# What a semester!

A big thanks to the TAs

Chris, Noor, Lianting, Junheng

# Social Engineering

Thierry Sans

# Social Engineering

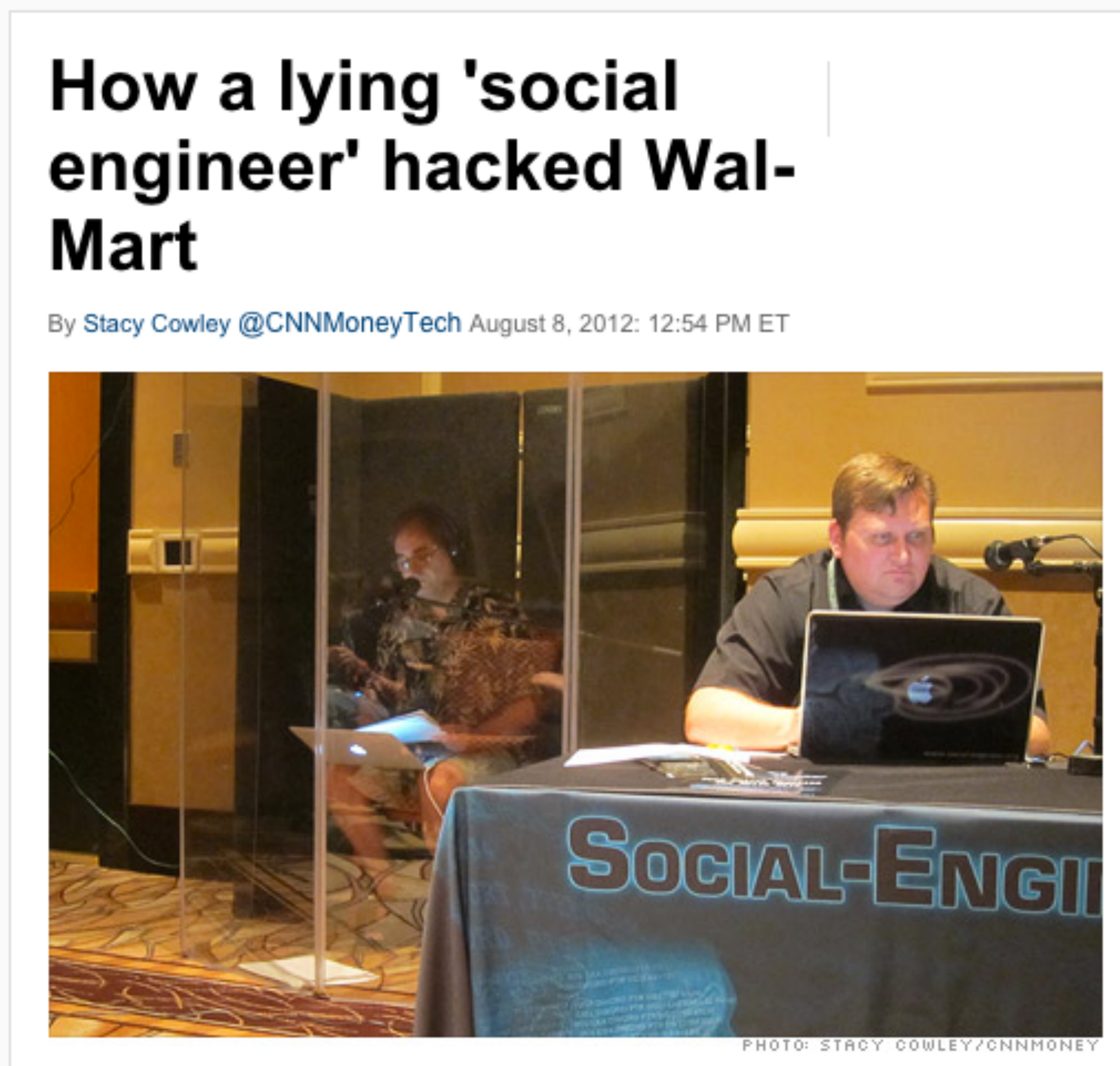
”The act of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical cracking techniques.” Wikipedia

Kevin Mitnick

# Social engineering nowadays

- Panel on Social Engineering - Hope Conference Series

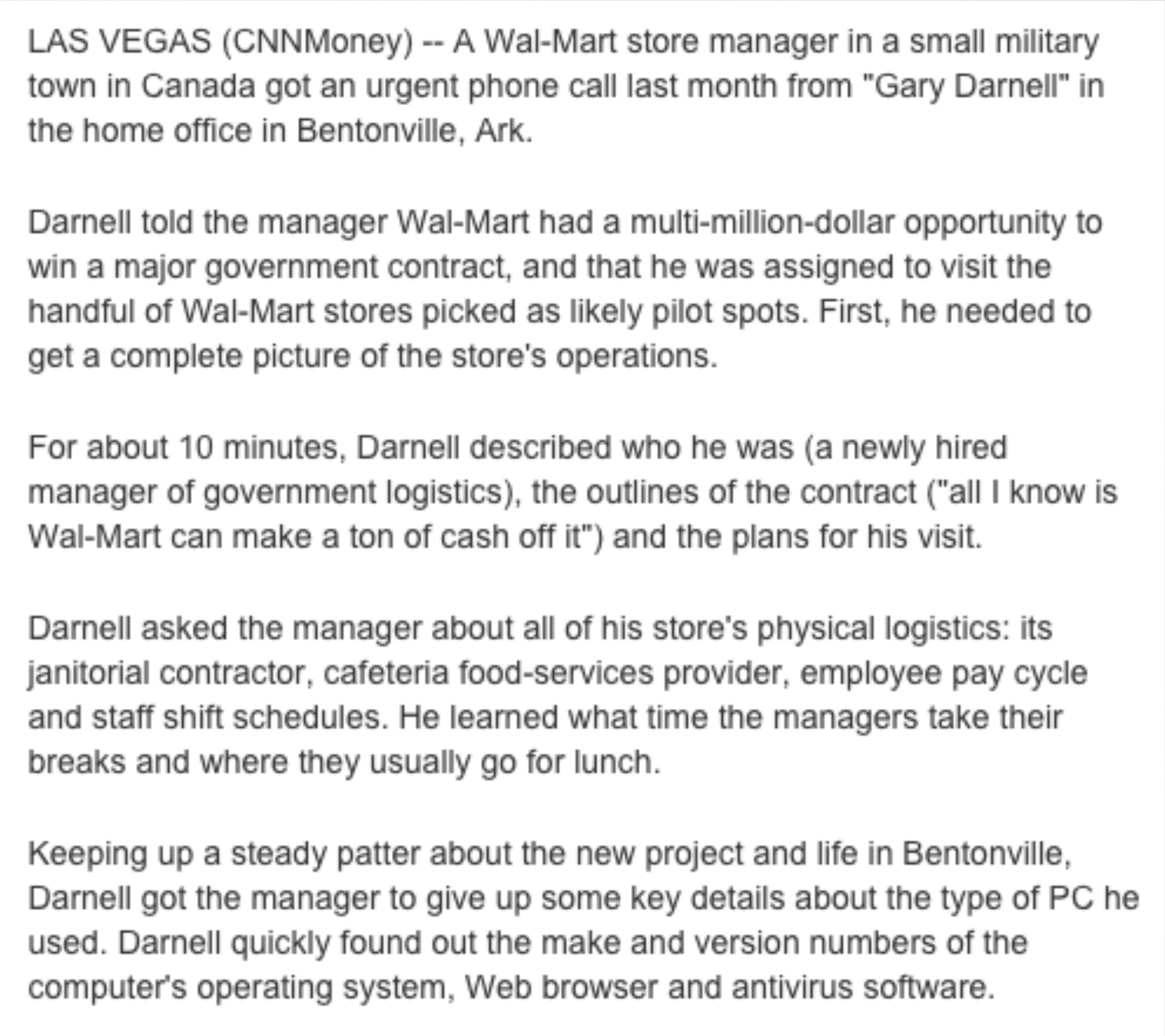
Hope number 9 (2012)



# How a lying 'social engineer' hacked Wal-Mart

By Stacy Cowley @CNNMoneyTech August 8, 2012: 12:54 PM ET

PHOTO: STACY COWLEY/CNNMONEY



LAS VEGAS (CNNMoney) -- A Wal-Mart store manager in a small military town in Canada got an urgent phone call last month from "Gary Darnell" in the home office in Bentonville, Ark.

Darnell told the manager Wal-Mart had a multi-million-dollar opportunity to win a major government contract, and that he was assigned to visit the handful of Wal-Mart stores picked as likely pilot spots. First, he needed to get a complete picture of the store's operations.

For about 10 minutes, Darnell described who he was (a newly hired manager of government logistics), the outlines of the contract ("all I know is Wal-Mart can make a ton of cash off it") and the plans for his visit.

Darnell asked the manager about all of his store's physical logistics: its janitorial contractor, cafeteria food-services provider, employee pay cycle and staff shift schedules. He learned what time the managers take their breaks and where they usually go for lunch.

Keeping up a steady patter about the new project and life in Bentonville, Darnell got the manager to give up some key details about the type of PC he used. Darnell quickly found out the make and version numbers of the computer's operating system, Web browser and antivirus software.

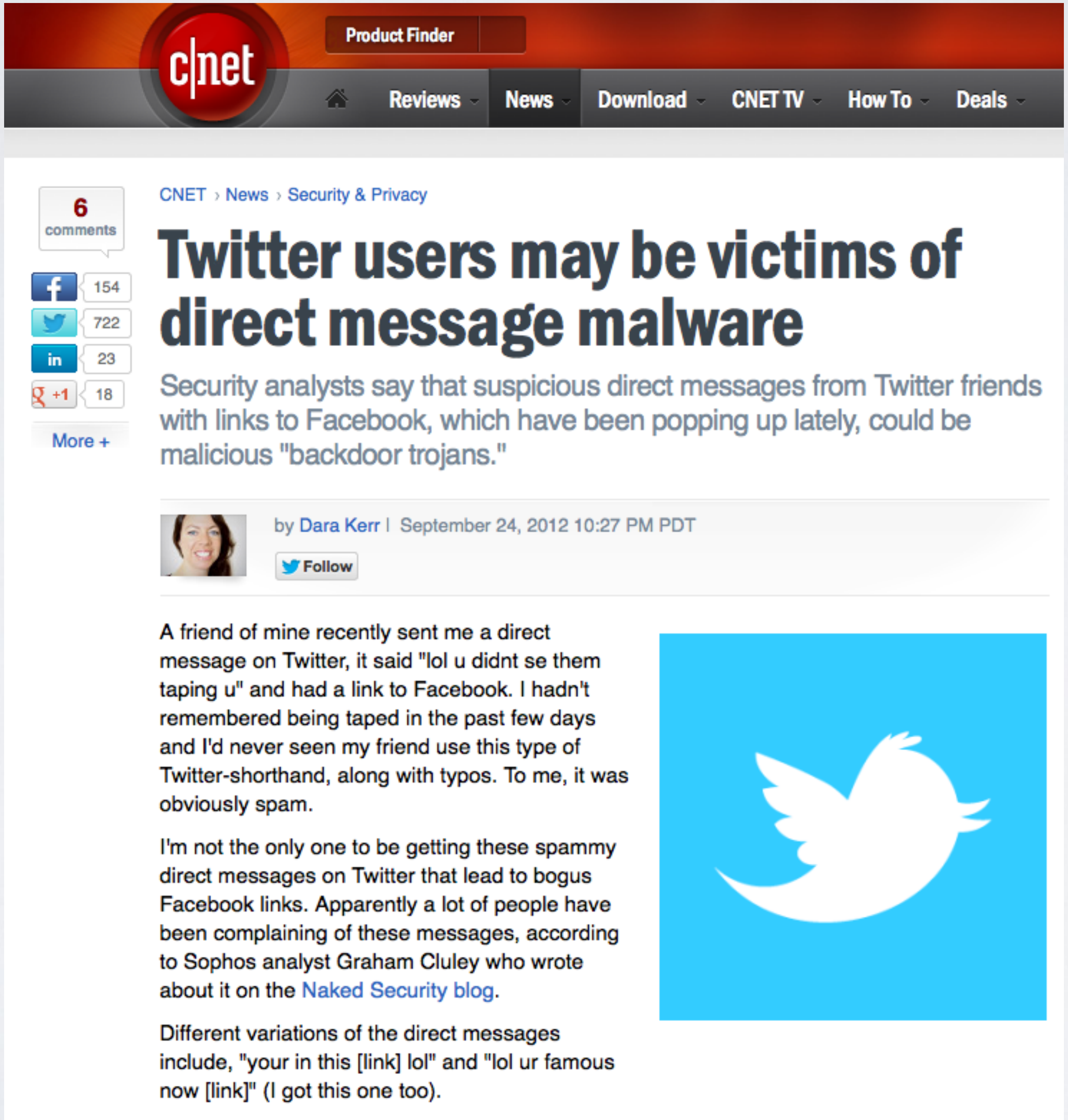
Link

# Phishing
# A modern version of social engineering

”The criminally fraudulent process of attempting to acquire sensitive information […] by masquerading as a trustworthy entity in an electronic communication.”Wikipedia

Google for Education - Stay Safe from Phishing and Scams

# Phishing on Social Networks



CNET › News › Security & Privacy

## Twitter users may be victims of direct message malware

Security analysts say that suspicious direct messages from Twitter friends with links to Facebook, which have been popping up lately, could be malicious "backdoor trojans."

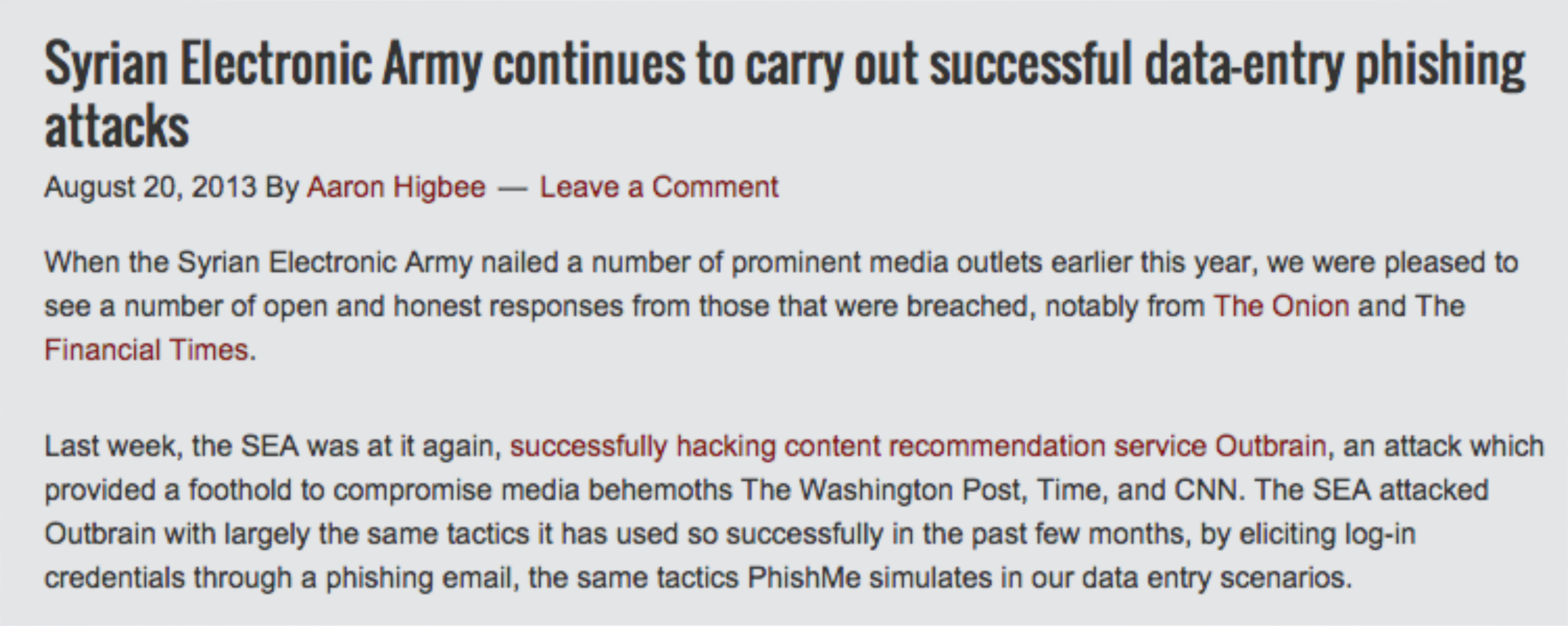
by Dara Kerr | September 24, 2012 10:27 PM PDT

A friend of mine recently sent me a direct message on Twitter, it said "lol u didnt se them taping u" and had a link to Facebook. I hadn't remembered being taped in the past few days and I'd never seen my friend use this type of Twitter-shorthand, along with typos. To me, it was obviously spam.

I'm not the only one to be getting these spammy direct messages on Twitter that lead to bogus Facebook links. Apparently a lot of people have been complaining of these messages, according to Sophos analyst Graham Cluley who wrote about it on the Naked Security blog.

Different variations of the direct messages include, "your in this [link] lol" and "lol ur famous now [link]" (I got this one too).

# Phishing + Social Engineering = Spear Phishing



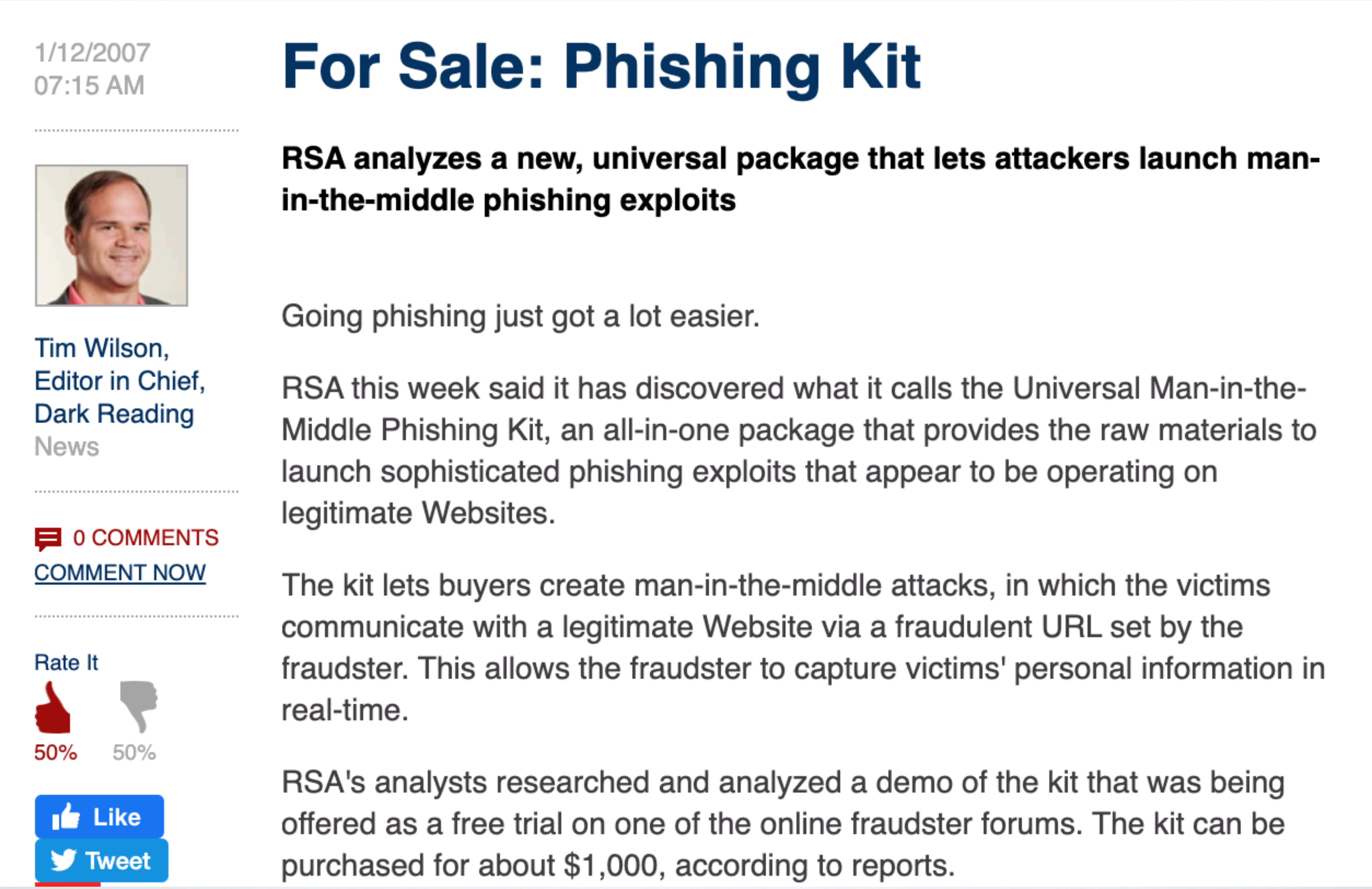
## Syrian Electronic Army continues to carry out successful data-entry phishing attacks

August 20, 2013 By Aaron Higbee — Leave a Comment

When the Syrian Electronic Army nailed a number of prominent media outlets earlier this year, we were pleased to see a number of open and honest responses from those that were breached, notably from The Onion and The Financial Times.

Last week, the SEA was at it again, successfully hacking content recommendation service Outbrain, an attack which provided a foothold to compromise media behemoths The Washington Post, Time, and CNN. The SEA attacked Outbrain with largely the same tactics it has used so successfully in the past few months, by eliciting log-in credentials through a phishing email, the same tactics PhishMe simulates in our data entry scenarios.

# Phishing as a service a.k.a phishing kit



1/12/2007
07:15 AM

Tim Wilson,
Editor in Chief,
Dark Reading
News

## For Sale: Phishing Kit

**RSA analyzes a new, universal package that lets attackers launch man-in-the-middle phishing exploits**

Going phishing just got a lot easier.

RSA this week said it has discovered what it calls the Universal Man-in-the-Middle Phishing Kit, an all-in-one package that provides the raw materials to launch sophisticated phishing exploits that appear to be operating on legitimate Websites.

The kit lets buyers create man-in-the-middle attacks, in which the victims communicate with a legitimate Website via a fraudulent URL set by the fraudster. This allows the fraudster to capture victims' personal information in real-time.

RSA's analysts researched and analyzed a demo of the kit that was being offered as a free trial on one of the online fraudster forums. The kit can be purchased for about $1,000, according to reports.

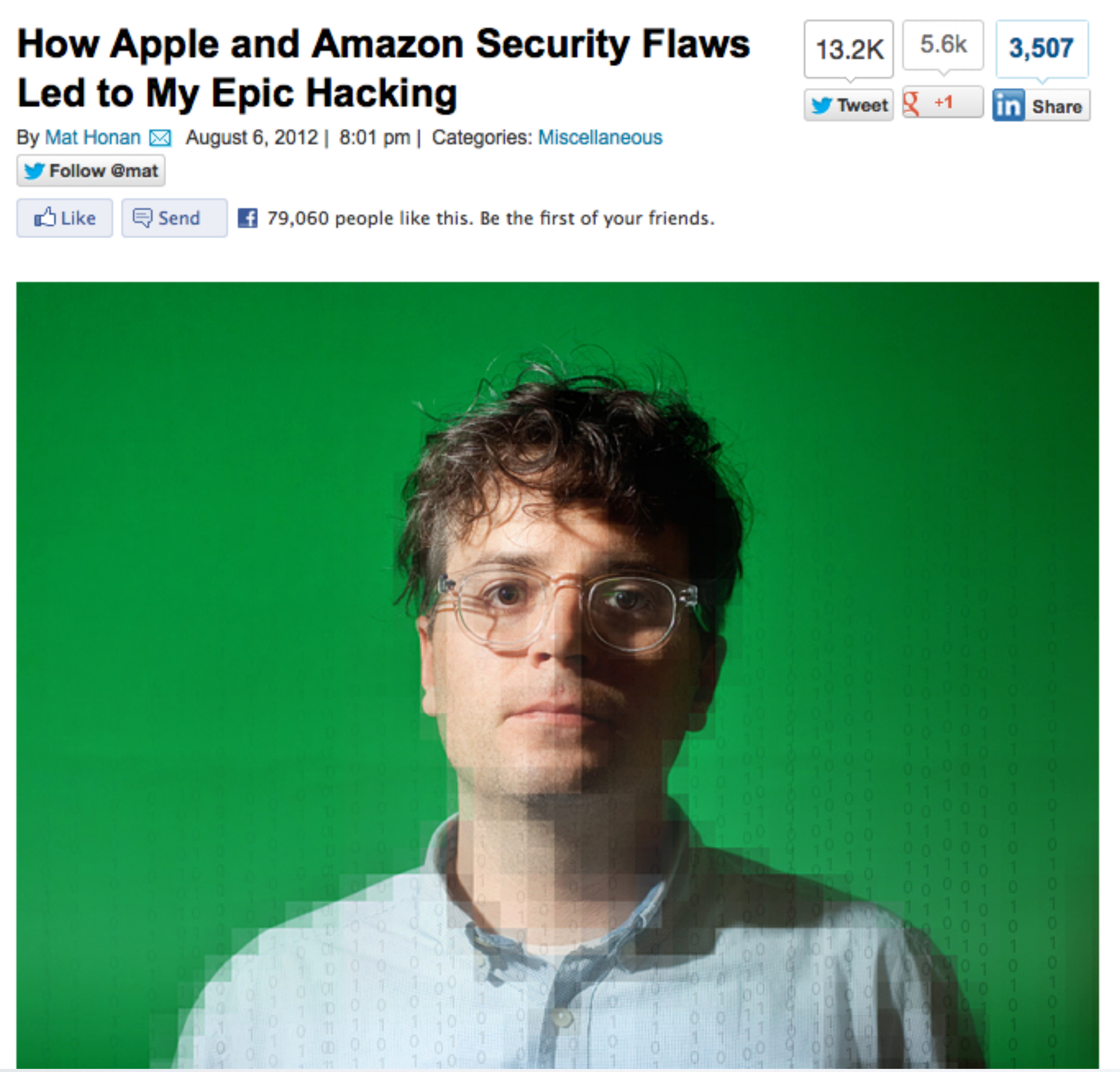
# “Security” Questions

## The problem of security questions

“A 2009 study from Microsoft Research found that acquaintances could answer such security questions 17 percent of the time, and strangers didn't fare too much worse, answering correctly within five tries 13 percent of the time, though that high figure may have been the result of a homogeneous sample.”
*Mat Honan - Wired*

Link

# A look at a recent case



## How Apple and Amazon Security Flaws Led to My Epic Hacking

By Mat Honan August 6, 2012 | 8:01 pm | Categories: Miscellaneous

79,060 people like this. Be the first of your friends.

"Ultimately, all you need in addition to someone's e-mail address are those two easily acquired pieces of information: a billing address and the last four digits of a credit card on file."

*Mat Honan - Wired*

Link

# From Information-Diving
# To Open-Source Intelligence

# Information Diving

”Information diving is the practice of recovering technical data, sometimes confidential or secret, from discarded material.” Wikipedia

UNIV
FOR COMPUTER SCIENCES DEPT.

# Google Hacking
# A modern version of information diving

”Technique that uses Google Search [...] to find security holes in the configuration and computer code that websites use.” Wikipedia

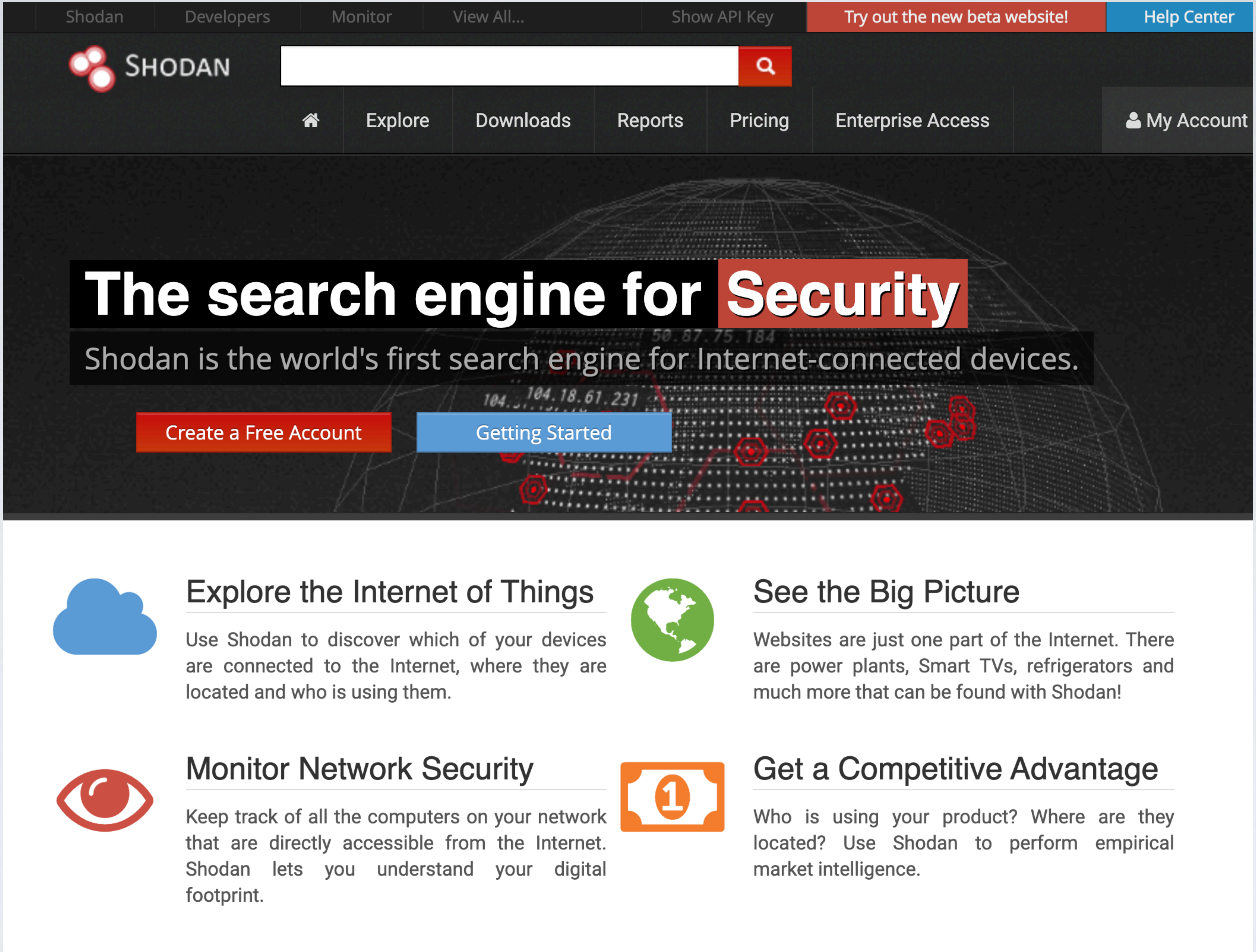
Null Byte- Find Vulnerable Services & Hidden Info Using Google Dorks

Tinkernut - Google Hacks 2.0

# OSINT - Open-Source Intelligence

”**Open-source intelligence** (**OSINT**) is a multi-methods (qualitative, quantitative) methodology for collecting, analyzing and making decisions about data accessible in publicly available sources to be used in an intelligence context.” Wikipedia

OSINT Framework



The search engine for Security

Shodan is the world's first search engine for Internet-connected devices.

### Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

### See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

### Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

### Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

Null Byte - Find Vulnerable Webcams Across the Globe Using Shodan