RSA Conference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: HUM-T07R

Phishing Dark Waters – Defending Against Malicious Emails

Michele Fincher
Chief Influencing Agent
Social-Engineer, Inc
@SocEngineerInc

What is Phishing?

"We define it as the practice of sending e-mails that appear to be from reputable sources with the goal of influencing or gaining personal information. "

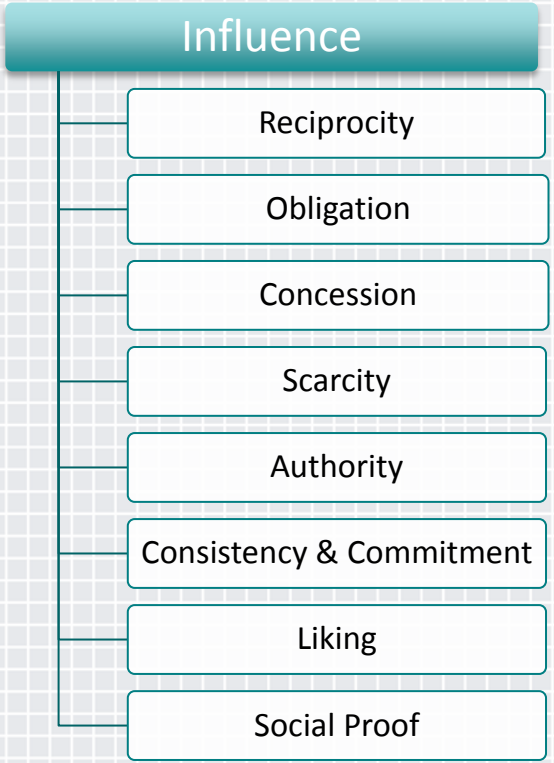
– *Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails (*2015 Wiley)

But come on… does it work?

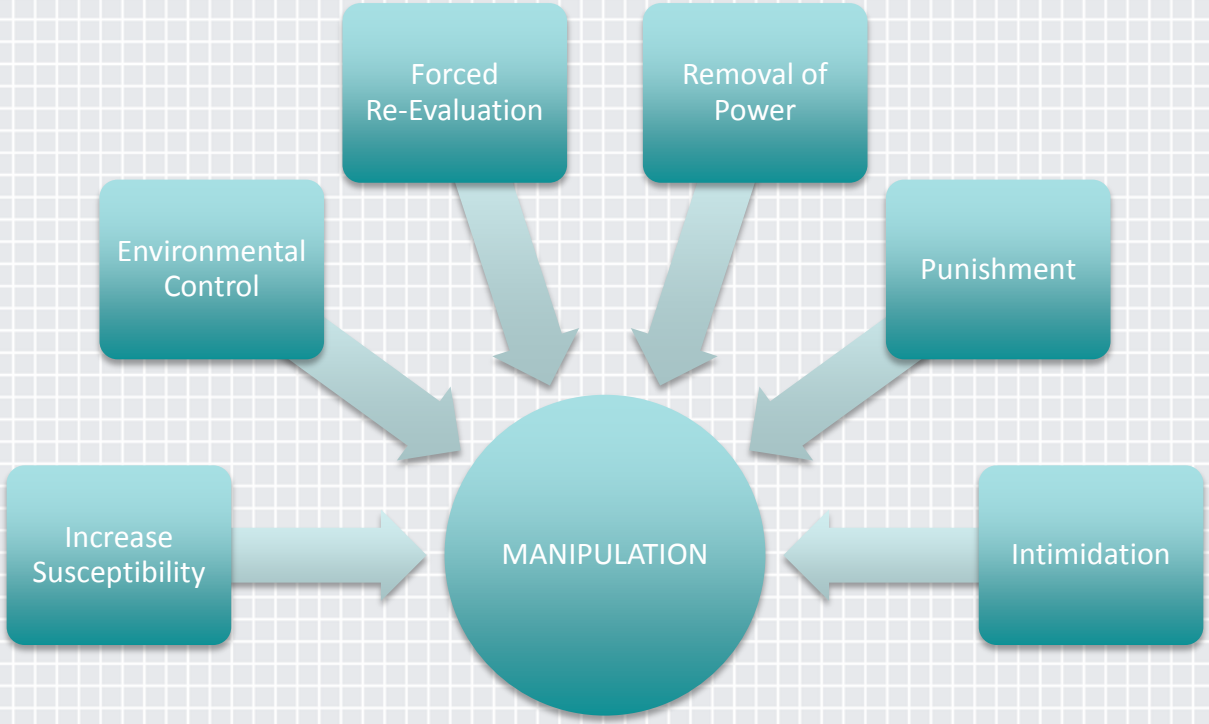
Don’t Forget the Domino Effect

After all of these breaches we see an increase in phishing against the victims of the breach…..

Why does Phishing Work? Influence

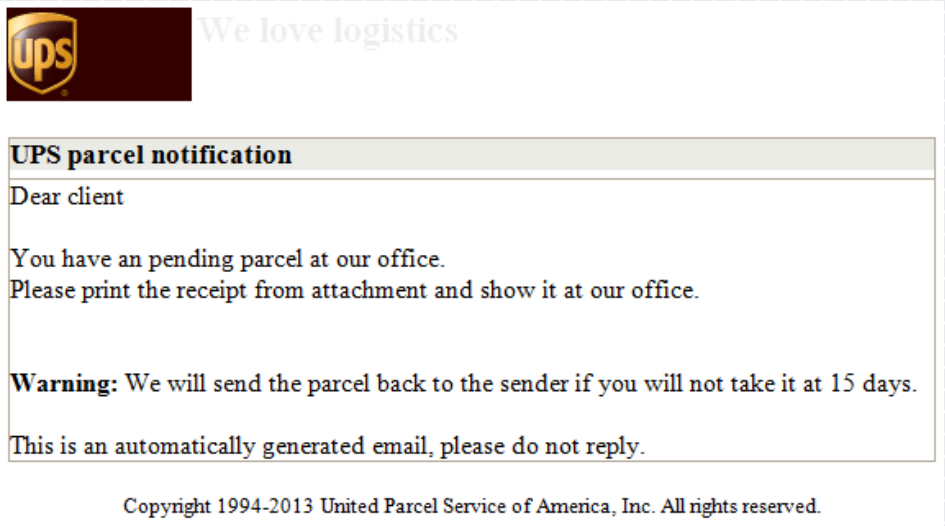


Why Does Phishing Work? Manipulation

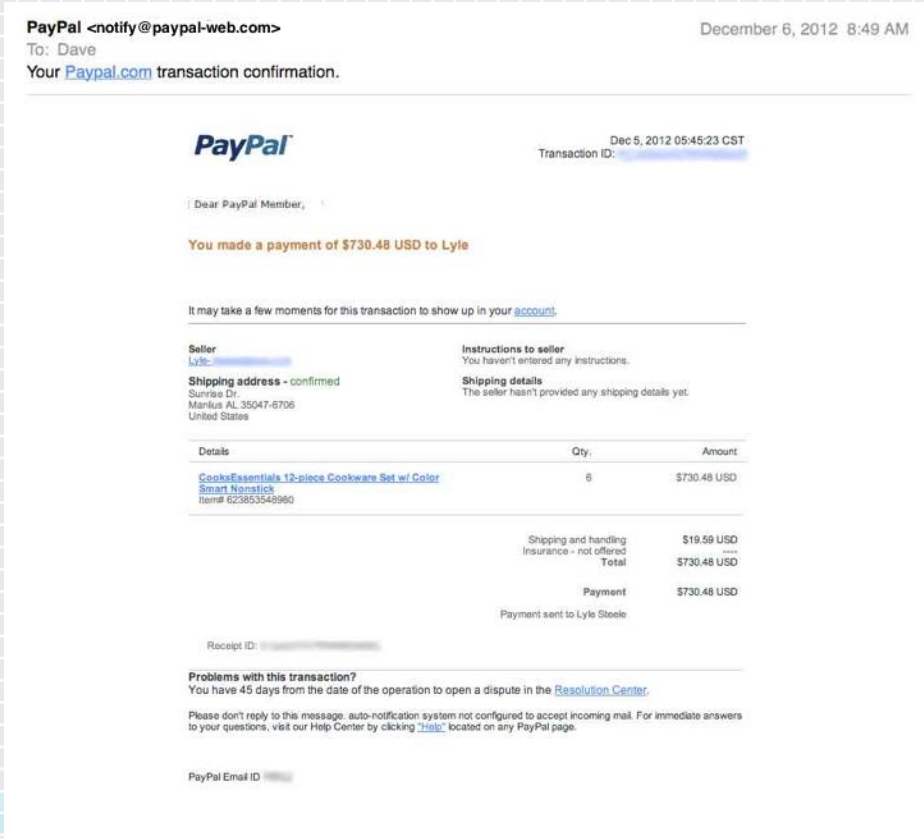


Why Does Phishing Work? Bottom Line

- Bad decision-making
  - Plays on base emotions
  - Uses our natural curiosity
  - We are often too busy to pay attention
- Bad guys are getting smarter
  - Better branding
  - More believable pretexts



Phishing - Example



PayPal <notify@paypal-web.com> December 6, 2012 8:49 AM

To: Dave

Your Paypal.com transaction confirmation.

PayPal

Dec 5, 2012 05:45:23 CST
Transaction ID:

Dear PayPal Member,

You made a payment of $730.48 USD to Lyle

It may take a few moments for this transaction to show up in your account.

Seller
Lyle

Instructions to seller
You haven't entered any instructions.

Shipping address - confirmed
Sunrise Dr.
Manlius AL 35047-6706
United States

Shipping details
The seller hasn't provided any shipping details yet.

Details	Qty.	Amount
CooksEssentials 12-piece Cookware Set w/ Color Smart Nonstick Item# 623853548960	6	$730.48 USD

Shipping and handling	$19.59 USD
Insurance - not offered	-----
Total	$730.48 USD
Payment	$730.48 USD
Payment sent to Lyle Steele	

Receipt ID:

Problems with this transaction?
You have 45 days from the date of the operation to open a dispute in the Resolution Center.

Please don't reply to this message. auto-notification system not configured to accept incoming mail. For immediate answers to your questions, visit our Help Center by clicking "Help" located on any PayPal page.

PayPal Email ID

PayPal <notify@paypal-web.com> December 6,

To: Dave

Your Paypal.com transaction confirmation.

PayPal

Dec 5, 2012 05:45:23 CST

Transaction ID:

Dear PayPal Member,

You made a payment of $730.48 USD to Lyle

It may take a few moments for this transaction to show up in your account.

Seller

Lyle-

Shipping address - confirmed

Sunrise Dr.
Manlius AL 35047-6706
United States

Instructions to seller

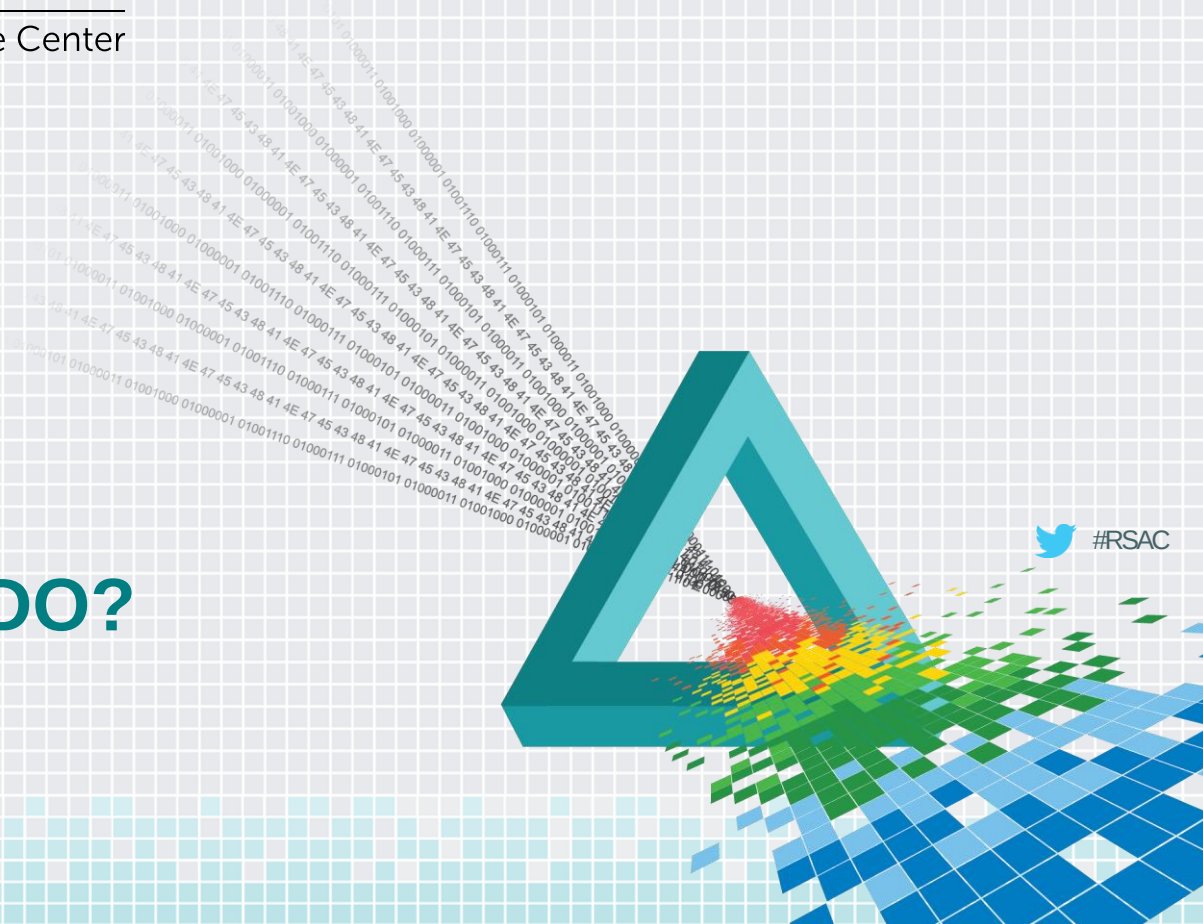
You haven't entered any instructions.

Shipping details

The seller hasn't provided any shipping details yet.

Details	Qty.	Amount

WHAT CAN YOU DO?



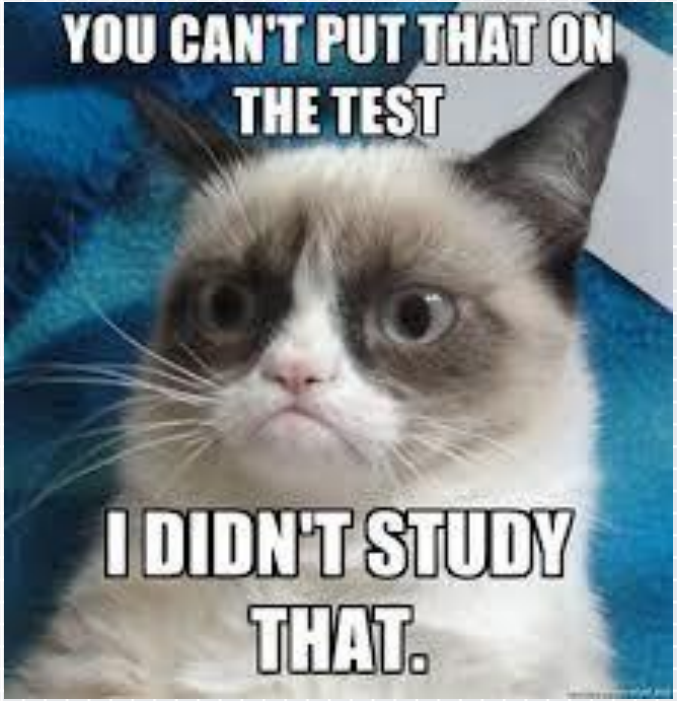
Apply What You've Learned

- Education
- Realistic simulations
- Effective teaching moments

Education

- More than once a year
- Consistent messaging
- Support from the top
- Include everyone - did I say consistent?

Realistic Simulations



- Is a SaaS going to meet your needs?
- How do you test and teach WITHOUT exploiting?
- Don’t expect perfection
- IMPORTANT – Reward the positive, educate the negative
- A good simulation will also set your baseline

Effective Teaching Moments

Use your training time wisely and ask yourself:

- When are you teaching the employee? (pre- or post-click)
- Are you rewarding and reinforcing the positive?
- Is safety a burden?
- Does it make them safer in their personal lives as well?

Key Points To Remember

- Realistic simulations are proven to help increase awareness
- Buy in must be from the top down
- Do not exclude anyone
- Use positive reinforcement of proper behavior
- Do not ever expect 100% success – it's just not HUMAN

RSAConference2015

San Francisco | April 20-24 | Moscone Center

QUESTIONS & ANSWERS

michele@social-engineer.com

www.social-engineer.com

@SocEngineerInc