Internet Security Issues

Robert M. Slade, MS, CISSP
rmslade@shaw.ca, rslade@vcn.bc.ca, rslade@computercrime.org

http://victoria.tc.ca/techrev/mnbksccd.htm
http://victoria.tc.ca/techrev/secmarks.htm
http://www.infosecbc.org/links
http://blog.isc2.org/isc2_blog/training
http://www.flickr.com/photos/rslade/
http://www.linkedin.com/in/rslade
http://www.facebook.com/rslade
http://twitter.com/rslade

Internet Security Issues

(Twitter version)

Sec study books http://m6dl3.tk
http://n1o0h.tk
terms http://svgav.tk
URLs http://relnn.tk
commented http://8znon.tk
blog http://xf5d2.tk

Internet Security Issues

- Hacking
- Malware
- Disclosure
- Misinformation
- Infrastructure
- Spyware
- Unsafe sites
- Phishing
- Botnets
- E-Commerce
- Spam
- Baloney
- Identity theft
- Cyberstalking
- Weirdos
- Hijacking
- Child Porn
- Chain letters
- Misdirection
- Fast-flux
- etc
- etc
- Here Be Dragons
- ...

Internet Security Issues
Confidentiality

- Too much information on social nets?
  - About you?
  - About office/company?
  - About others?

Internet Security Issues
Confidentiality

- About you?
  - Name
  - Address
  - Phone
    - cell, pager, email
  - Company
  - Pictures
  - Family
  - Friends
  - Musical preferences
  - Religious views
  - Sexual orientation

Internet Security Issues
Confidentiality

- Social media site protection
- Does “private” mean private?
  - Or private to you and **all** your friends?
- Does “deleted” mean gone?
  - Or just hidden
  - Or now belongs to the site?

- Did you read the agreement?
  - Or just sign it, unread?

Internet Security Issues Confidentiality

- “You keep on using that word “private.” I do not think it means what you think it means.”
  - The (Private) Princess Bride

Internet Security Issues
Confidentiality

- Company/office?
- Social engineering material

Internet Security Issues
Confidentiality

- Gossip about friends?
- Tag them on pictures?

Internet Security Issues
Confidentiality

- Agregate over time?
- Aggregate over many posters?
- Aggregate over systems?

Internet Security Issues
Integrity

- Research?
  - Twitter
    - Kelowna fires
    - Conficker

(4) #conficker - Twitter Search - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://search.twitter.com/search?max_id=1440978588&page=77&q=%23conficker

AltVsta Amzn wethr NVDPL SecrTm Robmks zSqd Dwnld vid SecSIG c: isc2 intr vwms cnvlib isc2blog

gobears1001: hahaha - **#conficker** internet test: http://has.conficker.destroyedtheinternetyet.com/

1 day ago from *web* · Reply · View Tweet

elephantattack: RT jenn Retweeting @lolunix: RT @fscker: http://has.conficker.destroyedtheinternetyet.com/ **#conficker**

1 day ago from *Power Twitter* · Reply · View Tweet

wildbill: RT @KevinBlalock: RT @jenn: Retweeting @lolunix: RT @fscker: http://has.conficker.destroyedtheinternetyet.com/ **#conficker**

1 day ago from *DestroyTwitter* · Reply · View Tweet

KevinBlalock: RT @jenn: Retweeting @lolunix: RT @fscker: http://has.conficker.destroyedtheinternetyet.com/ **#conficker**

1 day ago from *TweetDeck* · Reply · View Tweet

jenn: Retweeting @lolunix: RT @fscker: http://has.conficker.destroyedtheinternetyet.com/ **#conficker**

1 day ago from *twhirl* · Reply · View Tweet

ChaseWilson: RT @fscker: http://has.conficker.destroyedtheinternetyet.com/ **#conficker** (via @lolunix)

1 day ago from *Tweetie* · Reply · View Tweet

Raceday11: @luv70s oh not worried! Can't sleep so though we would hunt **#Conficker** down. He's an hour and 40 minutes late!

1 day ago from *TwitterFon* · Reply · View Tweet · Show Conversation

- AT&T
- Biz Stone
- G-20

Nifty queries:

- cool filter:links
- "is down"
- movie :)
- "happy hour" near:SF
- #haiku
- "listening to"
- love OR hate
- flight :(

Done

Twitter

- Popular
- Available (maybe)
- Up-to-the-minute
- Unmoderated
- Searching/trending
  - March 31st, 2009, ~8:30 pm PDT, "#conficker" #2 search term
    - ("American Idol" #1)

Wikipedia

- http://en.wikipedia.org/wiki/Computer_virus
  - "This article may contain *original research* or unverified claims."
  - virus ≠ malware, virus = malware, virus ≠ malware
  - some useful, some misleading, some erroneous
  - how do you tell?

(4) #conficker - Twitter Search - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://search.twitter.com/search?max_id=1440978588&page=77&q=%23conficker

AltVsta Amzn wethr NVDPL SecrTm Robmks z5qd Dwnld vid SecSIG c: isc2 intr vwms cnvlib isc2blog

gobears1001: hahaha - **#conficker** internet test: http://has.conficker.destroyedtheinternetyet.com/

1 day ago from *web* · Reply · View Tweet

elephantattack: RT jenn Retweeting @lolunix: RT @fscker: http://has.conficker.destroyedtheinternetyet.com/ **#conficker**

1 day ago from *Power Twitter* · Reply · View Tweet

wildbill: RT @KevinBlalock: RT @jenn: Retweeting @lolunix: RT @fscker: http://has.conficker.destroyedtheinternetyet.com/ **#conficker**

1 day ago from *DestroyTwitter* · Reply · View Tweet

KevinBlalock: RT @jenn: Retweeting @lolunix: RT @fscker: http://has.conficker.destroyedtheinternetyet.com/ **#conficker**

1 day ago from *TweetDeck* · Reply · View Tweet

jenn: Retweeting @lolunix: RT @fscker: http://has.conficker.destroyedtheinternetyet.com/ **#conficker**

1 day ago from *twhirl* · Reply · View Tweet

ChaseWilson: RT @fscker: http://has.conficker.destroyedtheinternetyet.com/ **#conficker** (via @lolunix)

1 day ago from *Tweetie* · Reply · View Tweet

Raceday11: @luv70s oh not worried! Can't sleep so though we would hunt **#Conficker** down. He's an hour and 40 minutes late!

1 day ago from *TwitterFon* · Reply · View Tweet · Show Conversation

- AT&T
- Biz Stone
- G-20

Nifty queries:

- cool filter:links
- "is down"
- movie :)
- "happy hour" near:SF
- #haiku
- "listening to"
- love OR hate
- flight :(

Duplications

Done

(2) #conficker - Twitter Search - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://search.twitter.com/search?q=%23conficker

AltVsta Amzn wethr NVDPL SecrTm Robmks zSqd Dwnld vid SecSIG c: isc2 intr vwms cnvlib isc2blog

oh_danny_boy: I'm like the conficker virus. I get into your system and you never know when I'll go off... **#conficker**

about 1 hour ago from *TweetDeck* · Reply · View Tweet

geekgrrl: RT @singe: NMAP 4.85BETA7 released with better detection thanks to Renaud Deraisson from Nessus. http://insecure.org/**#conficker**

about 1 hour ago from *Spaz* · Reply · View Tweet

singe: NMAP 4.85BETA7 released with better detection thanks to Renaud Deraisson from Nessus. http://insecure.org/**#conficker**

about 1 hour ago from *web* · Reply · View Tweet

PeyloW: What happened with **#conficker**? I feel cheated on some gloating.

about 1 hour ago from *Tweetie* · Reply · View Tweet

Freemor: Quick **#Conficker** test "Conficker eye chart" @ http://ur1.ca/30j5

about 1 hour ago from *Identica* · Reply · View Tweet

cyclingroo: Want a quick way to see if you might b e affected by **#Conficker**? Use the eye chart @ http://bit.ly/18BSVY (expand) (via Slashdot)

about 1 hour ago from *TweetDeck* · Reply · View Tweet

offtheroad: **#conficker** eye chart - quick, web-based conficker detection tool- if you can see images= most likely conficker free- http://twurl.nl/710csd (expand)

about 1 hour ago from *twhirl* · Reply · View Tweet

pubal: Retweeting @dakami: Better **#conficker** scanning at www.doxpara.com .

Nifty queries:

- cool filter:links
- "is down"
- movie :)
- "happy hour" near:SF
- #haiku
- "listening to"
- love OR hate
- flight :(

Done

Duplication

- “Me too!”
- Retweeting (RT)
- Redirectors and URL shortening
- Voting no guarantee of quality, utility, accuracy

eugenearmstead: Help slow **#conficker** and run labrea.sourceforge.net on your unused public IP's. Easily done with an old box and GRML.org. Its fun!

1 day ago from *web* · Reply · View Tweet

gisuck: Wow... my #virusoftheday consisted of 1 Win32/AutoRun.VQ worm from a usb stick... no **#conficker** here...

1 day ago from *TweetDeck* · Reply · View Tweet

HippieLogic: the greatest joke: depending on PCs when running a business #aprilfools **#conficker**

1 day ago from *web* · Reply · View Tweet

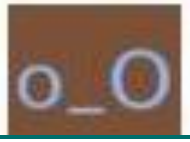
Misinformation or misinterpretation

axisds: @xoxidine **#Conficker** exploits your machine directly through email However, infection can also occure from using an infected NAS or USB key

1 day ago from *web* · Reply · View Tweet · Show Conversation

leosilvabreu: Em resumo: o **#conficker** é uma bomba armada e preparada para varrer a internet, onde o detonador ninguém sabe onde ou quem está com ele.

1 day ago from *web* · Reply · View Tweet



hackertweets: SteveMoitozo2: Blah, blah **#conficker** Patch #windows and update anti-virus/anti-malware. Better yet, reformat and install #linux or buy a..

On April 1st the Conficker worm, perhaps the most wide-spread malware program in history, is set to activate. We don't know what Conficker will do, but it's a safe bet it won't be anything nice to the hundreds of thousands of Windows PCs that have been infected with it. Will it strip out every credit-card number within these PCs? Launch a massive DDoS (Distributed Denial of Service) attack? Subscribe you to PETA porn!? We don't know.

I don't want to find out myself. There are several ways you can *try* to protect yourself from Conficker. These include disabling AutoRun, since Conficker can spread by infected USB drives; using current anti-virus software, use Windows' own malicious software removal tool; or, switch to OpenDNS for your DNS service. There are many ways to try to stop these attacks, unfortunately, the bad guys are always working on getting newer and better ways to infect your system.

The sad truth is no matter what you do with Windows, whether you're running XP, Vista, or the Windows 7 beta, you're not safe. Now, however there's a patch that will stop Conficker, and almost all other malware programs, in their tracks. It's called Linux.

News & Notes from the OpenDNS team

Do you have Conficker? Find out in your OpenDNS account.

by **Allison Rhodes** on Apr 2nd, 2009

Here at OpenDNS we've spent the past several months working to keep you safe from the Conficker worm. Using the OpenDNS service is widely considered to be one of the easiest and most guaranteed ways to protect your network. And today we roll out a **free Conficker detection tool** to give you actionable insight into whether or not you have Conficker on your network.

As David mentioned here, we're in a unique position as your DNS provider of choice to block the worm at the DNS level and prevent it from phoning home. We're also in a unique position to tell you, based on DNS queries coming from your account, if your network has been infected with Conficker. Log into your OpenDNS account now and **you'll see a banner indicating you either have Conficker or you don't**. This is a tremendously valuable service, and representative of a key innovation on the DNS. If

How Can I Avoid Infection?

Drain your savings account, buy a Mac, and hang out at Starbucks all day long. Or to appease the Linux crowd, ditch Windows and dive into Ubuntu. But you don't need to learn a brand new OS or invest in an overpriced computer to avoid Conficker.

One way to avoid Conficker is to disable AutoRun. Details on how to properly do so can be found here. And as with all security-related threats, safe computing habits apply. Avoid websites you're not familiar with, ensure that Windows is fully patched, invest in a security program and download the latest updates, and never download from an unknown or shady source.

Not helpful

Holy S#*t, I'm Infected!

We'll assume here you're talking about your PC (if not, stop scratching it and consult a doctor). There are a number of Conficker removal tools available, such as those found here, here, and here. If going this route, it's a good idea to download the tool(s) from a clean PC rather than your infected one. Note that Conficker also blocks tools with 'Conficker' in the name, so be prepared to rename the file(s) if necessary.

Another option is to create a bootable CD/DVD or USB thumb drive and outfit it with security programs. By doing so, you'll bypass Windows entirely and have a clean slate from which to work from. Just be sure to create bootable media from a clean PC. Also check your security vendor's website for information on creating a bootable rescue disk.

Finally, to err on the extreme side of caution, you can start fresh with a reinstallation of Windows. Whether or not you resort to this, it's a good idea to backup any important data -- work documents, family photos, groovy music -- right away.

Reaction?

(2) #conficker - Twitter Search - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://search.twitter.com/search?max_id=1440262195&page=2&q=%23conficker

AltVsta Amzn wethr NVDPL SecrTm Robmks zSqd Dwnld vid SecSIG c: isc2 intr vwms cnvlib isc2blog

chernobylheart: Some are now saying that Conficker was nothing more than an April Fool's joke to make a point. Thoughts on this, Twitterverse? **#conficker**

about 2 hours ago from *web* · Reply · View Tweet

thefrozencoder: The **#conficker** eye chart http://www.confickerworkinggroup.org/infection_test/cfeyechart.html

about 2 hours ago from *TwitterGadget* · Reply · View Tweet

geekgrrl: RT @dakami: Better **#conficker** scanning at www.doxpara.com . Bonus shout out to the cybereschatologists.

about 2 hours ago from *Spaz* · Reply · View Tweet

IOActive: RT @dakami Better **#conficker** scanning at www.doxpara.com. Bonus shout out to the cybereschatologists.

about 2 hours ago from *web* · Reply · View Tweet

smpatrick1: Funny story - Computerworld: **#Conficker** worm ends life as we know it; film at 11 - http://tinyurl.com/cuhzb9 (expand)

about 2 hours ago from *web* · Reply · View Tweet

dakami: Better **#conficker** scanning at www.doxpara.com . Bonus shout out to the cybereschatologists.

about 2 hours ago from *web* · Reply · View Tweet

theissler: Two fast **#conficker** tests for your pc: http://bit.ly/HqRV (expand) or http://bit.ly/10Bull (expand)

about 2 hours ago from *TweetDeck* · Reply · View Tweet

Any Language

Translate to English

Trending topics:

- G20
- #w2e
- #OfficeMax
- G-20
- Easter
- World Autism
- #techshow
- April Fools
- #BDSocial
- iPhone

Nifty queries:

- cool filter:links
- "is down"
- movie :)
- "happy hour" near:SF
- #haiku
- "listening to"
- love OR hate
- flight :(

Done

http://search.twitter.com/search?q=kelowna

Amzn wethr NVDPL SecrTm Robmks zSqd Dwnld vid SecSIG c: isc2 intr vwms

twitter kelowna Search

Realtime results for **kelowna**

0.03 seconds

382 more results since you started searching. Refresh to see them.

lorene1voice: RT @realreporter #kelownafire Send in yr pics of **Kelowna** fire & get published under yr name editor@vancouverite.com www.vancouverite.com

half a minute ago from *mobile web* · Reply · View Tweet

TheDaveCA: @catester checking out the fire here in **Kelowna**?

half a minute ago from *Summizer* · Reply · View Tweet

gpjoa: Home from work and watching some television. Had an update from my sister who was evacuated from her home near **Kelowna** due to the fires ...

1 minute ago from *twhirl* · Reply · View Tweet

Vombie: @Kelsey_FACE my allergies and asthma have certainly improved since I moved here, I don't miss stupid **Kelowna** smoky air at all

1 minute ago from *web* · Reply · View Tweet · Show Conversation

naymark: @bornk i love your live tweeting from **kelowna**. stay safe.

Internet Security Issues
Integrity

- Disinformation?
  - 4chan hacked Christian site ► Facebook

Internet Security Issues
Integrity

- Pointless babble
  - http://www.youtube.com/watch?v=PN2HAroA12w
  - http://current.com/items/89891774_twouble-with-twitters.htm

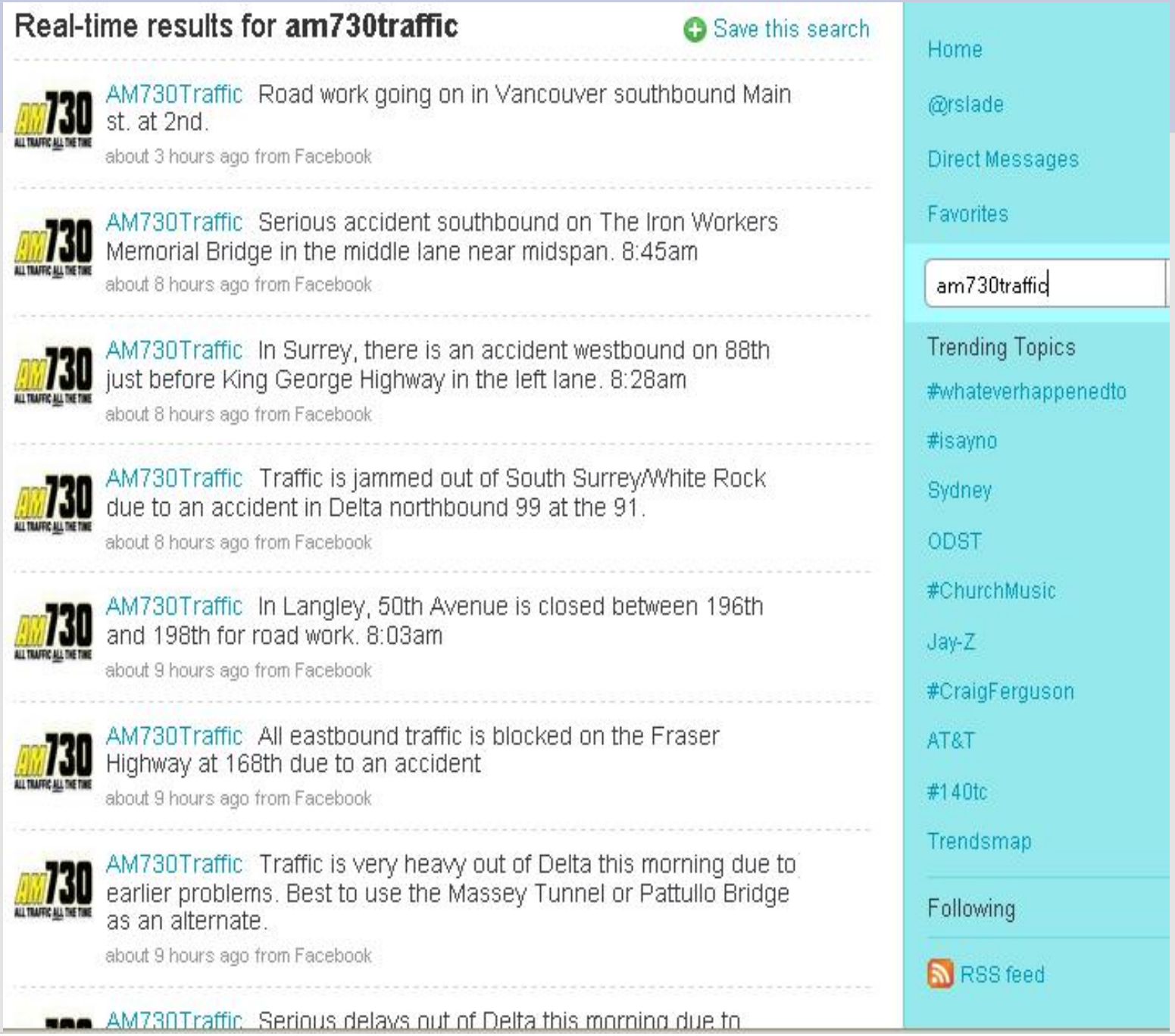
Internet Security Issues
Integrity

- Wikipedia
  - Anyone can add or edit
  - Wealth of information
  - And misinformation
- http://www.collegehumor.com/video:1830262
- http://en.wikipedia.org/wiki/Robert_Slade

Internet Security Issues
Integrity

I'm not feeling well

Internet Security Issues
Integrity



Internet Security Issues
Integrity

- The irony of the Information Age is that it has given new respectability to uninformed opinion.
  - John Lawton

Internet Security Issues
Availability

- Alert systems for emergencies
  - Telephone
    - Switches swamped by call volumes
  - Cell/mobile phones
    - Swamping even worse
  - Text/SMS
    - Quite resilient

Internet Security Issues
Availability

- Alert systems for emergencies
  - Twitter
    - Uses text/SMS
    - Points of failure
      - Cell system
      - Internet
      - Power (for computers)
      - Twitter itself
    - But generally accessible

Internet Security Issues
Availability

- Alert systems for emergencies
  - Facebook, LinkedIn
    - Limited to those with accounts
    - Must be checked
    - Creating divisions in the Internet

Internet Security Issues Availability

- Shortening/redirection risk
- http://blogs.securiteam.com/index.php/archives/1272
  - Malware
  - Spam
  - Privacy
  - Redirector swamping

Internet Security Issues

- Social networking is social
- Be civil
  - Understand other uses/systems
  - Lots of people
    - Some nice
    - Some not
  - Read carefully
    - React slowly

Internet Security Issues

Robert M. Slade, MS, CISSP
rmslade@shaw.ca, rslade@vcn.bc.ca, rslade@computercrime.org

http://victoria.tc.ca/techrev/mnbksccd.htm
http://victoria.tc.ca/techrev/secmarks.htm
http://www.infosecbc.org/links
http://blog.isc2.org/isc2_blog/training
http://www.flickr.com/photos/rslade/
http://www.linkedin.com/in/rslade
http://www.facebook.com/rslade
http://twitter.com/rslade