Cybersecurity “101”

Helping Reduce Your Business Risk

2018 ASBA Technical Meeting & Trade Show

Doug Wenger
President, 18Main Management, LLC
doug.wenger@18mainmgt.com
Me? My Company? Really?

~90% of Small Business Owners don’t feel like they are at risk of experiencing a cyber breach

Manta Poll of 1,420 Small Business Owners

“…every organization has, will have, or is experiencing a cybersecurity incident…”

National/NYSE Cybersecurity Conference Speaker

“…if I had only a dollar to spend on cybersecurity, I’d spend it on employee awareness…”

National/NYSE Cybersecurity Conference Speaker
Cybersecurity In the News

March 30, 2014 02:30 AM |

**Solon packaging company feels hit from a $500,000 wire fraud**

Forbes

Phishing Scams Cost American Businesses Half A Billion Dollars A Year

ASBA TECHNICAL MEETING & TRADE SHOW

NOVEMBER 30 - DECEMBER 4 | SCOTTSDALE, ARIZONA
Multi-faceted Threat

Internal
- Malicious/Mischief
- Social Engineering
- Planned

External
- Phishing
- Virus/Infections
- Hacking
- Random
- Ransomware
- Malware
- Many Others
- Sinister/Fraud/Theft
- External
Selected Basic Risk Areas

Acting on Fraudulent E-mails

Theft/Loss of Laptops, Mobile Devices and Portable Storage

Social Engineering

Compromised Accounts Payable/Vendor Management Procedures

Posting Sensitive Data on Social Media

Poor Password Management

Distractions
Selected Basic Risk Areas

- Acting on Fraudulent E-mails
- Social Engineering
- Posting Sensitive Data on Social Media
- Poor Password Management
- Distractions
- Theft/Loss of Laptops, Mobile Devices and Portable Storage
- Compromised Accounts Payable/Vendor Management Procedures

- Independently Verify Vendor Payment Changes
- Set Payment Level Thresholds
- Set Policies in Writing and Review
Basic Payable/Vendor Mgt Fraud (Fictitious Names)

• Your company buys materials from a supplier named Xintz Pigment Corporation
• Your employee Mark Miward manages your vendor payments and vendor database records, as well as performing many other roles in your company
• Mark is very busy and it’s your busiest season
• Mark receives an e-mail from Xintz informing him of a change in address/bank information for remitting payments
From: Finance Mgr <finance@xiintz.com
Sent: Thursday, October 4, 2018 8:07 AM
To: Miward, Mark
Subject: Change in Address

Dear Customer:

We have changed our remit-to location for receiving customer payments, effective immediately.

Please send payments to:

[New address or Bank/Lockbox #]

Thank YOU.
Basic Payable/Vendor Mgt Fraud

From: Finance Mgr <finance@xiintz.com
Sent: Thursday, October 4, 2018 8:07 AM
To: Miward, Mark
Subject: Change in Address

Dear Customer:

We have changed our remit-to location for receiving customer payments, effective immediately.

Please send payments to:

[New address or Bank/Lockbox #]

Thank YOU.
Basic Payable/Vendor Mgt Fraud

From: Finance Mgr <finance@xiintz.com
Sent: Thursday, October 4, 2018 8:07 AM
To: Miward, Mark
Subject: Change in Address

Dear Customer:

We have changed our remit-to location for receiving customer payments, effective immediately.

Please send payments to:

[New address or Bank/Lockbox #]

Thank YOU.
From: Finance Mgr <finance@xiintz.com>
Sent: Thursday, October 4, 2018 8:07 AM
To: Miward, Mark
Subject: Change in Address

Dear Customer:

We have changed our remit-to location for receiving customer payments, effective immediately.

Please send payments to:

[New address or Bank/Lockbox #]

Thank YOU.
Basic Payable/Vendor Mgt Fraud

From: Finance Mgr <finance@xiintz.com>
Sent: Thursday, October 4, 2018 8:07 AM
To: Miward, Mark
Subject: Change in Address

Dear Customer:

We have changed our remit-to location for receiving customer payments, effective immediately.

Please send payments to:

[New address or Bank/Lockbox #]

Thank YOU.
There’s More to the Story

• Xintz computer system was compromised - Xintz and their customers were unaware
• Hackers acquired customer names, contacts, e-mail addresses and Xintz e-mail information
• Hackers quickly created new “domain” name containing an extra “i” in the name and established a bank account to collect payments
• Hackers formulated e-mail’s to selected Xintz customer(s) with large invoices due soon
Basic Wire Fraud Example (Fictitious Names)

• Company Zbyovz is considering expansion through an acquisition as well as developing additional sources of material supply
• Zbyovz owner and president (Jane Smyther-Reens) is traveling extensively during this time
• Finance manager (Cal Lender) is covering many areas of the company for the owner
• Cal Lender receives an e-mail from Jane requesting a wire transfer be made to complete an important transaction
Basic Wire Fraud Example

From: Jane <jane.smyther-reens@Zbyovzz.com>
Sent: Thursday, October 5, 2018 9:09 AM
To: Lender, Cal
Subject: Wire Transfer

Cal,

I am working on a confidential project and we have a new supplier for a new product lines.

Please wire $50,000 to the following bank account. Code it to admin

[Bank Information]

Reply to me when done

Jane

Anything Suspicious?
Basic Wire Fraud Example

From: Jane <jane.smyther-reens@Zbyovzz.com>
Sent: Thursday, October 5, 2018 9:09 AM
To: Lender, Cal
Subject: Wire Transfer

Cal,

I am working on a confidential project and we have a new supplier for a new product line.

Please wire $50,000 to the following bank account. Code it to admin

[Bank Information]

Reply to me when done

Jane
Basic Wire Fraud Example

From: Jane <jane.smyther-reens@Zbyovzz.com>
Sent: Thursday, October 5, 2018 9:09 AM
To: Lender, Cal
Subject: Wire Transfer

Cal,

I am working on a confidential project and we have a new supplier for a new product lines.

Please wire $50,000 to the following bank account. Code it to admin

[Bank Information]

Reply to me when done

Jane
Basic Wire Fraud Example

From: Jane <jane.smyther-reens@Zbyovzz.com>
Sent: Thursday, October 5, 2018 9:09 AM
To: Lender, Cal
Subject: Wire Transfer

Cal,

I am working on a confidential project and we have a new supplier for a new product lines.

Please wire $50,000 to the following bank account. Code it to admin

[Bank Information]

Reply to me when done

Jane
Basic Wire Fraud Example

From: Jane <jane.smyther-reens@Zbyovzz.com>
Sent: Thursday, October 5, 2018 9:09 AM
To: Lender, Cal
Subject: Wire Transfer

Cal,

I am working on a confidential project and we have a new supplier for a new product lines. Please wire $50,000 to the following bank account. Code it to admin.

[Bank Information]

Reply to me when done.

Jane
There’s More to the Story

• Cyber theft perpetrators have harvested millions of e-mail addresses from various data breaches of companies and organizations
• Bank accounts are established – often outside of the U.S. – often with stolen identity information
• Scores of e-mail’s are sent automatically through compromised computers around the world
• E-mail address spoofing is established to redirect replies to a special account
• Several companies fall for the trap and wire the money
• The perpetrators collect the money, close the account and are gone
Passwords, Passwords, Passwords

Social Media

Loyalty Programs

Travel

Personal Finance

Many Others

- Common Passwords
- Sharing Passwords with Others
- Simple to Guess or Easily Socially Engineered Passwords
Passwords, Passwords, Passwords

Known to You – Not Others
Hard to Guess or Socially Engineer
Avoid Family/Personal Info (BDay, Children’s Names, ...)
Upper, Lower, Numbers, Spec Characters
Rotate
Substitutions
Passwords, Passwords, Passwords

Known to You – Not Others
Hard to Guess or Socially Engineer
Avoid Family/Personal Info (BDay, Children’s Names, ...)
Upper, Lower, Numbers, Spec Characters
Rotate
Substitutions

iLuvA5Ba!
L3t1tSn0w*
Snapshot of Other Areas

• It’s 11:00 PM, do you know where your laptop is?
  • 1-in-10 chance of your laptop being stolen

• Would you pick up a needle from the street and stick it in your arm?
  • Scan drives for virus threats and/or use secure flash drive technology

• “…hello, I’m calling from [software company]...we have to update your software license key...please log in to the link I am sending you…”
  • DO NOT DO IT!!!! EVER!!!!
Five Things to Consider When You Return Home

Create Awareness / Train Employees – Newsletter; Access to Free Resources; Develop Policies; Conduct Assessment

Change Passwords / Implement Strong Passwords; Change WiFi Password Regularly

Backup Important Data; Maintain an Offsite Copy; Test a Recovery; Encrypt Backups if Possible

Limit System Access Based on Role; Remove PC Administrator Access

Keep Computer Software Updated; Turn on Auto Updates for All SW & OS; Maintain Antivirus SW
Summary

• Many data breaches occur due to human actions
• Basic awareness is a good first step
• Be vigilant – threats continue to evolve and increase in sophistication over time
• When in doubt, ask a colleague
• Cybersecurity vigilance never ends
• Some resources to consider:
  • https://www.sans.org/security-awareness-training/ouch-newsletter
  • https://www.sans.org/security-awareness-training/ouch-newsletter/2017/passphrases
Cybersecurity “101”
Helping Reduce Your Business Risk

2018 ASBA Technical Meeting & Trade Show

Doug Wenger
President, 18Main Management, LLC
doug.wenger@18mainmgt.com