THINK LIKE A SPY
A Reflex-based Mindset - “What if” Somebody’s Watching Me?

SOCIAL ENGINEERING
#1
Tricking you into doing something you otherwise wouldn’t (or shouldn’t).

C’MON JOHN!!
The Art of Human Hacking
“I’m in charge”
“If you don’t, then…”
“Hurry up!”
“Quid Pro Quo”
“Let me stroke your ego”

John Sileo
Doubt it Out

Spear-Phishing

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

91%
Dell Human Element of Security Study

150 Nations, 40 Hospitals: WannaCry Phishing

80M Anthem Records: System Admin Phishing

500M Hacked Yahoo Accounts: A Single Click

DNC Breach: Bit.ly URL Phishing

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. Assistant initiates $47M wire xfer
7. Cyber Criminal Retires

Business Email Compromise
Imitating someone in a position of power to gain access, info or money.
When an Unverified Customer, IT Staff, Microsoft or IRS Calls...

SOS
SILEO ON SECURITY
IRS PHONE SCAMS

90% SUCCESSFUL ATTACK RATE

Misusing data to exert power.

SONY
Breach Analysis

WannaCry: The Devil you do know is often your worst enemy.

SONY Lessons
Target: Million $ tech doesn't solve poorly trained people.

@TARGET
Sony: Leverage your mistakes to avoid a disastrous sequel.

Don't taunt Unstable Dictators with Unflattering Movies.

@john_sileo
Kompromat:
The use of public or hacked information to sow distrust, extort ransom, destabilize power or manipulate outcomes.

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

Let's play a game...
If you don't PAY
You're files go AWAY
In Exactly...

Click-awareness Training +
Real-Time, Off-site Backup +
At-Rest Encryption (Doxxware)

1000 PERSONAL FILES WILL BE DELETED EVERY HOUR IF YOU DON'T SUBMIT $17,500 IN BITCOIN RIGHT NOW.

CLICK HERE TO CHAT
MAKE A BITCOIN PAYMENT
**IoT: Internet of Threats**

If we don’t protect our phones, how can we expect to protect our thermostats, ICS and sensors?

**35%**

Ponemon Cost of Breach

---

**Hotspot Sniffers**

“Free” Wi-Fi Hotspots are commonly “tapped” or “spoofed” by hackers.
A Prioritized Action-list of COUNTERMEASURES

1. Off-site, Real-time Backup: iDrive Bare Metal, SMB, Personal
2. 3rd-party Spam Filter/Anti-Virus-Phishing: ESET Small Business
3. Known Vulnerabilities: Security Updates, XP, Open ports, Phish
4. Encryption: BitLocker (Windows), FileVault (Apple), AxCrypt
5. Default-Deny Firewall: Whitelisted URLs, Wi-Fi Access, Devices
6. Password Management: Dashlane, Lastpass, 1Password
7. Security Assessment: Pen Test, Social Eng, Insider, Heat Map

Resilience is Revenge
Thank You FCBT!
sileo.com
SECURITY THAT STICKS
800.258.8076
john@sileo.com