PLUS

PROFESSIONAL LIABILITY UNDERWRITING SOCIETY

Quite a Catch!
Phishing for "Social Engineering" Fraud

September 1, 2016

Presented by PLUS Diamond Sponsors

ARGO GROUP Get there together | AXIS | beazley | CNA We can show you more.® | Endurance ENDURANCE INSURANCE | HISCOX encourage courage™ | TRAVELERS

PLUS

The information and opinions expressed by our panelists today are their own, and do not necessarily represent the views of their employers or of PLUS. The contents of these materials may not be relied upon as legal advice.

A copy of the presentation slides will be available following this webinar, on the PLUS website at: www.plusweb.org

Meet the Presenters

MODERATOR:

Alicia Santocki, Partner, Wilson Elser

PANELISTS:

Peter Hedberg, Senior Technology Underwriter, Hiscox

Jonathan Meer, Of Counsel, Wilson Elser

Introduction

What is Social Engineering

Manipulating someone into doing something by clandestine means

Types of Social Engineering

Quid Pro Quo
Phishing
Baiting
Pretexting
Diversion Theft

Statistics on Social Engineering Fraud

Reported losses of social engineering fraud in 2015 were nearly $1 Billion

In 2014 there were nearly 450,000 phishing attacks globally causing an estimated $5.9 billion in losses. The financial impact to an organization can be significant

29% of all data breaches in 2013 involved social engineering and 77% of those breaches used phishing

Certain industries are targeted more than other for fraud

General Background on Social Media Exposures

Pretexting / Impersonation – creating a fake scenario

Phishing – Sending out bait to fool victims into giving away their information

Fake Websites / Closing – Molded to look like the real thing. Log in with real credentials that are now compromised

Fake Pop-Up – Pops up in front of real web site to obtain user credentials

Malware-Infected Software (Keystroke Viruses)

Social Engineering Fraud

Attacker uses human interaction to obtain or compromise information

Attacker may appear unassuming or respectable

- Pretending to be a new employee, repair man, etc.
- May even offer credentials

By asking questions, the attacker may piece enough information together to infiltrate an organization's network

- May attempt to get information from many sources

Phishing

Fraudulently obtaining private information

Hacker sending an email that looks like it came from a legitimate business

Requesting verification of information and warning of some consequence if not provided

Usually contains link to a fraudulent web page that looks legitimate

User gives information to the social engineer

Example: Ebay Scam

Phishing (Continued)

From: Florida Bar Attorney Consumer Assistance Program [mailto:complaints@flabar.org]
Sent: Wednesday, May 25, 2016 2:20 AM
To: Curran, Francis M.
Subject: Florida Bar Complaint - Attorney Consumer Assistance Program

THE FLORIDA BAR

A complaint has been files against your law practice.

Generic Salutation, Unprofessional manner and poor grammar and/or misspelling

Enclosed is a copy of the complaint which requires your response. You have **10 days** to file a rebuttal if you so desire.

Statement demanding Immediate response

Rebuttals should not exceed 25 pages and may refer to any additional documents or exhibits that are available on request.

Please be advised that as an arm of the Supreme Court of Florida, The Florida Bar can investigate allegations of misconduct against attorneys, and where appropriate, request that the attorney be disciplined. The Florida Bar cannot render legal advice nor can The Florida Bar represent individuals or intervene on their behalf in any civil or criminal matter.

Please review the enclosed complaint. If filing a rebuttal please do so during the specified time frame.

Complaint number: **20160125697**
View Complaint number: 20160125697

Possible Disguise for improper link

Phishing (Continued)

Spear Fishing (Specific Fishing)

Example: email that makes claims using your name

Vishing – where criminals persuade victims to hand over personal details or transfer money over the telephone. They have a number of techniques at their disposal.

Smishing (compromising your smart phone)

"Whale Phishing" or "Whaling" - spear phishing but for bigger fish – in other words, CEO's, CFO's and other senior executives with the power to authorize major money transfers or release sensitive data.

Insurance Coverage Available

Cyber

Professional Liability

Financial Institution Bond

Crime

Cyber

No Standard Wording

Multiple Permutations on the Market

Constantly Evolving

New and Emerging Exposures

Hybrid Policy

First Party Coverage

Third Party Coverage

Professional Liability

While traditional insurance policies typically have not handled the emerging cyber risks, limited coverage under traditional policies may be available.

If a cyber incident resulted in a covered loss

Expressed provisions cover damage or disruption to electronic data

Coverage implicitly provided if (1) Insured engaged in professional services, (2) Insured was victim of, or negligently subjected to, scheme, and (3) no exclusion directly on point.

However, most have mandatory exclusion of coverage for personal and advertising injury claims arising from access or disclosure of confidential information.

Financial Institution Bond

Electronic / Computer Systems Fraud (includes online funds transfers)

First Party loss due to theft occurring within the bank's own computer system

Direct "hack" of funds in your care/custody/control within the bank

Telefacsimile, Email and Voice Instruction Transactions Coverage

Protects the bank for loss due to a fraudulent fax, email or voice instruction

Crime

Most traditional crime policies do not cover social engineering claims

Some have endorsement for loss when an employee is misled by an imposter email, phone call or text message

> "We will pay for loss of or damage to Money, Securities or Other Property resulting directly from the use of any computer to ***fraudulently*** cause a transfer of that property…"

> "We will pay for loss of Money and Securities resulting directly from a ***fraudulent instruction*** directing a financial institution to transfer, pay or deliver Money and Securities from Your Transfer Account"

Examples of Claims

Coverage Disputes Under Crime Policy

Bitpay, Inc. V. Mass. Bay Ins. Co., 2016 U.S. Dist. Lexis 39108 (N.D. Ga. Mar. 17, 2016)

Insurer denied coverage, though it appears a settlement has been reached

Apache Corp. V. Great Am. Ins. Co., 2015 U.S. Dist. Lexis 161683 (S.D. Tex. Aug. 7, 2015)

Coverage Found. Court held that the fraudulent email sent by the fraudsters was computer fraud and was the substantial factor in bringing the injury.

Pestmaster Services, Inc. v. Travelers Casualty and Surety Company of America, 2014 U.S. Dist. Lexis 108416 (C.D. Cal. July 17, 2014)

No Coverage Found. Court held that the insuring agreement does not cover authorized or valid electronic transactions, even though they may be associated with a fraudulent scheme.

Examples of Claims (Continued)

Professional Liability Coverage Disputes

Stark & Knoll Co., L.P.A. v. ProAssurance Cas. Co., 2013 U.S. Dist. Lexis 50325 (N.D. Ohio 2013)

Court found that the subject attorney had engaged in a professional service and the claim covered under its legal malpractice insurance policy.

O'Brien & Wolf L.L.P. v. Liberty Ins. Underwriters, Inc. 2012 U.S. Dist. Lexis 109089 (D. Minn. Aug. 3, 2012)

Court found that the depletion and then replenishment of IOLTA funds was a claim that triggered coverage, law firm engaged in professional services and had duty to safeguard such funds.

Practical Take Aways

The first line of defense is the best and latest software to filter out as much suspicious activity as possible.

Risk management awareness and training.

Strict protocols around wire transfers and information.

User Awareness

- User knows that giving out certain information is bad
- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about internal information
- Do not provide personal information, nor information about the company (such as internal network), unless authority of person is verified

Practical Take Aways (Continued)

Encourage caution & double-checking

Before transmitting personal information over the internet, check the connection is secure and check the url is correct

If unsure if an email message is legitimate, contact the person or company by another means to verify

Employ technology-based solutions to filter emails

Be paranoid and aware when interacting with others on anything that needs to be protected

PLUS

Questions

Thank You Presenters

MODERATOR:

Alicia Santocki, alicia.santocki@wilsonelser.com

PANELISTS:

Peter Hedberg, peter.hedberg@hiscox.com

Jonathan Meer, Jonathan Meer@wilsonelser.com

PLUS

Join us in New York!

PLUS

Thank you, PLUS Diamond Sponsors

PLUS

Thank you for your time.

A replay of this webinar will be available to PLUS Members at:
www.plusweb.org