



## **2016 MDRT Annual Meeting e-Handout Material**

**Title:** The Hacker's Blacklist: Cyber Security for Financial Professionals

**Speaker:** John Sileo

**Presentation Date:** Wednesday, June 15, 2016

**Presentation Time:** 10:00 - 11:00 a.m.

The Million Dollar Round Table® (MDRT) does not guarantee the accuracy of tax and legal matters and is not liable for errors and omissions. You are urged to check with tax and legal professionals in your state, province or country. MDRT also suggests you consult local insurance and security regulations and your company's compliance department pertaining to the use of any new sales materials with your clients. The information contained in this handout is unedited; errors, omissions and misspellings may exist. Content may be altered during the delivery of this presentation.

© 2016 Million Dollar Round Table

---

Million Dollar Round Table  
325 West Touhy Ave.  
Park Ridge, IL 60068 USA

# THE CYBER BLACKLIST

Top Threats & Countermeasures for Data Security



**John Sileo**

CEO, The Sileo Group

[Sileo.com](http://Sileo.com)

WHO ARE YOU?



[john\\_sileo](https://twitter.com/john_sileo)

# ASHLEY MADISON®

Life is short. Have an affair.®


Get started by telling us your relationship status:

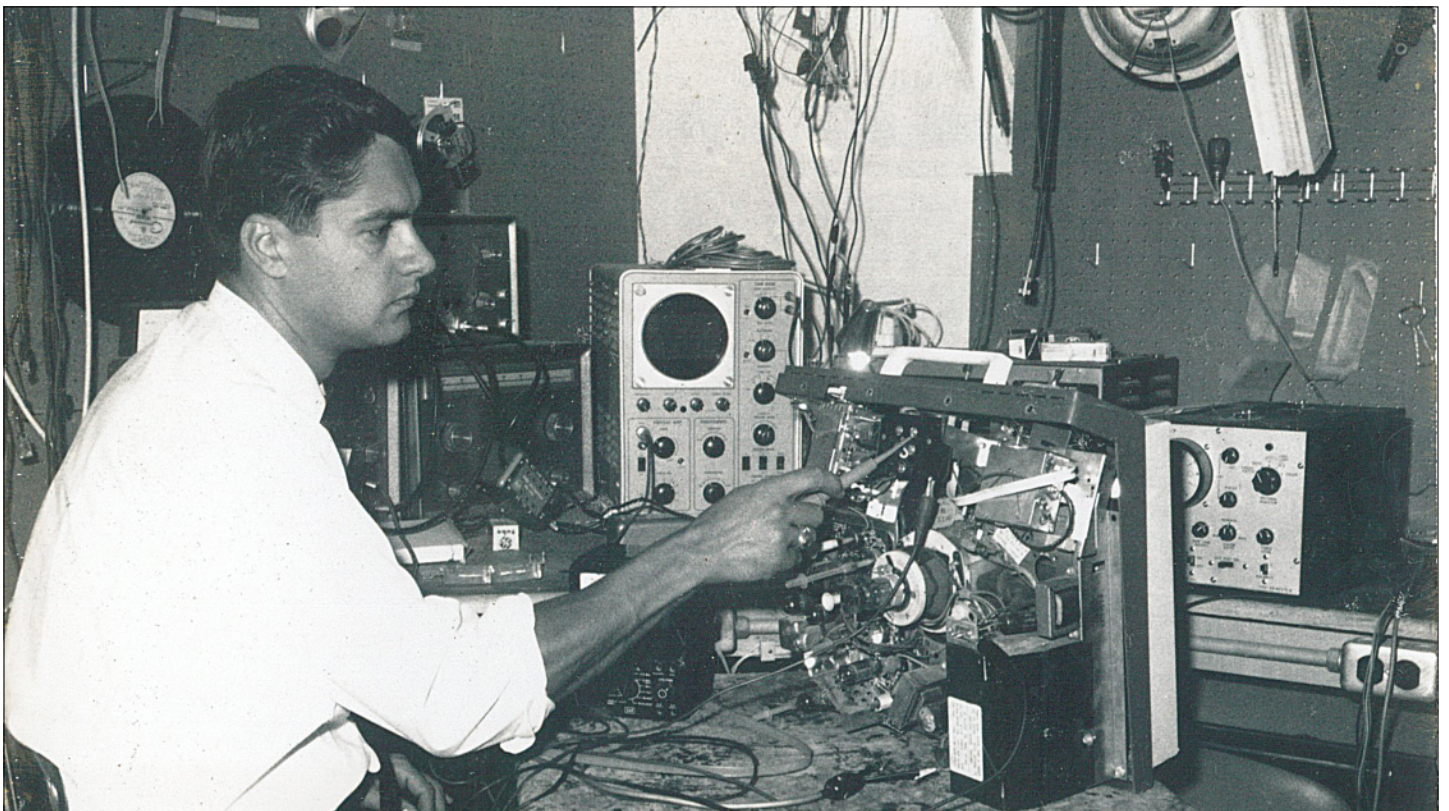
Please Select

See Your Matches »

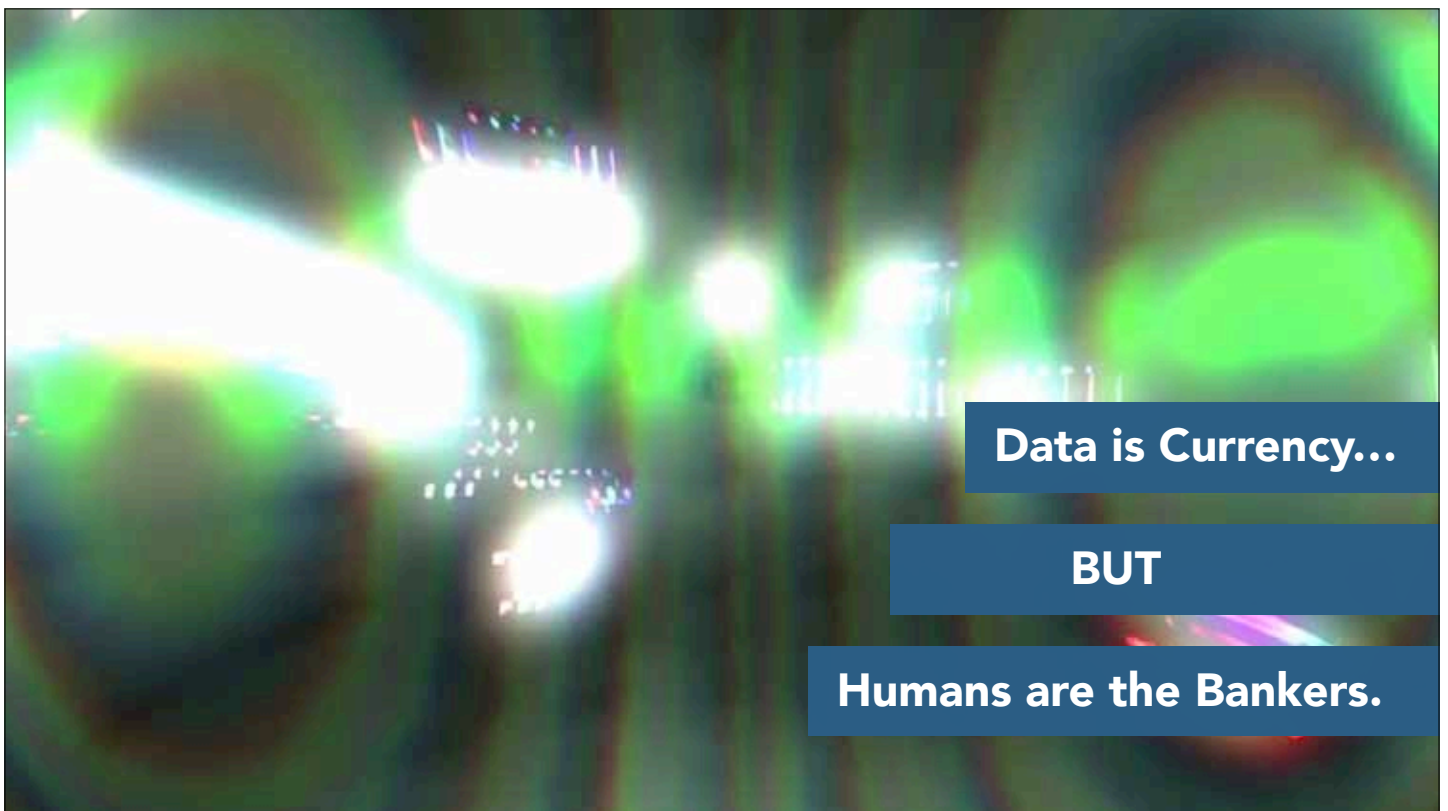
Over 37,610,000 anonymous members!

# HACKED











# THE CYBER BLACKLIST

**Top Threats & Countermeasures for Data Security.**

ING ACCOUNT TAKEOVER BLACK HAT HACKERS BROWSER-JACKING CARD SKIMMERS COOKIE TRACKING CREDIT FRAUDSTERS CYBER EXTORTION CYBER F  
TS CYBER WAR DUMPSTER DIVERS ELDER FRAUD OUR OWN WORST ENEMY EVILPRENEURS FACEBOOK TRAWLERS GEO-STALKERS GET RICH QUICK SCAMS  
FFERS IDENTITY THIEVES IOT SPIES IRS SCAMS MALWARE MOBILE-JACKERS NIGERIAN SCAMMERS PASSWORD CRACKERS PHARMERS PHISHERS R  
ERS SOCIAL ENGINEERS SPAM SPOOFING THE MOLE TRAVEL ESPIONAGE WAR DRIVERS WEARABLE TRACKERS WI-FI SNIFFERS WORK FROM HOME SCA  
SNATCHERS CLOUD-JACKERS COMPETITIVE ESPIONAGE EAVESDROPPING APP-JACKING ACCOUNT TAKEOVER BLACK HAT HACKERS BROWSER-JACKING CA  
ACKING CREDIT FRAUDSTERS CYBER EXTORTION CYBER PICKPOCKETS CYBER TERRORISTS CYBER WAR DUMPSTER DIVERS ELDER FRAUD OUR OWN WO  
FACEBOOK TRAWLERS GEO-STALKERS GET RICH QUICK SCAMS HACKTIVISTS HOTSPOT SNIFFERS IDENTITY THIEVES IOT SPIES IRS SCAMS MALWARE I  
MERS PASSWORD CRACKERS PHARMERS PHISHERS RANSOMWARE SHOULDER SURFERS SOCIAL ENGINEERS SPAM SPOOFING THE MOLE TRAVEL ES

# CYBER BLACKMAIL

90%

Successful Attack Rate

The use of illegally obtained data to influence organizations, manipulate people, extract a ransom or otherwise change behavior.

3D HDTV



**SONY**  
Breach Analysis



3D

HDTV

Is your reflex to **Judge the Breached** or learn from them?

Security must have a **Seat of Power** in the Boardroom (CISO)

Don't fail to **Leverage Early Mistakes** to avoid a sequel

**Failure of Culture:** CEO emails/phishing/filenames = **FIRED**

If **3rd-Party Access**, take pro-hacktive and contractual control

**Don't taunt Unstable Dictators with Unflattering Movies**

# Harvard Business Review

SEPTEMBER 2015

**44 The Big Idea**  
The Organizational  
"I'm Sorry"

Maurice E. Schweitzer et al.

**46 Risk Management**  
Cybersecurity: Lessons  
from the Pentagon

James A. "Bandy" Woodsfield Jr. et al.

**58 Managing Yourself**  
How to Embrace  
Complex Change

Linda Brison

# \$12.7M

"While technical upgrades are important, minimizing human error is even more crucial."

## CYBERSECURITY'S HUMAN FACTOR: LESSONS FROM THE PENTAGON

The vast majority of companies are more exposed to cyberattacks than they have to be. To close the gaps in their security, CEOs can take a cue from the U.S. military. Once

# SOCIAL ENGINEERING

The art (& science) of  
human manipulation.

@john\_sileo







# MICRO SPEAR-PHISHING

# 91%

Dell Human Element of Security Study

## HYPER-TARGETED

Use of social engineering to entice you to click a link that installs malware or steals data.



**Dear Target Guest,**

As you may have heard or read, Target systems and took guest information, in investigation, we learned that additional address, was also taken. I am writing to email address may have been taken o

I am truly sorry this incident occurred and value you as a guest and your trust is important to us, Target is offering one year of free credit monitoring to all Target guests who shopped in U.S. stores, through Experian's® ProtectMyID® product which includes identity theft insurance where available. To receive your unique activation code for this service, please go to [creditmonitoring.target.com](http://creditmonitoring.target.com) and register before April 23, 2014. Activation codes must be redeemed by April 30, 2014.

In addition, to guard against possible scams, always be cautious about sharing personal information, such as Social Security numbers, passwords, user IDs and financial account information. Here are some tips that will help protect you:

## Anthem Medical Hack: System Admin Phishing

# CEO-WHALING



1. Facebooks CEO's travel schedule
2. Phishes CEO's email credentials
3. LinksIn with CEO's assistant
4. Imitates CEO in email to assistant
5. Engineers her w/ "China Crisis"
6. Receives \$47M wire transfer

## 7. Retires

### Business Email Compromise

Imitating someone in a position of power to gain access, info or money.

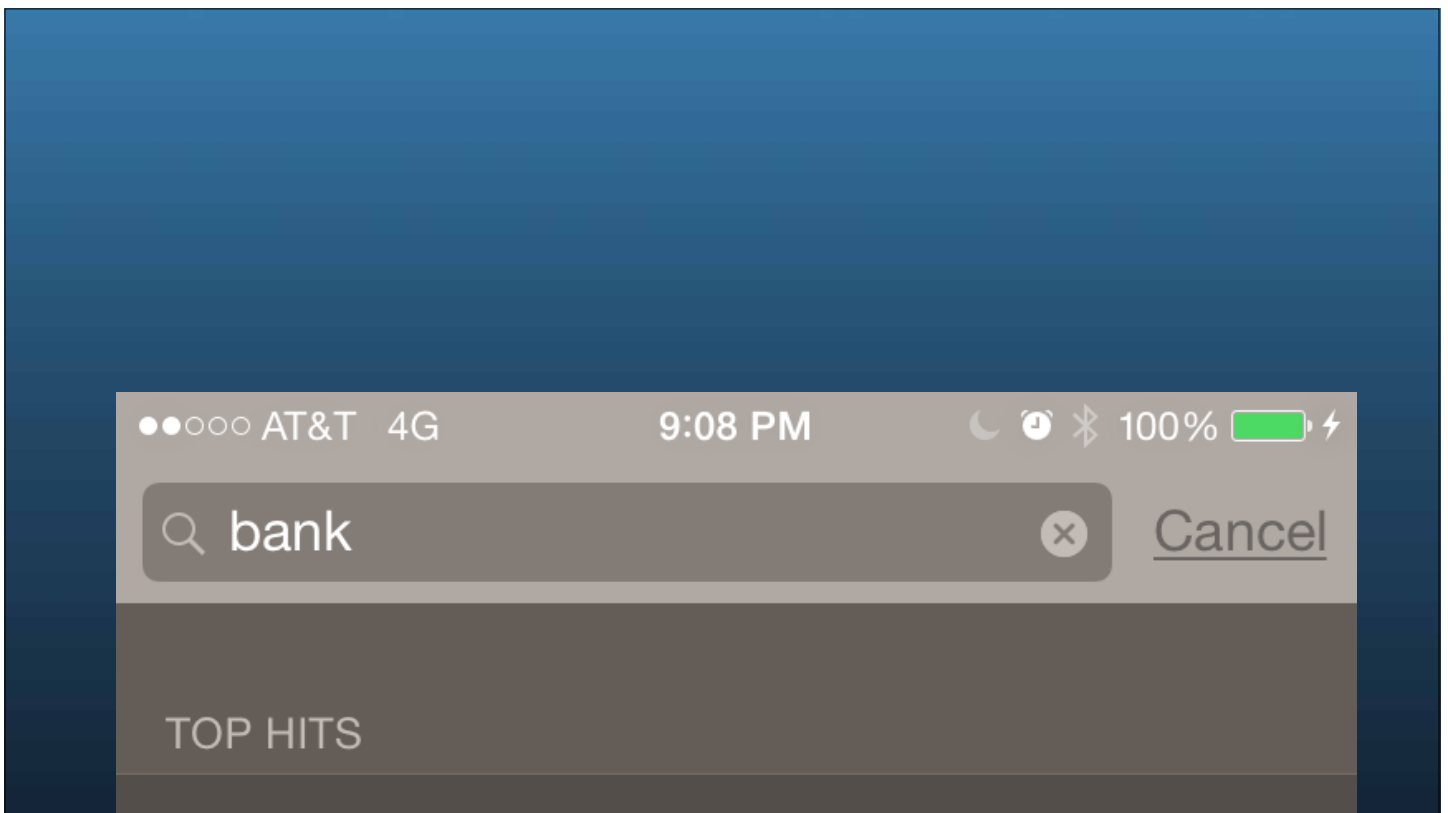
# MOBILE HIJACKERS

# 35%

Ponemon Cost of Breach 2013

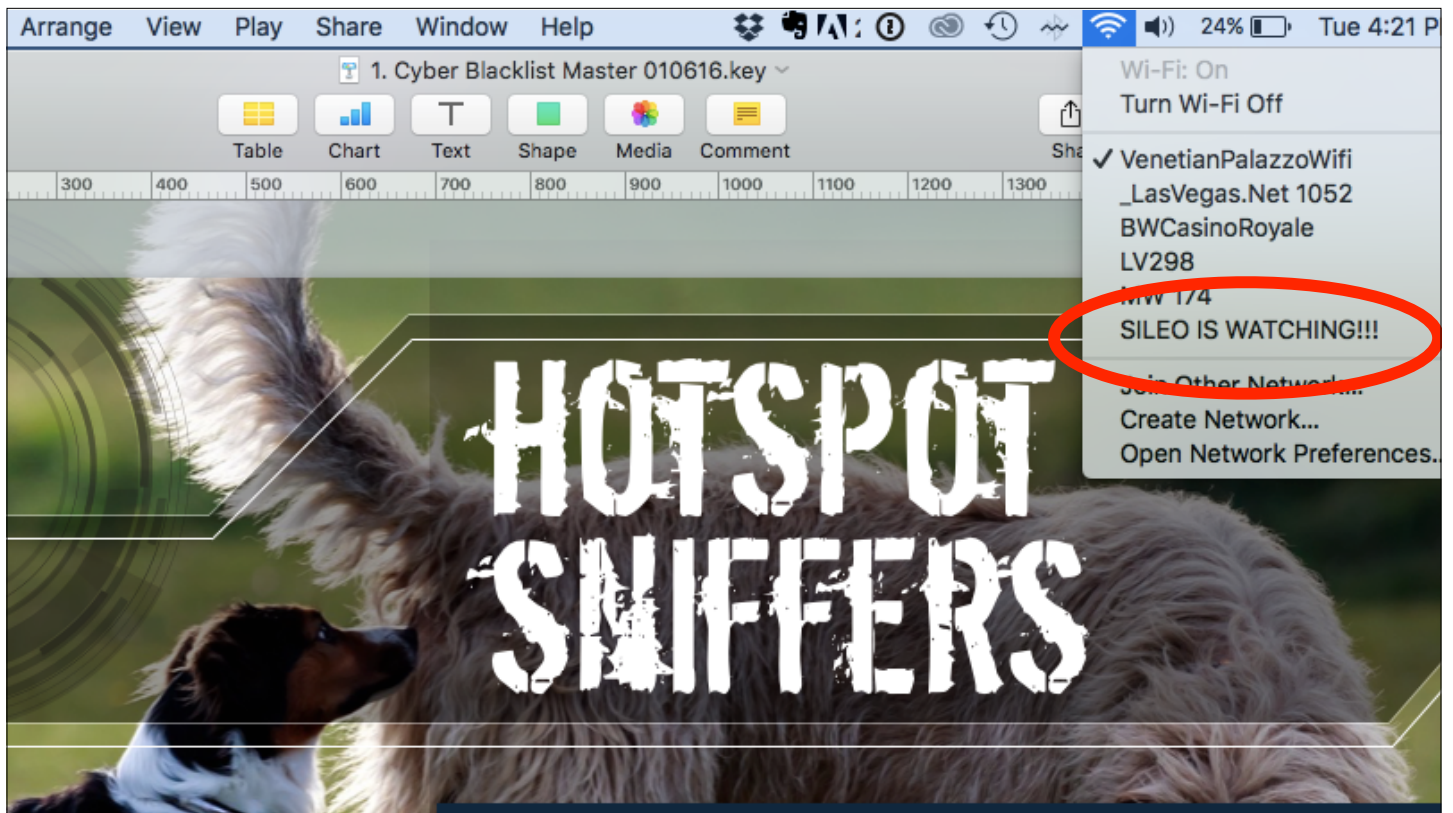
Things that are "mobile" have a tendency to "leave", making control a moving target.



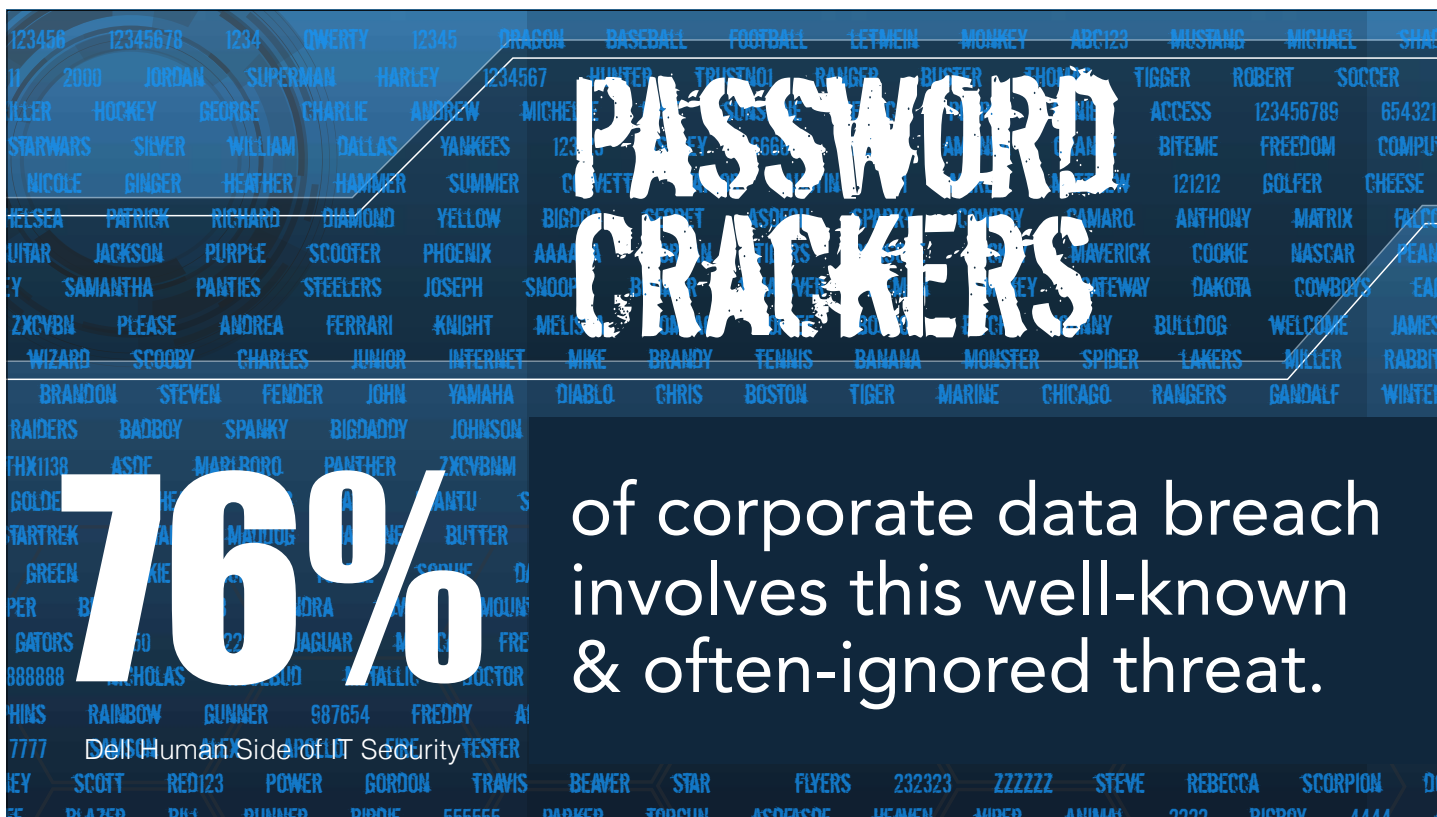


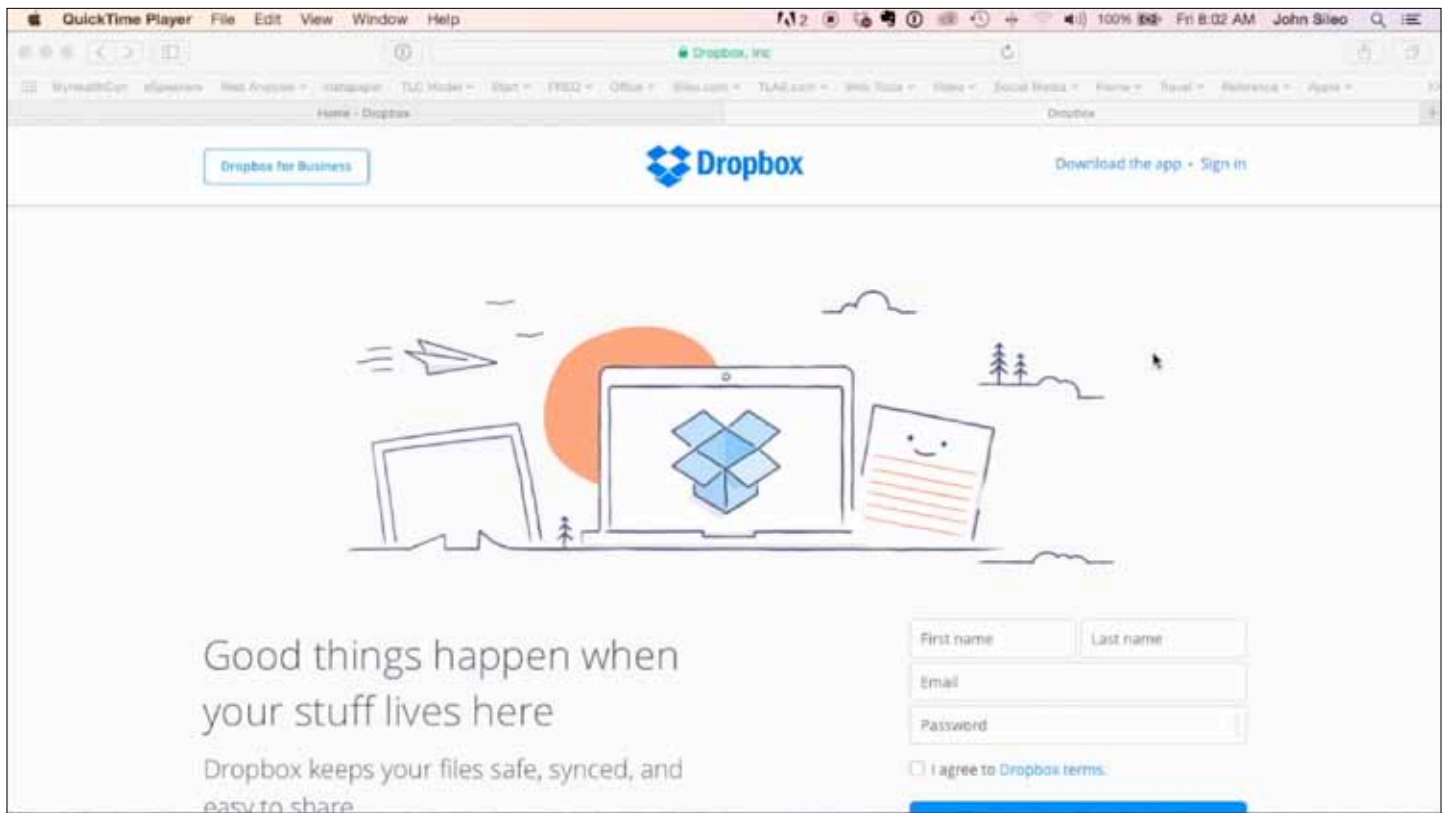












# CRYPTOLOCKER RANSOMWARE

Malware (via phishing)  
that holds data hostage  
until you pay the ransom.



# SOCIAL (MEDIA) ENGINEERS

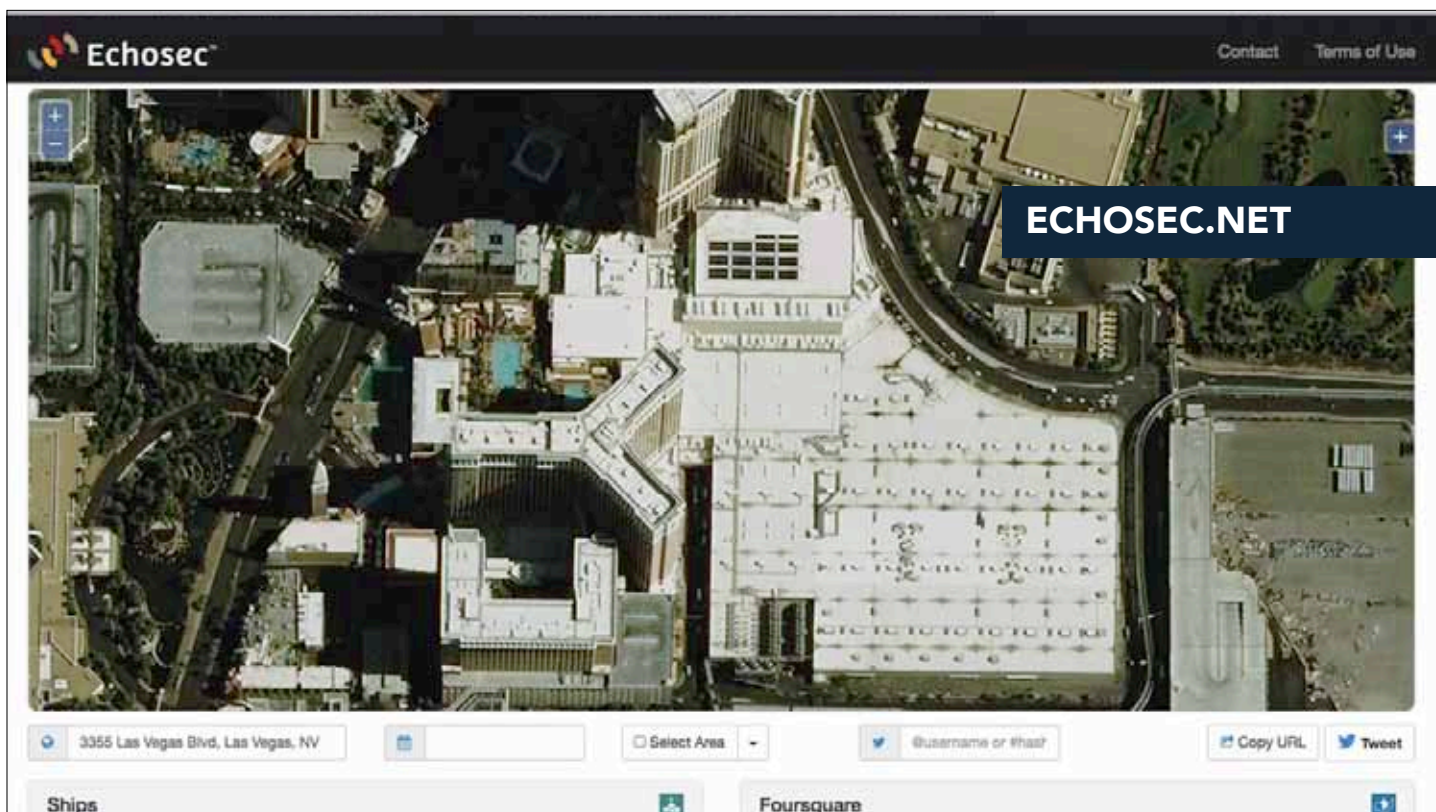
#1 source for social engineering reconnaissance.

A highly-public glossary of private information.

A platform that rewards oversharing with dopamine.







Prioritize, adapt and implement

sileo.com

## COUNTERMEASURES

1. An untrained, unengaged, **Socially Engineered** employee.
2. A **Phishing Attack** that installs malware or steals logins.
3. Bad **Password Habits** and lack of **Two-Step Logins**.
4. Inadequate **Data Encryption** at rest and in transit.
5. **Mobile Devices** w/o passcodes, tracking & App vetting.
6. **Unpatched Systems** with improper security configurations.
7. **Superfluous Data Collection**, retention and improper disposal.



A leader's guide to:

sileo.com

# HACKING THE HUMANS

1. Tap into **who they are** to gain ownership (Fireflies).
2. Start by **making security a selfish reflex** (Hogwash).
3. Understand that **feeling is believing** (Purse).
4. Shift to memorable, **sticky training** (The Hills are Alive).
5. Build a secure culture by **nudging "best" habits** (2-Factor).
6. Raise the bar on **social (media) trust** (Troop Locations).
7. **Leverage resilience** as the greatest source of security...





# Sileo's PrioritizAble COUNTERMEASURES

## PRIORITIZE

|

## ADAPT

|

## ACT

- ☐ Opt out of junk mail (Sileo.com/1)
- ☐ Freeze your credit (Sileo.com/2)
- ☐ Enable financial account alerts
- ☐ Convenience-based shredding
- ☐ Lockable filing & offsite storage
- ☐ Social engineering detection
- ☐ Turn on smartphone passcode
- ☐ Enable remote tracking & wiping
- ☐ Replace wi-fi hotspots w/ tethering
- ☐ H!11\$ @r3 a1!v3 quality passwords
- ☐ Enable 2-step logins/authentication
- ☐ 60 minutes in social media settings

## CYBER RISK AUDIT

- ☐ Automated OS patches
- ☐ Application updating
- ☐ Ubiquitous anti-virus
- ☐ BitLocker encryption
- ☐ FileVault encryption
- ☐ 3rd-party spam filter
- ☐ Default deny firewall
- ☐ Personal VPN
- ☐ Dedicated browser
- ☐ WPA2+ Wi-Fi security
- ☐ Password Software

### Enterprise Level

- ☐ User-Level Access
- ☐ External penetration test
- ☐ Enterprise VPN software
- ☐ Mobile Device Mngmnt
- ☐ Acceptable use policies
- ☐ Data Loss Prevention
- ☐ Application white-listing
- ☐ MAC Specific Wi-Fi
- ☐ SSID Masked Wi-Fi
- ☐ Cyber liability insurance