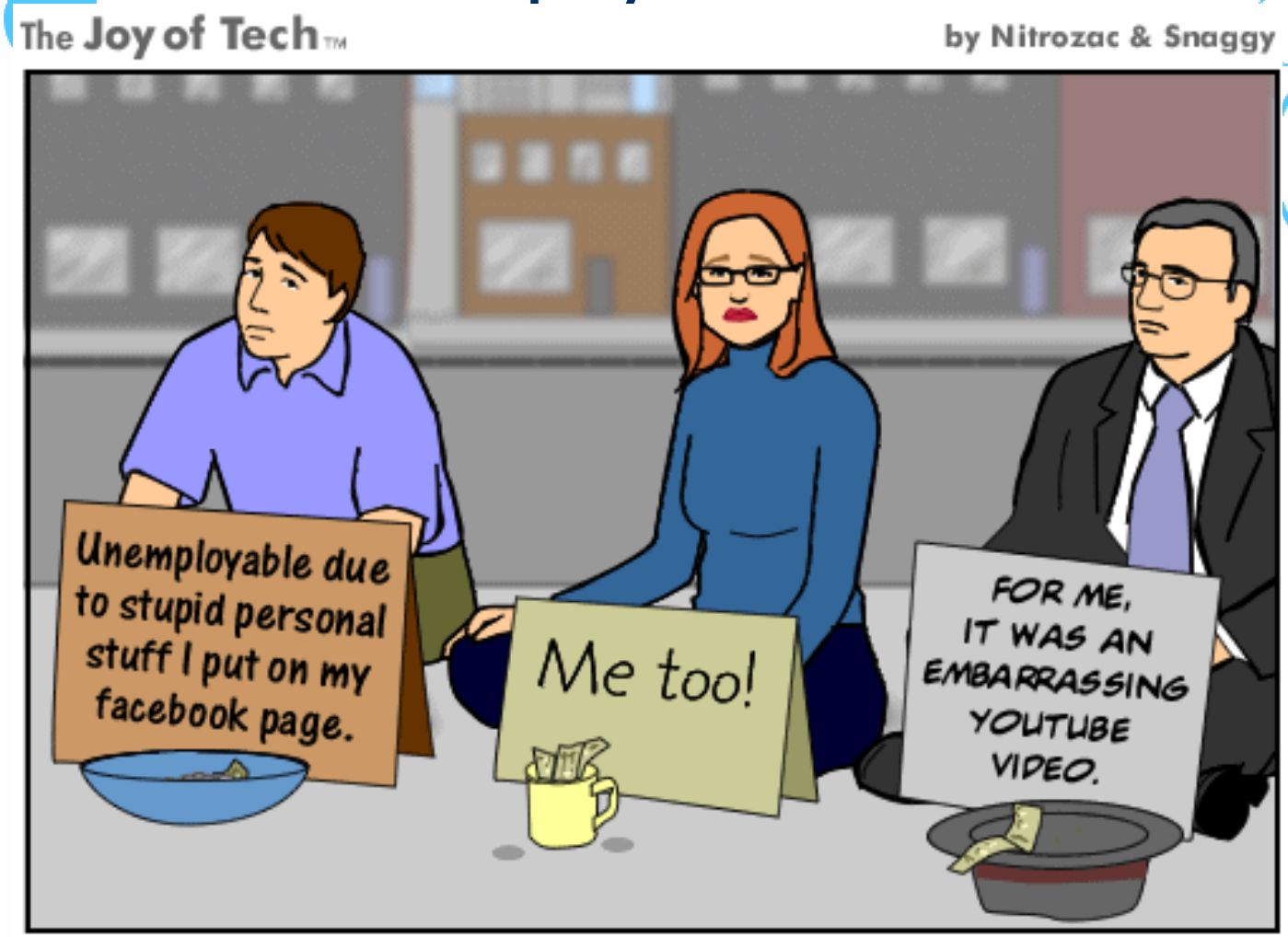
At least 11 people have been arrested across the UK after allegedly trying to use social media sites such as Facebook to incite riots.

Riot policemen in front of a burning building in Croydon on Monday night: police have warned Facebook users against attempting to incite any further violence (Picture: AFP/Getty)

Facebook, Twitter, RIM Meet For Riot Talks With U.K. Government

JILL LAWLESS | 08/25/11 12:34 PM ET | AP

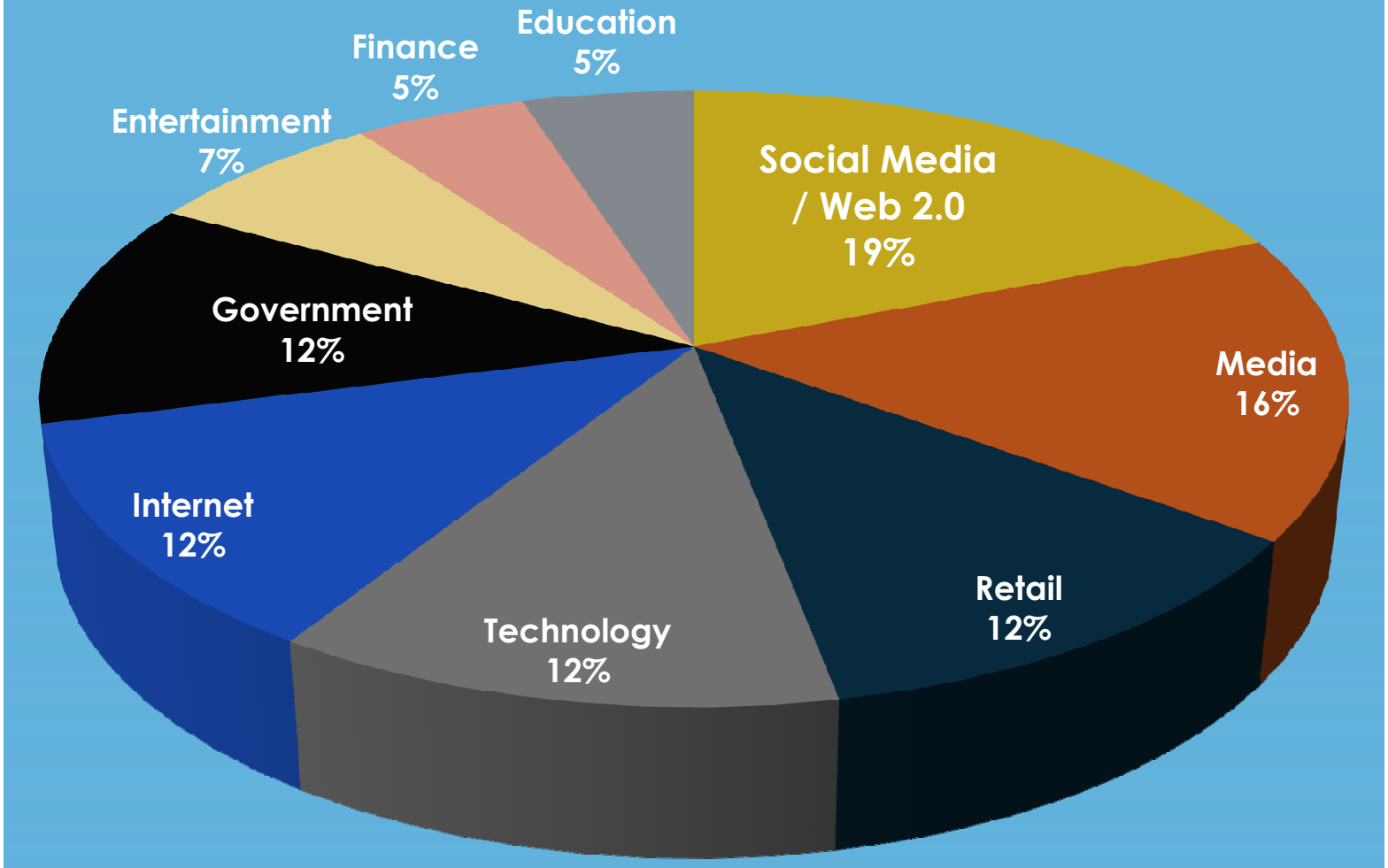
Employees @ Risk



Signs of the social networking times.

Nothing EVER goes away once it is posted online!

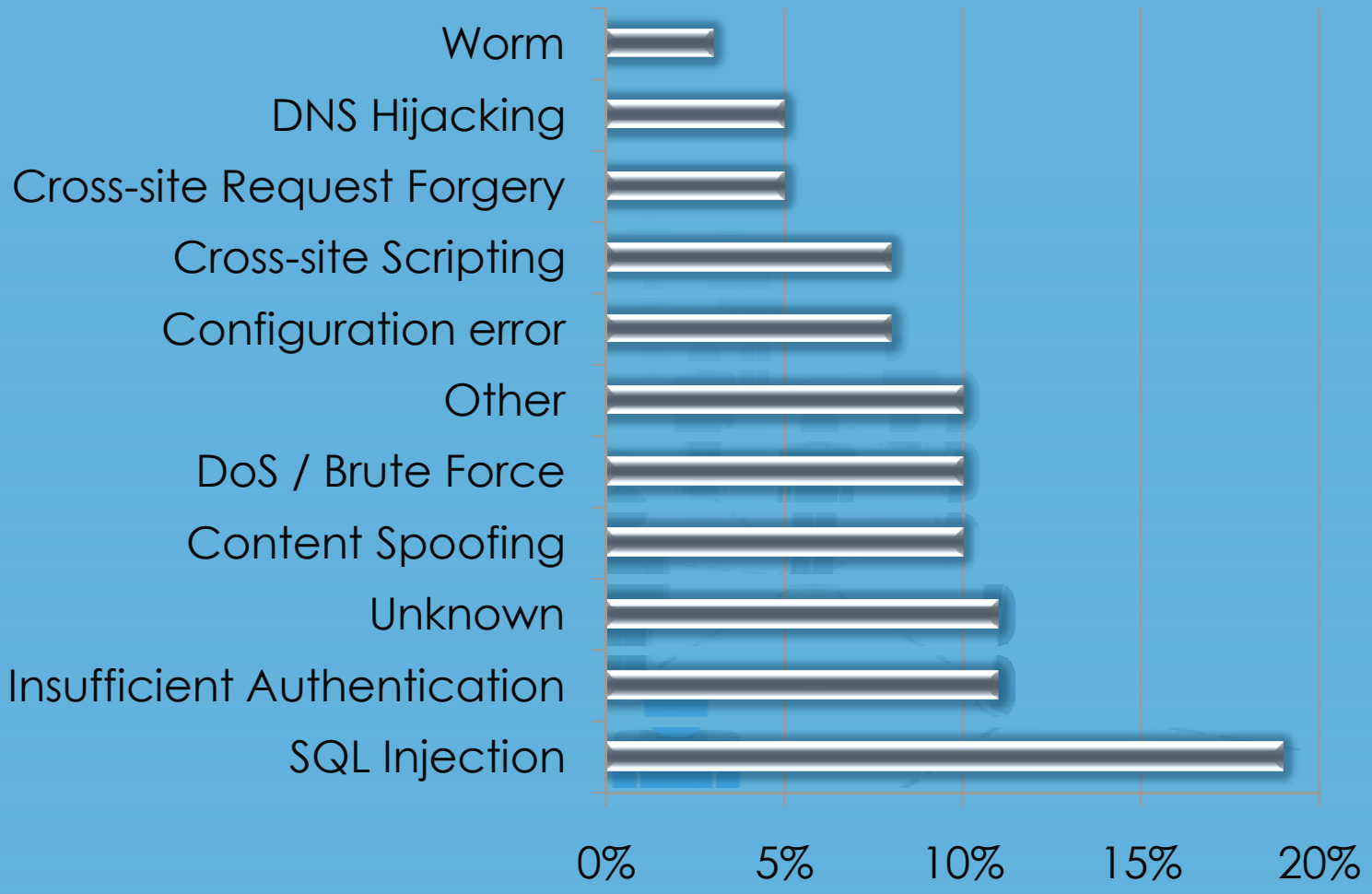
Hacking Trends: Targets



Social media / Web 2.0 sites are the biggest targets for the hackers.

Source: Web Application Security Consortium (WASC)

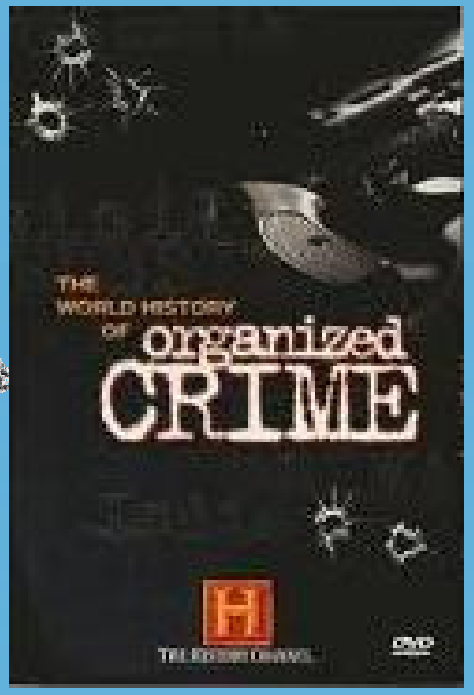
Trends: Threat Vectors



SQL injection is the most common threat vector used against web pages, content spoofing and XSS are also prominent- Social networks act as a good fodder for all three.

Source: Web Application Security Consortium (WASC)

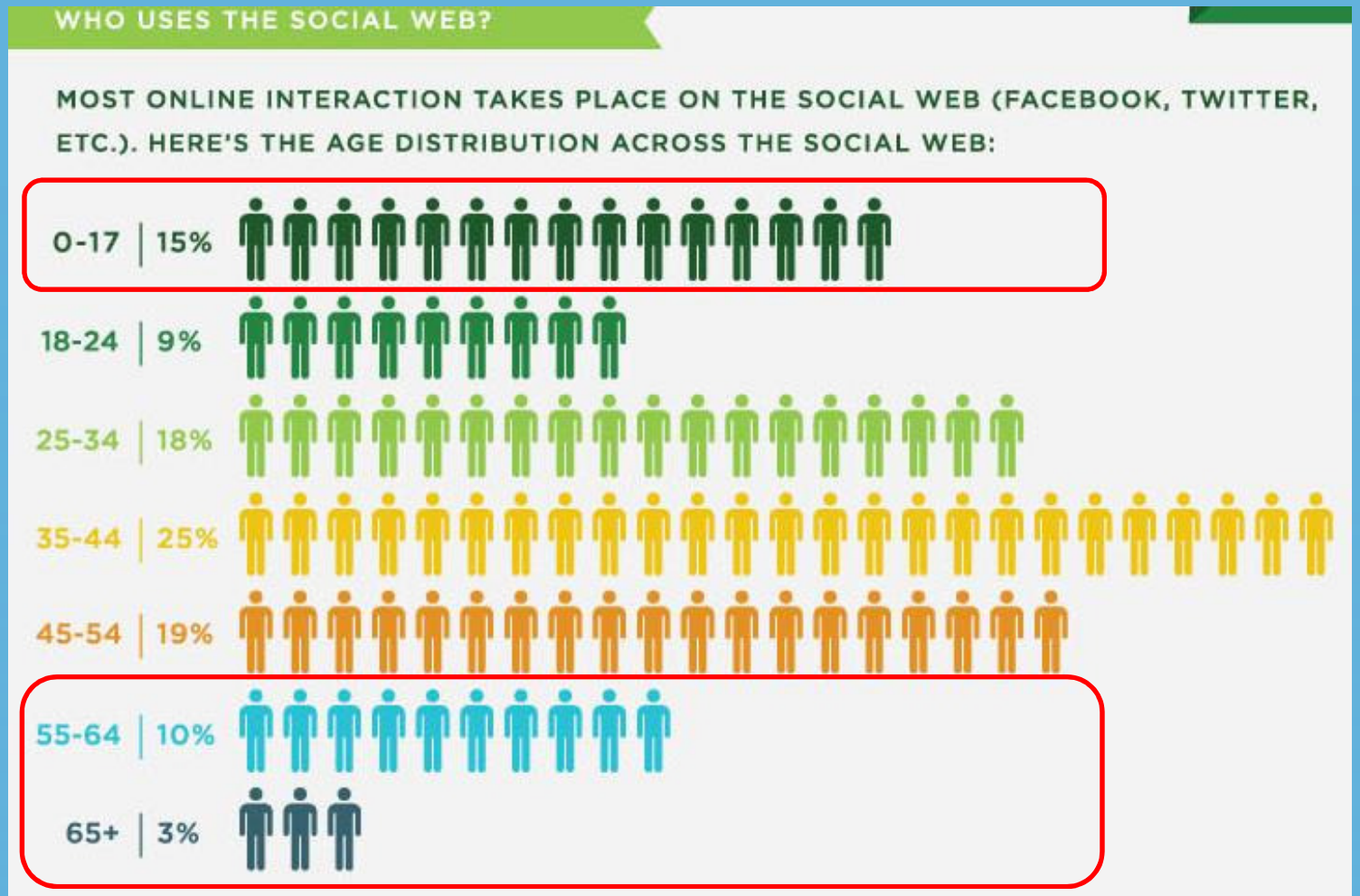
Trends



Hobby/ showing off

Organized crime

Trends



Facebook now allows to add your unborn baby to your list of family members via the "Expected: Child" option on Facebook profiles. Apparently too many parents were creating "illegal" fake profiles for their yet unhatched offspring — setting their fake babies' ages to 13 instead of negative.

Corporates @ Risk

- Data Leakage – Malware, Spyware, Phishing
- Data Loss – Data corruption
- External Attacks – Spam, Virus bringing down network, servers
- Inappropriate usage – objectionable material
- System overload from the heavy use of blogging and social networking sites, with implications for service availability andnon-productive activities
- Reputation loss – Employees, Customers can easily post complaints over social media
- Legal liabilities from defamatory blog postings by employees leading to reputational damage

MALWARE

- The Koobface worm and its associated botnet have gained notoriety in security circles for its longevity and history of targeting social networking sites.
- First surfacing in 2008 within MySpace and Facebook, the worm resurfaced in early 2009, this time targeting Twitter users.
- Message directs to a third-party website, where they are prompted to download what is purported to be an update of the Adobe Flash player.
- 11/10/2009 - As part of a new Koobface attack, links to Google Reader URLs controlled by cyber-criminals are being spammed by Koobface onto social network sites, including Facebook and MySpace.
- Koobface ultimately attempts, upon successful infection, to gather sensitive information from the victims such as credit card numbers.

MALWARE EXAMPLE

Shortened URLs

- The very concept of shortened URLs is a problem as we don't know the actual link.

http://www.hacker.com/badsite?%20attack-your-pc.html

is now

http://bit.ly/aaI9KV

- Takes you to a page that can use malware to infect your PC.
- Can be used as a Phishing bait
- Spam filters or malware scanners can be easily bypassed by using the shortened URLs as camouflage.

Corporates @ Risk

Lost Productivity

- Employers who allow access to Facebook at work lose 1.5% of employee productivity
- 77% of employees who have a Facebook account admit to using it at work; 87% of them admit having no business purpose for doing so.
- Social networking sites can be accessed through a computer or a mobile application (i.e., BlackBerry or iPhone)

You @ Risk

- Privacy
- Steal your money / assets-
  Malware, Spyware, Phishing, Geo-tagging
- Trick your friends and family into supplying personal data, money - **Nigerian scam**
- Identity theft
- Use your accounts to spread spam, malware etc.
- Blackmail – information / photographs,
- Divorce lawyers
- **Time!!!**

You @ Risk

What you share directly

- Your email address(As your login credentials)
- Likes/dislikes
- Regular updates about your day to day doing
- Pictures
- Your trips and plans
- Your relationship status
- Personal Details with third party application like Farmville, mafia wars

What you share indirectly

- Answers to your secret questions of other accounts(emails etc)
- Your where about`s
- People related / linked to you (via photo tagging and linked)
- Travel likes
- Your picture shows way your possessions
- Home address
- Your attitude and way of thinking

You @ Risk

The Register®

Hardware Software **Music & Media** Networks Security Public Sector Business Science

Burglars used social network status updates to select victims

I'm away from home PleaseRobMe.com

By **John Leyden** • **Get more from this author**

Posted in Music and Media, 13th September 2010 12:32 GMT

Free whitepaper – The Register Guide to Enterprise Virtualization

US police reckon a band of burglars used social network status updates to select victims.

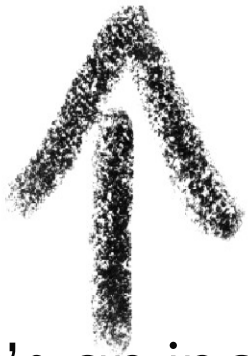
The alleged thieves carried out an estimated 50 burglaries in and around Nashua, New Hampshire, after gaining intelligence on properties that had been left vacant from status updates on social networking sites, such as Facebook.

www.theregister.co.uk/2010/09/13/social_network_burglary_gang/

SPAM

57%

of social networking users report being hit by spam via the services



That's an increase of

70.6%

from a year ago

You @ Risk

PHISHING

- Banks are not the only companies to fall prey to phishing attacks.
- Not uncommon to have websites that mimics the original
- Can be a huge threat, as the number of users keep increasing day by day.
- Very simple modus operandi- Sends you a bogus link, asks you to click on the same, once clicked asks you to enter your credentials and you are compromised

PERSONAL FINANCE FRUGAL LIVING CAREER MORE

Phishing Scams Continue to Plague Social Media Sites

by Adam Baker on 13 October 2009

Social Media is going through an unprecedented explosion in popularity right now. Don't believe me? See for yourself. There are no signs this trend is going to slow anytime soon.

theguardian

News | Sport | Comment | Culture | Business | Money | Life & style

News › Technology › Facebook

Facebook hit by phishing attack

Phishing scam that aims to steal login details hits Facebook

Charles Arthur, guardian.co.uk, Article history

A scam that tries to steal people's Facebook password details – using a website that mimics Facebook's login page – is spreading rapidly through the social networking site.

The scam's emergence comes as a report shows that Facebook was the seventh most popular target of such "phishing" scams in March – although it is some distance behind PayPal and eBay, the two most popular targets, and banks such as Bank of America, HSBC and Alliance Bank.

PHISHING EXAMPLE

facebook

Facebook sent you a message.

Facebook Security November 19, 2010 at 4:24am

Subject: [redacted]

Your account will be deactivated immediately.
Because someone has reported your actions.
Maybe you have written content that is abusiveOr upload a picture that can be insulting or harmful to other users.
You must confirm your account, to stop the warning deactivated on your account.

to suspension of your account, please click the link below:
http://apps.facebook.com/account-suspend/

We provide 1x24 hours to re-confirm your facebook account.
If not, we will block your account for the benefit of other users.

Facebook™ Game Network inc
phone:(650.543.4800) fax:(650.543.4801)

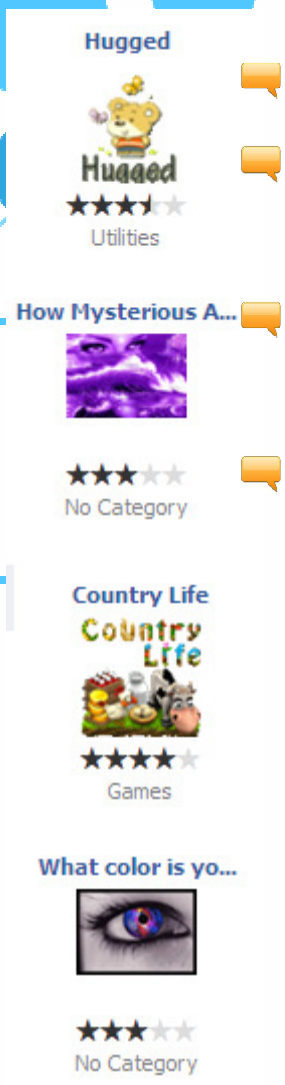
copyright © 2010 Facebook, inc.. All right reserved.

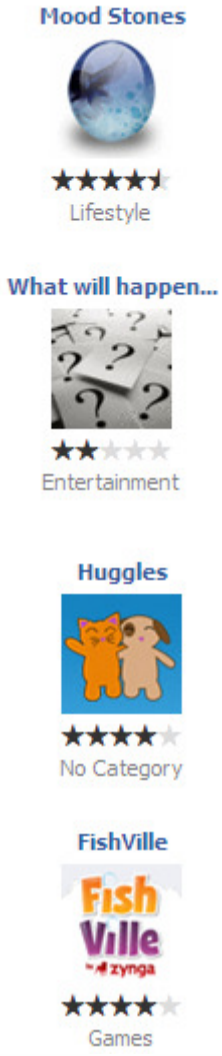
891 111 003 802 1166 100 00

To reply to this message, follow the link below:
http://www.facebook.com/n/?inbox%2Freadmessage.php&t=1697586485064&mid=34f6ca9G4155c87eG16ac6d9G0&n_m=bbonn%40sympatico.ca

3rd Party Applications

- Games, quizzes, cutesie stuff
- Untested by social network – anyone can write one
- No Terms and Conditions – you either allow or you don't
- Installation gives the developers rights to look at your profile and overrides your privacy settings!

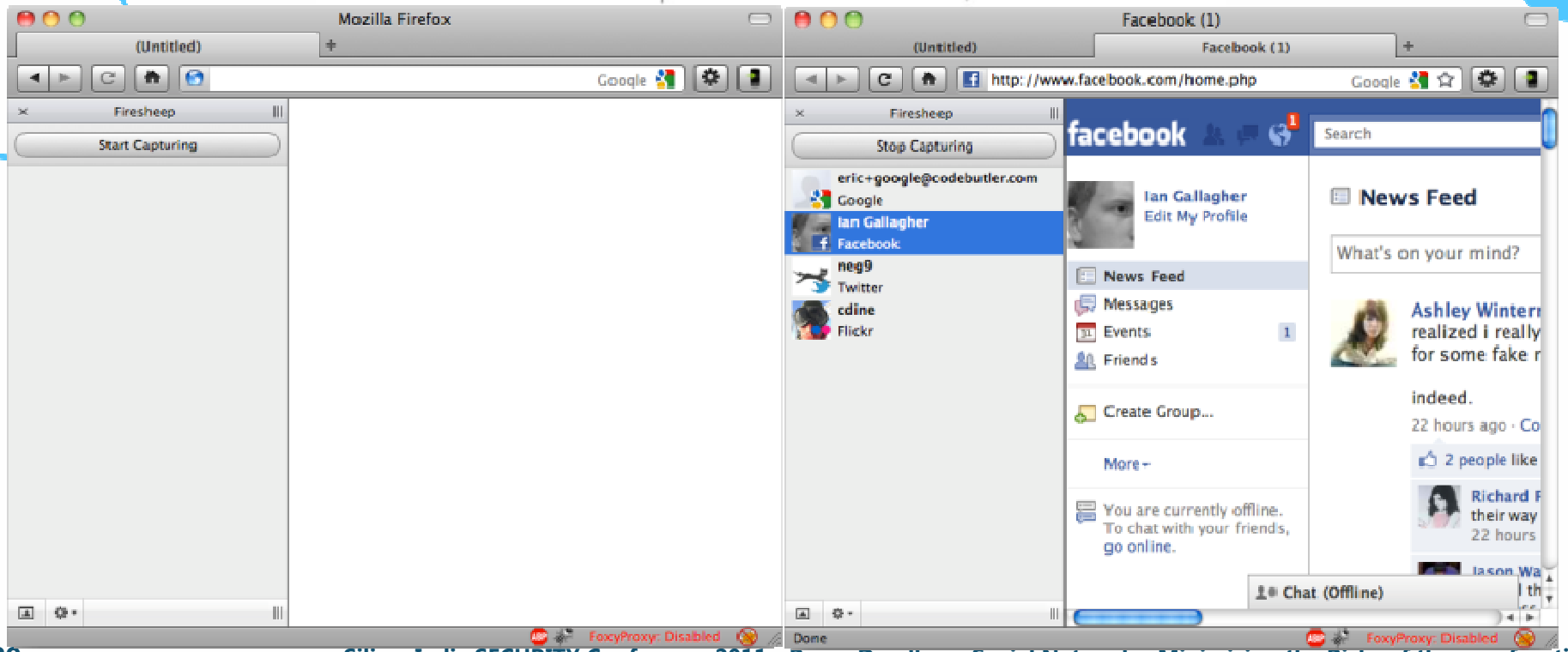




Mobile Social Networking: SIDEJACKING

Firesheep In Wolves' Clothing: Extension Lets You Hack Into Twitter, Facebook Accounts Easily

EVELYN RUSLI | posted on October 24th, 2010 | Comments



CLICKJACKING

- **Technique used by attackers to trick users into clicking on links or buttons that are hidden from view.**
- Security weakness in web browsers that allows web pages to be layered and hidden from view.
- You think you are clicking on a standard button, like the PLAY button on an enticing video, but you are really clicking on a hidden link.
- Since you can't see the clickjacker's hidden link, you have no idea what you're really doing. You could be downloading malware or giving away information without realizing it.
- One form of clickjacking is to hide a LIKE button underneath a dummy button – "Likejacking".

NIGERIAN SCAM

- At about 8 p.m. Bryan Rutberg's daughter ran into his bedroom and asked why he'd changed his status to: "BRYAN IS IN URGENT NEED OF HELP!!!“
- He realized his Facebook account had been hacked.
- Within minutes, his cell phone was ringing non-stop, with concerned friends calling to offer help.
- Many had received an e-mail with the story that Rutberg had been robbed at gunpoint while traveling in the United Kingdom, and needed money to get home. One even sent $1,200 to a Western Union branch in London.
- He was locked out of his own account - criminals had changed his login credentials so he couldn't access his own Facebook page. That meant he couldn't remove the dire status message.
- He tried to use his wife's account to put a message on his "wall" indicating he was fine, but the scammer had "de-friended," his wife, so that didn't work.

Children @ Risk

Cyber bullies

Both children and adults may use the Internet to harass or intimidate other children.

File-share Abuse

Unauthorized sharing of music, video, and other files may be illegal, and download malicious software.

Disturbing Content

If kids explore unsupervised, they could stumble upon images or information you may not want them exposed to.

Predators

These people use the Internet to trick children into meeting with them in person.

Invasion of Privacy

If kids fill out online forms, they may share information you don't want strangers to have about them or your family.

HOW TO BE SOCIALLY CORRECT

Controls @ Corporates

- Deploying technology to block, control and monitor usage
- Revising and updating organisational policies to include acceptable use of social networking and blogging sites
- Managing the risk of marketing initiatives that are using blogging and social networking in order to prevent brand damage
- Brand protection services to prevent brand damage
- Educating end users about blogging and social networking to reduce business impact.

Controls @ Corporates

Risks	Controls
Malware, Phishing, Spyware, Keyloggers etc.	Anti-Virus / Anti-Malware / Endpoint Protection
Dynamic Content	Real time Content Filtering
SSL Threats	SSL Decryption
Productivity loss	URL / Web filtering
Mobile access	Enterprise policies

Controls @ Corporates – Pen test

- Fake employee profile created of very attractive 28 year old female based on social reconnaissance of 1402 employees 906 of which used facebook. Target employees were were males between the ages of 20 and 40. Populated the profile with information about experiences at work by using combined stories collected from real employee facebook profiles.
- Joined target co's facebook group. Made 100s of friends easily - Including managers, executives, secretaries, interns, and even contractors.
- Began chatting - conversations were based on work related issues collected from legitimate employee profiles.
- Posted our specially crafted link on facebook profile - "Omigawd have you seen this I think we got hacked!"
- Fake web page was an alert that warned users that their accounts may have been compromised and that they should verify their credentials by entering them into the form provided. People started clicking on the link and verifying their credentials. These were submitted to us.
- Credentials used to access the web-vpn which in turn gave us access to the network. Credentials also allowed access to majority of systems on the network including the Active Directory server, the mainframe, pump control systems, the checkpoint firewall console, etc.
- It was game over, the Facebook hack worked yet again.

Control yourself

- KNOW THE RULES - check your organization's policy on social networking
- USE SECURE PASSWORDS
- CHECK THE DEFAULT PRIVACY & SECURITY SETTINGS - don't providing personal information by default
- BE PICTURE PRUDENT - think before posting images that might cause embarrassment
- YOU NEVER KNOW WHO'S WATCHING - assume everyone can read your posts, including hackers!
- SECURE YOUR COMPUTERS - use up-to-date security software and firewalls
- THINK BEFORE YOU CLICK - if the email looks dodgy it probably is
- STRANGER DANGER - beware of unsolicited invitations from spammers
- SUPERVISE – Monitor kids access

Remember the fundamental theory – Nothing comes for free and nobody likes you that much!!!

CONCLUSION

- ITS EASIER TO SOLVE A PROBLEM ONCE WE ACCEPT IT
- SOCIAL NETWORKS ARE PART OF OUR LIVES – LETS ACCEPT THE FACT
- IT'S A DOUBLE EDGED SWORD – HAS BENEFITS AS WELL AS RISKS
- USE SOCIAL NETWORKING EFFECTIVELY AND POSITIVELY TO ESTABLISH NEW RELATIONSHIPS, STRENGTHEN EXISTING ONES, INNOVATE, LEARN, COLLABORATE, AND HAVE FUN.
- BUT BEWARE OF THE RISKS SO YOU CAN DO YOUR BEST TO STEER CLEAR OF THEM
- **AND THINK BEFORE YOU CLICK!!!**

CREDITS

- Research: Visveshwar Rama – Bharti AXA
- Various websites and media
- Various security technology product and services companies.
- Social Media websites
- Addicts of social media

THANK YOU!!!