blackhat ABU DHABI 2012

DECEMBER 10 – 13, 2012
EMIRATES PALACE | UNITED ARAB EMIRATES

In partnership with:
TRA هيئة تنظيم الاتصالات
TELECOMMUNICATIONS REGULATORY AUTHORITY
KHALIFA UNIVERSITY

Supported by:
aeCERT Computer Emergency Response Team

SOCIAL ENGINEERING THREATS & COUNTERMEASURES IN AN OVERLY CONNECTED WORLD

SHANE MACDOUGALL
TACTICAL INTELLIGENCE INC.

About Me

- InfoSec since 1989
- Worked as pentester for 13 years,
- Defensive (mostly) side for 10 years
- Work for Tactical Intelligence Inc.
- Use SE regularly for intel gathering
- Two-time winner of Defcon SECTF
- Placed top 3 in call portion every year

WARNING/DISCLAIMER

Many of the techniques described in this Presentation are unethical/potentially illegal.

They are being discussed since they are used routinely by hackers/nation states/attackers.

The presenter does not condone any of these acts, however being informed allows you to be better prepared/protected.

What is Social Engineering?

An *interpersonal* interaction in which one person (attacker) manipulates the other part(ies) into revealing information they shouldn't or performing a task which the attacker desires.

What is Social Engineering?

Phishing is NOT social engineering.

It is a tool used by social engineers.

Big difference!

What is Social Engineering?

If no interpersonal communications involved,

It's NOT social engineering.

Can be phone or in person.
Not email.

If it can be automated, it's not SE (at least yet)

Famous SE?

Famous SE?

Famous (Recent) SE Incidents

White House Hack

Anonymous

Mat Honan

Coca-Cola

AT&T

Ugnazi

The Attack

- Identify the targets
- Create the dossier / perform OSINT recon
- Launch the attack – “social handshake”
- Create PST
- PROFIT!

Identify The Targets

For the purposes of this presentation, we assume you already know your target.

If you need to determine who best to target:

- Business resources
- Social media
- Government filings

Identify The Targets

Groups in turmoil usually yield:

- Disgruntled/alienated employees
- W/ layoffs current/past employees open to bribery/malicious intent
- With staff churn much easier to insert yourself as a “new employee”

The Attack

- Identify the targets
- Create the dossier / perform OSINT recon
- Launch the attack
- Create PST
- PROFIT!

The Dossier

Critical to success for creating a PST

Purpose is to generate either actionable intelligence, or create a repository of data to use in “push polling”

The Dossier

To create the PST we target:

- Company
- Employees
- Contractors
- Suppliers
- Competitors

The Dossier

To create the PST we target:

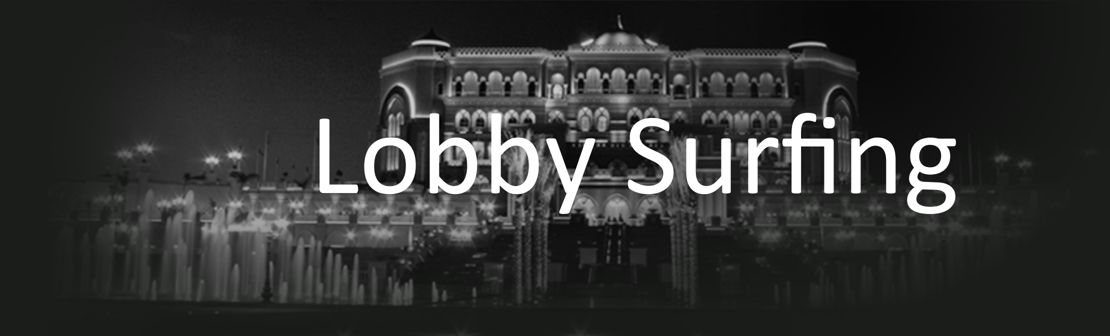
- Company
- Employees
- Contractors
- Suppliers
- Competitors

Company Flags

- Physical plant
- Security systems
- Internal Lingo
- Computer/phone systems
- Operational information
- Competitors

Company Flags

- Voicemail/Phone Directory enumeration
- Dumpster diving
- Lobby Surfing



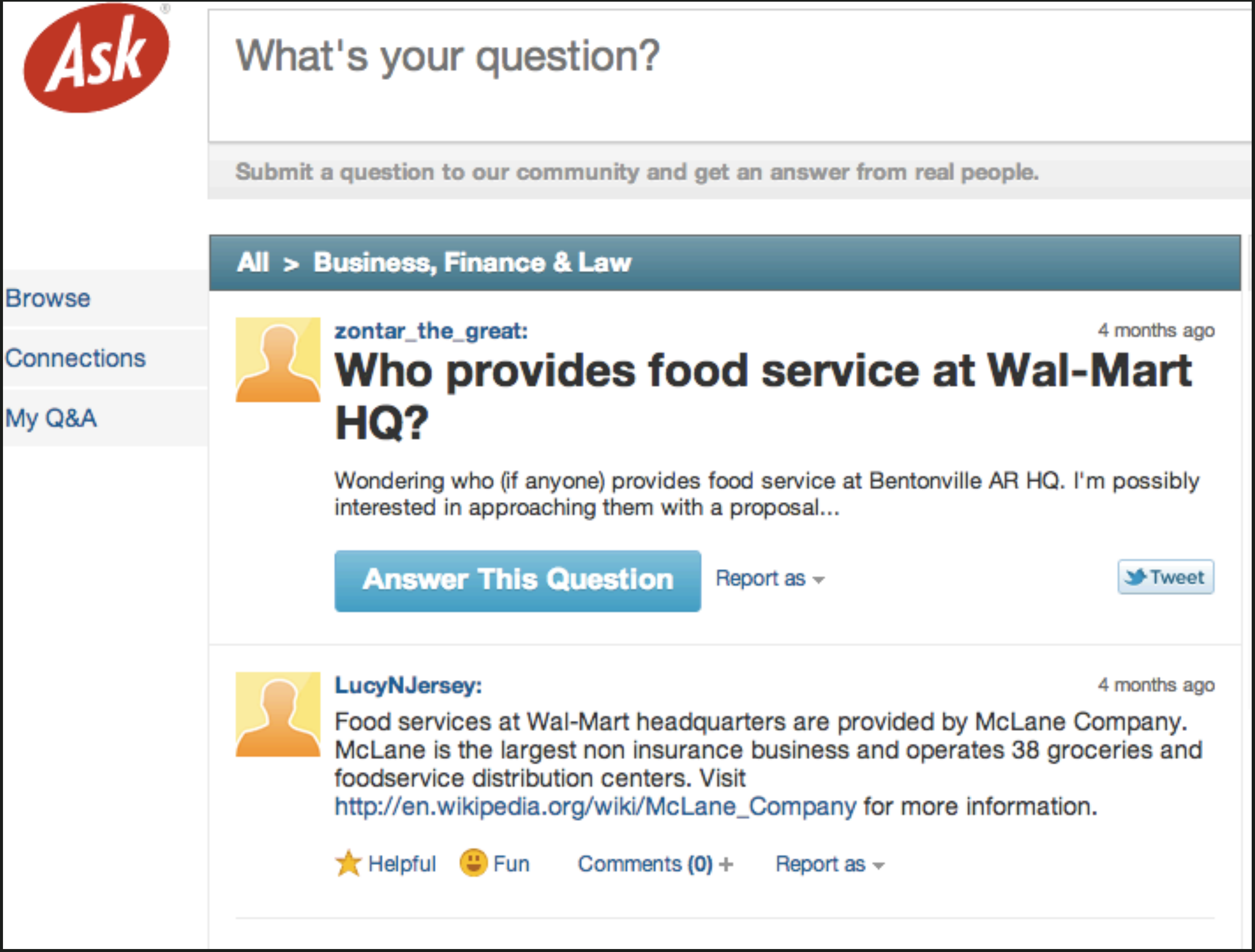
Lobby Surfing

- vendor/client/employee names (sign-in sheet/“welcome visitor” lobby signs)
- employee names, positions and home addresses (magazine labels)
- general assessment of overall security posture (is CCTV present? PTZ/fixed? Are proximity cards or biometrics in use? Guards? Is piggybacking allowed?)

Ask and Ye Shall Receive!

Want some hard to get / esoteric information about a client?

ASK for it (or ASK.com for it)



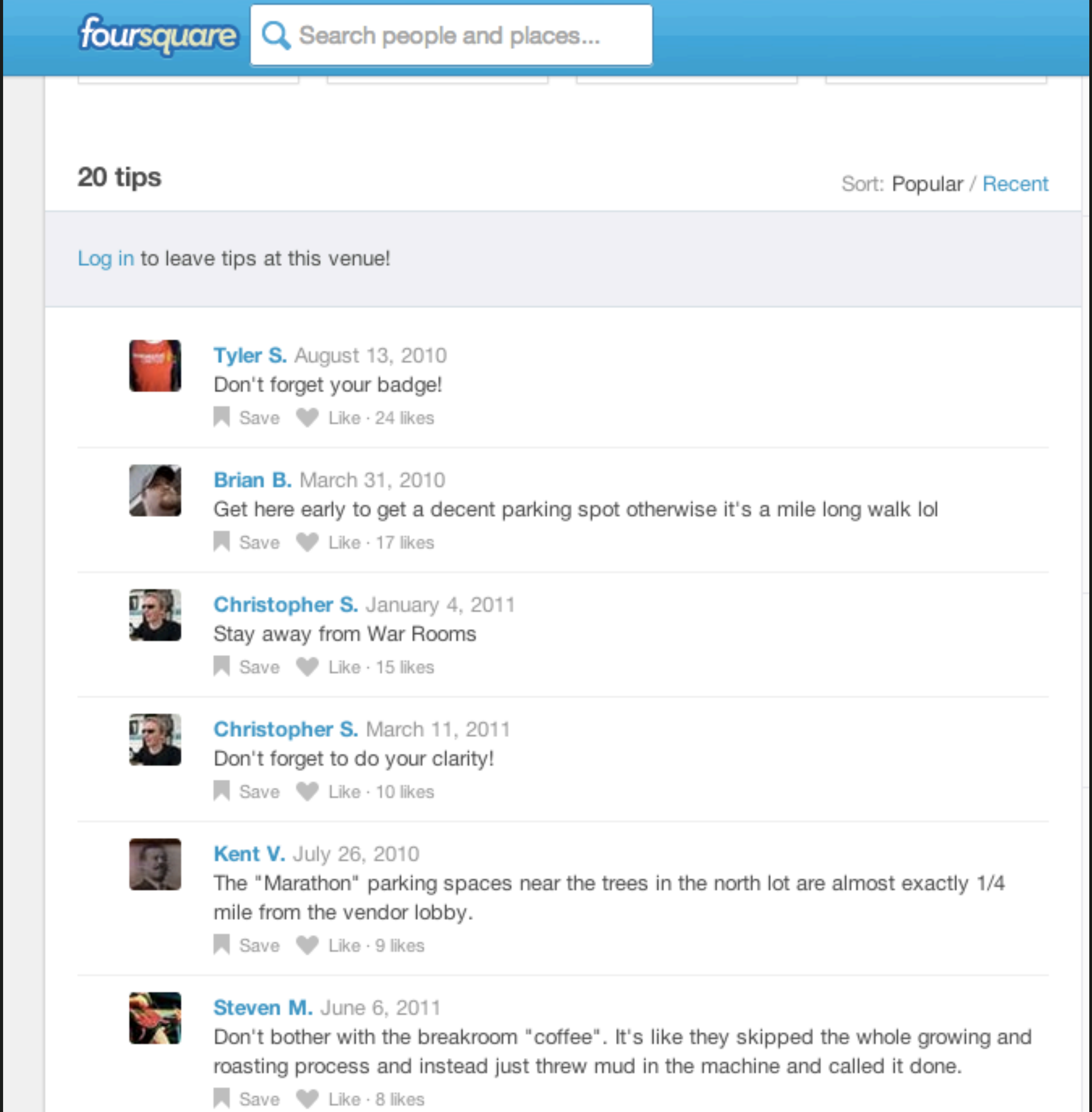
zontar_the_great: 4 months ago

Who provides food service at Wal-Mart HQ?

Wondering who (if anyone) provides food service at Bentonville AR HQ. I'm possibly interested in approaching them with a proposal...

LucyNJersey: 4 months ago

Food services at Wal-Mart headquarters are provided by McLane Company. McLane is the largest non insurance business and operates 38 groceries and foodservice distribution centers. Visit http://en.wikipedia.org/wiki/McLane_Company for more information.



20 tips

Sort: Popular / Recent

Log in to leave tips at this venue!

Tyler S. August 13, 2010
Don't forget your badge!
Save Like · 24 likes

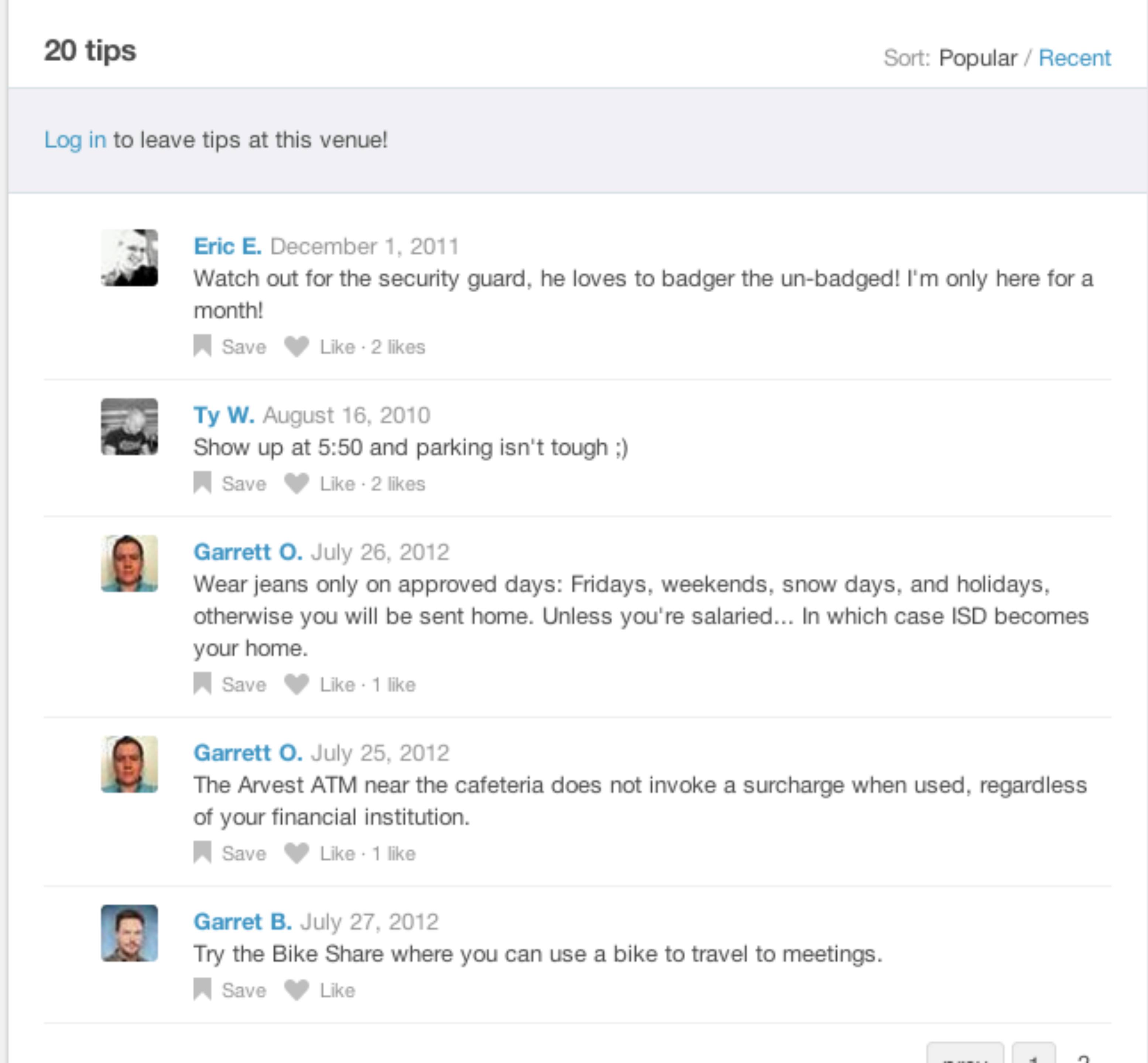
Brian B. March 31, 2010
Get here early to get a decent parking spot otherwise it's a mile long walk lol
Save Like · 17 likes

Christopher S. January 4, 2011
Stay away from War Rooms
Save Like · 15 likes

Christopher S. March 11, 2011
Don't forget to do your clarity!
Save Like · 10 likes

Kent V. July 26, 2010
The "Marathon" parking spaces near the trees in the north lot are almost exactly 1/4 mile from the vendor lobby.
Save Like · 9 likes

Steven M. June 6, 2011
Don't bother with the breakroom "coffee". It's like they skipped the whole growing and roasting process and instead just threw mud in the machine and called it done.
Save Like · 8 likes



20 tips

Log in to leave tips at this venue!

Eric E. December 1, 2011
Watch out for the security guard, he loves to badger the un-badged! I'm only here for a month!

Ty W. August 16, 2010
Show up at 5:50 and parking isn't tough ;)

Garrett O. July 26, 2012
Wear jeans only on approved days: Fridays, weekends, snow days, and holidays, otherwise you will be sent home. Unless you're salaried... In which case ISD becomes your home.

Garrett O. July 25, 2012
The Arvest ATM near the cafeteria does not invoke a surcharge when used, regardless of your financial institution.

Garret B. July 27, 2012
Try the Bike Share where you can use a bike to travel to meetings.

The Dossier

To create the PST we target:

- Company
- Employees
- Contractors
- Suppliers
- Competitors

Employee Flags

- Interests (political, sports)
- Common hangouts (4Square)
- Religion
- Pets / Relatives (password cracking)
- Open to “relationship” (single)
- Open to blackmail (dating sites, illicit sites)
- Open to bribery
- Open to phishing (sophistication)

Employee Data

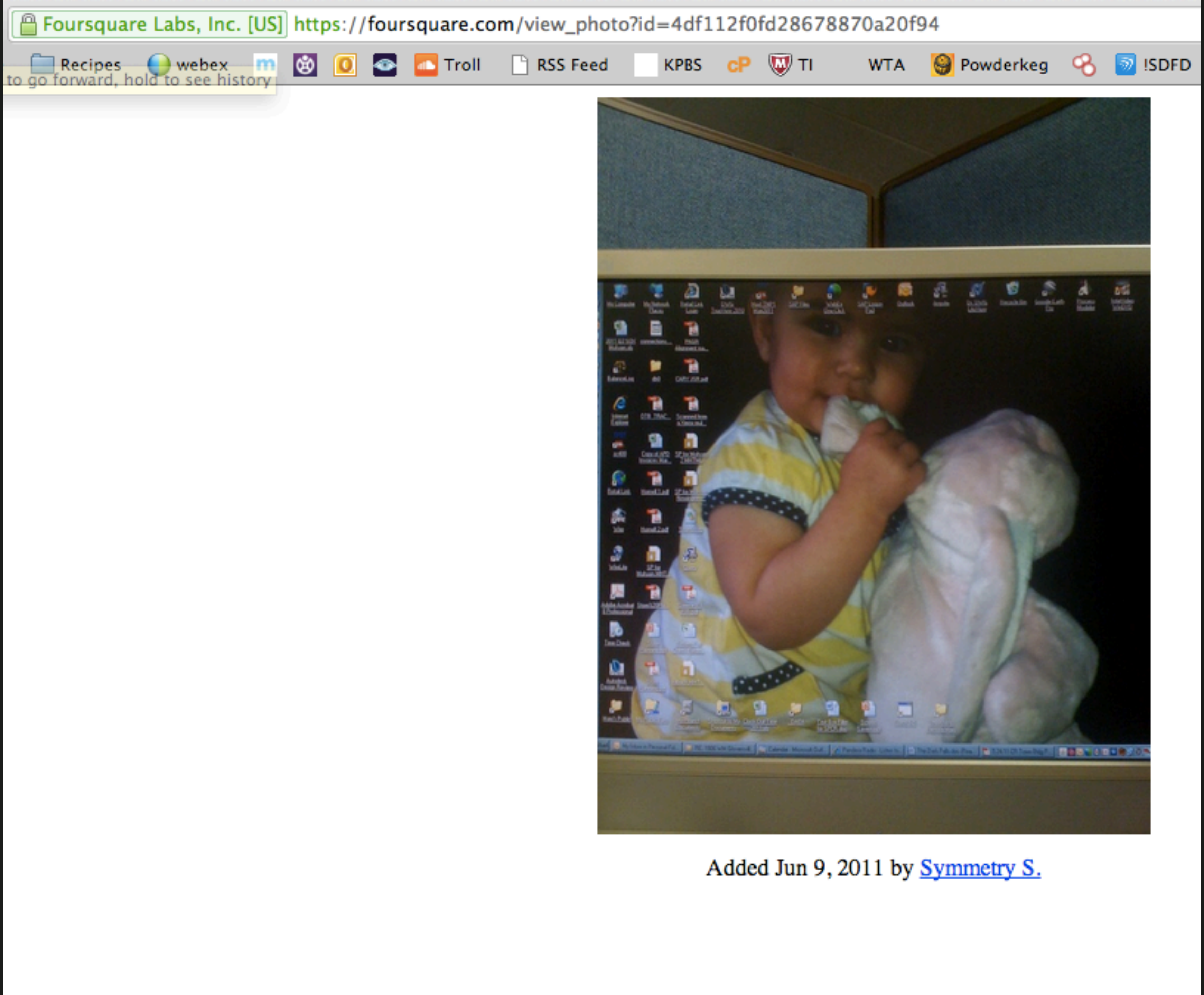
Spokeo
Flickr (Metadata)
LinkedIn
Facebook
Home address – networks / property vulnerable to penetration

Social Networks

Been beaten to death, but for a good reason:

Social networks are an OSINT goldmine!

FourSquare not only gives you realtime geolocation of a target (not to mention “tips” and person’s history of attendance)…



Foursquare Labs, Inc. [US] https://foursquare.com/view_photo?id=4df112f0fd28678870a20f94

Added Jun 9, 2011 by Symmetry S.

This is relevant to my interests
LOLCAT.COM

One Screenshot Yields…

Operating System
Type of AV
Program used to open PDF’s
Word processing, spreadsheet software
Internet browser used
Email client

ALL important pieces of information, all made with 0 packets sent to the target.

The Dossier

To create the PST we target:

- Company
- Employees
- Contractors
- Suppliers
- Competitors

Contractors

- Technical contractors (programmers, IT personnel)
- Janitorial service
- Security guards
- Alarm company
- HVAC

All have physical or logical access

The Dossier

To create the PST we target:

- Company
- Employees
- Contractors
- Suppliers
- Competitors

Suppliers

Often the easiest to manipulate.

- Security appliance manufacturers
- Security software
- Managed services
- Alarm company

Contact the security appliance vendor posing as the new POC.

The Dossier

To create the PST we target:

- Company
- Employees
- Contractors
- Suppliers
- Competitors

Competitors

Couched properly, probing competitors can yield great results.

Competitors will often maintain their own dossiers on the target

If it’s in their best interests to see you succeed and them fail, they might very well help you

OSINT

Great OSINT sources:

ASK.com
Forums.securityinfowatch.com
Blogspot
Cityfreq et al
Cnet forums
Data Center Knowledge

OSINT

Great OSINT sources:

Facebook

Flickr

FourSquare

Glassdoor

Google & Bing(!)

Gov’t sites

OSINT

Great OSINT sources:

Indeed.com

Information Week

LinkedIn (!)

MySpace

Pipl/PlaxoQuora

Reddit

OSINT

Great OSINT sources:

Spokeo

TinEye

Maltego

FOCA

Twitter

Yahoo Answers

OSINT

Many, many more.

For a complete list of OSINT resources:

Tacticalintelligence.org/BHAD.html

The Social Handshake

The presentation of the pretext to the target

Efficacy lift can be gained via:

- push polling (information gleaned by OSINT or observation)
- psychological gambits (humor/sympathy)
- trust transference (using an established social handshake to gain trust of another)
- authority-based pre-texts

The Social Handshake

The most critical part of a successful SE attack

Occurs during the initial interaction between the attacker and the victim

Somewhat akin to the TCP 3-way handshake

The Social Handshake

It is essentially SYN (presentation of attacker and his pre-text)

SYN-ACK (the target validating the attacker and the pre-text)

and ACK (acceptance of the attacker’s pretext by the target)

The Social Handshake

As in the TCP 3-way handshake, if any part of the interaction fails, the attack (connection) will fail. While a target can terminate the “connection” at any time, the author’s experience is that once the social handshake is completed, the attack will usually succeed (as long as the attacker sticks to a well-defined and targeted pre-text).

The Social Handshake

Establishing this initial connection is not nearly as difficult as one might think.

In fact, past history has shown that intelligence agents have an over 80% success rate with establishing connections over the phones with targets with extremely basic introductions, such as asking “can I have a few minutes of your time?”

The Social Handshake

As long as the caller has a proper response to the initial pushback (if any) the success rate is high.

What is not necessarily high is the acquisition rate of the flags. That is determined by the strength of the pre-text and the ability to continually groom the target throughout the interaction.

The PST

- Persistent Social Threat
- An ongoing social relationship that can last for years
- Targeted for their access/knowledge
- Not used in low-level / attacks / one-of’s
- Don’t use them (normally) directly for network attacks
- Want to avoid “burning” them

The PST

Incredibly devastating to an enterprise because:

- Not detectable via firewall logs
- Not blocked by anti-virus solutions
- The duped target is not likely to come forward and reveal themselves if attack uncovered

Why Does It Work?

An effective social engineer exploits common psychological weaknesses.

Humans are inefficient at detecting deception, on average only detecting deception correctly in 54% of interactions

Why Does It Work?

Most people rely on inaccurate methods such as eye contact and body languages that are not reflected in reality

As such, an effective attacker will maintain eye contact when telling critical lies, or avert eye contact when they want their target to think they are lying.

Successful Pretext

Pre-Text: The “story” the attacker tells.

A successful pretext is often driven by the end data points that the attacker desires to gather.

Defcon SECTF Examples

Delayed Validation

The attacker contacts the target and informs them that they will be coming on-site in the near future and that the call is to introduce himself and the purpose of the visit. This method is very effective since the attacker at first does not attempt to elicit any information, just to set the date.

Delayed Validation

After small talk, attacker asks for hotel recommendations, tourist attractions, etc.

As this is happening, the target is subconsciously at ease, since they think they will have lead-time to establish any inconsistencies, and as such they are at a lowered state of suspicion.

Delayed Validation

The target is lulled into a sense of safety since the attacker is not attempting to gather any information. It is only later in the conversation that the attacker begins to ask some questions, usually under the guise of getting some prep work out of the way while they have the target on the phone.

Delayed Validation

The lowered level of suspicion is maintained, since the most critical part of the social handshake comes at the beginning of the call. Since the target has already accepted the initial risk, and eventually established the social connection, they usually fail to reset their “awareness parameters” that they have in place during the initial interaction.

Elicitation Techniques

Elicitation can be a component of the pre-text, or can be done as part of the attack

Amazing the information you can gain via elicitation

Intelligence agencies use various methods – you can use them too!

On-Site Social Engineering

Phone interactions allow them the freedom to simply hang up with little threat of being physically detained

Attackers are somewhat hamstrung by the inability to visually gauge reactions from the target, as well as a lessened level of situational awareness.

On-Site Social Engineering

The simple act of presenting oneself to the target has a surprising effect:

There is an added legitimacy factor added to the victim’s mind.

Surely nobody would be bold enough to come onto the premises to try to fool their way inside..

On-Site Social Engineering

The common perception that attacks like this only take place in spy movies and TV shows biases most targets

Usually reinforced by a "I would know a scammer if I met one / it would never happen to me" attitude

On-Site Social Engineering

On-site attacks that are especially effective are those that involve the attacker presenting himself at a facility, while referencing a worker who is unavailable

On-Site Social Engineering

Sites such as FourSquare and Twitter are remarkably effective reference points, since they can give attackers real-time reconnaissance information.

Out of office email/voicemails are also golden

On-Site Social Engineering

The attacker can make sure the reference target is not reachable by phone via one of a few methods.

War-faxing the reference target’s cell phone

Ensure the reference target is physically separated from his phone - fake job interview

On-Site Social Engineering

When the receptionist or guardian of the site is unable to reach the reference target, they will either turn the attacker away, or allow them access.

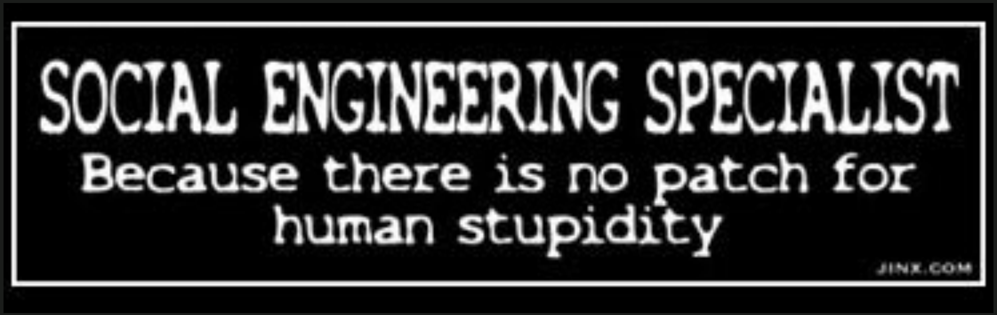
The latter is much more likely if a proper dossier has been collected, since the attacker can drop many reference points that infer they must be in the company's circle of trust.

On-Site Social Engineering

If the receptionist decides not to allow the attacker in, this can often be mitigated by calmly asking for them to call a taxi to take the attacker back to the airport. “I’ll have to reschedule and fly back in sometime next month.”

They usually err on the side of self-preservation, or in what they mistakenly believe to be in the best interests of the company.

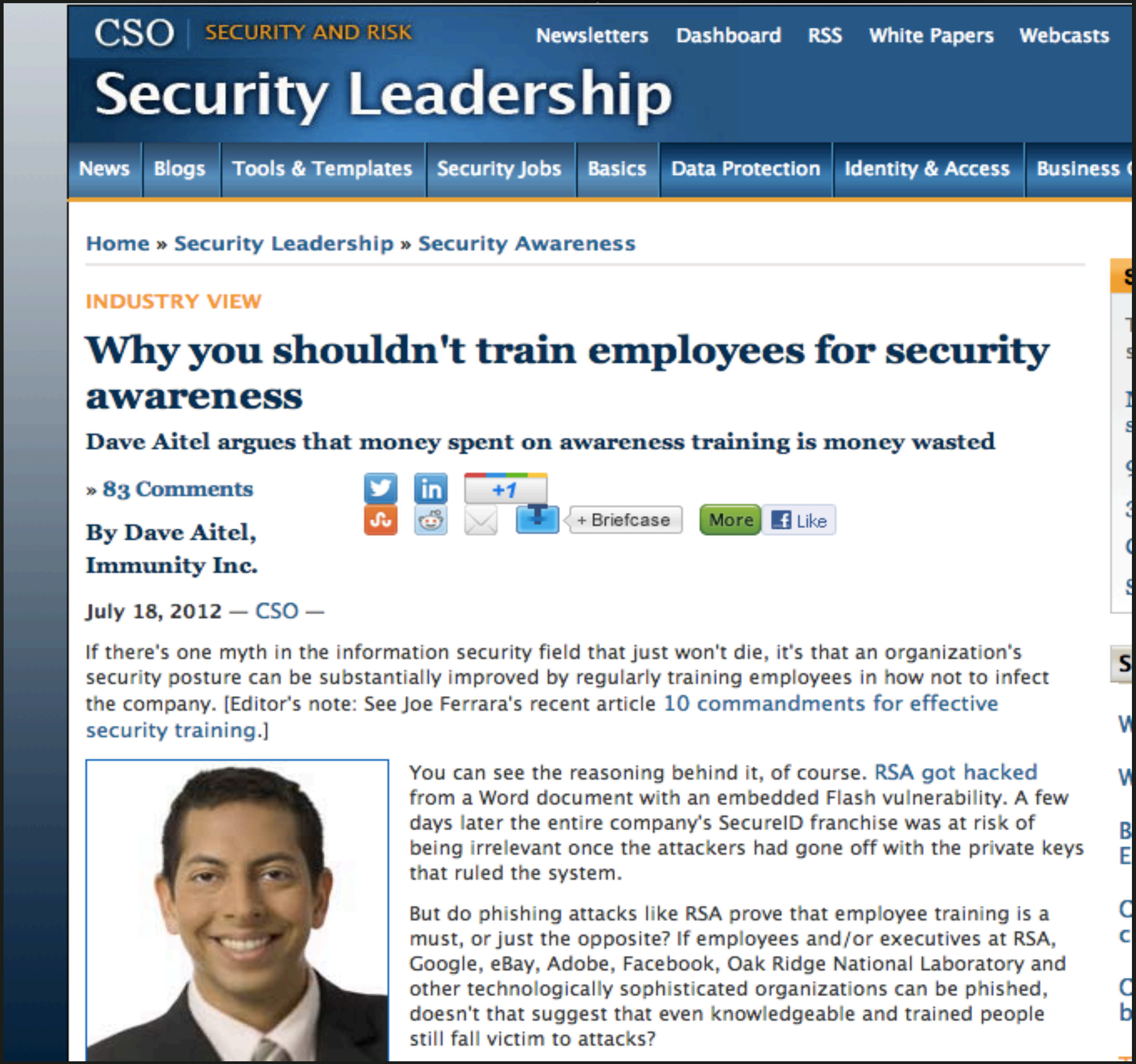
Effective Countermeasures



SOCIAL ENGINEERING SPECIALIST

Because there is no patch for human stupidity

JINX.COM



INDUSTRY VIEW

Why you shouldn't train employees for security awareness

Dave Aitel argues that money spent on awareness training is money wasted

» 83 Comments

By Dave Aitel, Immunity Inc.

July 18, 2012 — CSO —

If there's one myth in the information security field that just won't die, it's that an organization's security posture can be substantially improved by regularly training employees in how not to infect the company. [Editor's note: See Joe Ferrara's recent article 10 commandments for effective security training.]

You can see the reasoning behind it, of course. RSA got hacked from a Word document with an embedded Flash vulnerability. A few days later the entire company's SecureID franchise was at risk of being irrelevant once the attackers had gone off with the private keys that ruled the system.

But do phishing attacks like RSA prove that employee training is a must, or just the opposite? If employees and/or executives at RSA, Google, eBay, Adobe, Facebook, Oak Ridge National Laboratory and other technologically sophisticated organizations can be phished, doesn't that suggest that even knowledgeable and trained people still fall victim to attacks?

Countermeasures

It may seem that all is lost for the corporate security group when it comes to defending against social engineering attacks.

Nothing could be farther from the truth.

Countermeasures

There are many things that companies can do to mitigate these threats, but they involve much more than basic awareness training .

Most awareness programs are sorely lacking when it comes to training regarding social engineering.

Countermeasures

A truly effective program takes more than a 30 minute discussion of the threats!

Countermeasures

Very effective technique: complement a robust social engineering awareness lecture with having all employees create a dossier on a randomly assigned co-worker from social media sites.

Offer cash to make it REALLY effective!

Countermeasures

Not only does the information gathering process make all employees aware of the dangers of social media, it makes them think like attackers, and helps modify their own online behavior.

Often the also educate others in their social circle to the dangers…

Countermeasures

- Move away from the traditional "we won't ask for passwords over the phone" sort of mindset.
- A skilled SE will never ask for a password, since that instantly raises flags.
- Make program more around situational awareness (excessive laughter, emotional bonds, etc)

Countermeasures

Still, maintain a list of “hot button” questions to flag.

Log all SE attempts in a centralized database

Investigate EVERY attempt – ideally with PhySec and InfoSec together

SE attacks often followed by physical, vice versa

Countermeasures

- Do a social media deep dive
- Focus of information leakage, not just reputation!
- Know what employees are tweeting/posting what/where/when!
- Be careful of appropriate laws WRT employee monitoring

Countermeasures

- Password of the day/week
- Implement call-back/verification procedures
- Train your employees that it is “okay to say no”
- Commit to NEVER punishing employees for erring on the side of security

Countermeasures

TEST! TEST! TEST!

Ensure SE auditing is part of every PenTest

Do testing quarterly

Offer cash/prizes

SHMOOZEKIT DISCUSSION/DEMO

CONTACT INFO

Get the updated slide deck at:

http://tacticalintelligence.org/bhad.html

Contact Shane at:

Email: shane@tacticalintelligence.org

Twitter: @tactical_intel

black hat

ABU DHABI 2012