facebook

innovating to protect the graph

NDSS - 2013

facebook

innovation distinguishes between a leader and a follower

- Steve Jobs

if you're not failing every now and again, it's a sign you're not doing anything very innovative

- Woody Allen

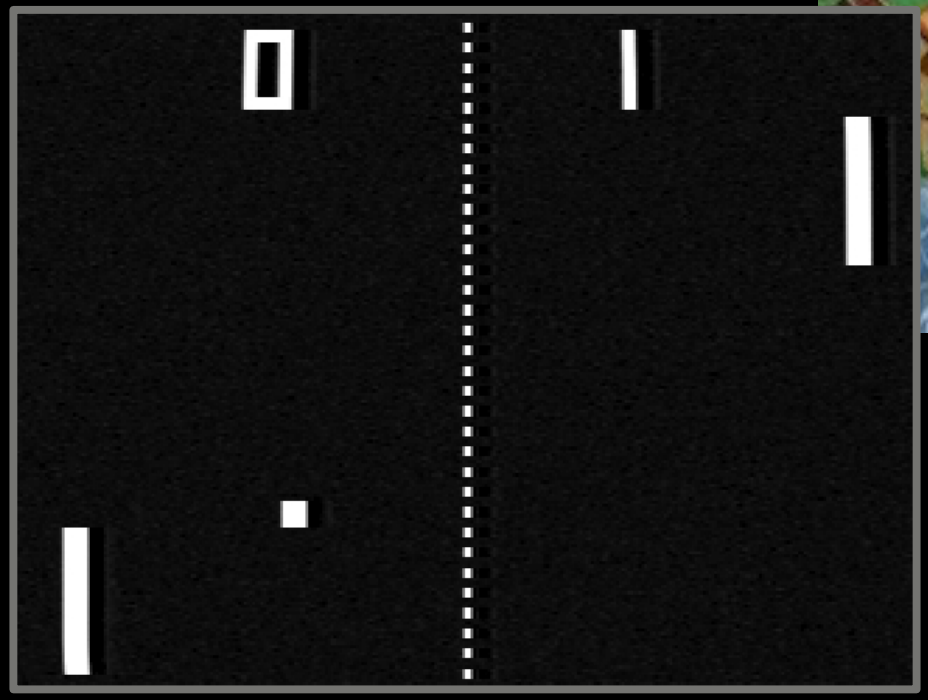
hack = a usually creative solution to a programming limitation

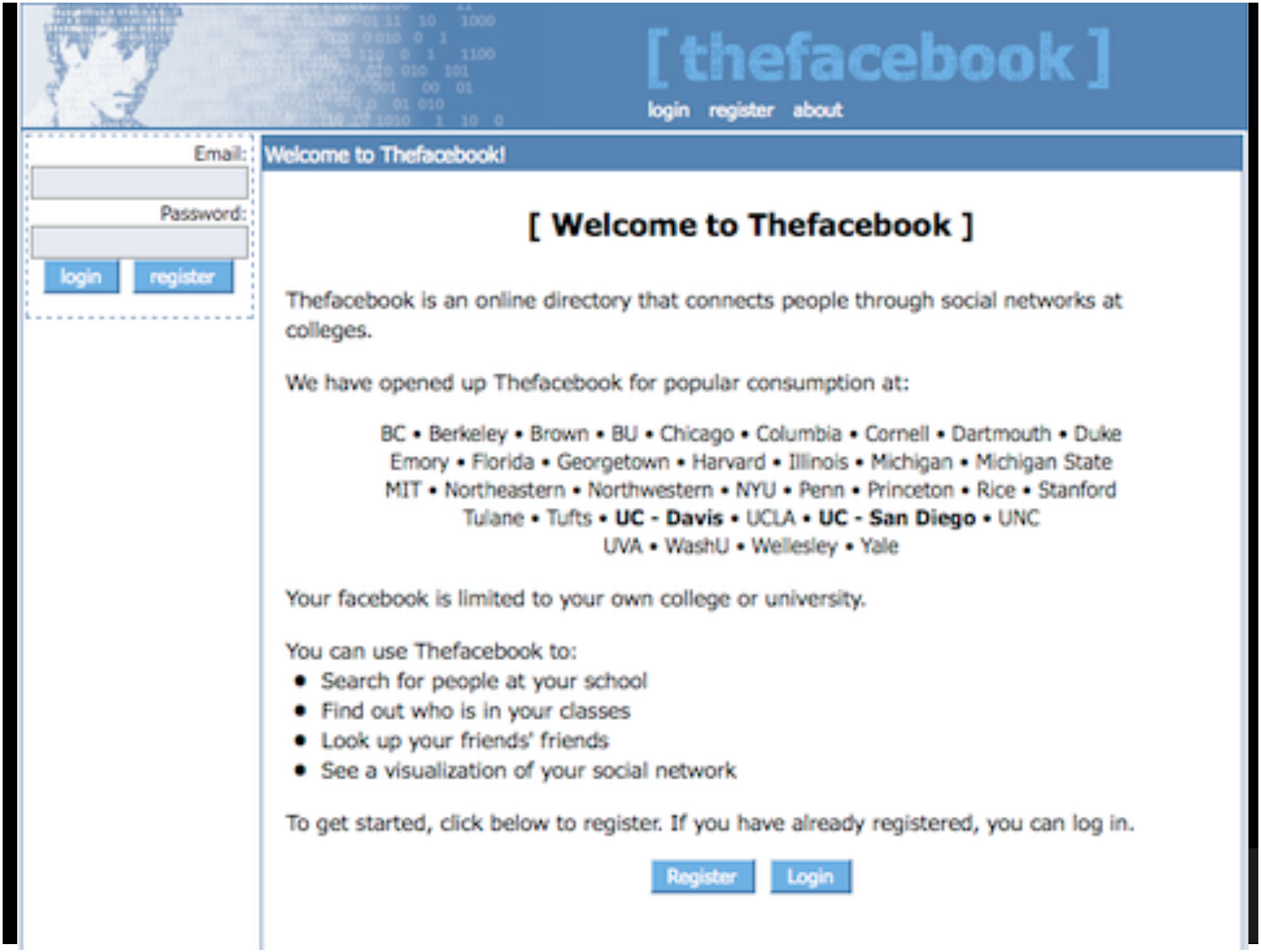
facebook

If they had stopped innovating

facebook

If they had stopped innovating




[thefacebook]
login register about
Email:
Password:
login
register
Welcome to Thefacebook!
[Welcome to Thefacebook]
Thefacebook is an online directory that connects people through social networks at colleges.
We have opened up Thefacebook for popular consumption at:
BC • Berkeley • Brown • BU • Chicago • Columbia • Cornell • Dartmouth • Duke
Emory • Florida • Georgetown • Harvard • Illinois • Michigan • Michigan State
MIT • Northeastern • Northwestern • NYU • Penn • Princeton • Rice • Stanford
Tulane • Tufts • UC - Davis • UCLA • UC - San Diego • UNC
UVA • WashU • Wellesley • Yale
Your facebook is limited to your own college or university.
You can use Thefacebook to:
• Search for people at your school
• Find out who is in your classes
• Look up your friends' friends
• See a visualization of your social network
To get started, click below to register. If you have already registered, you can log in.
Register
Login


Joe Sullivan
Update Info
Activity Log
CSO at Facebook
Studied Law at University of Miami
Lives in Pa
Married to
About
Friends 663
Photos 85
Fullerton
Living
Palo Alto, California
Current City
Cambridge, Massachusetts
Hometown
Relationship
Suzanne Sullivan
Married
History by Year
2008 Started work at Facebook
Ended work at PayPal
2006 Ended work at Ebay
1993 Graduated from University of Miami
1991 In a Relationship with Suzanne Sullivan
1990 Graduated from Providence College
1986 Graduated from Matignon High School

facebook

Facebook Scale…

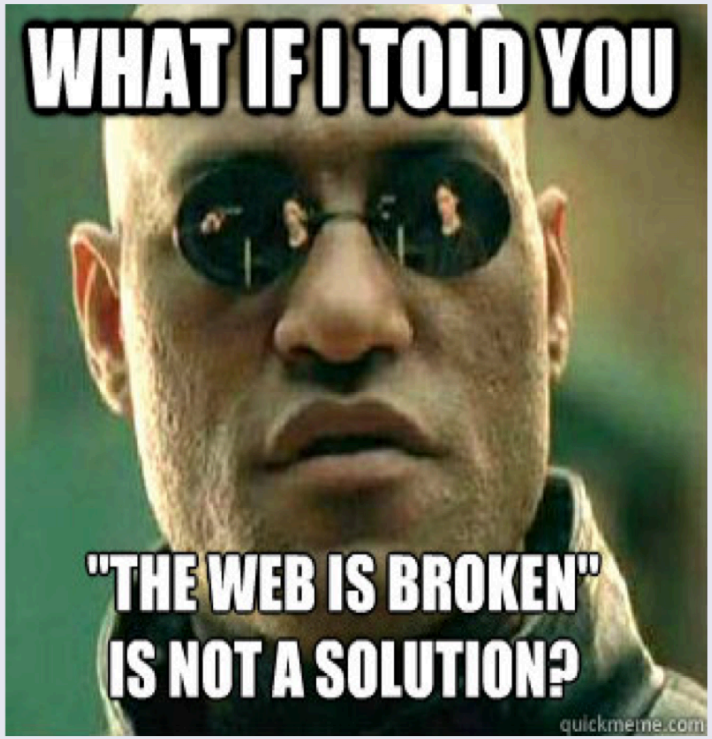
- Every day:
  - >2.5 billion shares
  - >2.7 billion likes
  - >300 million photos
  - >500 TB new data
- >100 PB cluster
- Code updated twice daily

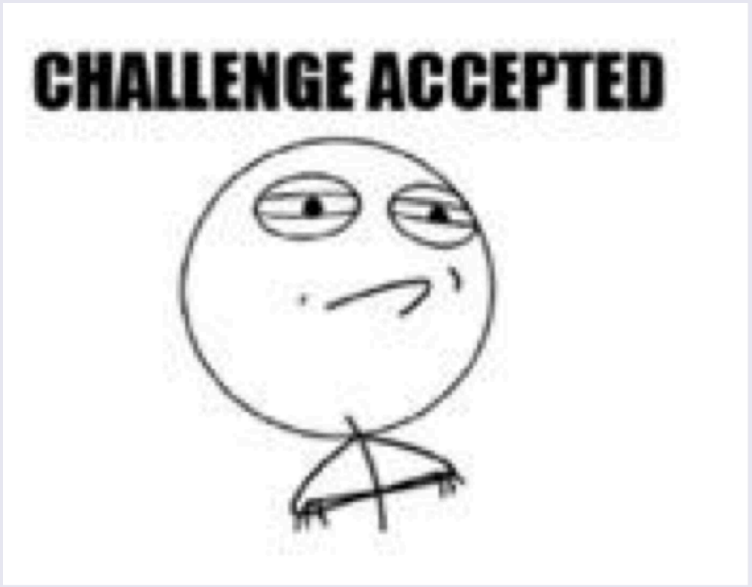
facebook

Threats Also Constantly Evolving

Move fast and break things

- Emphasis is placed on ‘moving fast’ ☺
- The ability to quickly iterate provides security benefits
- Archaic security models and thinking are not welcome





facebook

- Example Areas – Product
  - User Education
  - Content Screening
  - Event Screening
- Example Areas – Not Product
  - Enforcement
  - Bug Bounty
  - Drills
  - Employee Education
  - Corp InfoSec

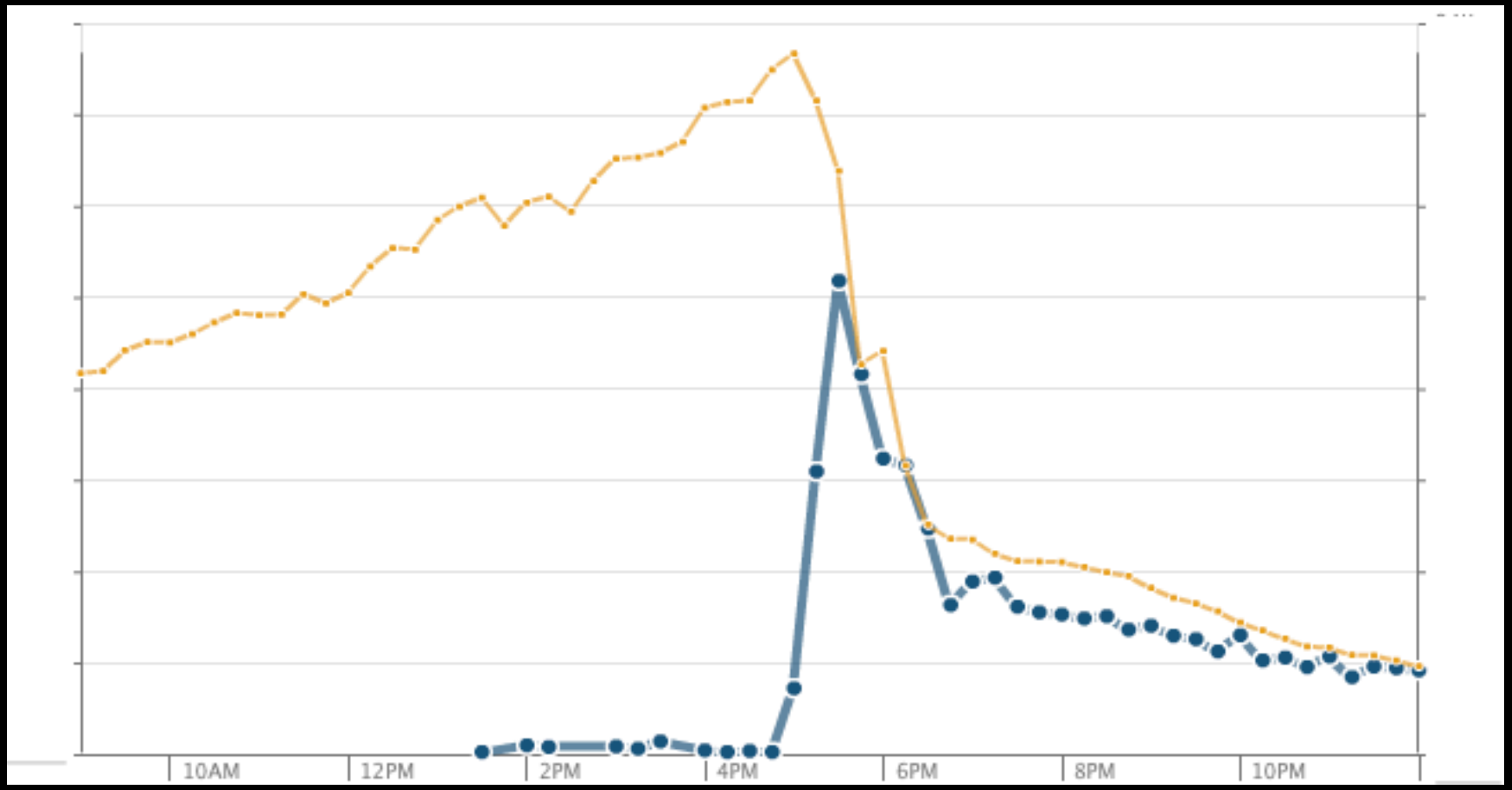
facebook

Data validates: user education works

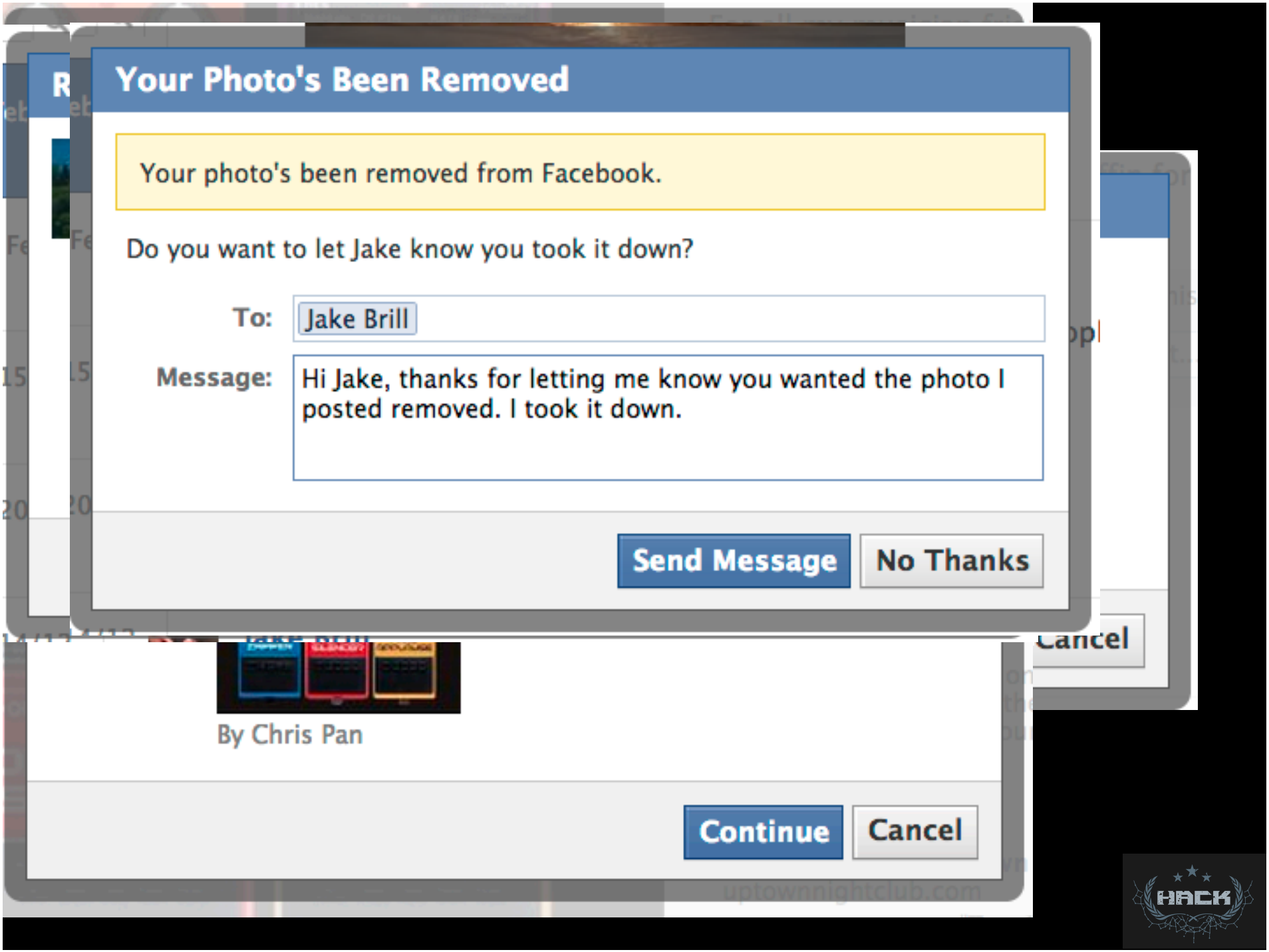
- Proof: contextual messaging
- Proof: social reporting
- Proof: HTTPS

facebook

impact of Self XSS education



orange = spam distro / blue = checkpoints

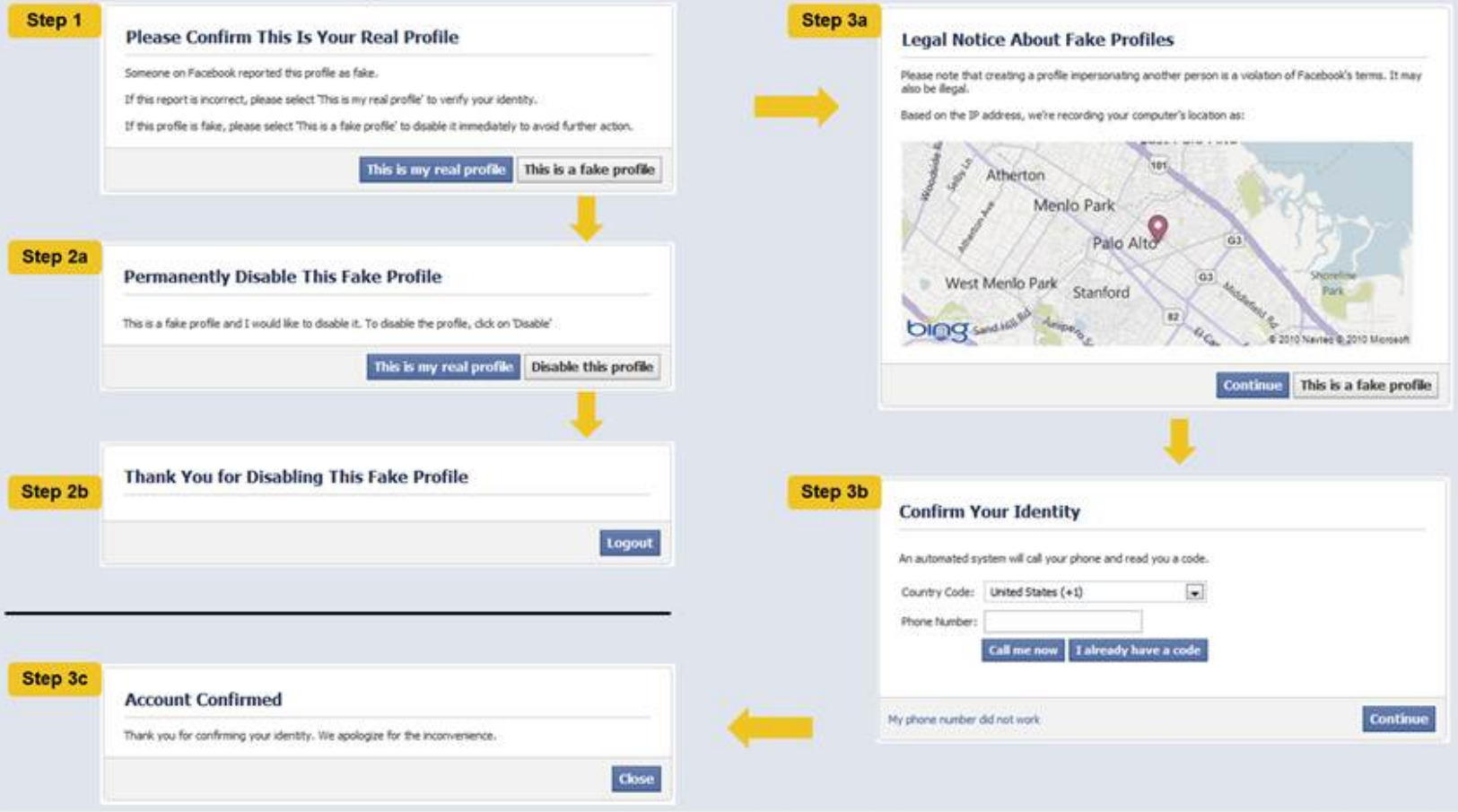

Your Photo's Been Removed
Your photo's been removed from Facebook.
Do you want to let Jake know you took it down?
To:
Jake Brill
Message:
Hi Jake, thanks for letting me know you wanted the photo I posted removed. I took it down.
Send Message
No Thanks
By Chris Pan
Continue
Cancel
Cancel

facebook

social reporting = 85% of time removal or conversation

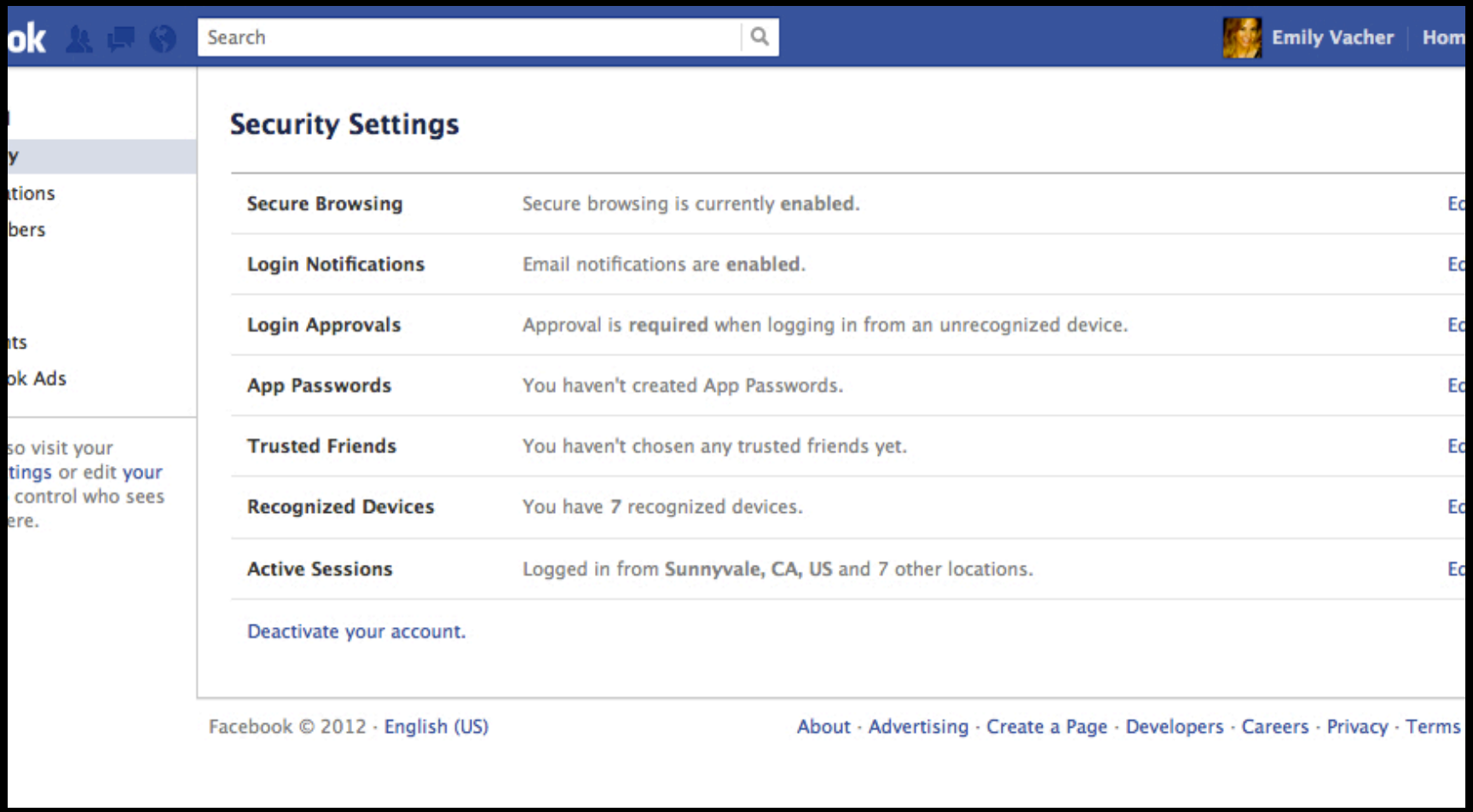
facebook

Impersonating Checkpoint - Stringent warning + location + phone confirmation



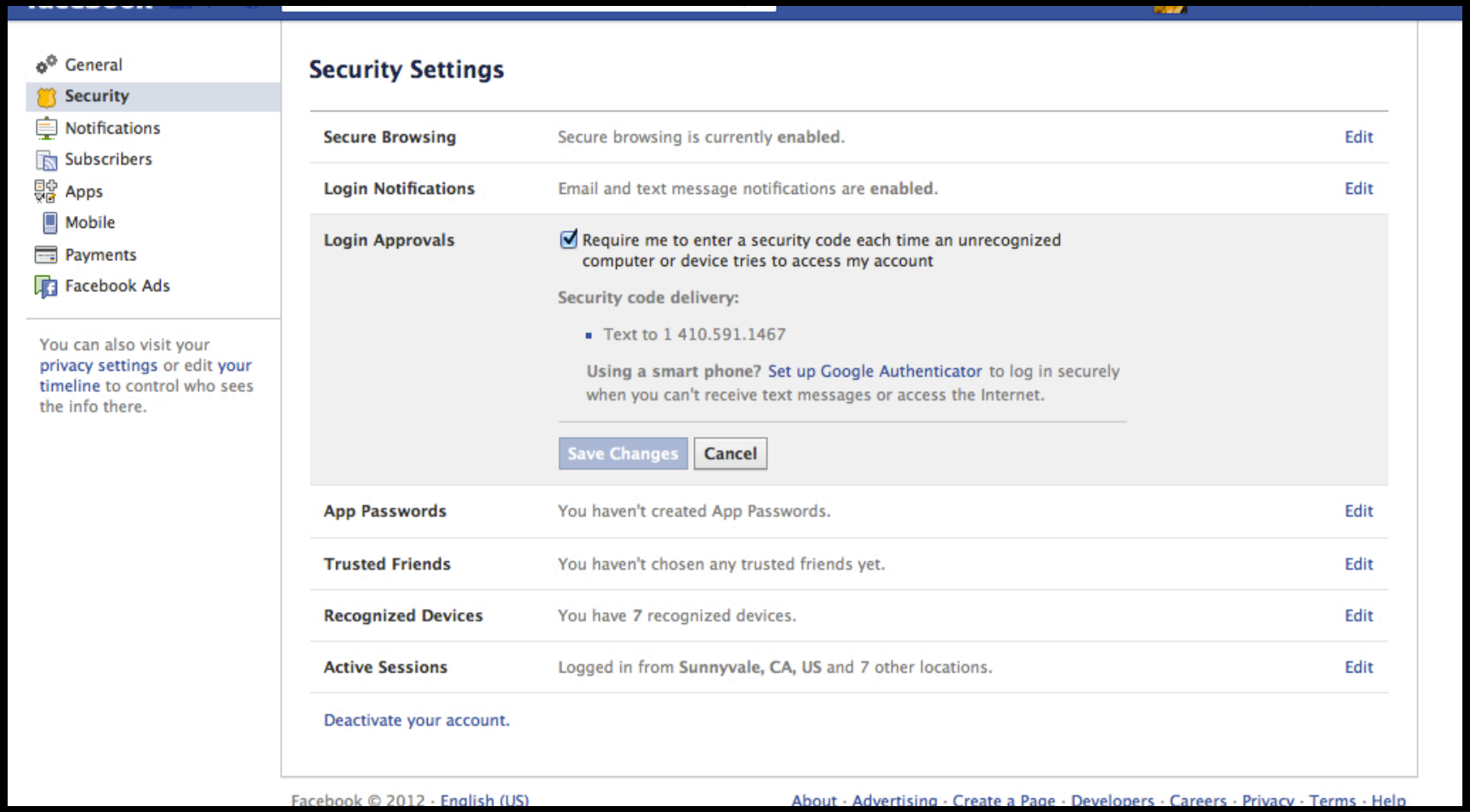
facebook

Security settings



facebook

Login approvals



facebook

Link Shim

- Intercept off-site links
- Screen against classifiers and industry lists
- Real-time warnings
- Prevent referrer leakage
- Hashes to avoid open redirects
- Dynamically rewrite for better usability

facebook

Photo DNA

- Run all uploaded photos against hashes provided by NCMEC.
- Immediately disable users who upload an image on the hash list and send image and User information to NCMEC.
- Investigate users caught by Photo DNA to locate other images and potentially escalate to law enforcement.

Facebook's New Way to Combat Child Pornography

By RIVA RICHMOND

PhotoDNA works by carving an image into blocks and subjecting it to an array of measurements, allowing it to identify offending images even if they have been cropped.

facebook

Facebook Immune System

- Every event is a classification problem
- Works in real time
- Combined with other resources and inputs
- Random Forests, Logistic Regression, SVMs, Naive Bayes, Boosting Trees…

facebook

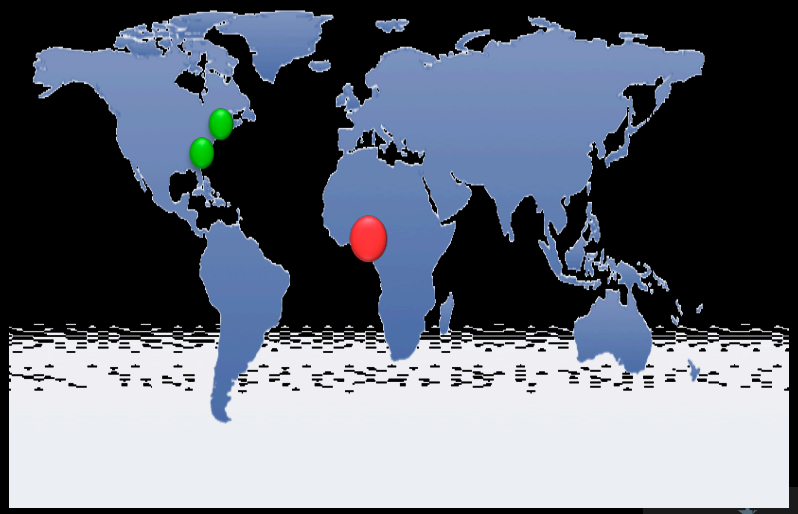
Classifying Spam

- User reports
- Keywords
- Links
- IP addresses
- And more!

facebook

Classifying Compromised Logins

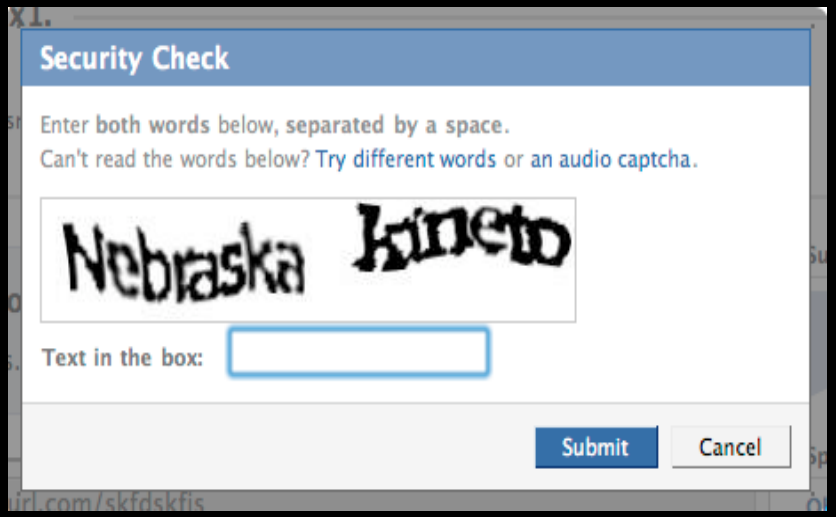
- Number of recent failures
- Geographic location
- Known or unknown device
- And more!



facebook

Roadblocks

- Captchas
- Rate limiting
- Disabling



facebook

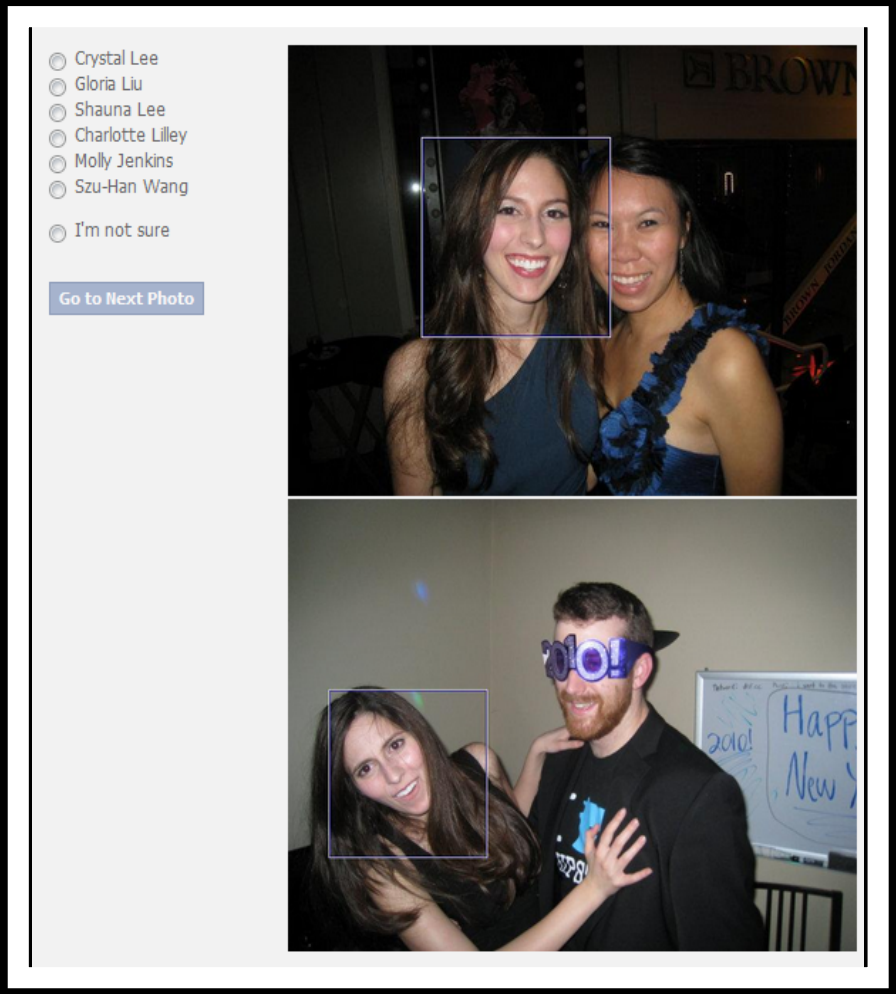
Malware Checkpoint

- Detect malware behaviors?
- Prompt for free anti-virus download
- Block login until malware is cleared

facebook

Social Authentication

- Shown photos of a friend
- Required to identify friend
- Easy for account owner, difficult for an attacker



facebook

sometimes the best defense is a good offense

Escalating Cases

- Investigations into high value suspects
- Suspects tied to real Facebook accounts
- Coordinate with Industry on technical takedowns
- Work with Legal on lawsuits
- Escalate to law enforcement when appropriate

facebook

Bug Bounty Program

- Hack Facebook
- Get Paid
- Get Press

facebook

political issues → security questions

- filtering?
- forced downgrades?
- MITM attacks?
- malicious javascript?
- bogus certificates?
- account takeovers?

The Inside Story of How Facebook Responded to Tunisian Hacks

JAN 24 2011, 1:20 AM ET | 76

Recommend 9K

It was on Christmas Day that Facebook's Chief Security Officer Joe Sullivan first noticed strange things going on in Tunisia. Reports started to trickle in that political-protest pages were being hacked. "We were

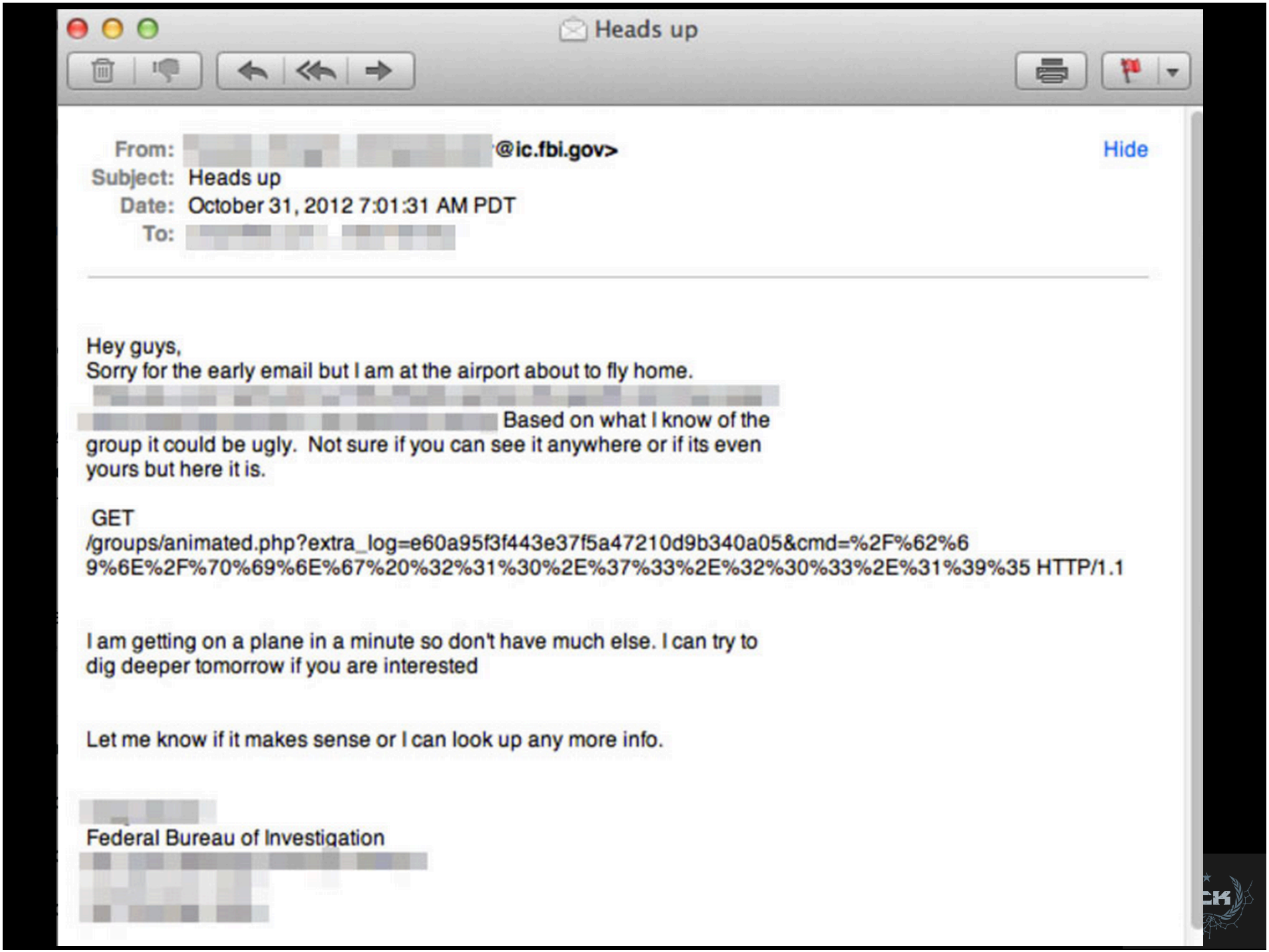
facebook


Sun
Jan 23
Mon
Tue
Wed
Thu
Fri
Sat
Sun
Jan 30
Mon
Tue
Wed
Thu
Fri
Sat
Sun
Feb 6
Mon

facebook

corp infosec

- Just as important
  - Expanded bug bounty
  - Teams cover both and think about both
- Products disappointing
- Endpoints also insecure
- “big data” investments interesting
- Ridiculous lack of talent available for hardening work


Heads up
From: [redacted]@ic.fbi.gov>
Hide
Subject: Heads up
Date: October 31, 2012 7:01:31 AM PDT
To: [redacted]
Hey guys,
Sorry for the early email but I am at the airport about to fly home.
[redacted] Based on what I know of the group it could be ugly. Not sure if you can see it anywhere or if its even yours but here it is.
GET /groups/animated.php?extra_log=e60a95f3f443e37f5a47210d9b340a05&cmd=%2F%62%69%6E%2F%70%69%6E%67%20%32%31%30%2E%37%33%2E%32%30%33%2E%31%39%35 HTTP/1.1
I am getting on a plane in a minute so don't have much else. I can try to dig deeper tomorrow if you are interested
Let me know if it makes sense or I can look up any more info.
[redacted]
Federal Bureau of Investigation
[redacted]

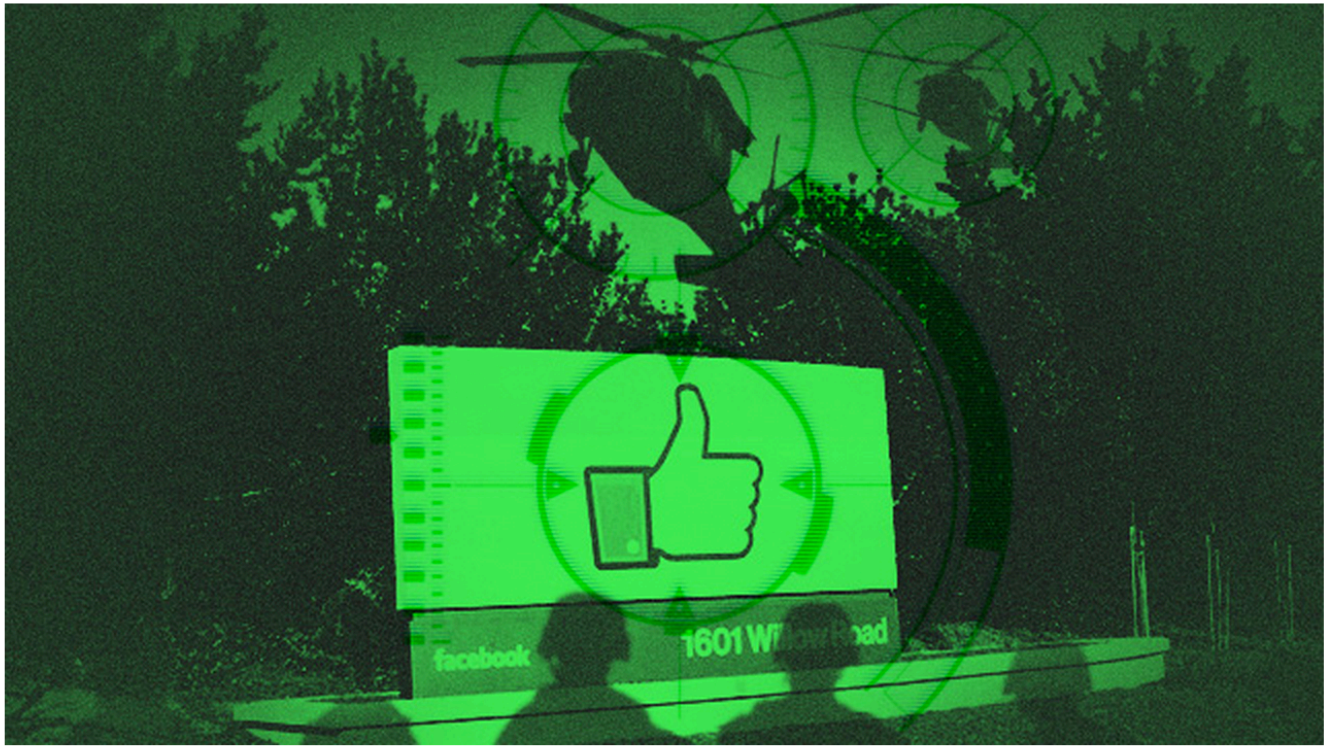
facebook

At Facebook, zero-day exploits, backdoor code bring war games drill to life

How do companies prepare for the worst? By exposing workers to lifelike crises.

by **Dan Goodin** - Feb 10 2013, 5:00pm PST

HACKING INTERNET CRIME 12



Aurich Lawson

Early on Halloween morning, members of Facebook's Computer Emergency Response Team received an urgent e-mail from an FBI special agent who regularly briefs them on security matters. The e-mail contained a Facebook link to a PHP script that appeared to give anyone who knew its location unfettered access to the site's front-end system. It also referenced a suspicious IP address

facebook

Watering Hole Attack

facebook

Research happens…

- Just announced Michigan partnership
- Regular dialogue with Stanford about projects
- Foundation work for enterprise anomalous behavior detection by 2012 intern
- MITM detection paper forthcoming
- Social Authentication related to MSFT paper
- User Trust work ongoing

facebook

- innovation is essential on the internet
- security teams cannot say no to opportunities, must show how to do it safely, and constantly adapt
- a culture of innovation starts at the top
- any team can be innovative if everyone feels broad responsibility