

SECURING THE WEAKEST LINK



Protect Your Company—and Yourself—From
Cyber Fraud

Jon Stockton – Director of Fraud, Umpqua Bank

Agenda

- Current Fraud Trends
 - Pause – Validate or Authenticate
 - Identifying Compromised Email Accounts
 - Business Email Compromise Timeline
 - Actions to Take
 - Preparedness
 - Security Awareness
-

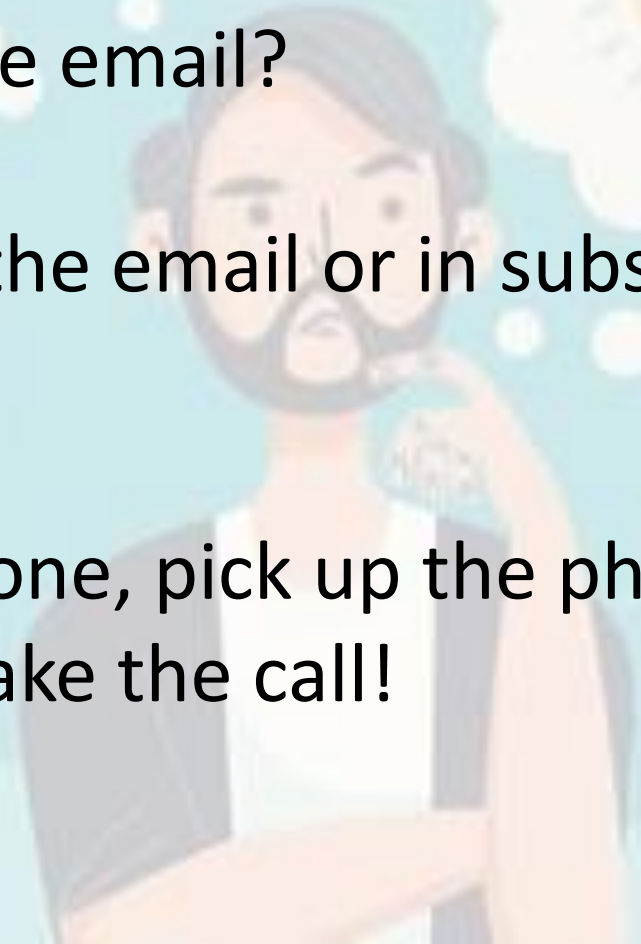
Current Fraud Risks

- **Business Email Compromise (BEC) = Receiving a spoofed or compromised email pertaining to a payment of some sort (invoice, accounts payable, etc), with payment instructions to the fraudsters account**
 - in 2020, there were 19,369 BEC crimes reported vs 2,474 ransomware attacks, \$1.8B in BEC losses and \$29.1MM ransomware
 - Consider multi-factor processes to validate requestor, i.e. phone call to requestor to go over details of payment instructions, establish codes with vendors to be confirmed verbally
- **Payroll / Direct Deposit fraud = Receiving spoofed or compromised email requesting a change in direct deposit account for employees**
 - Consider phone call to requestor to go over details
- **W-2 Tax Fraud = Receiving spoofed or compromised email requesting W-2 information (files for entity or individual data)**
- **General Check Fraud = counterfeit checks, forgeries, alterations, etc**
 - Consider utilizing your bank's 'positive pay' feature and the like for ACH transactions, allowing you to review variations from your check register
 - Review your accounts timely (daily preferred) for anomalous behavior; report timely to bank
 - Watch for insider threat, embezzlement

No Silver Bullet

Impersonation

- Who is behind the keyboard of an email or phone receiver?
- Were you expecting the email?
- Too good to be true?
- Are there links within the email or in subsequent emails?
- Tactics used.....
- Stay out of the fraud zone, pick up the phone!
Don't drop the ball, make the call!



Reconnaissance

Email Account Compromise

- WHO they communicate with
- HOW they communicate
- KEYWORDS used
- Create rules in compromised email account
- Create a spoofed email account



Reconnaissance and Action

- Seek to establish credibility
- Sense of urgency, ask for confirmation
- Grammatical errors in emails, including punctuation.
 - Tend to use term “kindly”

Bob,

Has invoice been processed for payment? Let me know if you need anything from me.

Bob,

We would like the payment to be paid into my bank account by ACH

Account Name : Company XYZ

Bank Name : Bank XYZ

Routing Number : 000000034

Account Number : 123456789

Good morning,

What the status of the payment?

Hello Bob,


We requester for ACH not check

I missed your call yesterday. I tried calling back this morning but I can't seem to reach out to you. Can you kindly email or call me back.



Who Are You Responding To?


- Take the time to read the email address(es) contained in the email



 Fred.Flintstone@BedrockBrewingCompany
Loan Account
Retention Policy Default Retention (5 years)

- Hover over the email to read actual email address


 Fred.Flintstone@BedrockBrewingCompany 
Loan Account
Retention Policy Default Retention (5 years)

 H3c43w2h5dwwkavu@att-mail.com
Presence Unknown – External Network

Who Are You Responding To?

- If you reply to the email, or when hovering over the email address, take note if the email address is spelled correctly.





Fred.Flintstone@BedrockBrewingCompany

Loan Account

[Retention Policy](#) [Default Retention \(5 years\)](#)

Send	To...	<input type="checkbox"/> Fred.Flintsone@BedrockBerwingCompany
	Cc...	
	Bcc...	

- Consider FWD email instead of REPLY - or -
- Type the known email address

Step 1: Identifying a Target



Organized crime groups target businesses in the U.S. and abroad by exporting information available online to develop a profile on the company and its executives.

Step 2: Grooming



Spearphishing emails and/or phone calls target a victim company's officials (typically in the financial department).

Perpetrators use persuasion and pressure to manipulate and exploit employees' human nature.

Grooming may occur over a few days or weeks.

Step 3: Exchange of Information



The victim is convinced they are conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

Step 4: Wire Transfer



Upon transfers, the funds are steered to a bank account control by the organized crime group.

Business Email Compromise Timeline

Outline of how the business email compromise is executed by some organized crime groups

Step 1: Identifying a Target



Organized crime groups target businesses in the U.S. and abroad by exporting information available online to develop a profile on the company and its executives.

Step 2: Grooming



Spearphishing emails and/or phone calls target a victim company's officials (typically in the financial department).

Perpetrators use persuasion and pressure to manipulate and exploit employees' human nature.

Grooming may occur over a few days or weeks.

Step 3: Exchange of Information



The victim is convinced they are conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

Step 4: Wire Transfer



Upon transfers, the funds are steered to a bank account control by the organized crime group.

Business Email Compromise Timeline

Outline of how the business email compromise is executed by some organized crime groups

Step 1: Identifying a Target



Organized crime groups target businesses in the U.S. and abroad by exporting information available online to develop a profile on the company and its executives.

Step 2: Grooming



Spearphishing emails and/or phone calls target a victim company's officials (typically in the financial department).

Perpetrators use persuasion and pressure to manipulate and exploit employees' human nature.

Grooming may occur over a few days or weeks.

Step 3: Exchange of Information



The victim is convinced they are conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

Step 4: Wire Transfer



Upon transfers, the funds are steered to a bank account control by the organized crime group.

Business Email Compromise Timeline

Outline of how the business email compromise is executed by some organized crime groups

Step 1: Identifying a Target



Organized crime groups target businesses in the U.S. and abroad by exporting information available online to develop a profile on the company and its executives.

Step 2: Grooming



Spearphishing emails and/or phone calls target a victim company's officials (typically in the financial department).

Perpetrators use persuasion and pressure to manipulate and exploit employees' human nature.

Grooming may occur over a few days or weeks.

Step 3: Exchange of Information



The victim is convinced they are conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

Step 4: Wire Transfer



Upon transfers, the funds are steered to a bank account control by the organized crime group.*



*Note: Perpetrators may continue to groom the victims into transferring more funds.

Business Email Compromise Timeline

An outline of how the business email compromise is executed by some organized crime groups

#BECareful

- Slow Down
 - i. Is this an irregular email or request?
 - ii. Is the language in the email consistent with previous communications.
 - iii. When responding, consider forwarding and typing the known email for the sender.
 - Authenticate
 - i. Confirm the request by calling the sender at a known phone number on record.
 - ii. Confirm the account information verbally.
 - iii. Consider adopting dual authorization processes to create and send a transaction.
 - Educate
 - i. Maintain a security and compliance culture.
 - ii. Share the risks and encourage collaboration.
 - Action
 - i. If fraud is determined, contact your bank immediately.
 - ii. Notify law enforcement agencies and review insurance policies.
-

Actions to Take

- **Online Banking**
 - Visibility and reconciliation
 - User entitlements
 - Review user activity – audits
 - Dual control
 - Strong passwords
 - Meaningful limits
 - Appropriate access
- **Protections from fraud w/ Online Banking Services**
 - **Positive Pay**
 - Helps reduce loss!!!!
 - Consider for ‘high volume’ check issuers
 - Payee positive pay
 - **ACH Positive Pay**
 - Helps AVOID loss!!!

What to Expect When You're NOT Expecting

Beyond cyber and fraud concerns, organizations should prepare for a range of disruptions. Before a disaster—

- Know your hazards and what makes you uniquely vulnerable
- Be clear on your core business and take the time to document how you do what you do
- Cross-train all functions, check for single-points of failure
- Talk about emergencies with your team, make sure everyone knows what to do and what to expect
- Get your succession planning done—who's in charge?
- Have your house in order—ethics, fraud control keeps you off the front page, good record keeping makes response and recovery possible
- Talk to your insurance company

Current Cyber Threats

- *Supply Chain Attacks*
 - Historically, supply chain attacks have referred to attacks against trusted relationships, in which an unsecure supplier in a chain is attacked in order to gain access to their larger trading partners.
- *Ransomware*
 - a type of malware that denies access to the target victims data. Advanced ransomware uses cryptoviral extortion (data kidnapping), encrypting the victims data so that it is impossible to decrypt without the decryption key.

Security Awareness

- Network monitoring
- Install anti-virus software – consistently update
- Consider email banner message for external emails
- Strong passwords – consider password safes
 - Require changing of passwords, length and complexity
- Ongoing training on current trends
- Test, measure, retest employees
- Create a culture where employees are comfortable validating requests and escalating security concerns

	EMAIL	TEXT	INCOMING PHONE CALL*
YOUR ACCOUNT NUMBER	NOPE	NAY	AS IF
USERNAME OR PASSWORD	NADA	PASS	NAH
YOUR SSN	NEVER	EW	DONT
YOUR PIN	UH-UH	REALLY?	NO WAY
YOUR BIRTHDAY	NO WAY	NAH	NOOO
YOUR ADDRESS	YIKES	NOPE	NAY
SHARE A ONE-TIME CODE	NO NO	NOT NOW	PASS
TO FILL OUT A FORM	DON'T	NEVER	NOPE
DOWNLOAD AN ATTACHMENT	NOOO	HOPE NOT	NO NO
REVEAL A SECURITY QUESTION ANSWER	PASS	NO	NEVER

Questions?

Jon Stockton
SVP, Director of Fraud
Financial Investigations Department
jonstockton@umpquabank.com
M 503-899-8790

