

A pineapple is positioned on the right side of the image, standing upright in a field of vibrant green grass. The background is a clear blue sky with soft, white clouds. The entire scene is framed by a white horizontal band in the center, which contains the text.

THE HOSPITALITY LAW CONFERENCE: SERIES 2.0

January 11, 2018 • San Diego, CA

The Unintentional Hacker

2018 HOSPITALITY
LAW CONFERENCE:
SAN DIEGO

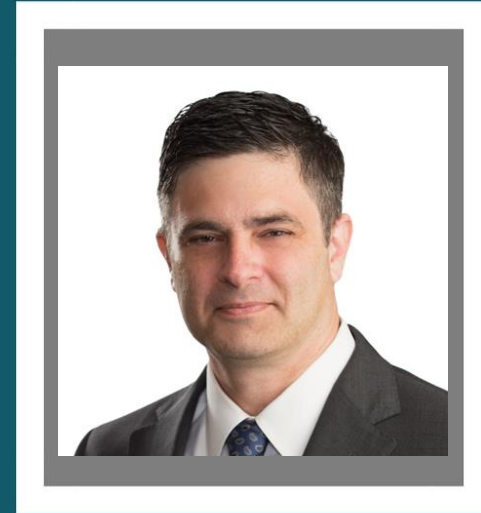
JANUARY 11



Eddie Block

Senior Attorney

- 20+ years in Information Technology & Security.
- Former Chief Information Security Officer for the State of Texas
- CISSP, CIPM, CIPP/G, CISA, CEH



**THE H^{HL}OSPITALITY LAW
C^{HL}ONFERENCE SERIES 2.0**

Social Engineering

Phishing	Spear Phishing	Vishing	Smishing
			
Mass SPAM mailing to lure unsuspecting users.	Directed attempt focused on specific high value targets.	Phone scams directed at users.	SMS / Text Message scams.
An Ethiopian Prince has died and has left you millions of dollars.	Utilize social networks and deep company insights.	I'm from Windows and I'm calling to help you remove a virus.	Confirms active phone numbers and connection to banks.

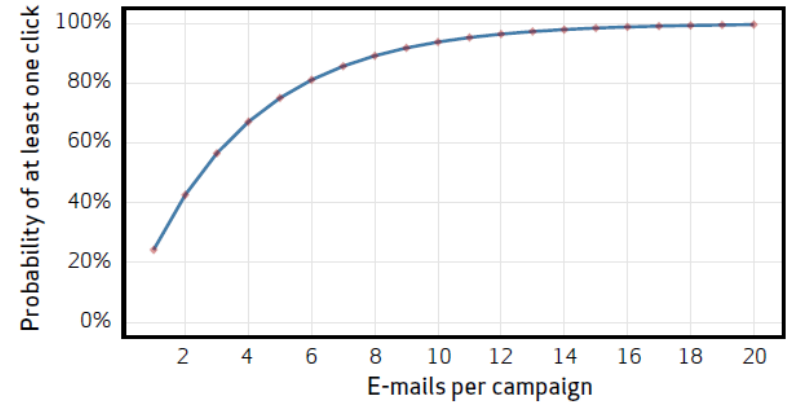


THE ^{HL}HOSPITALITY LAW
^{HL}CONFERENCE SERIES 2.0


Why Phish?


- Running a campaign with just three e-mails gives the attacker a better than 50% chance of getting at least one click.
- Run that campaign twice and that probability goes up to 80%
- Sending 10 phishing e-mails approaches 100%
- within 12 hours

Figure 28: The inevitability of the click



THE **HL**OSPITALITY LAW
CONFERENCE **HL**SERIES 2.0


 > SC US
 SC UK
 SC AUS/NZ


 Year-end content from our Reboot 2013 section.

NEWS PRODUCTS BLOGS RESOURCES VID

FOR IT SECURITY PROFESSIONALS

SC Magazine > Blogs > The Data Breach Blog > Phishing attack leads to breach at government agency


 Marcos Colon, Digital Content Coordinator

June 25, 2012

Phishing attack leads to breach at government agency


 News and Resources for HealthIT Security Pros

[Home](#)
[News](#)
[Topics](#)
[White Papers](#)
[Health IT Terms](#)
[Newsletter](#)

[HIPAA and Compliance](#) |
 [EHR Security](#) |
 [HIE Security](#) |
 [Mobile Security](#) |
 [Data Breaches](#) |
 [Cloud Security](#)

Home > Articles > Saint Louis University notifies 3,000 patients of data breach

Saint Louis University notifies 3,000 patients of data breach

Author Name **Patrick Ouellette** | Date **October 2012**



5 people like this. Sign Up to see what your friends like.

ComputerWeekly.com

[News](#)
[IT Management](#)
[Industry Factors](#)
[Technology Blogs](#)
[Topics](#)
[Multimedia Content](#)
[Jobs](#)
[Premium Content](#)

Home > Topics > IT security > IT risk management > RSA discloses phishing-attack data breach details

NEWS

RSA discloses phishing-attack data breach details

November 27, 2012
Speare Phishing Attack Cause of Massive South Carolina Data Breach



THE HOSPITALITY LAW
CONFERENCE SERIES 2.0

Case Study

- Department of Revenue Breached
 - 3.8 million tax payers and 1.9 million dependents
 - 5,000 credit cards and 3.3 million bank accounts
- Cause
 - Employee opened an infected email attachment
 - Attacker used employees credentials to harvest and create other accounts
- Estimated to cost the state \$25+ million



THE ^{HL}HOSPITALITY LAW
^{HL}CONFERENCE SERIES 2.0

USB Attack

Dropped infected USB in the company parking lot as a way of getting malware onto the company network

By Cory Doctorow at 4:00 pm Tue, Jul 10, 2012

Workers at the Dutch offices of DSM, a chemical company, report finding USB sticks in the company parking lot, which appeared to have been lost. However, when the company's IT department examined the sticks, they discovered that they were loaded with malware set to autorun in company computers, which would harvest employee login credentials. It appears that criminal dropped the keys in the hopes of tricking a employees into getting them into the company network.



THE ^{HL}HOSPITALITY LAW
C^{HL}ONFERENCE SERIES 2.0

Social Media



NSA contractors use LinkedIn profiles to cash in on national security

Employees and job seekers share surprisingly revealing spy project names in public posts on professional networking site



Christopher Soghoian

@csoghoian

Follow



LinkedIn profiles of people in Maryland that mention MARINA & NUCLEON have some fun other codenames like TRAFFICTHIEF

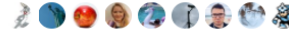


Jason Miller | Professional Profile | LinkedIn

View Jason Miller's professional profile on LinkedIn. LinkedIn is the world's largest business network, helping professionals like Jason Miller discover inside connections to recommended job
[linkedin.com](https://www.linkedin.com)

12:36 AM - 16 Jun 2013

68 Retweets 35 Likes



6



68



35



THE HOSPITALITY LAW
CONFERENCE SERIES 2.0

Plenty of Phish: Hackers Target Dating Sites

tom's
GUIDE

By Tom's Guide / Marshall Honorof
57 minutes ago



Scamming unsuspecting lovers via dating sites is not uncommon, but people can usually spot a fake profile from a mile away. Compromising legitimate profiles is a much smarter, albeit more insidious, way to go. A new wave of phishing attacks across some of the largest dating sites on the Web make it very simple to compromise your login credentials and let your profile fall into the hands of scammers.



Lovelorn individuals on match.com, Christian Mingle, PlentyOfFish, eHarmony, Chemistry.com,

Plenty of Phish: Hackers Target Dating Sites



THE **H**OSPITALITY LAW
C**H**ONFERENCE SERIES 2.0

Protect Yourself

- Never email personal or financial information, even if you are close with the recipient
- Communicate personal information only via phone or secure web sites
- Beware of links in emails that ask for personal information or impart a sense of urgency to reply
- Do not click on links, download files or open attachments in emails from unknown senders
- Protect your computer with a firewall, spam filters, anti-virus and anti-spyware software
- Check your online accounts and bank statements regularly



Thank You

Eblock@gardere.com

