innovating to protect the graph

NDSS - 2013
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
If they had stopped innovating
facebook

If they had stopped innovating
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.
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
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

**WHAT IF I TOLD YOU**

"THE WEB IS BROKEN" IS NOT A SOLUTION?

**CHALLENGE ACCEPTED**
facebook

• Example Areas – Product
  – User Education
  – Content Screening
  – Event Screening

• Example Areas – Not Product
  – Enforcement
  – Bug Bounty
  – Drills
  – Employee Education
  – Corp InfoSec
Data validates: user education works

- Proof: contextual messaging
- Proof: social reporting
- Proof: HTTPS
impact of Self XSS education

orange = spam distro / blue = checkpoints
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
facebook

social reporting = 85% of time removal or conversation
Impersonating Checkpoint - Stringent warning + location + phone confirmation

Step 1: Please Confirm This Is Your Real Profile
- Someone on Facebook reported this profile as fake.
- If this report is incorrect, please select 'This is my real profile' to verify your identity.
- If this profile is fake, please select 'This is a fake profile' to disable it immediately to avoid further action.

Step 2a: Permanently Disable This Fake Profile
- This is a fake profile and I would like to disable it. To disable the profile, click on 'Disable'.

Step 2b: Thank You for Disabling This Fake Profile

Step 3a: Legal Notice About Fake Profiles
- Please note that creating a profile impersonating another person is a violation of Facebook's terms. It may also be illegal.
- Based on the IP address, we're recording your computer's location as:

Step 3b: Confirm Your Identity
- An automated system will call your phone and read you a code.
- Country Code: United States (+1)
- Phone Number:
- Call me now | I already have a code
- My phone number did not work.

Step 3c: Account Confirmed
- Thank you for confirming your identity. We apologize for the inconvenience.
## Security Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Browsing</td>
<td>Secure browsing is currently enabled.</td>
</tr>
<tr>
<td>Login Notifications</td>
<td>Email notifications are enabled.</td>
</tr>
<tr>
<td>Login Approvals</td>
<td>Approval is required when logging in from an unrecognized device.</td>
</tr>
<tr>
<td>App Passwords</td>
<td>You haven't created App Passwords.</td>
</tr>
<tr>
<td>Trusted Friends</td>
<td>You haven't chosen any trusted friends yet.</td>
</tr>
<tr>
<td>Recognized Devices</td>
<td>You have 7 recognized devices.</td>
</tr>
<tr>
<td>Active Sessions</td>
<td>Logged in from Sunnyvale, CA, US and 7 other locations.</td>
</tr>
</tbody>
</table>

Deactivate your account.
Login approvals

Security Settings

Secure Browsing
Secure browsing is currently enabled.

Login Notifications
Email and text message notifications are enabled.

Login Approvals

- Require me to enter a security code each time an unrecognized computer or device tries to access my account

Security code delivery:
- Text to 1 410.591.1467

Using a smart phone? Set up Google Authenticator to log in securely when you can't receive text messages or access the Internet.

App Passwords
You haven't created App Passwords.

Trusted Friends
You haven't chosen any trusted friends yet.

Recognized Devices
You have 7 recognized devices.

Active Sessions
Logged in from Sunnyvale, CA, US and 7 other locations.

Deactivate your account.
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
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 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...
Classifying Spam

- User reports
- Keywords
- Links
- IP addresses
- And more!
Classifying Compromised Logins

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

Roadblocks

- Captchas
- Rate limiting
- Disabling
Malware Checkpoint

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

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

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
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
Hey guys,
Sorry for the early email but I am at the airport about to fly home.
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%6F%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.

Federal Bureau of Investigation
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

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
• 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