Protection Strategies for Yourself, Staff and Customers

Banking and the Economy:
A Forum for Women in Banking
March 28, 2017
Elaine Dodd, EVP Fraud
Oklahoma Bankers Association
What Are We Doing Here at OBA? And Why?

• First, and only, association fraud division
• Active since 2003
• Retired law enforcement with strong background in training and networking
• Rapport with law enforcement, seniors, bankers and retailers all critical pieces
• It’s great to be old, really
Risk Assessment Basics

Probability: High
Severity: Serious
So, It’s All About Living, Breathing Policies

• Do you have the right policies?
• Are they kept up-to-date?
• Are they concise enough to be read?
• Are they communicated to and understood by all?
Forms of Identity Theft:

- Credit card fraud
- Applying for loans in someone else’s name
- Raiding bank accounts
- Check fraud
- And on and on...
Identity Thieves Need Personal Identifying Information:

• Bank account numbers
• Credit card account numbers
• Social Security numbers
• Personal identification numbers (PINs)
• Passwords
• Stolen credit cards or checks
• Dates of birth
• Addresses and phone numbers
How ID Thieves Obtain Personal Information:

• Phone and Internet scams
• Stealing mail
• Working with dishonest employees with consumer information
• Searching through trash – dumpster diving
Shred, shred, shred

(Credit card offers, bank statements, any items with your personal information)
Physical Safety (Safe and Smart Shopping and Living)
Big 3 for Safety:

1. Check credit card statements monthly
2. Check bank statements monthly
3. Review Your Credit Report Each Year

Starting June 1, 2005

www.annualcreditreport.com

1-877-322-8228
If You Are an Identity Theft Victim

- Think like a police officer or lawyer
- Financial fraud is a crime, file a police report – be persistent
- Contact your bank and creditors.
- Contact the credit bureaus and place fraud alert.
- Call the FTC hotline 1.877.ID THEFT or online [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft).
- Document and organize your case
Social Engineering

Hi,

I’m a gentleman from Oklahoma, Tulsa!
Social Engineering Methods

Mediums / Methods of attack include:
- Telephone (impersonation, pretexting)
- Email (phishing, spearphishing, pharming)
- Internet (fake websites)
- Social Media (FaceBook)
- Mobile Devices (SMSishing, Bluesnarfing)
- Dumpster Diving (low tech, but very effective)
- Malware (jump/flash drive baiting)
MOVIE HACKING...

If I can just overclock the Unix Django, I can basic the DDOS Root. Damn. No dice. But wait... if I decrypt their kilobytes with a backdoor handshake then... Jackpot.

REAL HACKING...

Hi, this is Robert Hackerman. I'm the county password inspector.

Hi Bob! How can I help you today?
Don’t forget Rayleen’s articles!

On our website www.oba.com
Under Fraud Prevention Tab
Already There:
  FTC Guidelines for Small Business Cybersecurity
  Romance Scams
  Scrooge Stole Your Donation
  3 Common Social Engineering Techniques Your Business Needs to Know
    ▪ Tailgating
    ▪ Phishing
    ▪ Bogus Caller

Rayleen Pirnie – fraud consultant and true expert – formerly with EPCOR
We ARE the Weakest Link!

Listen for:

• Hesitations/clearing throat nervously
• Too many chances
• Inconsistencies
• How long does it take you to give a phone number?
WATCH THIS HACKER BREAK INTO MY CELL PHONE ACCOUNT IN 2 MINUTES
So how do we get to error states?

- Greed
- Emotion
- Fear

- So, are you in your “Planner” mode?
Or, have you been nudged over to “Doer”? 
What an Organization Should be Doing Now

Create and communicate clear-cut security policy guidelines that apply to ALL employees.
Rules should apply for:
- Email usage
- Web browsing
- Social networking
- Mobile devices

- Monitor and Test
c. **Written policies, procedures and guidelines for following:**

- Core banking system
- Imaging
- Wire transfer
- LAN or wide area networking
- Wireless networking
- Virtual private networking
- Voiceover IP telephone
- IMs
- Portable devices (PDAs, laptops, cell phones)
- Routers
- Modems
- Firewalls, et al
- Other remote devices (eg GoToMyPC)
Focus on mobile devices too such as smartphones, tablets, and other portable devices, including employee-owned devices that are being used in the workplace.

- By 2016, 38% of organizations will have stopped providing mobile devices to employees, instead allowing employees to choose and use their own devices in the workplace.
- By 2017, half of all employees will be using their own devices at work.
Got a computer in your pocket? Then we need to treat it like one!
Teach employees to avoid phishing scams. When in doubt, and even if the source is known, employees should NOT click on or re-post suspicious links in:

- Emails
- On-line ads
- Tweets
- Messages
- Posts
- Attachments
Don’t click the link. Or the attachment. Really Just don’t click.
Have you or your customers received the OPM breach notice?

• It’s probably real (hoaxes do spring out of real events, though)
• Vast numbers of breaches now merit placing security freeze on your credit files
• Great info at:
  • http://uspirg.org/sites/pirg/files/reports/USPIRGFREEZE_0.pdf
  • http://krebsonsecurity.com/2015/06/how-i-learned-to-stop-worrying-and-embrace-the-security-freeze/
Phishing, Vishing and now SMiShing (SMS Phishing)

Sample: Fraudulent Text messages are being sent to cell phones in Oklahoma:

“This is an automated message from XXXX bank. Your ATM card has been suspended. To reactivate call urgent at 18775895978.”
Password “hygiene”

Use your passwords like a toothbrush:
• *don’t let anyone else use it,*
• *and change it every six months.*
Passwords and Password Managers

• Post-Its, Really Now?
• Password Safe – yes – and free
• Dashlane Password Changer – works
• LastPass – former recs and story
Longest Password Ever

During a recent password audit by a company, it was found that one employee was using the following password: “MickeyMinniePlutoHueyLouieDeweyDonaldGoofySacramento”

When asked why she had such a long password, she rolled her eyes and said, “Hello! It has to be at least 8 characters and include at least one capital!”

- So, think about passphrases
- Nothing wrong with a good y’all
- Complex Passwords, Updated Regularly
What is this about Heartland/Global Payments, Home Depot, Target, Nieman, White Lodging etc, etc...
And what’s it mean to you?
Big Kudos and Thanks to our Buddy Brian Krebs, KrebsonSecurity.com

Alberto Gonzalez
What Else Do We Know Now? (Friendly Reminder. Third party. Third party.)

Third Party Vendors
BlackPOS
17 YOA Russian wrote code
Could POS be any funnier?
Counterfeit Credit Cards
Skimmers (Readers and Writers)
Contactless Payment (AKA Touch and Go or Wave and Pay)
RFID Questions and Controversy

• EMV not = to RFID
• Dynamic CVV possible on EMV
• RFID blockers do work for RFID cards
  (with 🔒 or 📱 eg, PayWave, PayPass, etc.)
• That is different from EMV
McDumpals
Upsurge in Cryptolocker and Morphed Versions: Continuing Reminder of Importance of Backups
Answer to Ransomware (and a Host of Problems)

Create systems to automatically back up work. Some computers will not allow shut down without first backing up the day’s work. Ensure that your backed up data is preserved and covers an adequate history.
It’s All About Networking
(and Understanding SAR’s)

Infragard – no or low cost training and FBI networking

OK Chief of Police CLEET Recertification Training

Adult Protective Services

Think about groups like our Info Security MAFIA

Topics like Suspicious Activity Report:

Or, Can You Say,

“Somethin’ Ain’t Right”???
Maintain a continuously open, two-way line of communication between IT and all other staff in your organization.

- Include ALL staff – on-site, satellite office, remote employees, etc., contractors too!
- Employ themes, such as, ‘If you see something, say something’, to combat social engineering fraud.
Map.norsecorp.com - Thanks, Brian Krebs!
• What is the magic of 229 days? To clarify, magic for the bad guys!
• What should your response be?
• SAR-able?
And, are you watching your wires?

- Social Engineering training critical on this topic
- Who signed the authorization for wires and is request new?
- Issues from fraudsters overseas and corporate embezzlers here

- New OBA Fraud Alert
Business Email Compromise
(Affectionately Referred to as BEC)

First seems unsophisticated relative to Dyre and ZeuS, but really more versatile and adept at sidestepping basic security strategies.

### 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>
Attempted (and Completed) Wire Frauds Abound

Don know if you want to forward this to IT law enforcement peeps. They have spoofed it to look like it is from Roger but it isn’t. I knew he wouldn’t phrase things in that way. Initially, I hit reply to confirm with him. The address on the reply message was ceo-private-email@usa.com I did confirm with Roger that he didn’t send the message. I haven’t deleted the message so let me know if I need to forward to anyone.

Lea Ann Jackson, CPA, CAE
Chief Operations Officer and
Chief Financial Officer
Oklahoma Bankers Association
643 NE 41st
Oklahoma City, OK 73105
405/424-5252

WE MAKE BANKERS BETTER!

From: Roger Beverage [mailto:roger@oba.com]
Sent: Monday, November 09, 2015 7:15 AM
To: Lea Ann Jackson <leaann@oba.com>
Subject: Invoice#003156

Hi,

Please I will need you to make a payment for me today and right away, respond asap?

Thanks,

Sent from my iPhone
And Another Crisis Averted
Rethinking These Will Help

- Your company “About” page
- Company postings for IT positions – add false triggers
- Security Questions
  - Honesty not always the best policy here
  - Car, Mom, School
  - Let’s be creative
Citizens as Money Mules

• Money Mules, aka Money Laundering
• Committing Fraud — Can Be Sued or Prosecuted
• Fall for it once, will likely fall for it again
• Educate Consumers, Stop The Traffic, Stop the Scams
Corporate Account Takeover —
Availability Exception Option
Approved September 8, 2011; Effective January 1, 2012

Option for an RDFI to exempt itself from the funds availability requirement for an ACH credit when it reasonably suspects that the ACH credit is not authorized.

Additional time to investigate a suspicious credit prior to making funds available to a Receiver. The additional time might enable ODFIs and RDFIs to identify instances of unauthorized credit entries due to Corporate Account Takeover, and recover funds on behalf of Originators before funds are withdrawn.
Craigslist, eBay, Amazon Convergence
and “the Need for Speed”

The BobCat loader, a weekend phone call, and help from one really big bank.
Helpful Practices

- Patch & Scan Regularly
- Stand Alone Computers
- Restrict Admin Privileges
  - Establish User Accounts
- Stay Informed of Threats
- Regular Audits
  - Review ACH & Wire (or accounts) daily
- Report Suspicious Activities
- Stronger Internal Controls
  - Mandatory Vacations
  - Dual Control
  - Limits
Counterfeit Cashiers Checks

• Always, *always* verify with issuing bank, using a phone number you have located yourself (not the one printed). (For their corporate “cousins” call the company supposedly issuing the check directly.)

• Verify routing number to the bank on which the check was written.

• Ensure customers know “funds available” is not the same as “funds collected”.

• Consider policies to increase holds, more strict policies on hold releases, *collection not deposit*
Counterfeit Corporate Checks

No, Dell has not funded a sweepstakes and sent you a check!

And, neither did Pro1 Automotive
Counterfeit Bills

This:

Not This: Old 5 Watermark

Or This: New 5 Watermark

Or, Seriously?!?!?!
Tell Me Again Just What Great Folks Our Bankers Are!
Lottery / Sweepstakes Scam

- Same old story – Still works
- Congratulations! You have won the “insert foreign country here” lottery!
- Fees and Taxes Required Up Front
- Past = Check
- Today = More ACH
- Stolen funds from hijacked originator accounts

- Or, is your new business deal a lottery scam on steroids
- Now moving from Western Union wires to pre-loaded cards (eg Green Dot and ITunes)
Or... Trust Me

• Swindle netting thousands or tens of thousands
• Caller claims to be grandchild or law enforcement
• Request to wire funds to help relative in legal trouble out of the country
• Ask that they be discreet (Don’t tell Mom and Dad) – fake embarrassment

• If your phone rings in the middle of the night, I’m betting your grandson is not really in Canada. Or in trouble, in jail. Or needing money!

• I’m with the IRS. You owe money and I’m taking you to jail if you don’t pay. Now.
Avoid Tech Support Phone Scams —
Friendly Advice from Microsoft (And Apple not immune)
Offer to help solve your computer problems or sell you a software license. Once access to your computer, they can do the following:

• Trick you into installing malicious software and then charge you to remove this software.
• Take control of your computer remotely.
• Request credit card information for phony services.
• Direct you to fraudulent websites and ask you to enter credit card and other personal or financial information there.
Find What Resonates with that Probable Victim!

- Quick walk through a social engineering response
- “India loan”
- Huge losses through the years
- Family attempts to help
Getting a New Wife...From Ghana?

Romance Scams Surging for all Ages
SHE MET HIM ONLINE...

HE SAID HE LIVED IN A GATED COMMUNITY
Handy Sites to Know

- www.krebsonsecurity.com
- www.fraud.org/scams/internet-fraud
- www.scambusters.org
- http://www.verizonenterprise.com/DBIR/
Examples of Tools Offered

On OBA.com, backlink available by request from elaine@oba.com
23 minute video by OBA and OK APS to train bankers on senior fraud and responses.

OK Securities Info at www.invested.org
Seniors Tab
Investor Protection Kit
My Money Handbook
EIFFE Info (Including Clinician’s Pocket Guide)

Federal Trade Commission
www.ftc.gov
Saveandinvest.org

All available at:
http://promotions.usa.gov/cfpbpubs.html
Questions???

• Contact Info:

• Elaine Dodd
  • Oklahoma Bankers Association
  • 405.424.5252
  • elaine@oba.com