Social Engineering –
Hacking the Human

WHAT ARE BAD GUYS DOING NOW, AND HOW DO WE STOP THEM?

PRESENTED BY:

UTAH BANKERS ASSOCIATION AND

JON WALDMAN – PARTNER, SENIOR IS CONSULTANT - SBS
Contact Information

• Jon Waldman
  ◦ Partner, Senior IS Consultant
  ◦ CISA, CRISC
  ◦ Masters of Info Assurance – DSU
  ◦ Mission: Save the World!
  ◦ Phone: 605-380-8897
  ◦ jon@protectmybank.com

• www.protectmybank.com
Our Experience

PROCESS:
- Information Security Program design and roll-out
- IT Risk Management
- Vendor Management
- Technology Selection
- Business Continuity / Disaster Recovery
- Incident Response
- Information Security Consulting
- IT Audit
  - ISP Audit
  - Controls Audit
  - Wire Transfer Audit
  - ACH Audit
  - Internet Banking Audit

TECHNOLOGY:
- Penetration Testing
- Vulnerability Assessment
- System Configuration Assessment
- Acceptable Use Scanning

PEOPLE:
- Social Engineering
- Awareness Programs
- ISO Training
- CATO Training

© Secure Banking Solutions, LLC
www.protectmybank.com/sbsinstitute
Dakota State Nationally Recognized

- National Security Agency
- Department of Homeland Security
- 4,000 universities in the country
- Only 100 named national centers in the past 10 years
- National Center of Excellence in Information Assurance
- www.dsu.edu
Cybersecurity State of the Union

- Trends (new tech, greater adoption)
- 2014 – Year of the Data Breach
- New and widespread vulnerabilities
- Cybercrime – increasing rapidly!
- Commercial Account Takeover
- New Regulatory Guidance
  - Cybersecurity Assessments
  - FFIEC IT Management Handbook
  - New Exam Procedures
Why are we talking about this?

• Where’s your data?
• Who’s ultimately responsible for your data?
• Where is information trending?
• Is this whole “world wide web” thing a fad?
Technology Trends

• Remote Banking
  ◦ Consumer Online Banking
  ◦ Commercial Online Banking
  ◦ Mobile Banking

• Mobile Payments
  ◦ Mobile Deposit Capture
  ◦ Commercial Mobile Deposit
  ◦ P2P Payments

• Interactive Teller Machines
• Contactless Payments
• Increased Outsourcing
• Data Breaches...
Digital Banking Trends

• More or less access to money digitally?
  ◦ $96,000 of sales are made on Amazon every minute
  ◦ $612,000 is spent online by consumers every minute
  ◦ http://www.retale.com/info/retail-in-real-time/

• More or less in-person customer interaction?

• Greater or fewer brick-and-mortar locations?

• More or less employees?

• More or less investment into technology?
Banking Method Trends

Source: American Banker’s Association, Nielsen Research
Changes in the Paradigm

“Banking is quickly changing from a place you go to something you do everyday,” stated Brett King, author of bestselling “Bank 2.0” and “Bank 3.0,” as well as founder of mobile banking start-up Movenbank.
Data Security Issues

• Data Breaches
  ◦ Target, Home Depot, so many more

• Widespread Vulnerabilities

• Cybercrime – who are the new bad guys?
  ◦ Social Engineering using (Malware/Phishing)
  ◦ DDOS

• ATM Security Issues

• Wire Fraud
  ◦ Fraud from within the Bank

• Corporate Account Takeover
  ◦ Fraud from outside the Bank
Verizon DATA BREACH INVESTIGATIONS REPORT (DBIR)

- 1367 confirmed data breaches (2014)
- 63,437 security incidents (2014)
- 92% stemmed from external agents
  - Organized criminal group 55%
- 55% utilized some form of hacking
- 29% utilized some form of social engineering
- 40% incorporated malware
- 75% of victims were opportunistic attacks
- 97% of breaches were avoidable through simple or intermediate controls (*2012)
Target (Nov/Dec 2013)

- 40M Credit/Debit Cards
  - Card data for sale online.

- 70M Customer Records
  - Names, mailing addresses, phone numbers or email addresses

- Malware-laced email phishing attack sent to employees at an HVAC firm (which supported Target)

- From HVAC company, accessed Target’s “Vendor Portal”

- Jumped inside the network and infected many Point of Sale systems
World's Biggest Data Breaches

Selected losses greater than 30,000 records
(updated 11th August 2015)
The evolution of Cyber Crime

• Used to be the “hacker”
• Now, it’s Organized Crime
  ◦ Overseas operations
  ◦ Want $$$ to fund their organization
  ◦ Using Low Tech Attacks
  ◦ Target PEOPLE
  ◦ They purchase specialized software
  ◦ Marketing Material
Phishing Trends

- 91% of cyberattacks and the resulting data breach begin with a “spear phishing” email – Trend Micro
Phishing... for “low hanging fruit”

From: "Andrea Keith@irs.gov" <Andrea_Keith@irs.gov>
To:
Sent: Friday, 10 February, 2012 6:42:03
Subject: Rejected Federal Tax transfer

Your Tax transaction (ID: 152757344464), recently sent from your checking account was returned by your Bank.

<table>
<thead>
<tr>
<th>Rejected Tax transaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tax Transaction ID:</td>
</tr>
<tr>
<td>Return Reason</td>
</tr>
</tbody>
</table>

Important Information for Home-care Service Recipients

If you are a home-care service recipient who has a previously assigned EIN either as a sole proprietor or as a household employer, do not apply for a new EIN. Use the EIN previously provided. If you can not locate your EIN for any reason, follow the instructions on the Misplaced Your EIN? Web page.

If you are a home-care service recipient who does not have an EIN, do not use the online application to apply for one. You must apply for your EIN using one of the other methods (phone, fax or mail). For additional information, visit the How to Apply for an EIN Web page.
Spear Phishing

Board of Governors of the Federal Reserve System

The Federal Reserve, the central bank of the United States, provides the nation with a safe, flexible, and stable monetary and financial system.

The outgoing Wire fund transfer, a short time ago sent from your banking account, was not processed by the Federal Reserve Wire Network.

Please click here to view further information.

This service is provided to you by the Federal Reserve Board. Visit us on the web at http://www.federalreserve.gov

Wire Fraud vs. CATO

Wire Transfer Fraud – INTERNAL

• a new trend in which cyber criminals are using spam and phishing e-mails, keystroke loggers, and Remote Access Trojans (RAT) to compromise financial institution networks and obtain employee login credentials.

• Amounts varied between $400k and $900k

• Raised the wire transfer limit on the customer’s account to allow for a larger transfer

• Most of the identified wire transfer failures, the actor(s) were only unsuccessful because they entered the intended account information incorrectly

© Secure Banking Solutions, LLC
www.protectmybank.com/sbsinstitute
Wire Fraud vs. CATO

Commercial Account Takeover - EXTERNAL

• Cyber criminals are targeting small businesses
• Small businesses don’t have security controls in place!
• Small businesses are using Internet Banking - Cash Management systems
  ◦ Bill Pay, Wire Transfers, Direct Deposit, Mobile Capture, etc.
• Cyber criminals take over small business internet banking accounts and transfer money
• CATO = bad news bears for everyone involved
Newest forms of CATO

- Business Email Compromise
- Payroll takeover
- Extortion

### BEC vs. Malware

<table>
<thead>
<tr>
<th></th>
<th>Malware</th>
<th>BEC</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Matches Victim</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Device Print Matches Victim</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Behavioral Match</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Ability to Bypass Dual-Custody</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Ability to Delay Detection/Recall</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
ATM Security

• http://krebsonsecurity.com/all-about-skimmers/

• Do your ATMs use Windows XP?

• Have you addressed other ATM threats?
  ◦ Skimming
  ◦ Cash-out
  ◦ Malware
  ◦ Physical Security
Skimming examples...
How to manage these risks?

• How should you manage the risk to your institution on a go-forward basis?
Answers!

- **Plan**
  - Assess your risk
  - No, REALLY assess it

- **Do**
  - Build your ISP
  - Implement controls

- **Check**
  - Test your people
  - Test your process
  - Test your technology

- **Act**
  - Apply lessons learned
  - Continuously improve!
The McCumber Cube!

Security Goals (the “what”)

Countermeasures (the “how”)

Information States (the “where”)
How does Risk Assessment work?

ASSET (PP) × THREAT = INHERENT RISK

INHERENT RISK - MITIGATING CONTROLS = RESIDUAL RISK
Keys to assessing your Risk (Plan!)

• Get rid of your subjectivity... it’s time to QUANTIFY your risk

• If you can’t quantify your risk, how can you measure it? How can you improve?

• Set goals!

• Know your Acceptable Levels of Risk

• Not just IT Assets, but for other areas
  ◦ Business processes
  ◦ Vendors
  ◦ Enterprise Risk
Build your ISP (Do!)

What does your Risk Assessment tell you? (Identify Risk)

How will you mitigate risk? (Make Decisions)

Document risk mitigating actions in your ISP (Document decisions)

Operationalize your decisions (Implement controls)
How do you Patch your People?

WHAT DO YOU DO WHEN WATCHING ONE 60-MINUTE VIDEO ON PHISHING ISN’T ENOUGH?
Bad Guys Are After 2 Things

1. Information
2. Money
Continuous Security Awareness

• Identify the key elements you need in your training program.
• Consider who should receive the method.
• Decide how often they need to receive it.
• Document the completion of each.
• Measure results whenever possible with quizzes, surveys, or assignments.
• Get others involved in executing each method, create a security culture.
Regular Email Notifications

- From the ISO...

Phishing Scams

Cybercriminals worldwide continue to use phishing scams as a method of infecting your home or work computer to further their malicious agendas. Phishing is a fraudulent email that attempts to acquire sensitive information (such as usernames, passwords, and credit card details), convince the user to click website links, or open email attachments by masquerading as a trustworthy entity. Often times, these website links or email attachments contain malicious software that is designed to steal information, steal usernames/passwords, or give remote control of your computer to the cybercriminal.

General advice for detecting Phishing:

- Be suspicious of ALL email communications. Remember, any sender’s name, email address, or business can be forged
- Often times the email uses a common business name (ex. FedEx, IRS, Federal Reserve)
- Message generally attempts to raise concern or alarm, then ask you to take prompt action such as clicking a link or opening an attachment
- Message is often times generic and will not be addressed specifically to you, but in some cases CAN address you by name or be related specifically to banking processes or vendors
- Often times the website links in the emails do not use HTTPS (secure websites) and link to a fake website that closely resembles a legitimate website

Response Procedures:

If you suspect that you have received a phishing email please use the following procedures:

- Do not open any attachments in the email
Securing the Human

The Monthly Security Awareness Newsletter for Computer Users

OUCH! | March 2013

IN THIS ISSUE...
• Overview
• Privacy
• Security

Social Networking Safely

GUEST EDITOR
Ted Demopoulos is the guest editor for this issue. He is a longtime security consultant and has been teaching SANS courses for a decade, including SEC401/501 and MGT414/512. Learn more about Ted at http://demop.com.

OVERVIEW
checks. Embarrassing or incriminating posts, no matter how old, can prevent you from getting hired or promoted. In addition, many universities conduct similar checks for new student applications. Privacy options may not protect you, as these organizations can ask you to “Like” or join their pages prior to the application.

http://www.securingthehuman.org/
Dont get hooked

Protect yourself from phishing scams

1. Never click links or open attachments from unknown senders.
2. Never send passwords or confidential customer information via email.
3. Never respond to emails that request personal financial information.
4. Always verify the sender's email address before you open an email.
5. Always inform your manager immediately if you receive suspicious email.
6. Remember: If it's too good to be true, it almost certainly is delete it!

www.protectmybank.com
## Online Learning Report

<table>
<thead>
<tr>
<th>first_name</th>
<th>last_name</th>
<th>email</th>
<th>enabled</th>
<th>enrolled</th>
<th>started</th>
<th>last_accessed</th>
<th>completed</th>
<th>score</th>
<th>status</th>
<th>%_complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amy</td>
<td>Star</td>
<td>amy@example</td>
<td>Yes</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>100%</td>
<td>Passed</td>
<td>100%</td>
</tr>
<tr>
<td>Tom</td>
<td>Jones</td>
<td>tom@example</td>
<td>Yes</td>
<td>11/7/2014</td>
<td>11/13/2014</td>
<td>11/13/2014</td>
<td>11/13/2014</td>
<td>70%</td>
<td>Passed</td>
<td>100%</td>
</tr>
<tr>
<td>Ken</td>
<td>Smith</td>
<td>ken@example</td>
<td>Yes</td>
<td>11/7/2014</td>
<td>11/10/2014</td>
<td>11/10/2014</td>
<td>11/10/2014</td>
<td>100%</td>
<td>Passed</td>
<td>100%</td>
</tr>
<tr>
<td>Barb</td>
<td>Hanson</td>
<td>barb@example</td>
<td>Yes</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>90%</td>
<td>Passed</td>
<td>100%</td>
</tr>
<tr>
<td>Kevin</td>
<td>Johnson</td>
<td>kevin@example</td>
<td>Yes</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>90%</td>
<td>Passed</td>
<td>100%</td>
</tr>
<tr>
<td>Jon</td>
<td>Waldman</td>
<td>jon@example</td>
<td>Yes</td>
<td>11/10/2014</td>
<td>11/10/2014</td>
<td>11/10/2014</td>
<td>11/10/2014</td>
<td>90%</td>
<td>Passed</td>
<td>100%</td>
</tr>
<tr>
<td>Ken</td>
<td>Streff</td>
<td>ken@example</td>
<td>Yes</td>
<td>11/10/2014</td>
<td>11/10/2014</td>
<td>11/10/2014</td>
<td>11/10/2014</td>
<td>100%</td>
<td>Passed</td>
<td>100%</td>
</tr>
<tr>
<td>Molly</td>
<td>Knutson</td>
<td>molly@example</td>
<td>Yes</td>
<td>11/10/2014</td>
<td>11/10/2014</td>
<td>11/10/2014</td>
<td>11/10/2014</td>
<td>80%</td>
<td>Passed</td>
<td>100%</td>
</tr>
<tr>
<td>Chad</td>
<td>Hansen</td>
<td>chad@example</td>
<td>Yes</td>
<td>11/10/2014</td>
<td>11/10/2014</td>
<td>11/10/2014</td>
<td>11/10/2014</td>
<td>80%</td>
<td>Passed</td>
<td>100%</td>
</tr>
<tr>
<td>Nick</td>
<td>Pods</td>
<td>nick@example</td>
<td>Yes</td>
<td>11/10/2014</td>
<td>11/10/2014</td>
<td>11/10/2014</td>
<td>11/10/2014</td>
<td>100%</td>
<td>Passed</td>
<td>100%</td>
</tr>
<tr>
<td>Frank</td>
<td>Larson</td>
<td>frank@example</td>
<td>Yes</td>
<td>11/10/2014</td>
<td>11/10/2014</td>
<td>11/12/2014</td>
<td>11/12/2014</td>
<td>100%</td>
<td>Passed</td>
<td>100%</td>
</tr>
<tr>
<td>Teri</td>
<td>Jones</td>
<td>teri@example</td>
<td>Yes</td>
<td>11/10/2014</td>
<td>11/10/2014</td>
<td>11/14/2014</td>
<td>11/14/2014</td>
<td>100%</td>
<td>Passed</td>
<td>100%</td>
</tr>
<tr>
<td>Aaron</td>
<td>Lawson</td>
<td>aaron@example</td>
<td>Yes</td>
<td>11/12/2014</td>
<td>11/12/2014</td>
<td>11/12/2014</td>
<td>11/12/2014</td>
<td>100%</td>
<td>Passed</td>
<td>100%</td>
</tr>
<tr>
<td>Lori</td>
<td>Sky</td>
<td>lori@example</td>
<td>Yes</td>
<td>11/12/2014</td>
<td>11/12/2014</td>
<td>11/12/2014</td>
<td>11/12/2014</td>
<td>100%</td>
<td>Passed</td>
<td>100%</td>
</tr>
<tr>
<td>Jim</td>
<td>Knutson</td>
<td>jim@example</td>
<td>Yes</td>
<td>11/12/2014</td>
<td>11/12/2014</td>
<td>11/13/2014</td>
<td>11/13/2014</td>
<td>90%</td>
<td>Passed</td>
<td>100%</td>
</tr>
<tr>
<td>Brenda</td>
<td>Franklin</td>
<td>brenda@example</td>
<td>Yes</td>
<td>11/13/2014</td>
<td>11/13/2014</td>
<td>11/14/2014</td>
<td>11/14/2014</td>
<td>90%</td>
<td>Passed</td>
<td>100%</td>
</tr>
<tr>
<td>Tim</td>
<td>Donnelly</td>
<td>tim@example</td>
<td>Yes</td>
<td>11/13/2014</td>
<td>11/13/2014</td>
<td>11/13/2014</td>
<td>11/13/2014</td>
<td>90%</td>
<td>Passed</td>
<td>100%</td>
</tr>
<tr>
<td>Sam</td>
<td>Burns</td>
<td>sam@example</td>
<td>Yes</td>
<td>11/19/2014</td>
<td>11/19/2014</td>
<td>11/19/2014</td>
<td>11/19/2014</td>
<td>100%</td>
<td>Passed</td>
<td>100%</td>
</tr>
</tbody>
</table>
Infragard Awareness

- https://www.infragardawareness.com/
Top 100 Banks Surveyed

- What threat represents the most cyber security risk to a bank?
  - 1. Phishing 44
  - 2. Malware 27
  - 3. Data Loss 14
  - 4. ACH Fraud 13
  - 5. ATM 2

Get Board involved and get more security conscious as well
Customer Awareness Materials

Ten Essential Cybersecurity Best Practices
Banking • Business • Employees

Brought to you by:

Secure Banking Solutions
www.protectmybank.com

Onsite Security Awareness Day

Business Seminar: Managing Your Security Risk
February 12, 2012

Businesses are invited to this free seminar.
Attendees will walk away with the information and tools to assess their businesses online security strengths and potential weaknesses.

Lunch is provided.

Presenters include:
Chad Knutson, Consultant, Secure Banking Solutions
Banker 1 Vice President of Information Systems, Information Security Officer
Banker 2 Vice President of Business Banking

Please RSVP using the eform below or by emailing banker@bank.com. If you are unable to attend, but would like more information, contact your Business Banker.

RSVP by February 02, 2012

Registration is closed.
Test your Program (Check!)

1. Assess Risk
2. Implement Controls
3. Audit Controls
   - People
     - Social Engineering Assessment
   - Process
     - Info Technology / Security Audit
   - Technology
     - Vulnerability Assessment
     - Penetration Testing
Social Engineering

• Test your PEOPLE
• Check effectiveness of training program
• Types Include:
  ◦ Phishing Emails
  ◦ Phone Impersonation
  ◦ Physical Impersonation
  ◦ Dumpster Diving
• How often should you test your People?
• Can do you do some SE testing yourself?
Phishing Emails

• Phishing, Spear Phishing, and Whaling
Physical Impersonation

WORK ORDER

CUSTOMER: ********* (Madison)
408 Hwy 77
Madison SD 57042
(605) 427-3076

ASSIGNED TO: Knutson, Chad

PROPERTY ID: 16

WORK ORDER NUMBER: 5553

EMPLOYEE ID: 1009

DATE REPORTED: 10-27-11

DATE ASSIGNED: 10-31-11

TARGET DATE: 11-04-11

WORK DESCRIPTION:
Manually update firmware (rfw-201101.5) on internet router to address issues with remote installation administration.

Work scheduled and approved by Scott Hanson.

Century Link
105 S Technopolis Ave
Sioux Falls SD 57106
Phone: (605) 488-3366
Pretext Calling

FREE CALLER ID SPOOFING TRIAL

Your Number
1
Enter the number you are calling from

Destination Number
1
Enter the number you would like to call

Spoofer Number

Enter the number you would like displayed

Voice Pitch
Adjust the pitch of your voice

Soundboard
Name

Place Call

Restrictions apply

Phone Impersonation Script: Customer

Company: Good morning, <company>, this is ___________
Consultant: ___________

SAM

TARGET: <target>

Company: Hi, how are you today?
Consultant: Just fine, how may I help you?

Company: This is ___________ from ___________.
Consultant: We are having issues logging into our services and was wondering if you could help us out by verifying the username that you have on file for us. <use first last example: "Jscarlata"> If they tell you username act like you are trying to log in >
Consultant: It still won't log in could you tell me what password that you have on file, to see if it's any of the passwords that I have in front of me. <If Password is given tell them thanks and try to get them to change the email that they have on file same as before>

Consultant: My Company decided to use a third party email service for sending and receiving secure communications and I would like send the email to the secure email.
Company: Sure. <If they resist, tell them it will only take a few seconds & it will greatly help you out>

Consultant: <securedmessages.com> send the password to verify that the account information has been successfully updated and we will change the password according to the new company password policy.

URL received: 
User Name: 
New Password: 

Company: <Either they will send you the password recovery URL through the new email OR Deny>
Consultant: Thank you. <If customer account information is changed, immediately notify the customer service representative that this is a test and have SBS notify the contact>
Dumpster Diving

© Secure Banking Solutions, LLC
www.protectmybank.com/sbsinstitute
## Analyze Results of Training vs Testing

### Phishing Results

<table>
<thead>
<tr>
<th>first_name</th>
<th>last_name</th>
<th>email</th>
<th>Clicked</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amy</td>
<td>Star</td>
<td>amy@exam</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Tom</td>
<td>Jones</td>
<td>tom@exam</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Ken</td>
<td>Smith</td>
<td>ken@exam</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Barb</td>
<td>Hanson</td>
<td>barb@exam</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Kevin</td>
<td>Johnson</td>
<td>kevin@exam</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Jon</td>
<td>Waldman</td>
<td>jon@exam</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Ken</td>
<td>Streff</td>
<td>ken@exam</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Molly</td>
<td>Knutson</td>
<td>molly@exam</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Chad</td>
<td>Hansen</td>
<td>chad@exam</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Nick</td>
<td>Pods</td>
<td>nick@exam</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Frank</td>
<td>Larson</td>
<td>frank@exam</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Teri</td>
<td>Jones</td>
<td>teri@exam</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Lori</td>
<td>Sky</td>
<td>lori@exam</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Jim</td>
<td>Knutson</td>
<td>jim@exam</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Brenda</td>
<td>Franklin</td>
<td>brenda@ex</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Tim</td>
<td>Donnelly</td>
<td>tim@exam</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Sam</td>
<td>Burns</td>
<td>sam@exam</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Online Learning Exam Results

<table>
<thead>
<tr>
<th>first_name</th>
<th>last_name</th>
<th>email</th>
<th>enabled</th>
<th>enrolled</th>
<th>started</th>
<th>last_accessed</th>
<th>completed</th>
<th>score</th>
<th>status</th>
<th>% complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amy</td>
<td>Star</td>
<td>amy@exam</td>
<td>Yes</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>100% Passed</td>
<td>100%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tom</td>
<td>Jones</td>
<td>tom@exam</td>
<td>Yes</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>100% Passed</td>
<td>100%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ken</td>
<td>Smith</td>
<td>ken@exam</td>
<td>Yes</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>100% Passed</td>
<td>100%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Barb</td>
<td>Hanson</td>
<td>barb@exam</td>
<td>Yes</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>100% Passed</td>
<td>100%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kevin</td>
<td>Johnson</td>
<td>kevin@exam</td>
<td>Yes</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>100% Passed</td>
<td>100%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jon</td>
<td>Waldman</td>
<td>jon@exam</td>
<td>Yes</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>100% Passed</td>
<td>100%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ken</td>
<td>Streff</td>
<td>ken@exam</td>
<td>Yes</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>100% Passed</td>
<td>100%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Molly</td>
<td>Knutson</td>
<td>molly@exam</td>
<td>Yes</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>100% Passed</td>
<td>100%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chad</td>
<td>Hansen</td>
<td>chad@exam</td>
<td>Yes</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>100% Passed</td>
<td>100%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nick</td>
<td>Pods</td>
<td>nick@exam</td>
<td>Yes</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>100% Passed</td>
<td>100%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Frank</td>
<td>Larson</td>
<td>frank@exam</td>
<td>Yes</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>100% Passed</td>
<td>100%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Teri</td>
<td>Jones</td>
<td>teri@exam</td>
<td>Yes</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>100% Passed</td>
<td>100%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aaron</td>
<td>Lawson</td>
<td>aaron@exam</td>
<td>Yes</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>100% Passed</td>
<td>100%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lori</td>
<td>Sky</td>
<td>lori@exam</td>
<td>Yes</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>100% Passed</td>
<td>100%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jim</td>
<td>Knutson</td>
<td>jim@exam</td>
<td>Yes</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>100% Passed</td>
<td>100%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tim</td>
<td>Donnelly</td>
<td>tim@exam</td>
<td>Yes</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>100% Passed</td>
<td>100%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sam</td>
<td>Burns</td>
<td>sam@exam</td>
<td>Yes</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>11/7/2014</td>
<td>100% Passed</td>
<td>100%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© Secure Banking Solutions, LLC
www.protectmybank.com/sbsinstitute
Social Engineering Best Practices

• ALWAYS validate requests for information if you’re not 100000% sure

• NEVER insert unknown media devices into workstations or servers without making 100% sure they are clean or that the device has been approved

• NEVER submit confidential or information into a website that originated with a link from an emails

• ALWAYS ASK QUESTIONS!
  ◦ Is this who I think it is for sure?
  ◦ Did someone mention this to me personally, or was it discussed at a staff meeting?
  ◦ Is this the FIRST I’m hearing about this?

• USE YOUR SECURITY SPIDER SENSE!
That’s all she wrote...

• Any questions, comments, or concerns?
• Also, for a much deeper dive on Information Security specifically for financial institutions, check out our Cybersecurity Certification Programs!
  ◦ CB Security Professional (CBSM)
  ◦ CB Technical Professional (CBSTP)
  ◦ CB Vendor Manager (CBVM)
  ◦ CB Ethical Hacker (CBEH)
  ◦ CB Incident Responder CBIH)
  ◦ CB Business Continuity Professional (CBBCP)
  ◦ Ask us about it!
Questions?

• Contact Information

• Jon Waldman
  ◦ Partner, Senior IS Consultant
  ◦ CISA, CRISC
  ◦ Master’s of Information Assurance, Dakota State University
  ◦ Mission: save the world!
  ◦ Phone: 605-380-8897
  ◦ jon@protectmybank.com
  ◦ www.protectmybank.com