

ASAP WEBINAR

FRAUD & CYBERCRIME

Is your business/employee the next target?

May 5, 2022

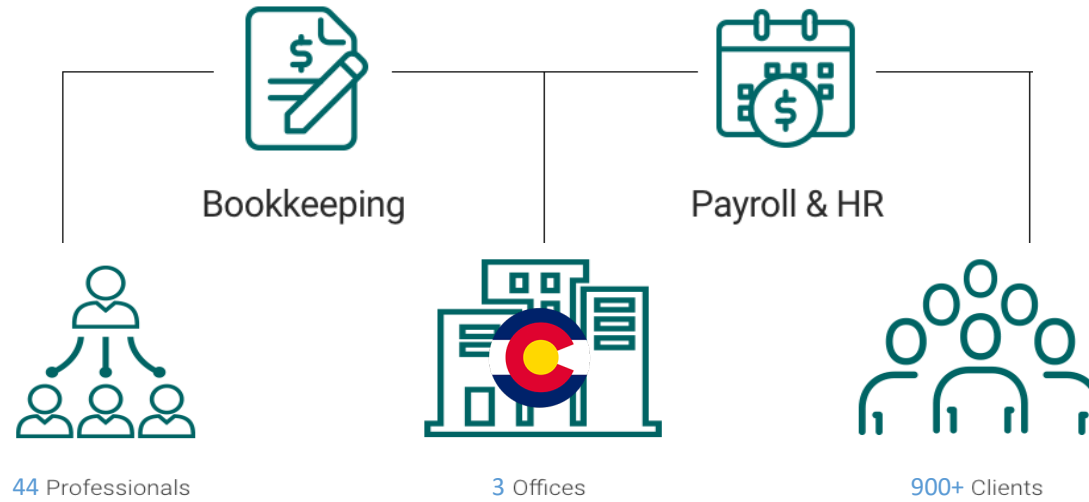


Ralph Gagliardi, Agent in Charge

Colorado Bureau of Investigation, High Tech Crimes Unit



ASAP
ACCOUNTING & PAYROLL



REAL PEOPLE. REAL CONNECTIONS.



What We'll Cover Today



Diana Murray, CEO
ASAP Accounting & Payroll

- 1. Cybersecurity threats to small businesses:
Ransomware, business ID theft, payroll diversion / wire fraud**
- 2. Cybercrime tactics:
Social engineering, identity theft, phishing/spear-phishing,
spoofing**
- 3. Cybersecurity policy & training guidance:
How to identify fraudulent requests and lock-down sensitive info**
- 4. What to do if your organization is the victim of a cybercrime**
- 5. Q&A**

The Fine Print

This information is provided as a self-help tool and does not constitute as legal advice. Decisions as to whether or how to use this information and/or what actions to take are solely those of the employer. The providers of this information disclaim any and all responsibility and liability for its accuracy, completeness or fitness for your particular business purposes.

Meet Our Presenter



Ralph A. Gagliardi

Agent in Charge, Colorado Bureau of Investigation
High Tech Crimes Unit

Ralph Gagliardi is a Certified Fraud Examiner (CFE) who oversees the CBI High Tech Crimes Unit that investigates fraud and identity theft, and other crimes committed via technology. Ralph and his team also conduct cybercrime & identity theft education focusing on best practices, prevention and awareness. As a subject matter expert in complex fraud and organized crime investigations, Ralph also assists in development of policy and legislative efforts pertaining to identity theft, fraud and cybercrime.





COLORADO
Bureau of Investigation
Department of Public Safety

Ralph Gagliardi

High Tech Crimes Unit

Schemes Affecting You



Business - Email Compromise Identity Theft Ransomware



What

CYBER?



Methods / Schemes

Phishing
Ransomware
Malware
Romance Scams
Work From Home



Business Identity Theft
Business Email Compromise
Payroll Diversion
Vender Impersonation
W2 / PII Fraud



Tactics

- Social Engineering
- Open Source Research About YOU
- Identity Theft - Past Breaches (Repetitive Passwords?)
- Phishing / Spear Phishing - **92% of *EVERY* Breach**



What's Changed?



What's Changed?



Social Media – What We Share





How Is Your Business Vulnerable



Phishing Kits For Sale

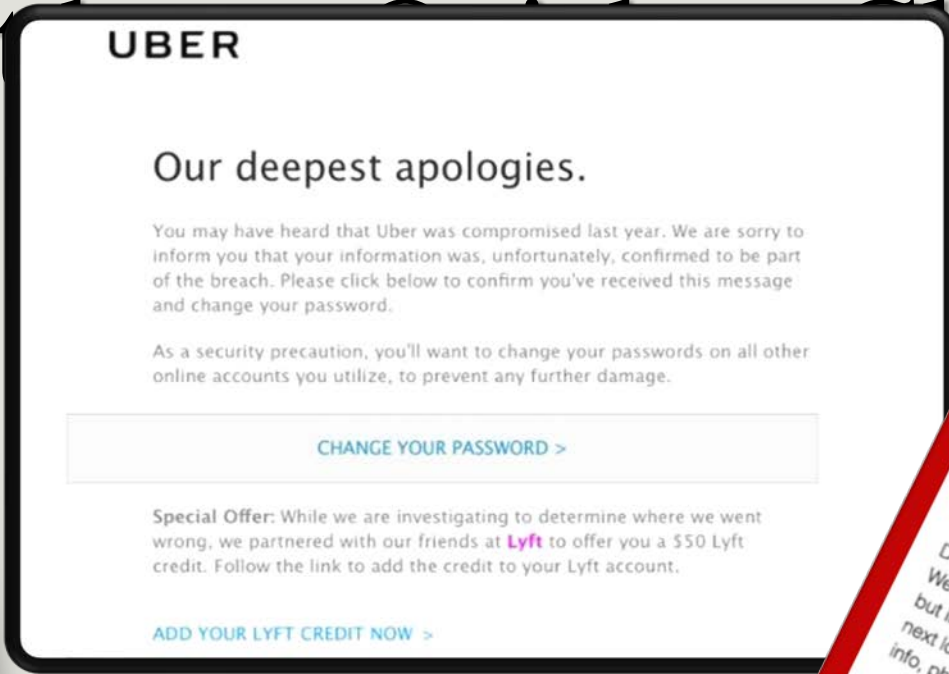
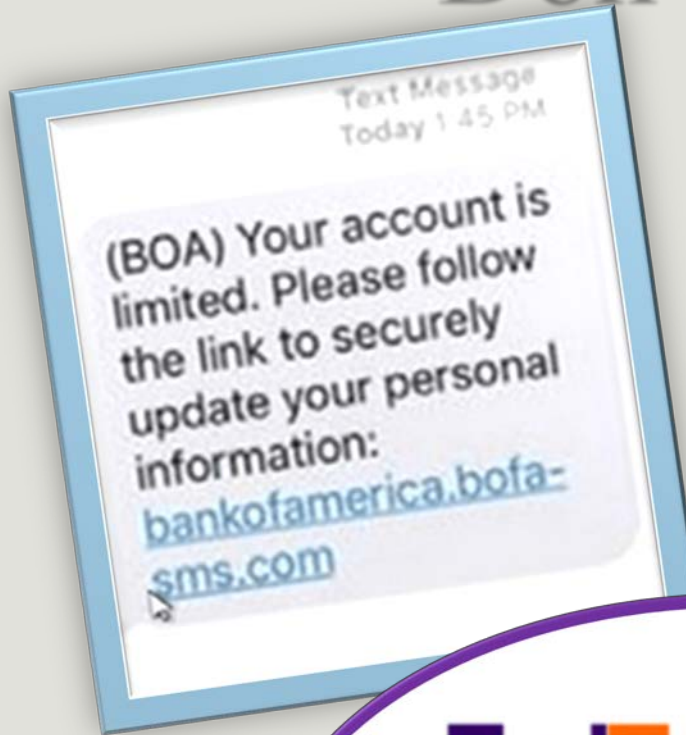
**Over 1,300 Phishing
Kits For Sale on
Hacker Forum:**

News Article 7.11.20

Kits are widely
available – Price?
\$25.00 Each!



Don't click!



Ransomware



Ransomware - Malware



Ransomware & Business Email Compromise

By Victim Loss			
Crime Type	Loss	Crime Type	Loss
BEC/EAC	\$1,866,642,107	Overpayment	\$51,039,922
Confidence Fraud/Romance	\$600,249,821	Ransomware	**\$29,157,405
Investment	\$336,469,000	Health Care Related	\$29,042,515
Non-Payment/Non-Delivery	\$265,011,249	Civil Matter	\$24,915,958
Identity Theft	\$219,484,699	Misrepresentation	\$19,707,242
Spoofing	\$216,513,728	Malware/Scareware/Virus	\$6,904,054
Real Estate/Rental	\$213,196,082	Harassment/Threats Violence	\$6,547,449
Personal Data Breach	\$194,473,055	IPR/Copyright/Counterfeit	\$5,910,617
Tech Support	\$146,477,709	Charity	\$4,428,766
Credit Card Fraud	\$129,820,792	Gambling	\$3,961,508
Corporate Data Breach	\$128,916,648	Re-shipping	\$3,095,265
Government Impersonation	\$109,938,030	Crimes Against Children	\$660,044
Other	\$101,523,082	Denial of Service/TDos	\$512,127
Advanced Fee	\$83,215,405	Hactivist	\$50
Extortion	\$70,935,939	Terrorism	\$0
Employment	\$62,314,015		
Lottery/Sweepstakes/Inheritance	\$61,111,319		
Phishing/Vishing/Smishing/Pharming	\$54,241,075		

According to the FBI - IC3.gov



Ransomware

Locked up data and/or Exfiltration of data
Be prepared - Have a plan

- Who to call
- Backups
- Policy
- Practice

Pay or not to Pay – What will you do?



Ransomware

Stolen Data

Extort Customers

Leaking to Dark Web

Smaller percentage merely ask for Ransom



Business Identity Theft



Business Identity Theft

What's in a Name?



Business Identity Theft

Business Names Have

- Legitimacy
- Credit
- Layer or Hide (identity)



Business Identity Theft

Impacts

- Small Businesses
- Credit
- Fraudulent Websites
- Customers
- Expense of correcting
- Reputation damage (real or perceived)



Business Identity Theft

FINANCIAL GAIN

- Secure lines of credit or loans
- Acquire items which are easily sold for cash
- Sell your compromised business to a third-party
- PPP Fraud
- Import Fraud – Counterfeit Items



Business Identity Theft

FINANCIAL GAIN – Recent Example

33 Colorado Biz's - \$2.3m PPP Fraud

(August 26, 2021 9news)





Colorado
Secretary of State
Jena Griswold

For this Record...
[Filing history and documents](#)
[File a form](#)
[Subscribe to email notification](#)
[Unsubscribe from email notification](#)

[Business Home](#)
[Business Information](#)
[Business Search](#)

[FAQs, Glossary and information](#)

CL

#

1

Summary

Details			
Trade name	Acme Widgets		
Registrant name	Thomas David Traynor		
Status	Expired	Formation Date	04/02/2008
ID number	20081181551	Form	Individual
Renewal month	February	Expiration Date	05/01/2012
Primary residence or usual place of business street address	810 Lincoln Ave, Ste 200, Steamboat Springs, CO 80477, United States		
Primary residence or usual place of business mailing address	Box 771041, Steamboat Springs, CO 80477, United States		

[Filing history and documents](#)

[Get certified copies of documents](#)

[File a form](#)

[Set up secure business filing](#)

[Subscribe to email notification](#)

[Unsubscribe from email notification](#)

[Expiration Date](#)

04/02/2008

Business Identity Theft

Colorado Stats

From CBI's Investigative Reports

Annual Cases of Business Identity Theft in Colorado	
2010	226
2011	162
2012	72
2013	159
2014	115
2015	23
2016	240
2017	221
2018	2551
2019	153
2020	3864
2021	9736
Total	17522



Business Email Compromise



Business Email Compromise

- **Change Bank Account Information**
- **All Types and Sizes of Businesses Affected**
 - Public & Private**
 - Anyone who wires or transfers funds**
 - Access To PII / W-2's or other documents**
 - Payroll**
 - Invoices**
 - Vendors**



Email Spoof

Suspect Spoofs Email

- Display Name
- Replace – Substitute – Transpose Characters

Examples

- John_Doe vs John Doe (Use of underscore)
- An 'M' in the email name becomes a 'r' 'n' = 'rn'
- Lower case L 'l' with the number '1' = l or 1
- Change '.com' with '.net' or other suffix



EMAIL SPOOF

Can You Tell?

Client@aol.com

Huckelberrylaw@outlook.com

JOHN.SMITH.LAW@gmail.com

Client@aol.com

Huckelberry1aw@outlook.com

JOHN.SMITH.LAW@gmail.com



EMAIL SPOOF

Can You Tell?

Client@aol.com

Huckelberrylaw@outlook.com

JOHN.SMITH.LAW@gmail.com

Client@aol.com

Huckelberry1law@outlook.com

JOHN.SMITH.LAW@gmail.com

LI li 00 1I



Hover Over 'From' Name

From: Jim@lotsparking.com

Date: January 24, 2018 at 3:08:25 PM EST

To: John Smith

Subject: Re: Parking Meters

Display name is:

"Jim@lotsparking.com" or "Jim"

Email is actually:

"HackYouAllDay@gmail.com" - Bad



Vendor Fraud – Change Bank Details

***BANK / BUSINESS or LETTER HEAD
CUT AND PASTED to MAKE LOOK
LEGIT***

Company INC of INC
LLC
1234 Main St
Where Ever, CO 88888

Jan 10 2020

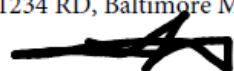
To whom it may concern

Please take this letter as confirmation that the below mentioned account is open with BANK of BANKS. All information is verified below

Bank Name: Bank of Banks
Account Name: YOUR Vendors / Customer NAME
Account No : 12345678
Rounting No : 012345678
Bank Address : 6504 Main St - LEGIT ADDRESS

Kind Regards

Mickey SMITH
Client Service Officer
1234 RD, Baltimore MD 21215



The CBI's Statistics - BEC

BUSINESS EMAIL COMPROMISE					
YEAR	Reported	ATTEMPT	SENT	RECOVERED	Recovery Percentage
2016	22	\$430,773	\$618,578	\$405,504	65.55%
2017	33	\$2,458,790	\$4,291,988	\$4,215,875	98.23%
2018	57	\$3,492,338	\$4,898,527	\$4,108,318	83.87%
2019	100	\$12,958,192	\$6,355,972	\$5,250,044	82.60%
2020	100	\$9,426,658	\$9,220,408	\$7,428,875	80.57%
2021	94	\$10,155,805	\$10,865,121	\$6,624,869	60.97%
Total	406	\$38,922,556	\$36,250,594	\$28,033,485	77.33%



BEC - Take Quick Action For Return of Funds!

Victim of a BEC - *Don't become a victim in the first place!*

Have Plan? (**Policy - Training**)

Who do you contact?

Where do you send information?

Relationships with?

Bank

Law Enforcement

Others



BEC - Take Quick Action For Return of Funds!

BEC Victim Should Gather & Be Ready to Provide:

- *E-mail* requesting funds - with *wiring instructions*
- E-mail *headers and IP's* (Request they get assistance from their I.T. or other trusted expert)
- *Contact your bank – Start the RECALL*

RULES?

Report to Local Authority

FBI website is: www.ic3.gov

FTC website is: www.ftc.gov



BEC - Take Quick Action For Return of Funds!

Contact the CBI through *one* of the following methods:

Email the Wire Fraud Response Team:

- **Reportwirefraud@state.co.us**

Report online:

- **www.Reportwirefraud.com**



PREVENTION

Training and Policy/Procedures

Careful Clicking

Who Initiated - Email or Faxed or Called

Verify!!!! – Phone CALL – *last best number of record*

Email: Forward vs Reply

Email: Grammar – Odd Times - Urgency



PREVENTION

Passwords – Strong / Complex

2FA

Virus Protection - Computer & Cell

No Public Wi-Fi

Insurance?

Training and Policy/Procedures!!!



QUESTIONS?



Ralph Gagliardi, CFE
Agent in Charge
Identity Theft Unit
303-239-4287
Ralph.Gagliardi@state.co.us

Thank you!



COLORADO
Bureau of Investigation
Department of Public Safety