CSE 484 / CSE M 584
Computer Security:
Online Ecosystem Studies

TA: Adrian Sham

adrsham@cs

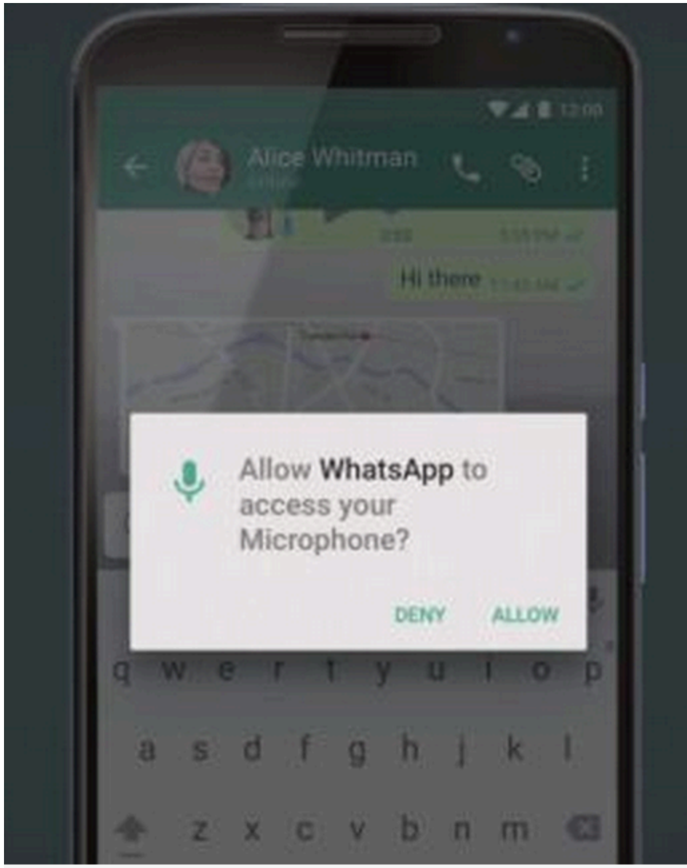
With material from Franzi and various sources

Reminders

- Homework #3 due tomorrow (5/29) at 5pm
- Lab #3 due next Friday (6/5)
  - Part 3 is extra credit, out **now**
- Office hour tomorrow after class
  - Office hours will be held in the lab #3 room until lab #3 deadline – CSE 003D
  - You should have access to the room

Today in the news

- Android M announced
- Changes existing permissions system
  - Break down user permissions into specific categories
  - Having apps ask the user for permission at the time access to a feature is required



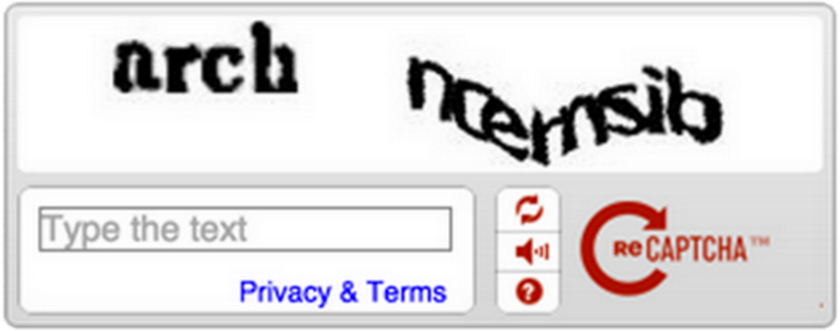
Hi there

Allow **WhatsApp** to access your Microphone?

http://www.anandtech.com/show/9291/google-announces-android-m-at-google-io-2015

CAPTCHA

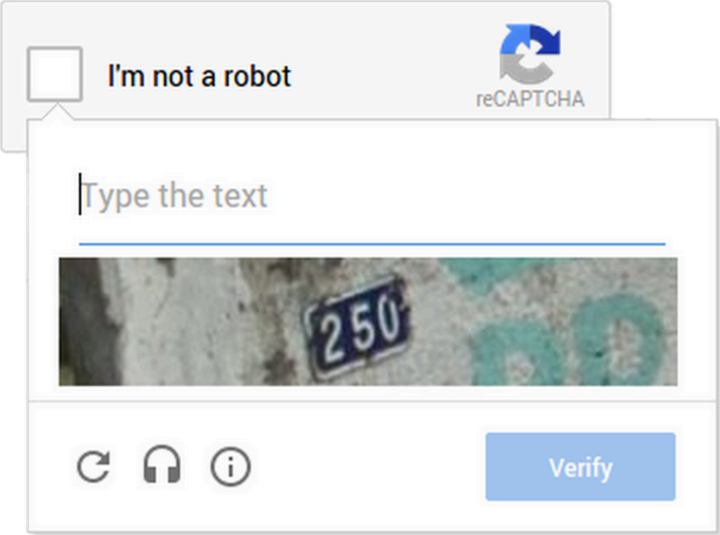
- CAPTCHA (**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part)
- Artificial Intelligence technology can solve 99.8%

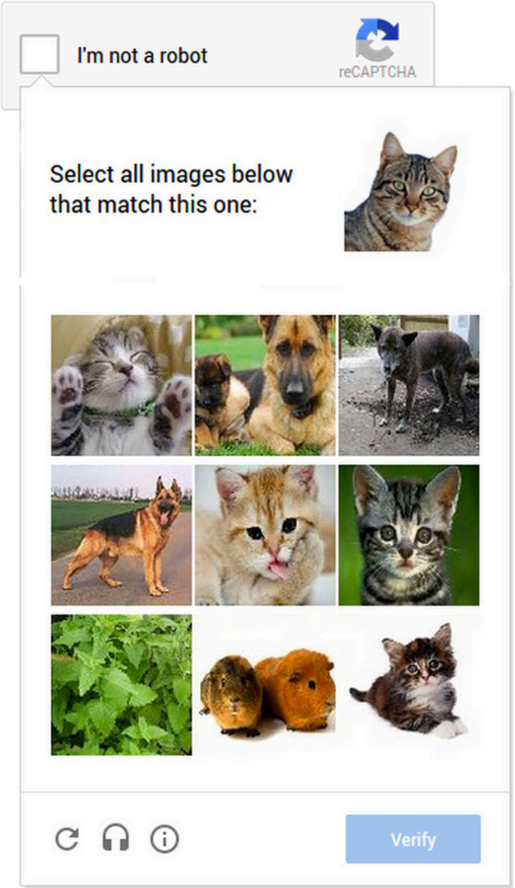


http://googleonlinesecurity.blogspot.com/2014/12/are-you-robot-introducing-no-captcha.html

reCAPTCHA

- Use risk analysis, provide better user experience





Select all images below that match this one:

[Motoyama et al.]

Dirty Jobs – The Role of Freelance Labor in Web Service Abuse

Following slides by : Marti Motoyama, Damon McCoy, Kirill Levchenko, Stefan Savage, and Geoffrey M. Voelker UC San Diego

https://www.usenix.org/legacy/events/sec11/tech/slides/motoyama.pdf

[Motoyama et al.]

Vulnerability of Web Services

- Many web services today are free/open access
  - Supported by advertising revenue
  - Reaching critical mass requires low barrier to entry
  - Page views driven by user-generated content
    - Videos, social networking updates, blogs, etc
- However, openness leaves sites vulnerable to abuse
  - Exploitation of free resources
    - Sending spam from web based email accounts
  - Unsanctioned advertising channels
    - Spamming links on blog comments

[Motoyama et al.]

Abuse Labor Markets

- Abuse is profitable
  - Kanich et al. estimated $7k/day email spam revenue
- Labor markets have evolved to supply workers
  - Online freelancing sites
- Why outsource abuse jobs?
  - Cost effective: Low wage regions
  - Agile: Workers are adept and technically capable
  - Scale: ~one million workers on Freelancer.com

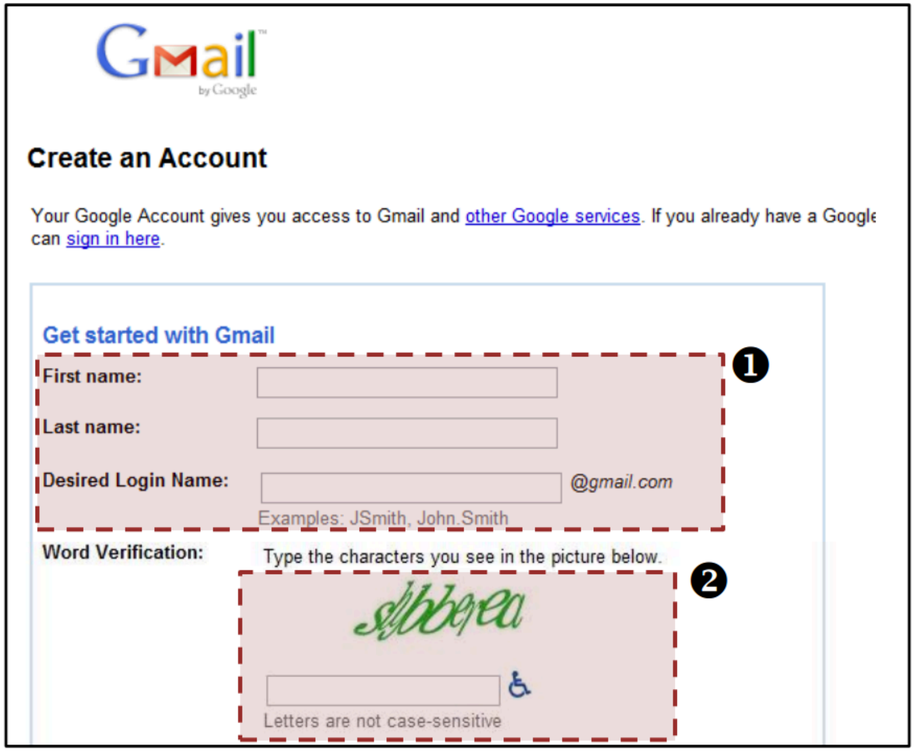
[Motoyama et al.]

Outsourcing jobs

- Freelancer.com: one of the largest outsourcing and oldest freelancing sites
  - Claims over 2 million employers and workers
  - User population covers 234 countries / regions
- How it works:
  - Buyer/employers post jobs
  - Workers bid on jobs
  - Buyers select workers

[Motoyama et al.]

- Scenario: Abuser wants to send spam via Web email
- Prerequisite: Bulk accounts on Gmail



Create an Account

Your Google Account gives you access to Gmail and other Google services. If you already have a Google
can sign in here.

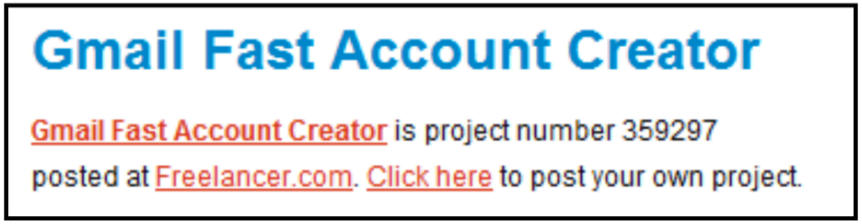
Get started with Gmail

❶

First name:	
Last name:	
Desired Login Name:	@gmail.com Examples: JSmith, John.Smith
Word Verification:	Type the characters you see in the picture below. Letters are not case-sensitive

❷

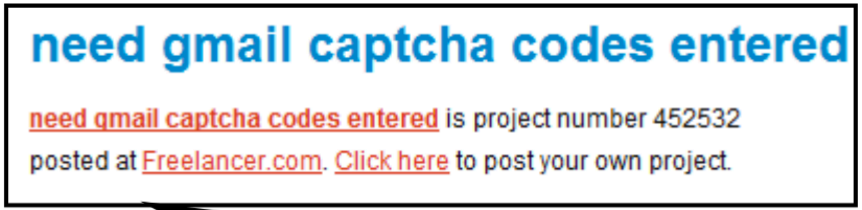
❶



Gmail Fast Account Creator

Gmail Fast Account Creator is project number 359297 posted at Freelancer.com. Click here to post your own project.

❷



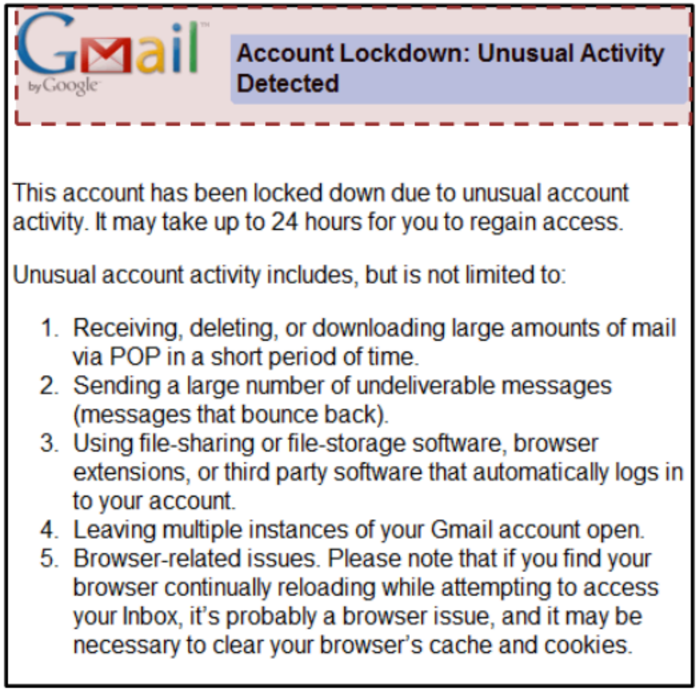
need gmail captcha codes entered

need gmail captcha codes entered is project number 452532 posted at Freelancer.com. Click here to post your own project.

"i need gmail captcha entry agent immediately. 1000's new captcha entrys per week

[Motoyama et al.]

- Problem: Google detects mass account creation
- Solution: Purchase IP proxy services

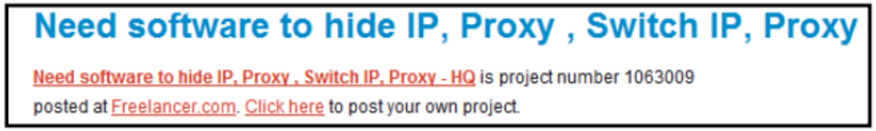


Account Lockdown: Unusual Activity Detected

This account has been locked down due to unusual account activity. It may take up to 24 hours for you to regain access.

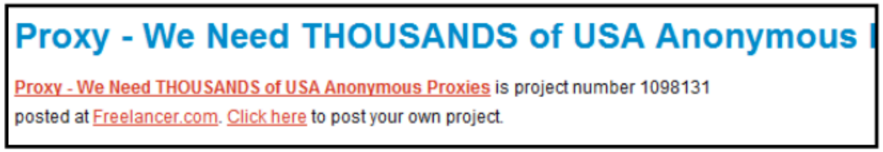
Unusual account activity includes, but is not limited to:

1. Receiving, deleting, or downloading large amounts of mail via POP in a short period of time.
2. Sending a large number of undeliverable messages (messages that bounce back).
3. Using file-sharing or file-storage software, browser extensions, or third party software that automatically logs in to your account.
4. Leaving multiple instances of your Gmail account open.
5. Browser-related issues. Please note that if you find your browser continually reloading while attempting to access your Inbox, it's probably a browser issue, and it may be necessary to clear your browser's cache and cookies.



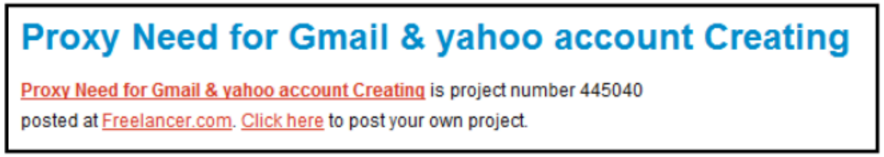
Need software to hide IP, Proxy , Switch IP, Proxy

Need software to hide IP, Proxy , Switch IP, Proxy - HQ is project number 1063009 posted at Freelancer.com. Click here to post your own project.



Proxy - We Need THOUSANDS of USA Anonymous I

Proxy - We Need THOUSANDS of USA Anonymous Proxies is project number 1098131 posted at Freelancer.com. Click here to post your own project.

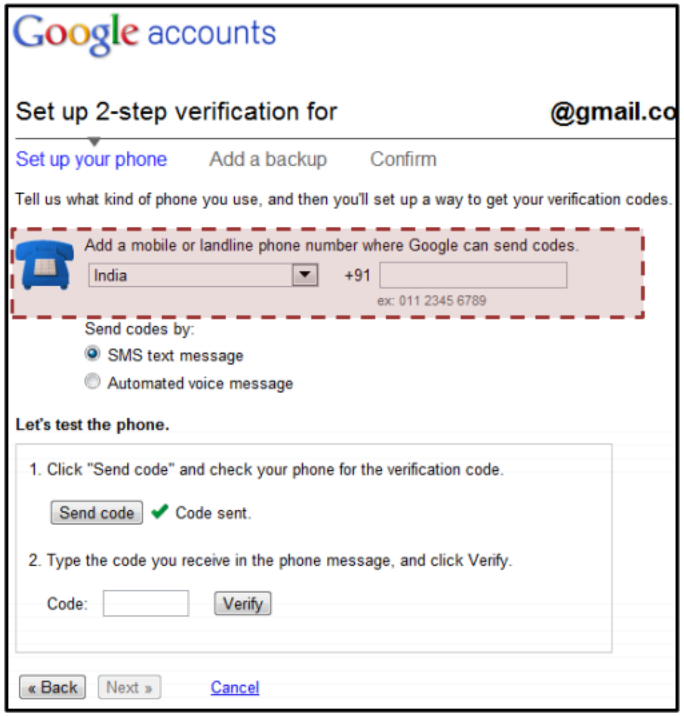


Proxy Need for Gmail & yahoo account Creating

Proxy Need for Gmail & yahoo account Creating is project number 445040 posted at Freelancer.com. Click here to post your own project.

[Motoyama et al.]

- Problem: Google implements phone verification
- Solution: Buy telephone numbers



Google accounts

Set up 2-step verification for @gmail.co

Set up your phone   Add a backup   Confirm

Tell us what kind of phone you use, and then you'll set up a way to get your verification codes.

Add a mobile or landline phone number where Google can send codes.

India ▾ +91 ex: 011 2345 6789

Send codes by:

● SMS text message

○ Automated voice message

Let's test the phone.

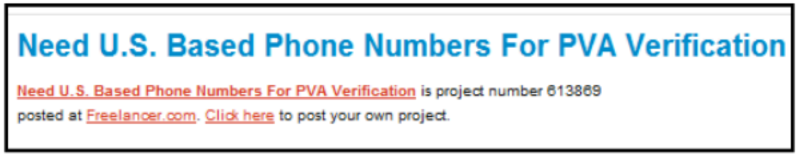
1. Click "Send code" and check your phone for the verification code.

Send code ✓ Code sent.

2. Type the code you receive in the phone message, and click Verify.

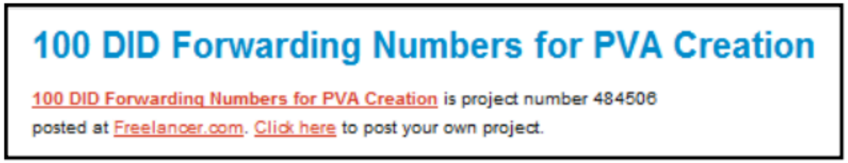
Code: Verify

« Back   Next »   Cancel



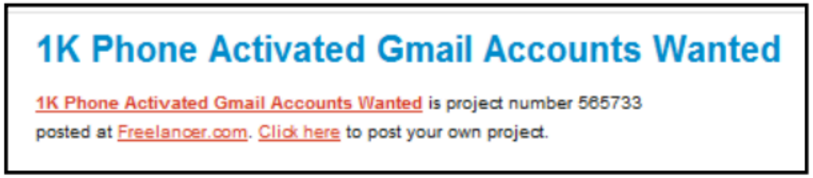
Need U.S. Based Phone Numbers For PVA Verification

Need U.S. Based Phone Numbers For PVA Verification is project number 613869 posted at Freelancer.com. Click here to post your own project.



100 DID Forwarding Numbers for PVA Creation

100 DID Forwarding Numbers for PVA Creation is project number 484506 posted at Freelancer.com. Click here to post your own project.



1K Phone Activated Gmail Accounts Wanted

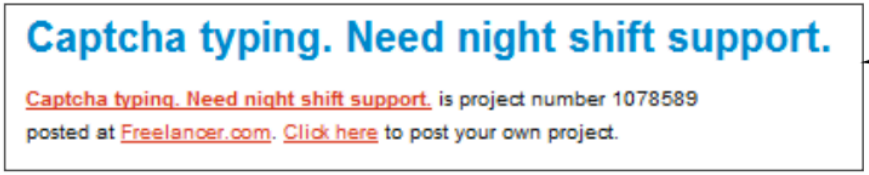
1K Phone Activated Gmail Accounts Wanted is project number 565733 posted at Freelancer.com. Click here to post your own project.

6

[Motoyama et al.]

CAPTCHA Solving

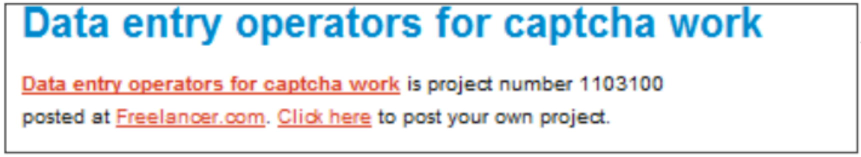
- Overview: Using humans to solve CAPTCHAs
- Employers post daily ads on Freelancer.com:



Captcha typing. Need night shift support.

Captcha typing. Need night shift support. is project number 1078589 posted at Freelancer.com. Click here to post your own project.

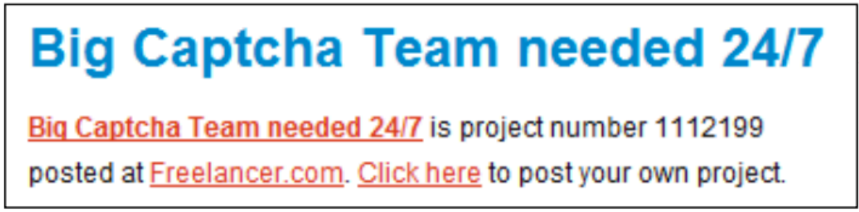
Nightshift support on following servers: Qlink , Goodearners, Fasttypers, Mars dooms.



Data entry operators for captcha work

Data entry operators for captcha work is project number 1103100 posted at Freelancer.com. Click here to post your own project.

Rate is.80$-.85$ per 1k … Bangladeshi workers are preferable



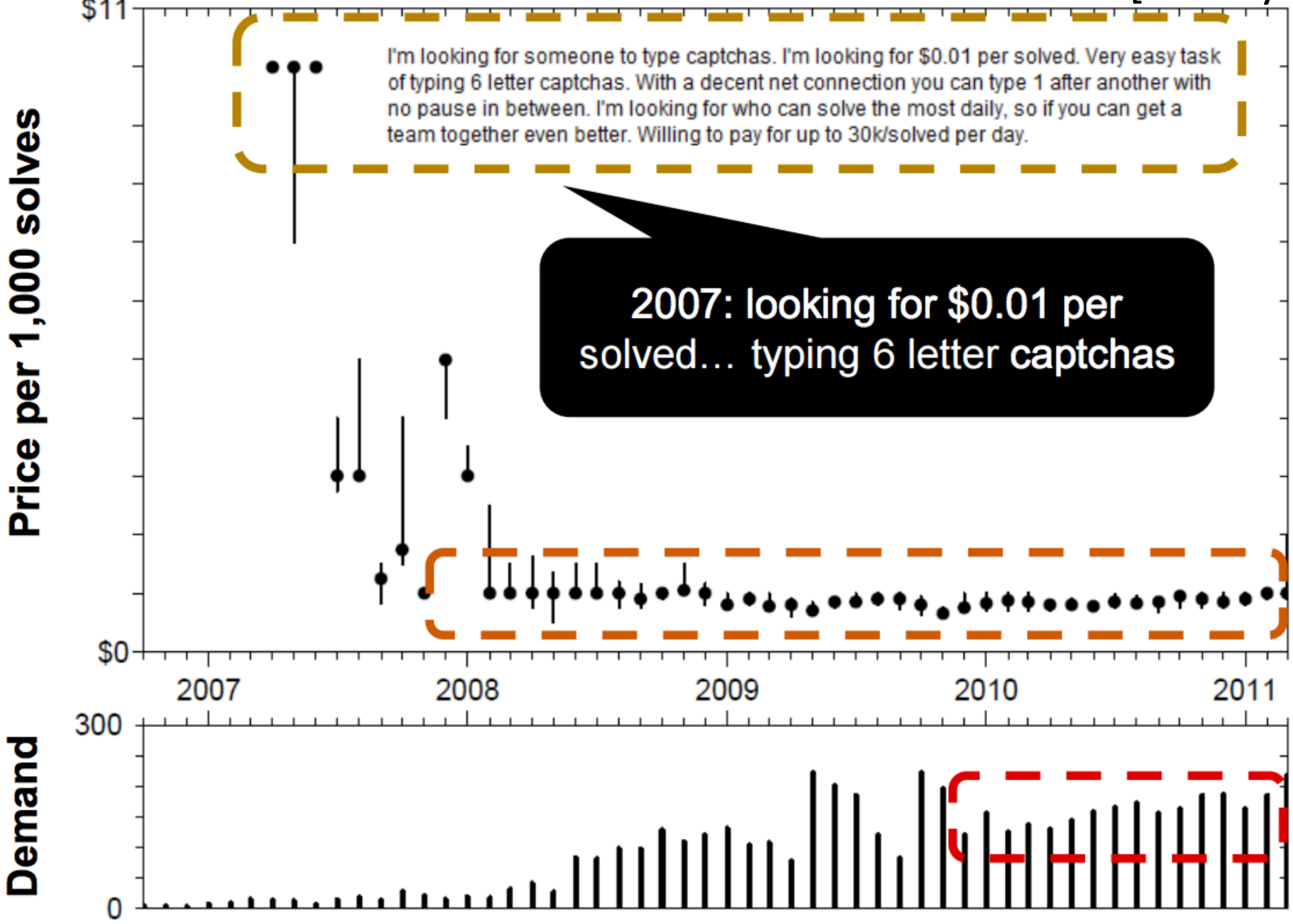
Big Captcha Team needed 24/7

Big Captcha Team needed 24/7 is project number 1112199 posted at Freelancer.com. Click here to post your own project.

3000-4000 output per hour … image is yahoo captcha

40

[Motoyama et al.]



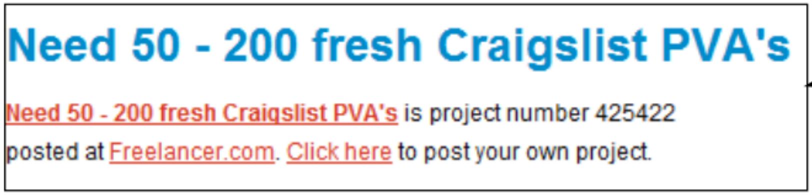
I'm looking for someone to type captchas. I'm looking for $0.01 per solved. Very easy task of typing 6 letter captchas. With a decent net connection you can type 1 after another with no pause in between. I'm looking for who can solve the most daily, so if you can get a team together even better. Willing to pay for up to 30k/solved per day.

2007: looking for $0.01 per solved… typing 6 letter captchas

- CAPTCHA solving began at nearly $10/1,000 solves
- Price stabilized to roughly $1/1,000 solves
- Demand has remained stable since 2010

[Motoyama et al.]

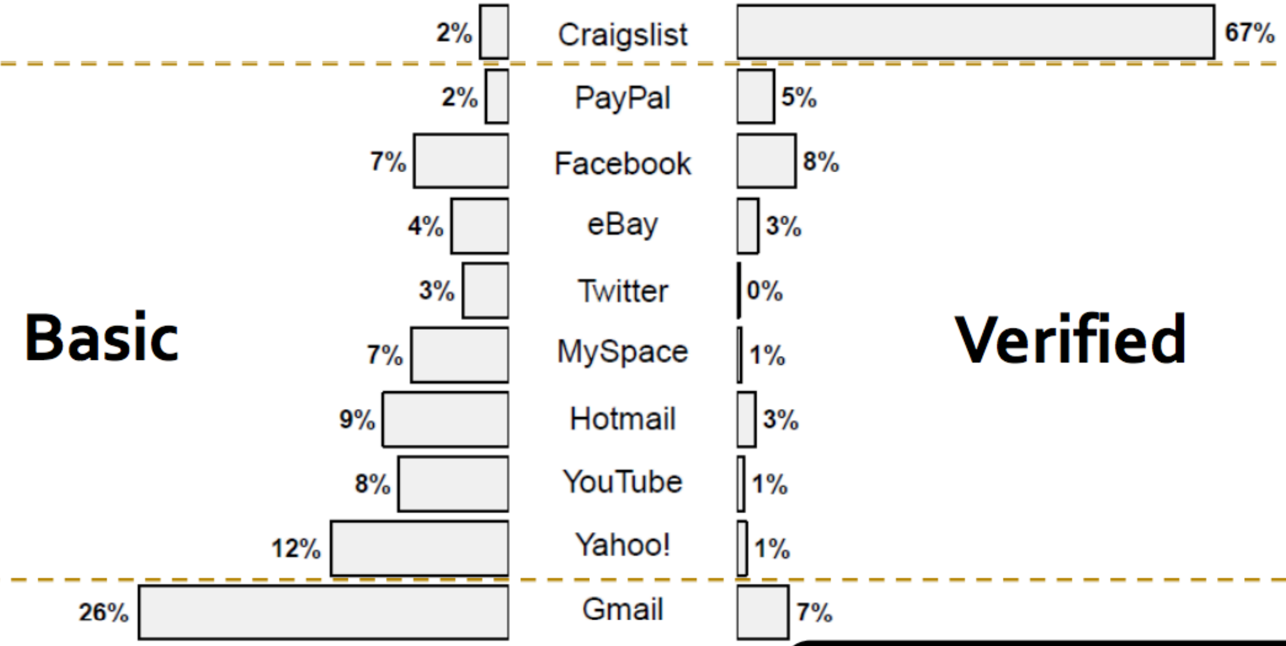
Example Jobs: Accounts

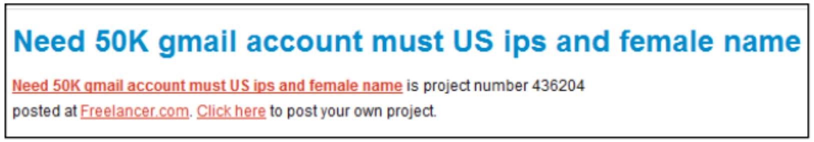


Need 50 - 200 fresh Craigslist PVA's

Need 50 - 200 fresh Craigslist PVA's is project number 425422 posted at Freelancer.com. Click here to post your own project.

50-200 fresh Craigslist PVA's… made with different US IP… U.S phone number





Need 50K gmail account must US ips and female name

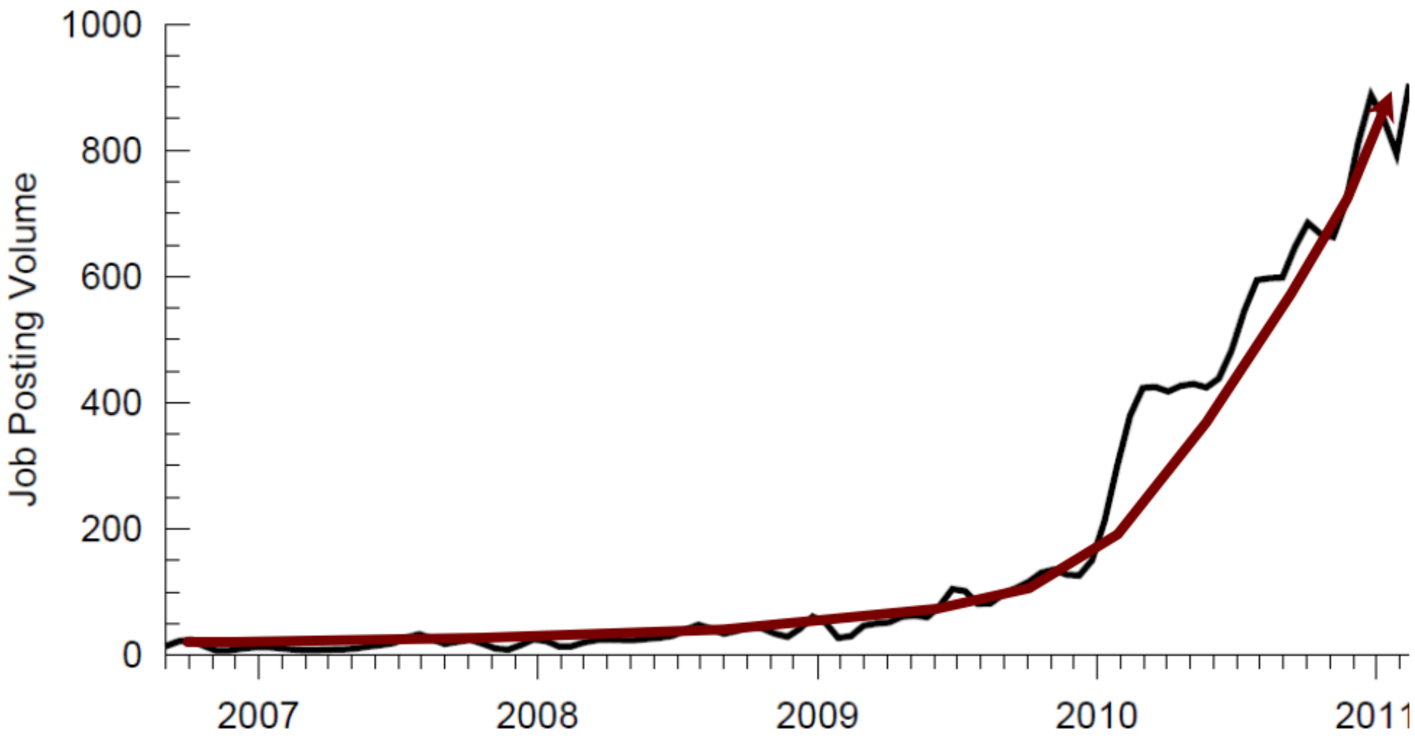
Need 50K gmail account must US ips and female name is project number 436204 posted at Freelancer.com. Click here to post your own project.

Gmail accounts…US ips and female name … rate $9/1000, need 50k

[Motoyama et al.]

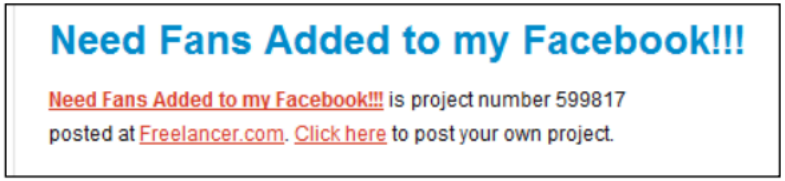
OSN Linking

- Buying friends, Facebook fans/lines for website pages, Twitter followers, YouTube subs, etc



[Motoyama et al.]

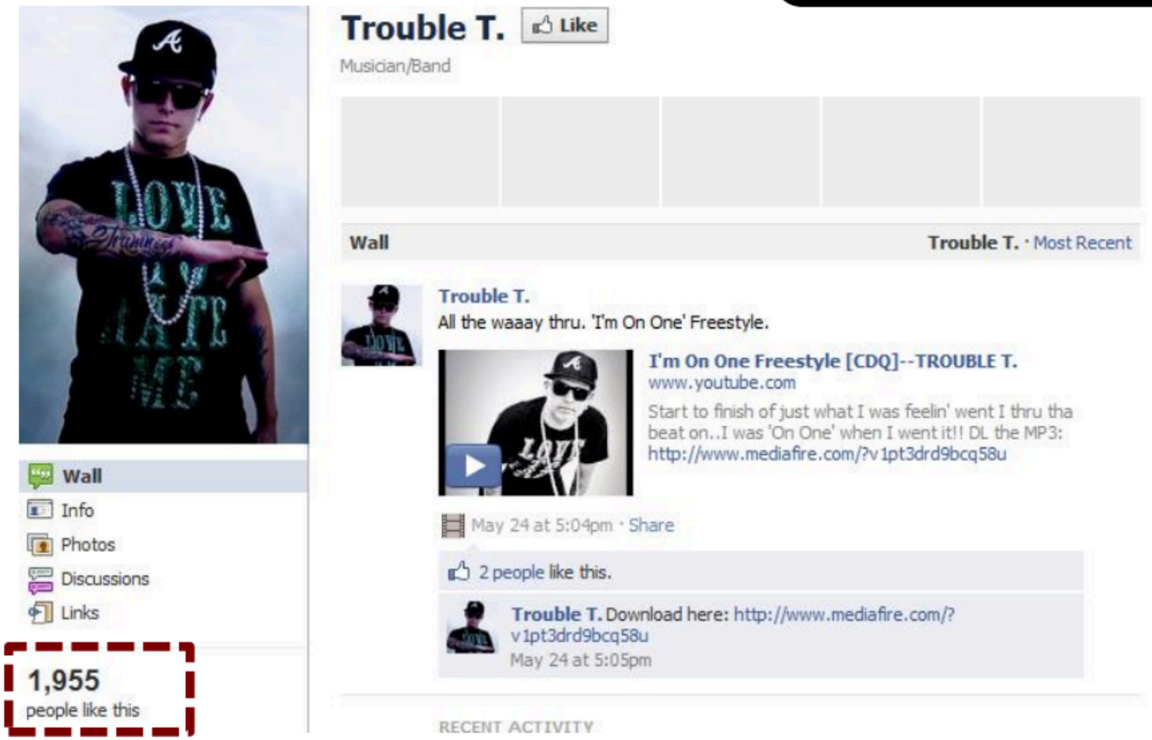
Example: Online Social Network Link



Need Fans Added to my Facebook!!!

Need Fans Added to my Facebook!!! is project number 599817 posted at Freelancer.com. Click here to post your own project.

I need to build up my fan base on Facebook for my musician page… Here is **link to my** page…



Trouble T.
All the waaay thru. 'I'm On One' Freestyle.

I'm On One Freestyle [CDQ]--TROUBLE T.
www.youtube.com
Start to finish of just what I was feelin' went I thru tha beat on..I was 'On One' when I went it!! DL the MP3: http://www.mediafire.com/?v1pt3drd9bcq58u

May 24 at 5:04pm · Share

2 people like this.

Trouble T. Download here: http://www.mediafire.com/?v1pt3drd9bcq58u
May 24 at 5:05pm

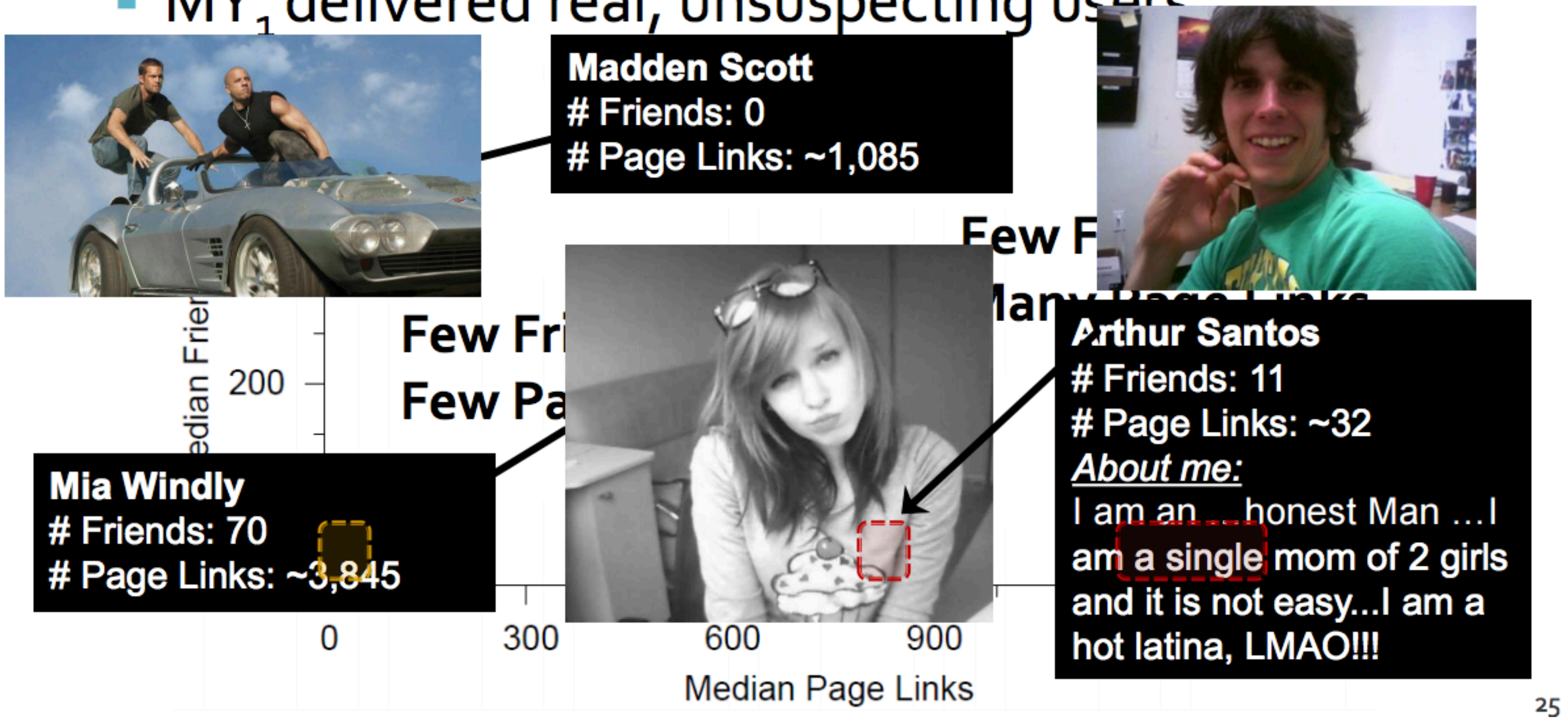
RECENT ACTIVITY

1,955
people like this

[Motoyama et al.]

User accounts

- Users are fake: few friends, substantial number of links to other websites
  - MY_1 delivered real, unsuspecting users



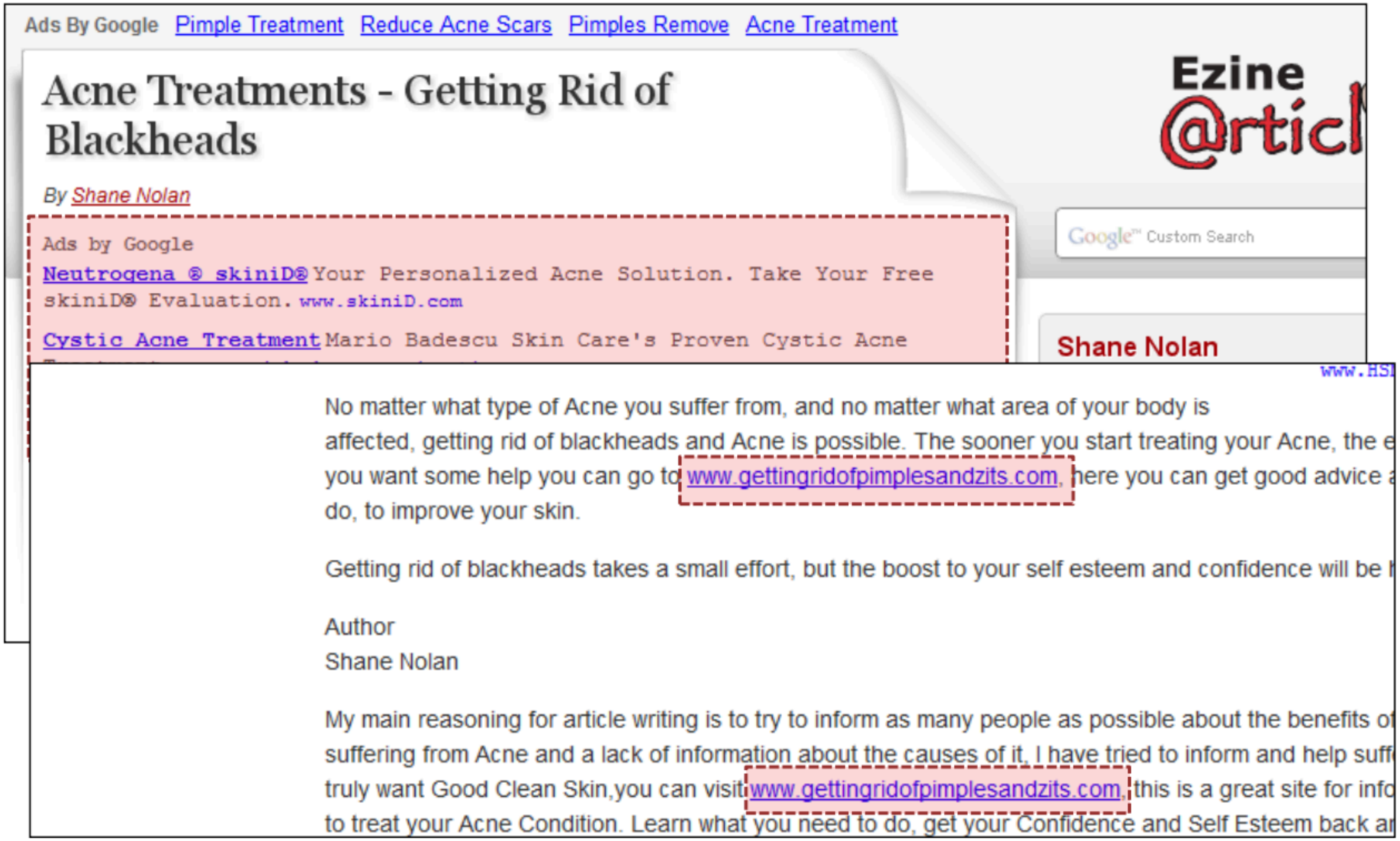
Madden Scott
Friends: 0
Page Links: ~1,085

Mia Windly
Friends: 70
Page Links: ~3,845

Arthur Santos
Friends: 11
Page Links: ~32
About me:
I am an …honest Man …I am a single mom of 2 girls and it is not easy...I am a hot latina, LMAO!!!

[Motoyama et al.]

Search Engine-Oriented Content



Ads By Google Pimple Treatment Reduce Acne Scars Pimples Remove Acne Treatment

Acne Treatments - Getting Rid of Blackheads

By Shane Nolan

Ads by Google

Neutrogena ® skiniD® Your Personalized Acne Solution. Take Your Free skiniD® Evaluation. www.skiniD.com

Cystic Acne Treatment Mario Badescu Skin Care's Proven Cystic Acne

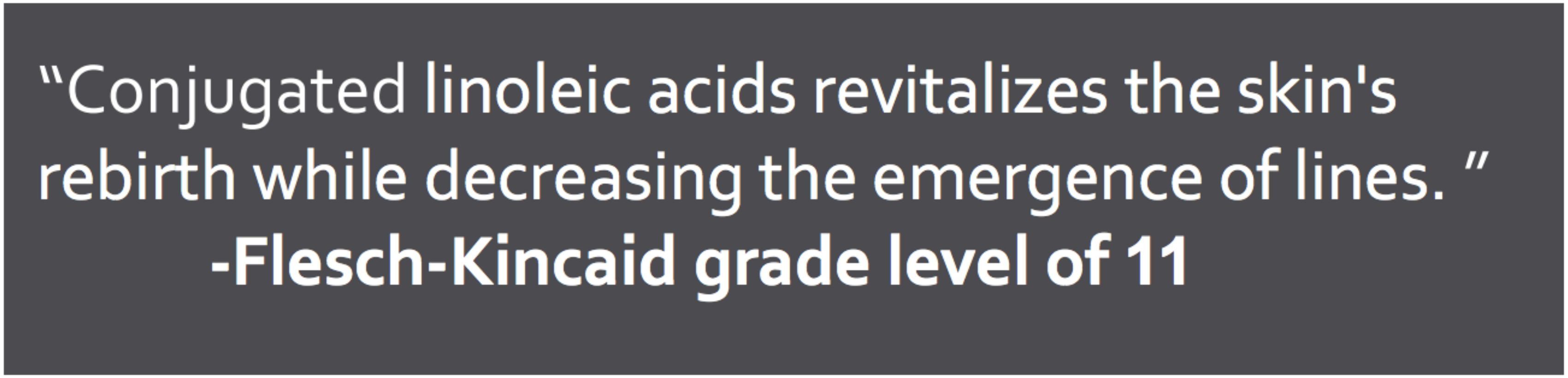
No matter what type of Acne you suffer from, and no matter what area of your body is affected, getting rid of blackheads and Acne is possible. The sooner you start treating your Acne, the e
you want some help you can go to www.gettingridofpimplesandzits.com, here you can get good advice a
do, to improve your skin.

Getting rid of blackheads takes a small effort, but the boost to your self esteem and confidence will be l

Author
Shane Nolan

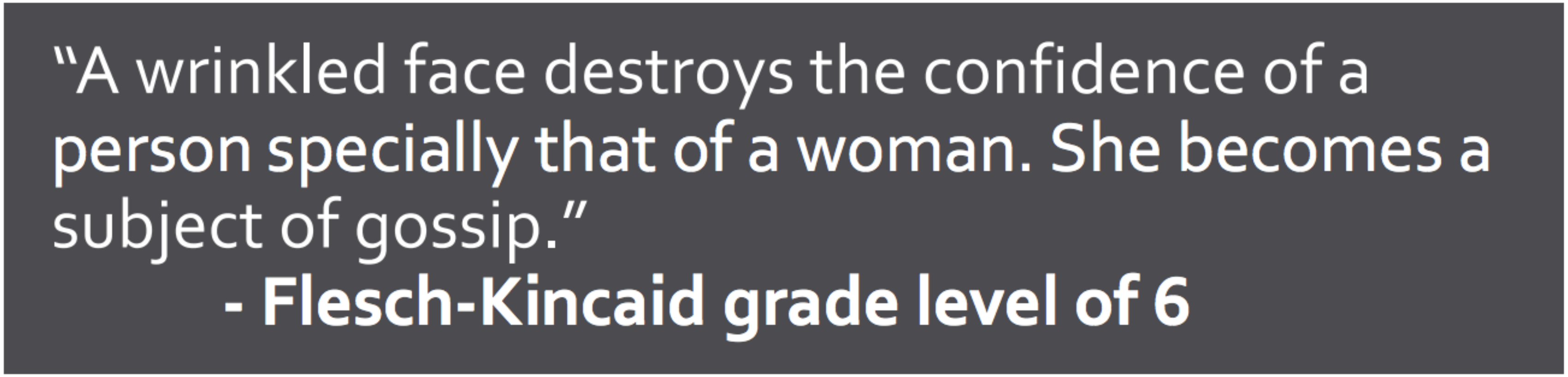
My main reasoning for article writing is to try to inform as many people as possible about the benefits of
suffering from Acne and a lack of information about the causes of it, I have tried to inform and help suff
truly want Good Clean Skin,you can visit www.gettingridofpimplesandzits.com, this is a great site for info
to treat your Acne Condition. Learn what you need to do, get your Confidence and Self Esteem back ar

Quality of work



"Conjugated linoleic acids revitalizes the skin's rebirth while decreasing the emergence of lines. "

-Flesch-Kincaid grade level of 11

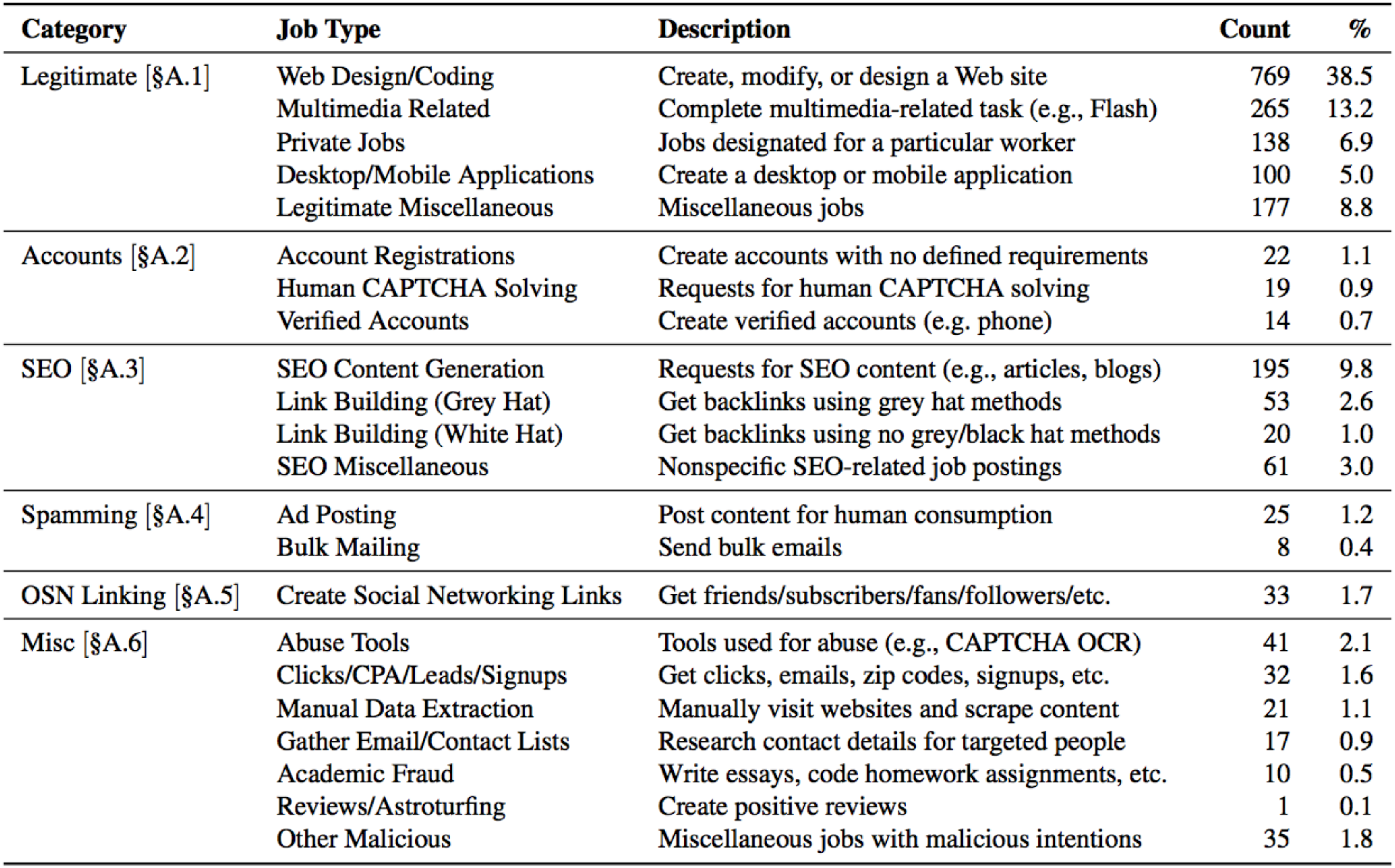


"A wrinkled face destroys the confidence of a person specially that of a woman. She becomes a subject of gossip."

- Flesch-Kincaid grade level of 6

[Motoyama et al.]

Freelance Abuse (USENIX 2011)



Category	Job Type	Description	Count	%
Legitimate [§A.1]	Web Design/Coding	Create, modify, or design a Web site	769	38.5
	Multimedia Related	Complete multimedia-related task (e.g., Flash)	265	13.2
	Private Jobs	Jobs designated for a particular worker	138	6.9
	Desktop/Mobile Applications	Create a desktop or mobile application	100	5.0
	Legitimate Miscellaneous	Miscellaneous jobs	177	8.8
Accounts [§A.2]	Account Registrations	Create accounts with no defined requirements	22	1.1
	Human CAPTCHA Solving	Requests for human CAPTCHA solving	19	0.9
	Verified Accounts	Create verified accounts (e.g. phone)	14	0.7
SEO [§A.3]	SEO Content Generation	Requests for SEO content (e.g., articles, blogs)	195	9.8
	Link Building (Grey Hat)	Get backlinks using grey hat methods	53	2.6
	Link Building (White Hat)	Get backlinks using no grey/black hat methods	20	1.0
	SEO Miscellaneous	Nonspecific SEO-related job postings	61	3.0
Spamming [§A.4]	Ad Posting	Post content for human consumption	25	1.2
	Bulk Mailing	Send bulk emails	8	0.4
OSN Linking [§A.5]	Create Social Networking Links	Get friends/subscribers/fans/followers/etc.	33	1.7
Misc [§A.6]	Abuse Tools	Tools used for abuse (e.g., CAPTCHA OCR)	41	2.1
	Clicks/CPA/Leads/Signups	Get clicks, emails, zip codes, signups, etc.	32	1.6
	Manual Data Extraction	Manually visit websites and scrape content	21	1.1
	Gather Email/Contact Lists	Research contact details for targeted people	17	0.9
	Academic Fraud	Write essays, code homework assignments, etc.	10	0.5
	Reviews/Astroturfing	Create positive reviews	1	0.1
	Other Malicious	Miscellaneous jobs with malicious intentions	35	1.8

[Motoyama et al.]

Summary

- Attackers outsource abuse jobs
  - ~30% of Freelancer.com jobs abusive
  - Jobs spanned range of categories from spamming to account registration
- Quality of product is highly variable
- Large, cheap labor pool changes threat model
  - Automation is not the only way
  - Largely removes difficulty in executing abuse task
- Outsourced workforce enables new attacks

[McCoy et al.]

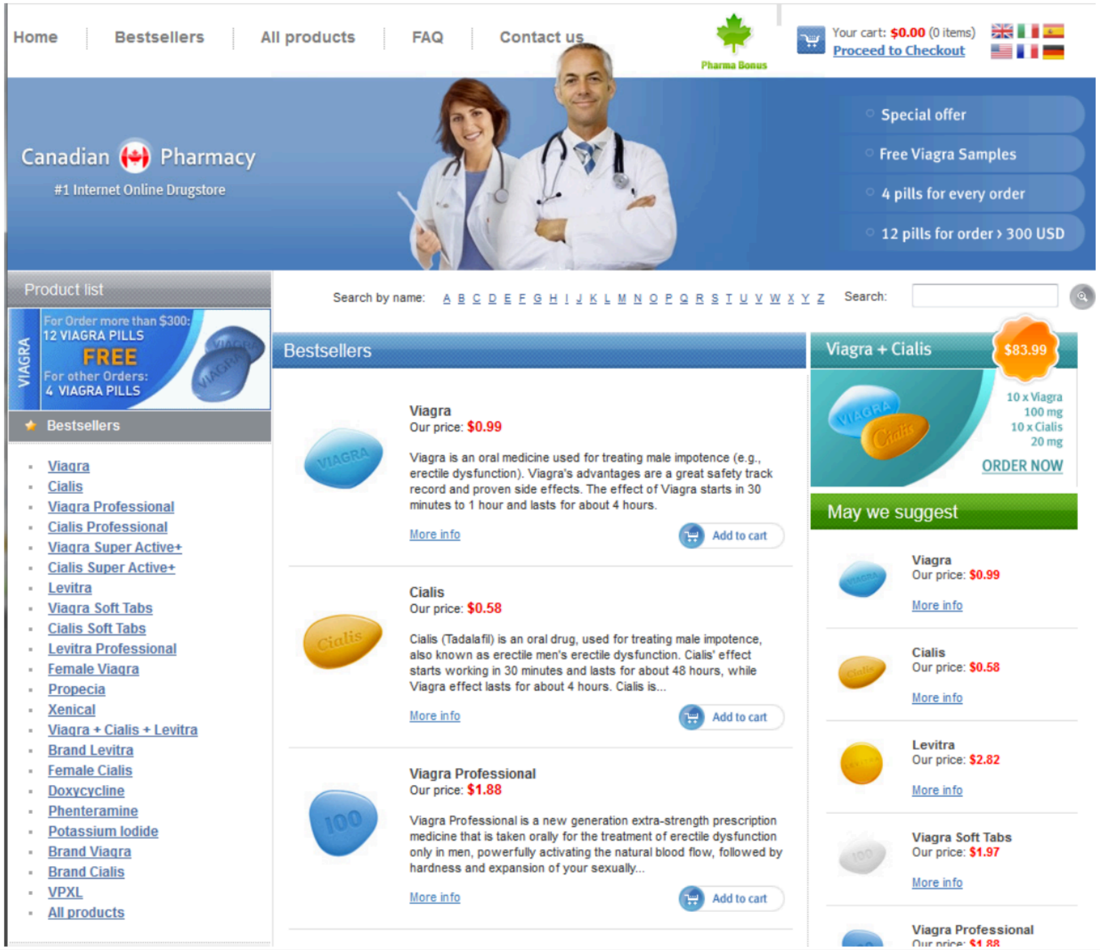
PharmaLeaks

Understanding the Business of Online Pharmaceutical Affiliate Programs

By: Damon McCoy, Andreas Pitsillidis, Grant Jordan, Nicholas Weaver, Christian Kreibich, Brian Krebs, Geoffrey M. Voelker, Stefan Savage, and Kirill Levchenko

[McCoy et al.]

Storefront



Viagra
Our price: $0.99

Viagra is an oral medicine used for treating male impotence (e.g., erectile dysfunction). Viagra's advantages are a great safety track record and proven side effects. The effect of Viagra starts in 30 minutes to 1 hour and lasts for about 4 hours.

More info — Add to cart

Cialis
Our price: $0.58

Cialis (Tadalafil) is an oral drug, used for treating male impotence, also known as erectile men's erectile dysfunction. Cialis' effect starts working in 30 minutes and lasts for about 48 hours, while Viagra effect lasts for about 4 hours. Cialis is...

More info — Add to cart

Viagra Professional
Our price: $1.88

Viagra Professional is a new generation extra-strength prescription medicine that is taken orally for the treatment of erectile dysfunction only in men, powerfully activating the natural blood flow, followed by hardness and expansion of your sexually...

More info — Add to cart

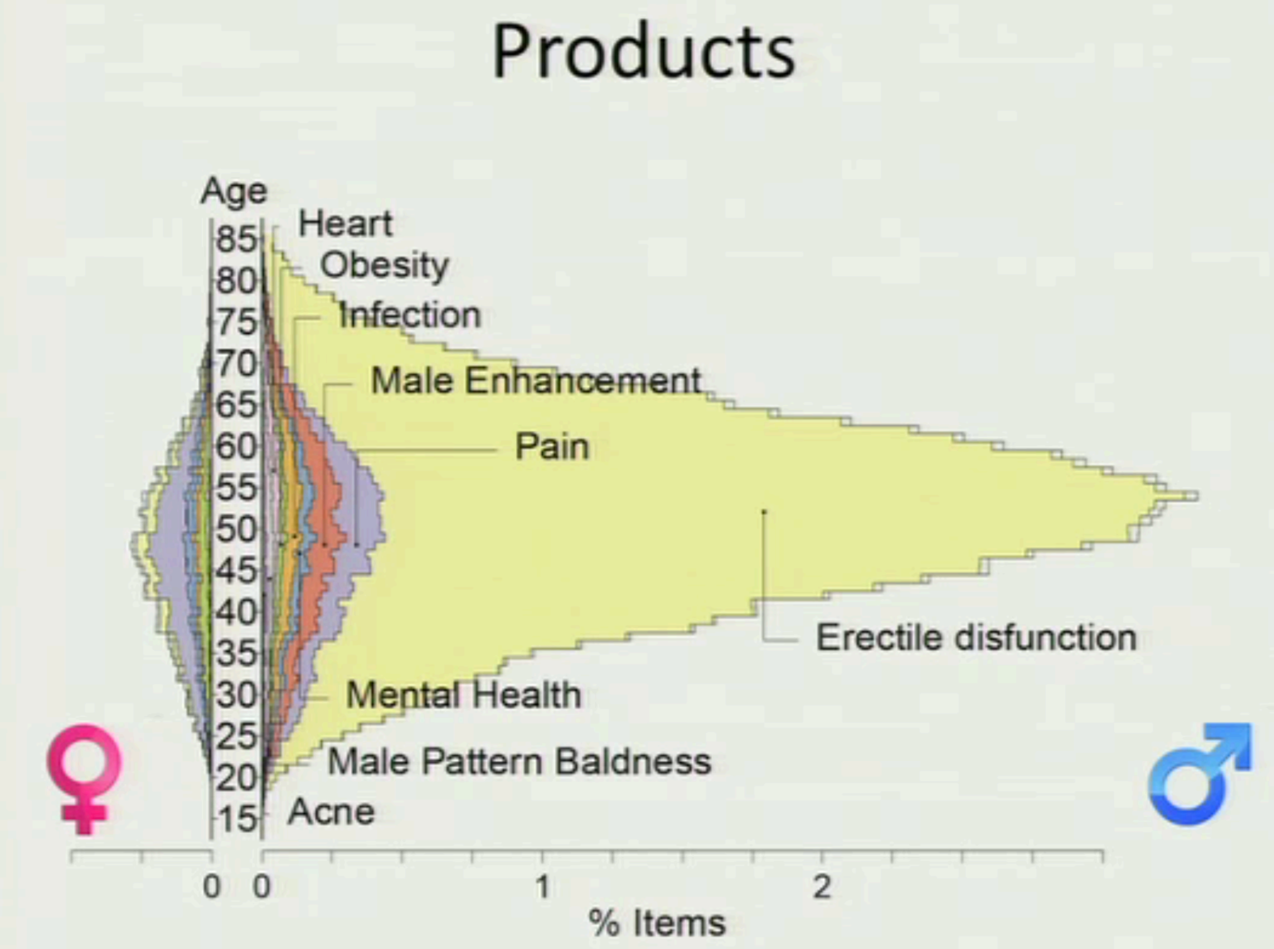
[McCoy et al.]

Pharmaceutical Affiliate Business

- Online pharmaceutical affiliate programs are a major sponsor of spam (email and web)
  - Affiliates (spammers) paid on commission
  - Suppliers
  - Payment processors
- Operates as a business that maintains financial records
- 185M in gross revenue, 1+ million customers, 1.5+ million purchases, 2600+ affiliates
- 95% of customers from US(75%), Canada, Europe and Australia

[McCoy et al.]

Popular products



[McCoy et al.]

Pharmaceuticals (USENIX 2012)

- Analyzed 3 pharmaceutical affiliates programs from the inside (transaction logs)
- Find that payment processors are “weak link”
- Market is not saturated, spamming works

USENIX 2011 [Kanich et al.]

Other Ecosystem Studies (a selection)

- Spamalytics (CCS 2008)
- *Freelance Abuse Labor* (USENIX 2011)
- Spam Revenues (USENIX 2011, Oakland 2011)
- *Pharmaceutical Affiliate Programs* (USENIX 2012)
- Fraudulent Accounts (USENIX 2013)
- Bitcoin (IMC 2013)
- Clickfraud (CCS 2014)

[Kanich et al.]

Spamalytics (CCS 2008)

Infiltrated existing botnet, used it to analyze spam campaigns:

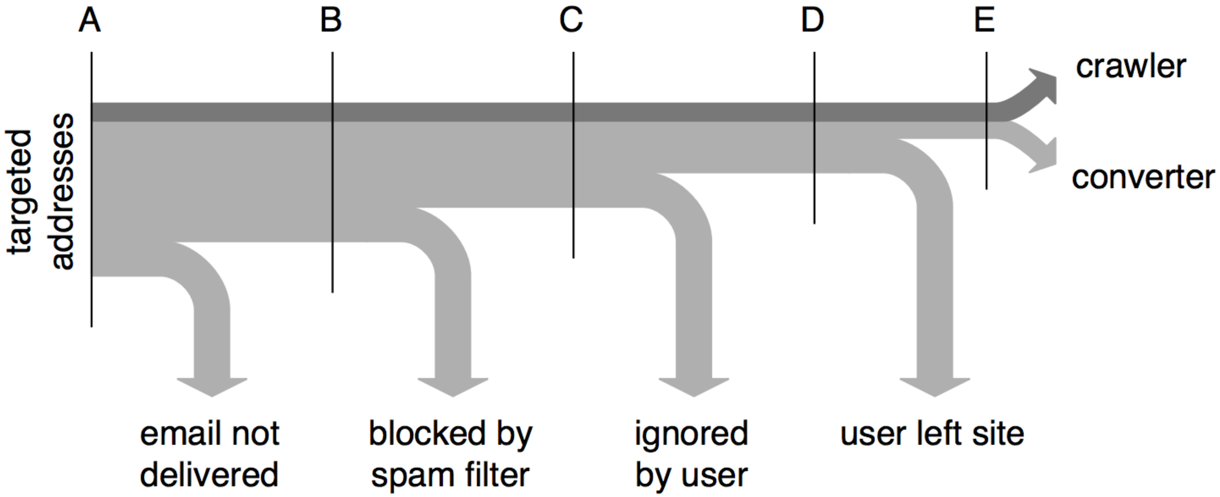
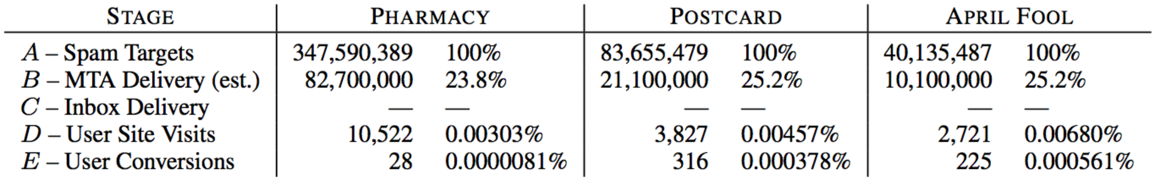


Figure 6: The spam conversion pipeline.



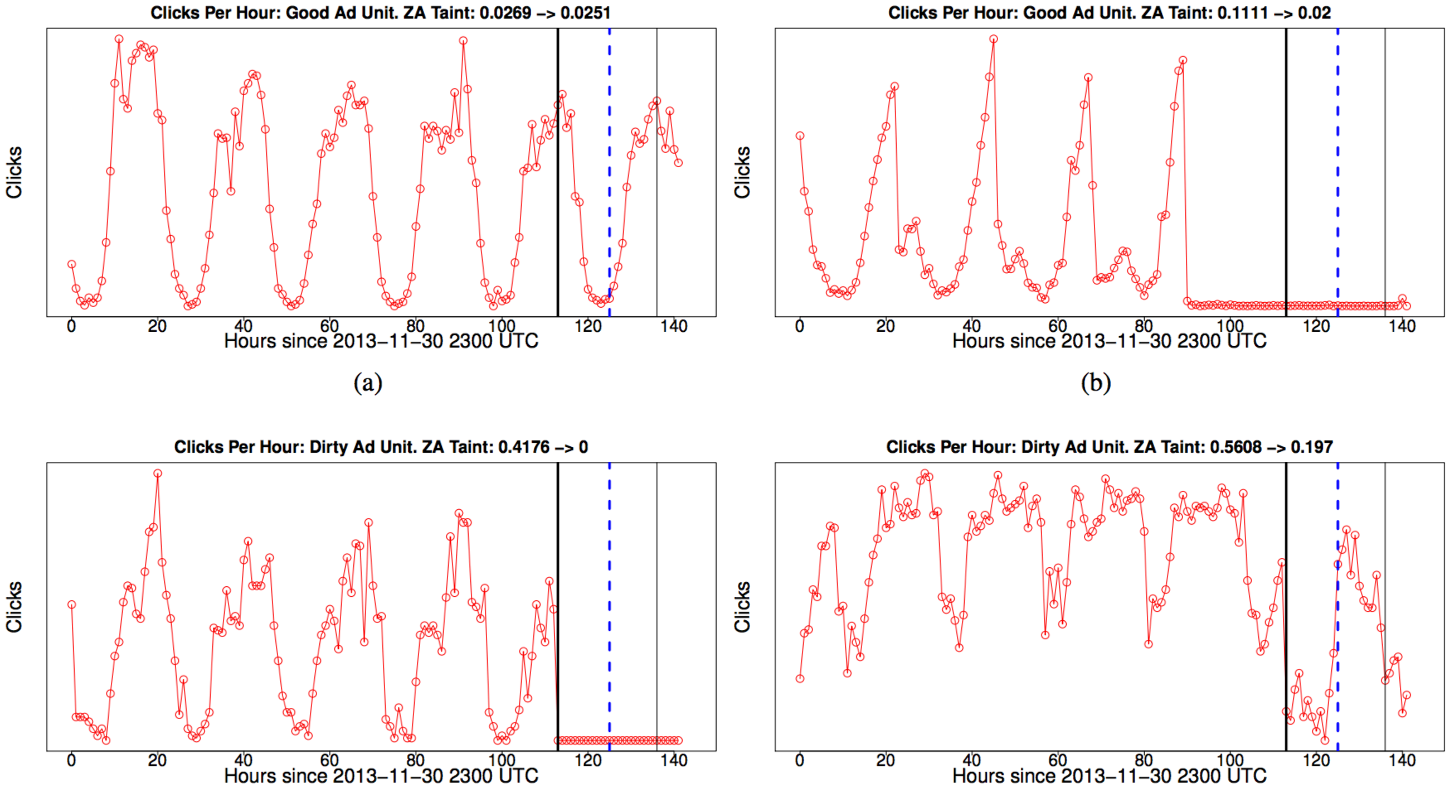
Stage	Pharmacy		Postcard		April Fool	
A – Spam Targets	347,590,389	100%	83,655,479	100%	40,135,487	100%
B – MTA Delivery (est.)	82,700,000	23.8%	21,100,000	25.2%	10,100,000	25.2%
C – Inbox Delivery	—	—	—	—	—	—
D – User Site Visits	10,522	0.00303%	3,827	0.00457%	2,721	0.00680%
E – User Conversions	28	0.0000081%	316	0.000378%	225	0.000561%

Table 3: Filtering at each stage of the spam conversion pipeline for the self-propagation and pharmacy campaigns. Percentages refer to the conversion rate relative to Stage A.

[Pearce et al.]

Clickfraud (CCS 2014)

Observed ad clickfraud coming from ZeroAccess botnet (before/after attempted takedown):



(a)

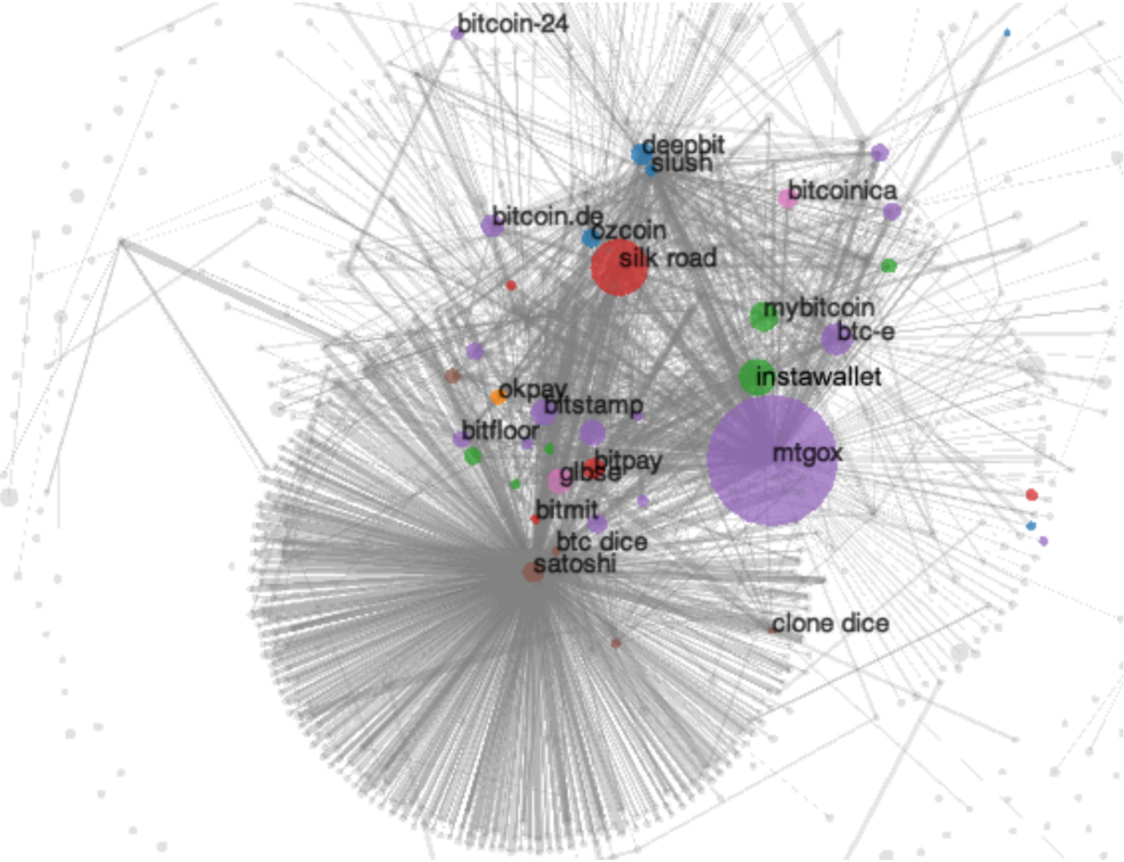
(b)

(c)

(d)

Bitcoin (IMC 2013)

Longitudinal analysis of Bitcoin ecosystem, including clusters of addresses belong to same entity:



HTTP://XKCD.COM/329/

Turing Test

TURING TEST EXTRA CREDIT:
CONVINCE THE EXAMINER THAT HE'S A COMPUTER.
YOU KNOW, YOU MAKE SOME REALLY GOOD POINTS.
I'M ... NOT EVEN SURE WHO I AM ANYMORE.