“Hi, I’m Tom from IT”

Cyber Risk Management: Tools & Tactics Working Together to Solve Information Security Challenges

Tom DeSot

EVP, Chief Information Officer

Digital Defense

DIGITAL DEFENSE INCORPORATED

What Is Social Engineering?

"…the art of manipulating people into performing actions or divulging confidential information." (Wikipedia)

DIGITAL DEFENSE INCORPORATED

State of Security - Real World Examples

- Ubiquiti Networks Inc., the San Jose based manufacturer of networking high-performance networking technology for service providers and enterprises, announced in its fourth quarter fiscal results that it was the victim of an email business fraud incident resulting in the loss of **$39.1 million dollars**.

Source: https://www.csoonline.com/article/2961066/supply-chain-security/ubiquiti-networks-victim-of-39-million-social-engineering-attack.html

State of Security - Real World Examples

- An individual called into Citibank's customer service bureau claiming to be Paul Allen (Co-founder of Microsoft)
- Caller claimed he had misplaced his debit card (did not want to report it stolen)
- Caller was able to change the mailing address for the account to his residence in Pittsburgh over the phone
- Had a new card overnighted
  - Card was used to make a $658 payment to a bank loan account
  - Attempted to make a $15,000 wire transfer and a purchase at Game Stop, but transactions were denied

Source: http://www.wired.com/threatlevel/2012/03/paul-allen-debit-card-caper/

Remote Social Engineering Tactics

Top 3 Scams for 2017

1. The IRS scam
2. Ransomware
3. Business Email Compromise

Source: https://www.forbes.com/sites/laurashin/2017/01/04/be-prepared-the-top-social-engineering-scams-of-2017/

DIGITAL DEFENSE INCORPORATED

Remote Social Engineering Examples

The IRS scam

Scenario

- From now until the end of the tax season, hackers will call from a "spoofed" phone number and claim they are from the Internal Revenue Service (IRS). They declare that a previous tax return has accrued a late penalty, usually around $2,000-$5,000.

- If the target takes the bait, hackers say that because the debt is outstanding, credit card payments are not acceptable. Payment must be via money transfer, which of course is nonrefundable and non-traceable.

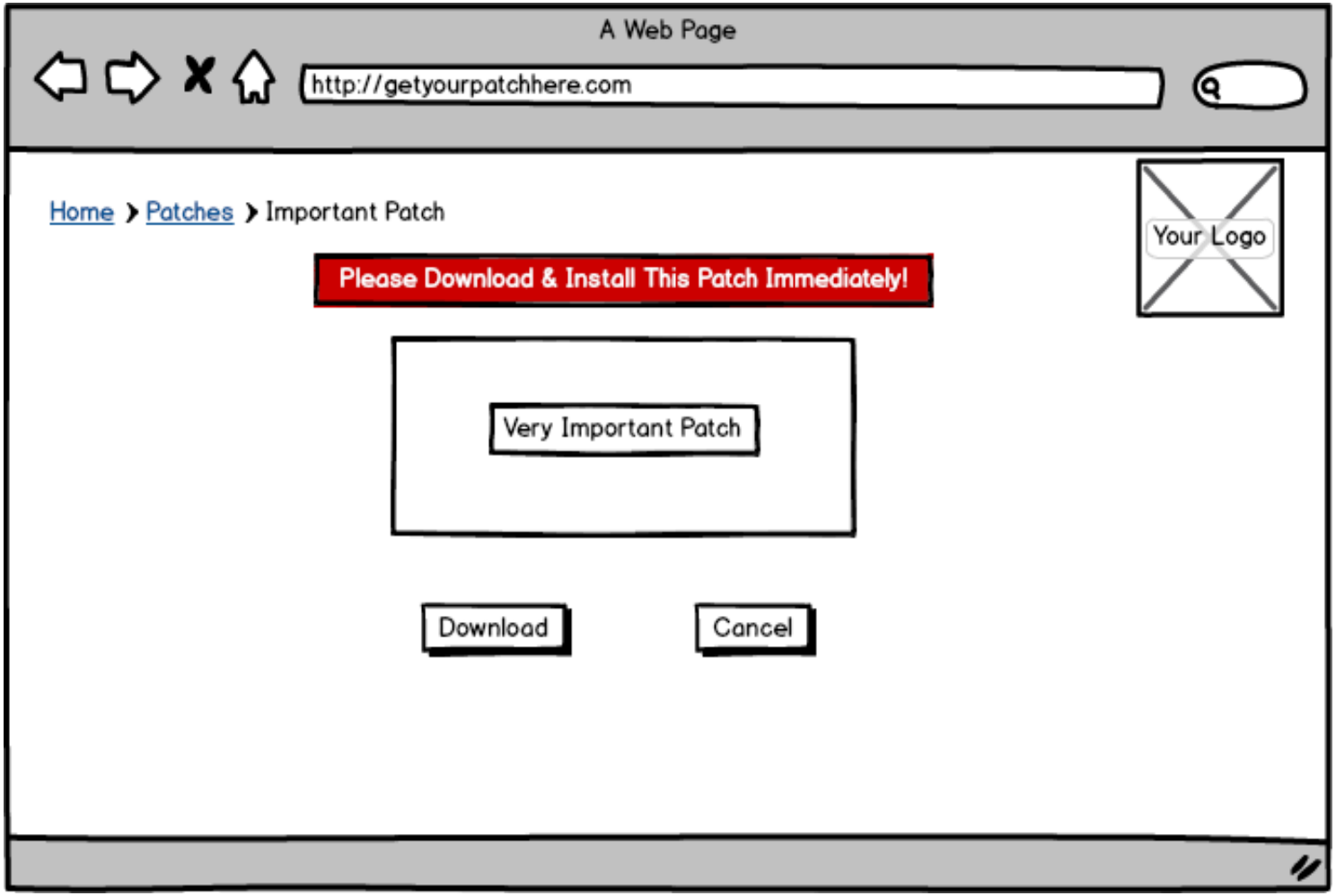
Remote Social Engineering Examples

Ransomware

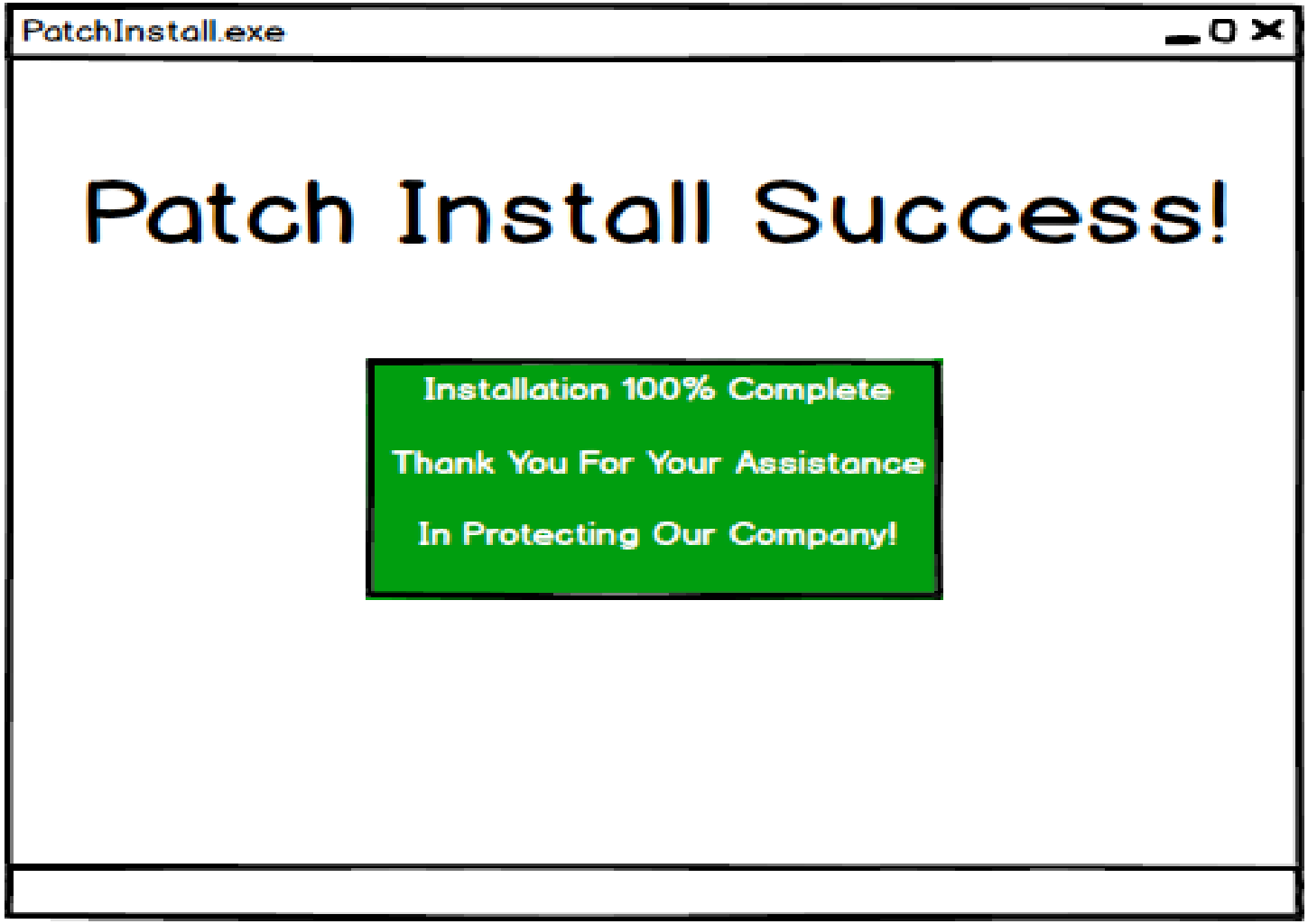
Scenario

- Hacker claiming to be from Microsoft reports malicious activity has been detected on the target's computer.
- The hacker directs the target to a website (Ex. TeamViewer) that downloads a program or patch to install, which then gives them control of the computer.

Sample Site



Sample Dialog Box



DIGITAL DEFENSE INCORPORATED

Remote Social Engineering Examples

Ransomware

Scenario

- Once the hacker has control, they lock the computer so it's inaccessible and demand a ransom.
- Unfortunately, the hacker will often take the ransom but not unlock the computer, so now they have both the money or credit card information and also the computer data, which can allow them access into all kinds of other accounts.

Remote Social Engineering Examples

Business Email Compromise

Scenario

- Hackers gain access to the email account by sending the target a document containing malware. Once opened, the malware infects the computer, allowing the attacker to browse the machine remotely.

- Example: Per CEO, "I'm heading out of town for the holidays and will be out of reach for the next several hours, but we need to make a wire transfer asap to bank account #XXXXXXX."

Other Social Engineering Tactics

BonusPlan2017.xls

Scenario

- The analyst will drop USB fobs in areas where employees congregate
- The test focuses on determining if employees will insert unknown removable media into corporate computers
- When inserted, Excel spreadsheets are shown with file names like “BonusPlan2017.xls”
- Excel does not open; the program silently sends the IP address, hostname and username of the individual to a DDI server

How Successful Are We?

95-98%
Successful

DIGITAL DEFENSE INCORPORATED

What Is Onsite Social Engineering?

Onsite Social Engineering uses several onsite testing methods, including…

- Attempting to gain physical access to the premises
- Attempting to obtain records, files, equipment, sensitive information, network access, etc.
- Attempting to garner information to permit unauthorized network access

Onsite Social Engineering Tactics

Scenario 1: New Employee

- The analyst pretends to be a new employee and enters through employee entrance
- Will typically have already “cased” the organization and will wear the appropriate attire
- Will already have a fake badge before they come onsite

Onsite Social Engineering Tactics

Scenario 2: Trusted Vendor

- The analyst pretends to be someone from a trusted vendor such as the local telephone company, A/C repair, etc.
- Will typically have already called in to see what firms the organization uses
- Shirts are easy to buy at local thrift stores or to have made

DIGITAL DEFENSE INCORPORATED

How Successful Are We?

90-95%
Successful

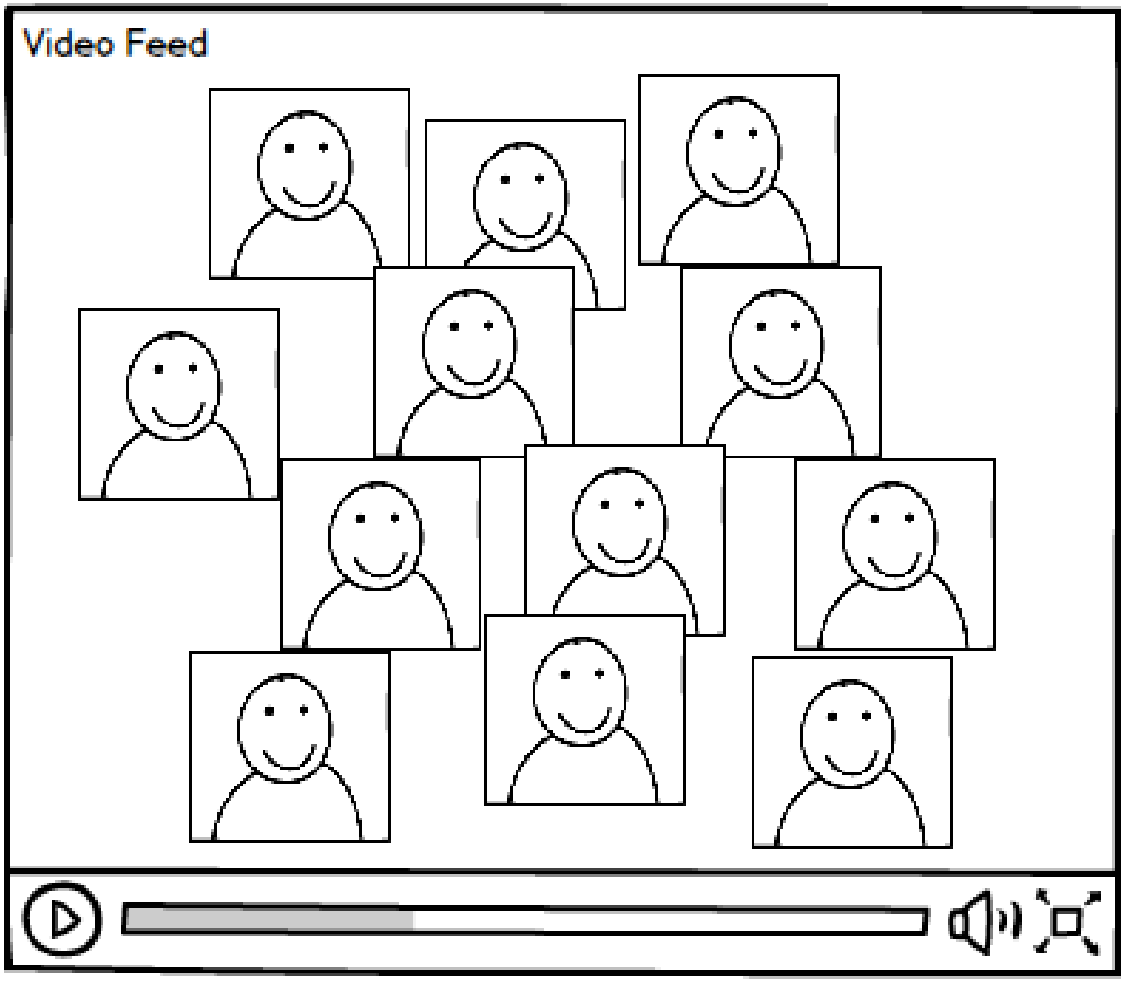
DIGITAL DEFENSE INCORPORATED

What About My Badge System?

DIGITAL DEFENSE INCORPORATED

What About My Door Locks?

What About My Cameras?



What To Do?

- As seen in prior slides, technology will not save you from someone conducting a social engineering attack.
- Most technologies can be circumvented, in some cases very quickly and easily.
- That leaves the question…What *Can* I Do?

Information Security Training!

DIGITAL DEFENSE INCORPORATED

Training Topics

- Social Engineering
  - Remote attacks
  - Onsite attacks

- Password Development and Safety
  - How to develop a strong password or passphrase.
  - Protecting your password once it is developed.

Training Topics

- Clean Desk
  - Make sure any physical content (reports, print outs, etc.) with sensitive information is properly stored and protected while not in use.

- Mobile Security
  - Protecting smartphones and tablets that contain sensitive information.
  - Ensuring the proper policies and procedures are in place to limit the exposure of sensitive data on mobile devices.

Training Topics

- Phishing
  - Ensure employees know how to spot a phishing or whaling attack.
  - Ensure employees understand how to thwart phishing or whaling attacks.
- Acceptable Use of Computer Systems
  - What is and isn't allowed on corporate computers.

Training Topics

- Social Media Dangers
  - What an employee can and cannot say about corporate practices on social media.
  - How employees should respond to direct inquires that come in via social media.
  - Why employees should not click on links coming from someone on social media.

Training Topics

- Securing Protected Data
  - Ensure a document sensitivity marking is in place so that employees know what data needs to be protected.
  - Help employees understand what documents must be destroyed via shredding or other disposal means.

Training Topics

- Safe Web Browsing Habits
  - Help employees understand why the Internet can be a very dangerous place and what they need to do to protect the company and themselves.
  - Educate employees on what constitutes a malicious website.
  - Show employees how to spot a fraudulent website.

DIGITAL DEFENSE INCORPORATED

Digital Defense, Inc.

9000 Tesoro Drive, Suite 100

San Antonio, TX 78217

888.273.1412

www.DigitalDefense.com

tom.desot@digitaldefense.com