SOCIAL ENGINEERING: HOW STRONG IS YOUR "HUMAN FIREWALL"?

PRESENTED BY: BRAD MOODY, CFE, CFI

EVP, OPERATIONS

LOWERS & ASSOCIATES

AGENDA

- The threat of social engineering
- Social engineering mediums & methods
- The weak link – Human Nature
- What bankers should be doing now
- Seniors
  -Understanding what is occurring
- Seniors
  -Education events- CRA
- Business Email Compromise (BEC)
- Sources of additional information/tools

SOCIAL ENGINEERING METHODS

Mediums/Methods of attack include:

Telephone	Email	Internet	Social Media	Mobile Devices	Dumpster Diving	Malware
impersonation, pretexting	phishing, spearphishing, pharming	fake websites	FaceBook	SMSishing, Bluesnarfing	low tech, but very effective	jump/flash drive baiting

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?

WHAT AN ORGANIZATION SHOULD BE DOING NOW

#1 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

WHAT AN ORGANIZATION SHOULD BE DOING NOW

#2 Monitor and test employee adherence to those security policy guidelines.

- For both new and existing employees

- Tests can be administered on-line and be tied to performance/incentive guidelines

- Be sure to provide updates about new social engineering threats as they arise

- Stress employee vigilance at EVERY level!

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?
- "Tone at the top"

|Code| of Ethics

WHAT AN ORGANIZATION SHOULD BE DOING NOW

#3 Require and make use of complex passwords that are updated regularly.

According to Splash Data, the most popular password for 2016 was '123456'

2016 was **123456**

Computers can get infected with key logging malware

Beware of Key Logging

LONGEST PASSWORD EVER

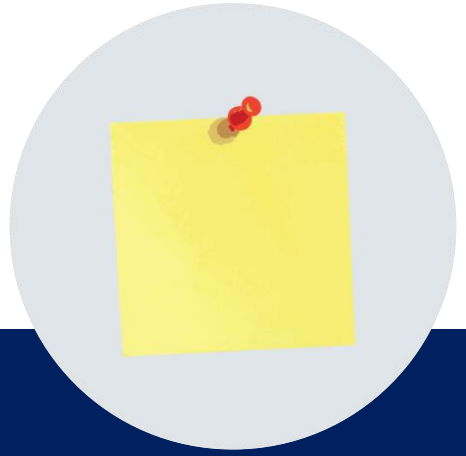
During a recent password audit by a company, it was found that one employee was using the following password:

“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

PASSWORDS AND PASSWORD MANAGERS



Post-Its, Really Now?

Password Safe – Yes – and Free

Dashlane Password Changer – Works

LastPass – Enterprise capable

WHAT AN ORGANIZATION SHOULD BE DOING NOW

#4 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 | Tweets | Posts | On-line Ads | Messages | Attachments

WHAT AN ORGANIZATION SHOULD BE DOING NOW

#5 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

UPSURGE IN CRYPTOLOCKER AND MORPHED VERSIONS:

Continuing Reminder of Importance of Backups

WHAT AN ORGANIZATION SHOULD BE DOING NOW

#6 Education

Partners

- Retailers, social engineering, cyber issues
- Networking with law enforcement and fed partners

Customers

- All with emphasis on seniors

Staff

- On SE outcomes
  - Including money mules

EFFECTIVE EDUCATION FOR SENIORS MUST HAVES

- Better in groups (in community)
- Someone they trust and who has rapport
- Real, current stories
- Humor to increase retention
- If you feed them, they will come
- Great to include family who are often assisting and even better to educate whole communities

CITIZENS AS MONEY MULES

Money Mules, aka Money Laundering

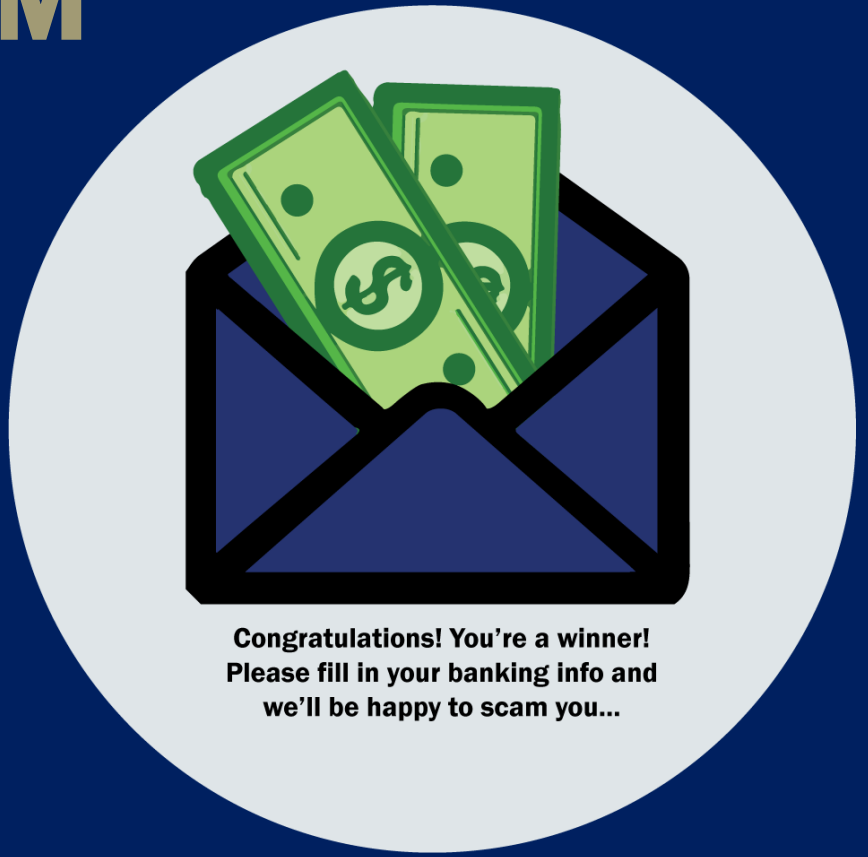
Committing fraud — Can be sued or prosecuted

Fall for it once, will likely fall for it again

Educate consumers, stop the traffic, stop the scams

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, 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 Mexico. 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

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

GETTING A NEW WIFE... FROM RUSSIA?

ROMANCE SCAMS SURGING FOR ALL AGES

FIND WHAT RESONATES WITH THAT CUSTOMER!

- Quick walk through a social engineering response
- “India loan”
- Huge losses through the years
- Family attempts to help

WHAT AN ORGANIZATION SHOULD BE DOING NOW

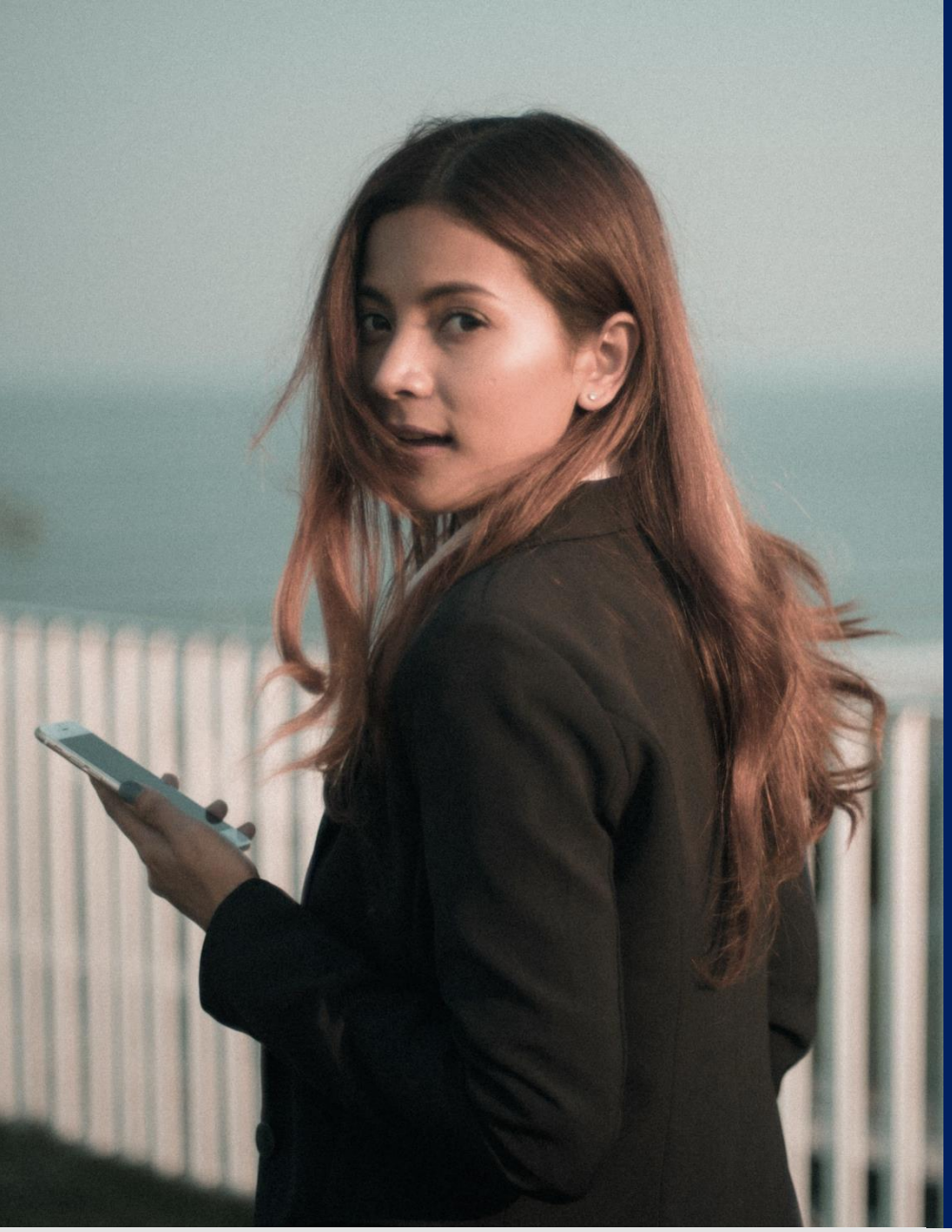
#7 Utilize system management tools to more effectively handle O/S and software updates and patches across multiple user endpoints within your organization. Such a centralized, automated approach allows for:

Scanning of all endpoints for vulnerabilities and unused network services

Detection and analysis of vulnerable apps

Easy updating of components and apps

Restricting access where software updates/fixes are not yet up-to-date



WHAT AN ORGANIZATION SHOULD BE DOING NOW

#8 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.

WHAT AN ORGANIZATION SHOULD BE DOING NOW

#9 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.

WHAT AN ORGANIZATION SHOULD BE DOING NOW

#10 Identify and establish a relationship with a trusted security partner.

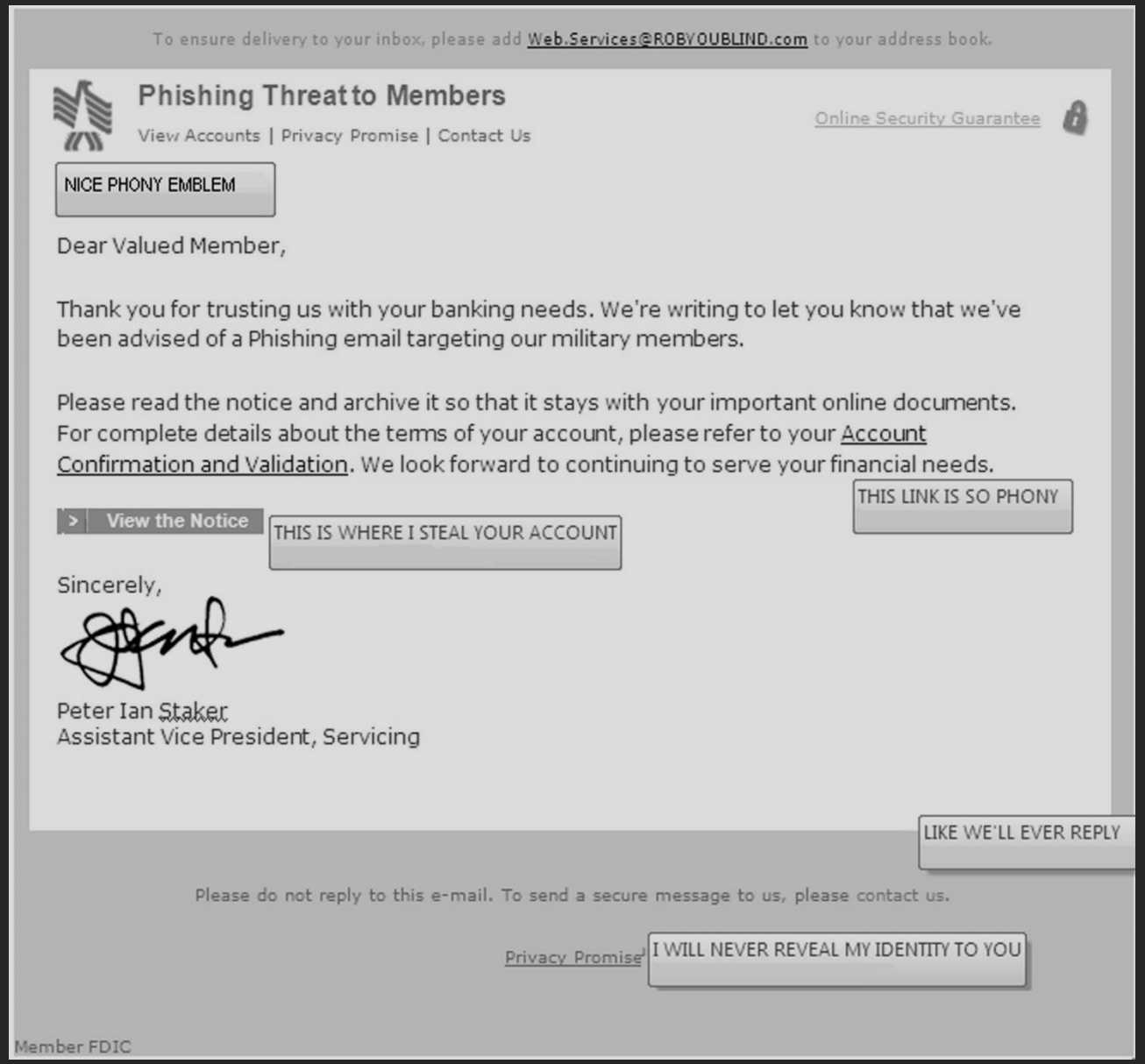
- Look for technical competency as well as people skills to aid in staff training and expanding social engineering fraud risk awareness.

BUSINESS EMAIL COMPROMISE

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

BEC vs. Malware

	MALWARE	BEC
IP Matches Victim	✓	✓
Device Print Matches Victim	✓	✓
Behavioral Match	✗	✓
Ability to Bypass Dual-Custody	✓	✓
Ability to Delay Detection/Recall	✓	✓



A PHISHING SCHEME UNCOVERED

NEXT STEPS TO GET STARTED

0 to 30 Days

- Name your top 2 digital assets
- Practice a Digital Disaster

30 to 90 Days

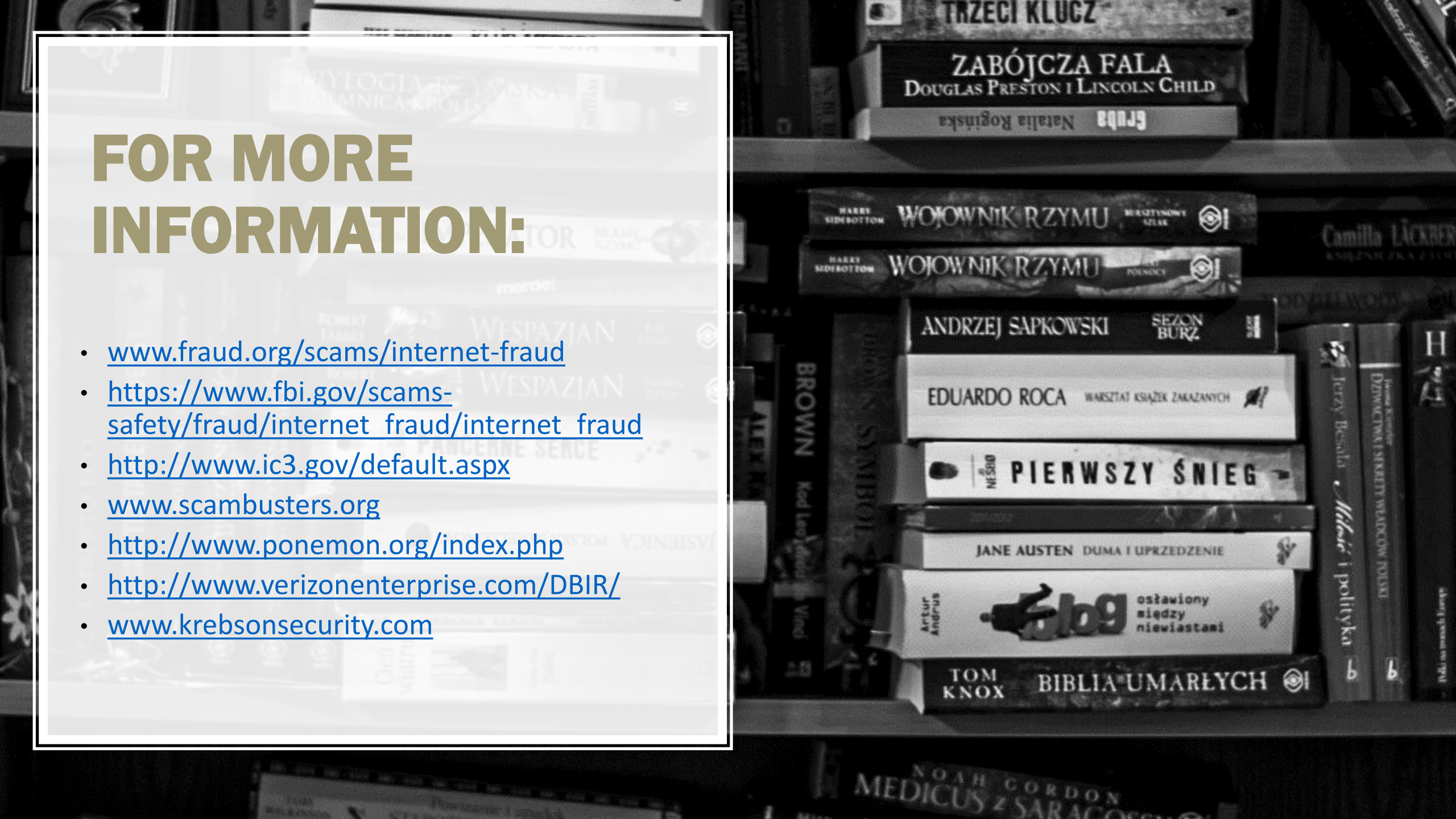
- Update policies and procedures
- Employee & vendor education and awareness programs
- Acceptable use agreements (signed / dated)
- Targeted assessments focused specifically on the top 2 digital assets

90+ Days

- Establish a Cross Functional Fraud & Security Council
- Work with Legal to discuss your data privacy and security standards
- Work with your Insurance company to plan out the coverages you need for cyber liability

FOR MORE INFORMATION:

- www.fraud.org/scams/internet-fraud
- https://www.fbi.gov/scams-safety/fraud/internet_fraud/internet_fraud
- http://www.ic3.gov/default.aspx
- www.scambusters.org
- http://www.ponemon.org/index.php
- http://www.verizonenterprise.com/DBIR/
- www.krebsonsecurity.com




QUESTIONS & WRAP-UP

LOWERS
& ASSOCIATES
International Risk Mitigation Partners

lowersrisk.com

BRAD MOODY, CFE, CFI | EVP, OPERATIONS

125 East Hirst Rd, Suite 3C, Purcellville, VA 20132 | Office: 540.338.7151 | Cell: 704.401.6619 | Fax: 540.338.3131