



1

---

---

---

---

---


---

---

---


Private Sector vs Government

Eye of the Lion



Two Issues

- Ownership: Government Agency or OIG
- Good or Bad News when you find fraud in a Government Agency?



2

---

---

---

---

---

---

---

---

Red Flags for Internal Fraud

Introduction

There was fraud occurring under your nose and you didn't even see it. Why didn't you see it? or better yet, why didn't you recognize it?

Recent surveys conducted by the Association of Certified Fraud Examiners (ACFE), occupational fraud substantially increases businesses costs.

3

---

---

---

---

---

---

---

---

### Red Flags for Fraud

**What is Fraud?**  
ACFE defines occupational fraud as “the use of one’s occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization’s resources or assets.”

**What is the nature of Fraud or what can be used to describe the nature of Fraud?**

4

---

---

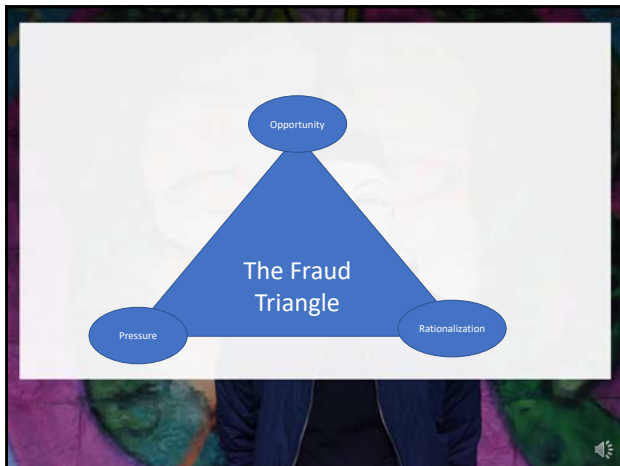
---

---

---

---

---



5

---

---

---

---

---

---

---



### Red Flags for Fraud

Opportunity is an open door for solving a non-shareable problem in secret by violating a trust. Opportunity is generally provided through weaknesses in the internal controls. Some examples include inadequate or no:

- Supervision and review
- Separation of duties
- Management approval
- System controls

The opportunity to commit and conceal the fraud is the only element over which the local government has significant control.

6

---

---

---

---

---

---

---



### Red Flags for Fraud

Rationalization is a crucial component of most frauds because most people need to reconcile their behavior with the commonly accepted notions of decency and trust. Some examples include:

- “I really need this money and I’ll put it back when I get my paycheck”
- “I’d rather have the company on my back than the IRS”
- “I just can’t afford to lose everything – my home, car, everything”

7

---

---

---

---

---

---

---

### Contributing Factors to Fraud

- Poor Internal Controls
- Management override of internal controls
- Collusion between employees
- Collusion between employees and third parties

8

---

---

---

---

---

---

---

### How are fraud Discovered

- 34.2% through tips
- 25.4% by accident
- 20.3% through internal audits
- 20.1% not discovered

9

---

---

---

---

---

---

---

### What is a Red Flag?

- A Red flag is a set of circumstances that are unusual in nature or vary from the normal active
- It is an indication that something is potentially wrong
- Red flags do not indicate guilt or innocence, but are warning signs that there may be an issue.
- Do not ignore red flags – fraud studies have indicated that red flags were always present in cases reviewed, but were either not recognized or were not acted upon when discovered.
- Once a red flag is discovered, it should be acted upon, sometimes its only an error and no fraud has been committed
- Responsibility for follow-up investigation of a red flag should be placed in the hands of a measured and responsible person.

10

---

---

---

---

---

---

---

### Types of Red Flags and Fraud

- General Red Flags. Red flags that are common to most types of fraudulent activity can be categorized as:
- Employee Red Flags.
- Management Red Flags

\*Before we give you examples of employee and management red flags, it is important to understand more about employee and organizational profiles of fraud perpetrators.

11

---

---

---

---

---

---

---

### Types of Red Flags and Fraud

**Fraud Perpetrator Profile :** Pink Collar Crime

- The majority of occupational fraud cases (41.2 percent) are committed by employees. However, the median loss for fraud committed by managers was \$218,000, which is almost three times greater than the loss resulting from an employee scheme. Approximately 61 percent of the fraud cases were committed by men. The median loss resulting from fraud by males was \$250,000, which is more than twice the median loss attributable to women.
- Most fraud perpetrators (87.9 percent) have never been charged or convicted of a crime. This supports previous research which has found that those who commit occupational fraud are not career criminals.
- Nearly 40 percent of all fraud cases are committed by two or more individuals. The median loss in these cases is \$485,000, which is almost five times greater than the median loss in fraud cases involving one person. The median loss attributable to fraud by older employees is greater than that of their younger counterparts. The median loss by employees over the age of 60 was \$713,000. However, for employees 25 or younger, the median loss was \$25,000.

12

---

---

---

---

---

---

---

### Types of Red Flags and Fraud

Blue Collar Crime	White Collar Crime	Pink Collar Crime
<ul style="list-style-type: none"> <li>• Armed Robbery</li> <li>• Sexual Assault</li> <li>• Burglary</li> <li>• Drug Abuse</li> </ul>	<ul style="list-style-type: none"> <li>• Wage Theft</li> <li>• Embezzlement</li> <li>• Copyright Infringement</li> <li>• Identity Theft</li> </ul>	<ul style="list-style-type: none"> <li>• Low level crimes</li> <li>• Check kiting</li> <li>• Bookkeeping</li> <li>• Typically committed by women</li> </ul>

13

---

---

---

---

---

---

---

---

Everyone knows the saying White Collar Criminal (think Bernie Madoff or a young, male hedge fund trader in Showtime's Billions), but when I say Pink Collar Criminal they have a puzzled look. Most people don't realize it but they probably are neighbors, co-workers, friends or acquaintances with either a Pink Collar Criminal or someone who has been embezzled by a Pink Collar Criminal. A Pink Collar Criminal can be a PTA mom, your dentist's office manager, and yes even someone's grandma. The statistics on Pink Collar Criminals are alarming. According to the FBI, male embezzlers have increased only 4% since 1990 while Pink Collar Criminals have increased over 40% during that time period.

The term pink-collar crime was popularized by Dr. Kathleen Daly during the 1980s to describe embezzlement type crimes that typically were committed by females based on limited opportunity. In this context, women were more likely to have committed low level crimes such as check kiting and book-keeping fraud from positions of less power compared to men who had engaged in acts of white-collar crime. Can a man be a pink collar criminal? The simple answer is yes. It's the position not the gender but in these "pink" positions there are just more women than men.

In 2018 the Association of Certified Fraud Examiners Report to the Nations on Occupational Fraud and Abuse found that men were responsible for stealing larger amounts of money (median = \$156,000) compared to women (median = \$89,000). A handful of embezzlement studies, though dated, have focused on female offenders and have confirmed trends that women tend to commit embezzlement at a higher rate, steal less money. Women also invoke different rationalizations for their actions compared to men. The glass ceiling as we know it today represents women making about .81 on the dollar compared to men. However, when they steal they only steal about .43-.50 on the dollar.

### Pink Collar Crime

14

---

---

---

---

---

---

---

---

### Types of Red Flags and Fraud

- **Fraud Organizational Profile :**
  - Most costly abuses occur within organizations with less than 100 employees.
  - Management ignores irregularities.
  - High turnover with low morale.
  - Staff lacks training.

15

---

---

---

---

---

---

---

---

Types of Red Flags and Fraud

• **Employee Red Flags :**

- Employee lifestyle changes: expensive cars, jewelry, homes, clothes
- Significant personal debt and credit problems
- Behavioral changes: these may be an indication of drugs, alcohol, gambling, or just fear of losing the job
- High employee turnover, especially in those areas which are more vulnerable to fraud
- Refusal to take vacation or sick leave
- Lack of segregation of duties in the vulnerable area

16

---

---

---

---

---

---

---

---

Types of Red Flags and Fraud

• **Management Red Flags :**

- Reluctance to provide information to auditors
- Managers engage in frequent disputes with auditors
- Managers display significant disrespect for regulatory bodies
- There is a weak internal control environment
- Accounting personnel are lax or inexperienced in their duties
- Decentralization without adequate monitoring
- Excessive number of checking accounts
- Frequent changes in banking accounts
- Frequent changes in external auditors
- Company assets sold under market value
- Significant downsizing in a healthy market
- Continuous rollover of loans
- Excessive number of year end transactions

17

---

---

---

---

---

---

---

---

Types of Red Flags and Fraud

• **Management Red Flags :**

- High employee turnover rate
- Unexpected overdrafts or declines in cash balances
- Compensation program that is out of proportion
- Any financial transaction that doesn't make sense - either common or business
- Service Contracts result in no product
- Photocopied or missing documents

18

---

---

---

---

---

---

---

---



Types of Red Flags and Fraud

- **Changes in Behavior “Red Flags”**
- The following behavior changes can be “Red Flags” for Embezzlement:
  - Borrowing money from co-workers
  - Creditors or collectors appearing at the workplace
  - Gambling beyond the ability to stand the loss
  - Excessive drinking or other personal habits
  - Easily annoyed at reasonable questioning
  - Providing unreasonable responses to questions
  - Refusing vacations or promotions for fear of detection
  - Bragging about significant new purchases
  - Carrying unusually large sums of money
  - Rewriting records under the guise of neatness in presentation

19

---

---

---

---

---

---

---

---

Types of Red Flags and Fraud

- **Cash/Accounts Receivable “Red Flags”**
- Since cash is the asset most often misappropriated, local government officials and auditors should pay close attention to any of these warning signs.
  - Excessive number of voids, discounts and returns
  - Unauthorized bank accounts
  - Sudden activity in a dormant banking accounts
  - Discrepancies between bank deposits and posting
  - Abnormal number of expense items, supplies, or reimbursement to the employee
  - Presence of employee checks in the petty cash for the employee in charge of petty cash
  - Excessive or unjustified cash transactions
  - Large number of write-offs of accounts
  - Bank accounts that are not reconciled on a timely basis

20

---

---

---

---

---

---

---

---

Types of Red Flags and Fraud

- **Payroll “Red Flags”**
- Red flags that show up in payroll are generally worthy of looking into. Although payroll is usually an automated function, it is a vulnerable area, especially if collusion is involved.
  - Inconsistent overtime hours for a cost center
  - Overtime charged during a slack period
  - Overtime charged for employees who normally would not have overtime wages
  - Budget variations for payroll by cost center
  - Employees with duplicate Social Security numbers, names, and addresses
  - Employees with few or no payroll deductions

21

---

---

---

---

---

---

---

---

### Types of Red Flags and Fraud

- **Purchasing/Inventory "Red Flags"**
  - Lack of physical security over assets/inventory
  - Charges without shipping documents
  - Payments to vendors who aren't on an approved vendor list
  - High volume of purchases from new vendors
  - Purchases that bypass the normal procedures
  - Vendors without physical addresses
  - Vendor addresses matching employee addresses
  - Purchasing agents that pick up vendor payments rather than have it mailed

22

---

---

---

---

---

---

---

---

### Red Flags for External Fraud

- Social Engineering – The Human Hack "Red Flags"
- the psychological manipulation of people into performing actions or divulging confidential information.
  - Trying to get you to bypass security protocol
  - Introducing distracting tactics
  - Playing on your sympathy
  - Displays urgency in getting you to assist
  - Takes control of the conversation

23

---

---

---

---

---

---

---

---

### Red Flags for External Fraud

**Social Engineering**  
Comfort and familiarity are tactics used to lower your guards and siphon information such as your password.

**Vishing**

**Phishing**

**Smishing**

**IoT**

24

---

---

---

---

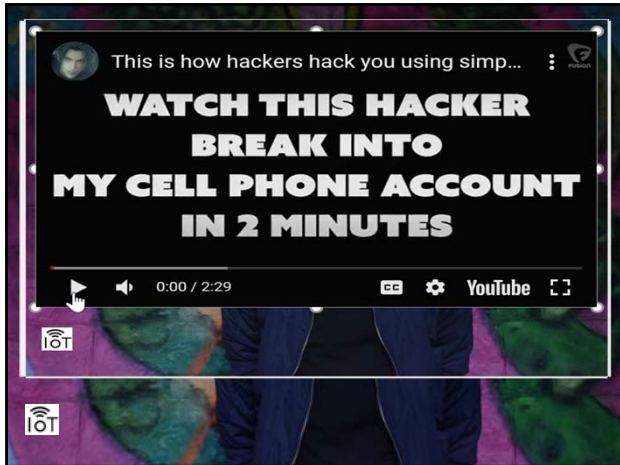
---

---

---

---





25

---

---

---

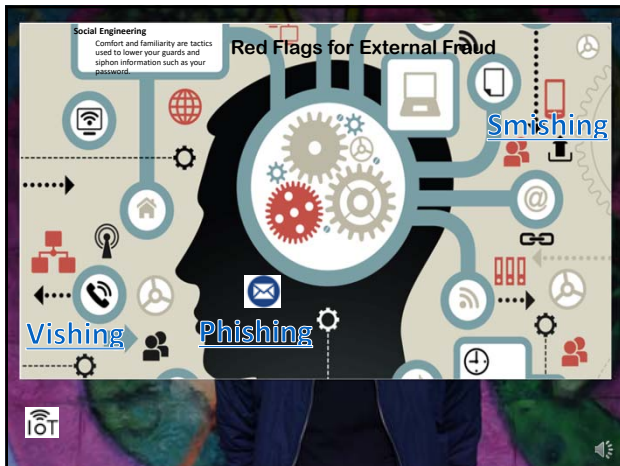
---

---

---

---

---



26

---

---

---

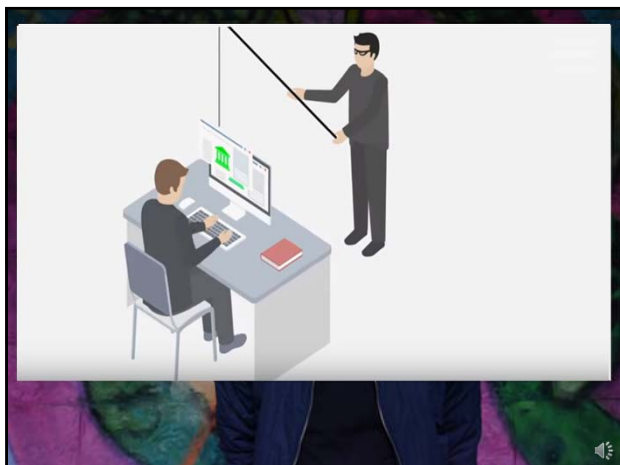
---

---

---

---

---



27

---

---

---

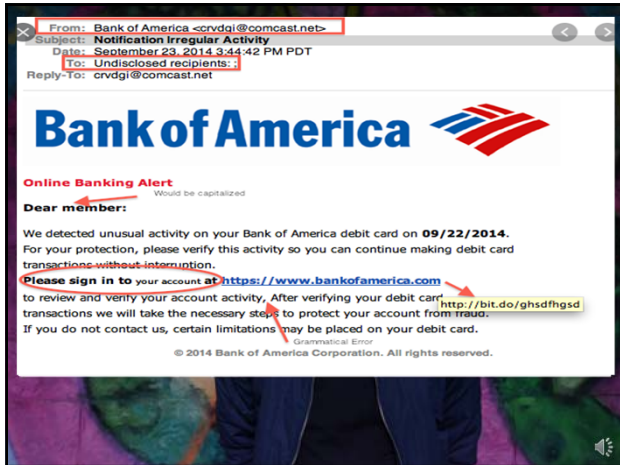
---

---

---

---

---



28

---

---

---

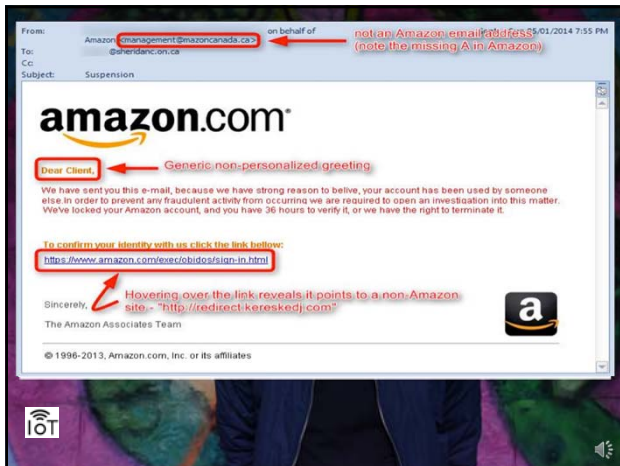
---

---

---

---

---



29

---

---

---

---

---

---

---

---



30

---

---

---

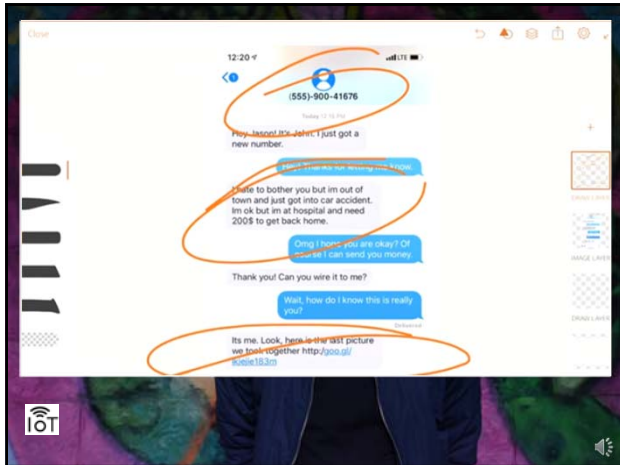
---

---

---

---

---



31

---

---

---

---

---

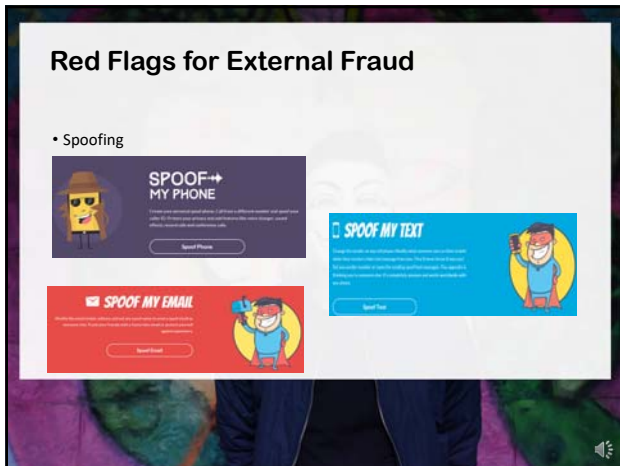
---

---

---

---

---



32

---

---

---

---

---

---

---

---

---

---



33

---

---

---

---

---

---

---

---

---

---

## SPOOFING

How do you view an email header or the "original message"?

- In Gmail, while viewing the email, click the **More** icon (three vertical dots) at the top right and select **"Show original"** from the list.
- In Outlook, open the email, then go to **File > Properties** and look in the **Internet headers**

If the authenticated sender, or "from" address, in the email's properties matches your email address, then your account was compromised. But if the sender's email address in the properties isn't your address, then it may have simply "spoofed" your email while actually sending from a different account.

34

Delivered-To: josh@techlicious.com  
Received: by 2002:a0f:f8b4:9b:0:8:0 with SMTP id u4-v6csp338072burp;  
Wed, 31 Oct 2018 06:57:13 -0700 (PDT)  
X-Google-Smtp-Source: A3d8T5uT0u1yVj4u0fEg80mHwagQTLcck05Zk2z7Izm80Y0MGd2R1X1hyLva47Cjap0d43V  
X-Received: by 2002:a0f:dc87:1 with SMTP id r7-v6m3152022urj.143.1540994233690;  
Wed, 31 Oct 2018 06:57:13 -0700 (PDT)  
ARC-Seal: i=1; a=rsa-sha256; t=1540994233; cv=none;  
d=google.com; s=arc-20160816;  
b=FNPawRfDYt1PcFg3V16Jv9qEhKArBb3+0tNNT61SPtA5ncl6/baGBBp08b754JGOC  
F8B4eT0T03L4eNkAP0C/LuE7a9JhV2B5Z2a0JhVmcC3F3JnFmG3Fcmu0K0Gh  
LWQ1a91/Q351+u0Fr+1a0cePv0G08E3IXMvAF1N0Lc0u37Vp0tFrng00z0rP+tc  
0715Q0Fm3h05u0m:1111111000L1U/L00ZFF02F0u0G0m0PvL1c0F0u0L0L0K0C  
A00uZ/1k4809010q3u71C35Q0H2V0LncF0X0N0Q0u1y0vR0tT2L0vZv0u03AF00re  
v00g+  
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;  
b=Date:Message-Id:Reply-To:Errors-To:Importance:From:Subject:To:  
b0=0u0v0ec2d0Hf+Q0F061C0K0K02g0v0x0dAT31t0gV+;  
b0=V0h0ck0d0L0L1P0S0Sj0u0P0L14+0D1P50D10W1y0C0u0D03j0W0R1A0K+1S0P0U  
uY0Q1L035h0y0u0Q0F2F0u0Z0h0F0u2J51C1fnc0F0R0F0U+mZ0u0W0gT210K0U10Kf/5W  
J180eTh0v/30hJ0a0u0p0v0J0U5H0B7v0u3r0c0S0Hf/0J0u0L1Q0u2u0G0C10r0W0  
I10u0tTP0B10M0J0u0F0u0N0D0V0n0L1f0c/v020hTKJ3/0dV10bT0mZyH30V0B0u0uHtG0  
S0r/010f03h0Q0u01001g0TJ3050Y1V1F0M0N0A0u0v0g0Q0K3YD2F0r1n0gTh3v0X0  
Q0Q0+  
ARC-Authentication-Results: i=1; mx.google.com;  
spf=softfail (google.com: domain of transitioning josh@techlicious.com does not designate  
46.167.245.200 as permitted sender) smtp.mailfrom=josh@techlicious.com;  
dmarc=softfail (p=NONE sp=NONE dis=NONE) header.from=techlicious.com  
Return-Path: <josh@techlicious.com>  
Received: from emkei.cz [emkei.cz. [46.167.245.200]]  
by mx.google.com with ESMTPS id 15-v0s1331606dur.171.2018.10.31.06.57.13  
for <josh@techlicious.com>  
(version=TLS1\_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);  
Wed, 31 Oct 2018 06:57:13 -0700 (PDT)  
Received-SPF: softfail (google.com: domain of transitioning josh@techlicious.com does not designate  
46.167.245.200 as permitted sender) client-ip=46.167.245.200;  
Authentication-Results: mx.google.com;  
spf=softfail (google.com: domain of transitioning josh@techlicious.com does not designate  
46.167.245.200 as permitted sender) smtp.mailfrom=josh@techlicious.com;  
dmarc=softfail (p=NONE sp=NONE dis=NONE) header.from=techlicious.com  
Received: by emkei.cz (Postfix) id 4702E06020; Wed, 31 Oct 2018 14:57:13 +0100 (CET)  
To: josh@techlicious.com  
Subject: This is a spoof email scam test  
From: Josh Scammer <josh@techlicious.com>  
X-Priority: 3 (Normal)  
Importance: Normal

As you can see above, the domain name this email being sent from is [emkei.cz](#) (the email spoofing site), not [techlicious.com](#), so that's a dead giveaway.

35

## Omaha's Scoular Co. loses \$17 million after spearphishing attack

Fraudsters convinced an Omaha company to send \$17.2 million to a bank in China

By Maria Karlov  
Contributing Writer, CSO

FEB 13, 2015 4:20 PM PST

36

### Red Flags for External Fraud

- Password Protection\*
- Comfort and familiarity are tactics used to lower your guards and siphon information such as your password.

1l2Ttf@C&b!t\*

37

---

---

---

---

---

---

---

---

### Red Flags for External Fraud



0:00 / 2:49

38

---

---

---

---

---

---

---

---

Your identity is a steal on the Dark Web. Here are what the most common pieces of information sell for.

Experian.

<b>Social security number</b> \$1	<b>Online payment services login info</b> (e.g. PayPal) \$20-\$200	<b>Credit or debit card</b> (credit cards are more popular) \$5-\$110 With CVV number: \$5, With basic info: \$15, Full card: \$30
<b>Drivers license</b> \$20	<b>Loyalty accounts</b> \$20	<b>General non-financial institution logins</b> \$1
<b>Diplomas</b> \$100-\$400	<b>Passports (US)</b> \$1000-\$2000	<b>Subscription services</b> \$1-\$10
		<b>Medical records</b> \$1-\$1000**

\*Full info is a bundle of information that includes a "full" package for fraudulent use, such as birth date, account numbers and other data that makes them more valuable since they can often do a lot of immediate damage.  
\*\*Depends on how complete they are as well as if it is a single record or an entire database.  
Note: Prices can vary over time and prices listed below are an estimation and aggregation based on reference articles and based on experience of Experian cyber analyst the last two years.

39

---

---

---

---

---

---

---

---





40

---

---

---

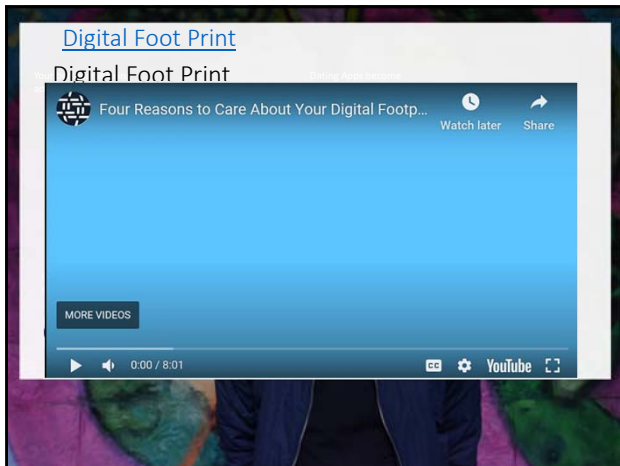
---

---

---

---

---



41

---

---

---

---

---

---

---

---



42

---

---

---

---

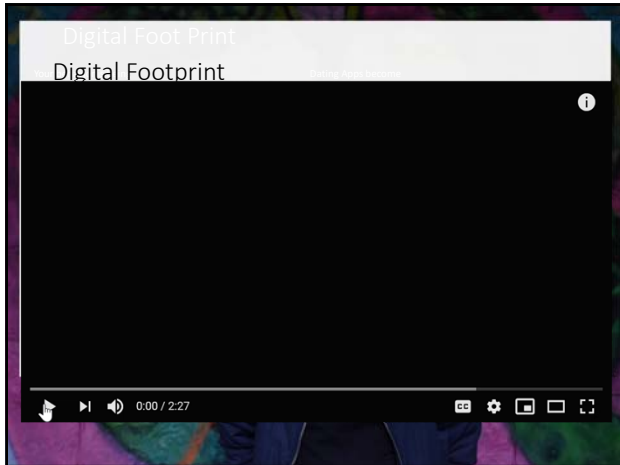
---

---

---

---





43

---

---

---

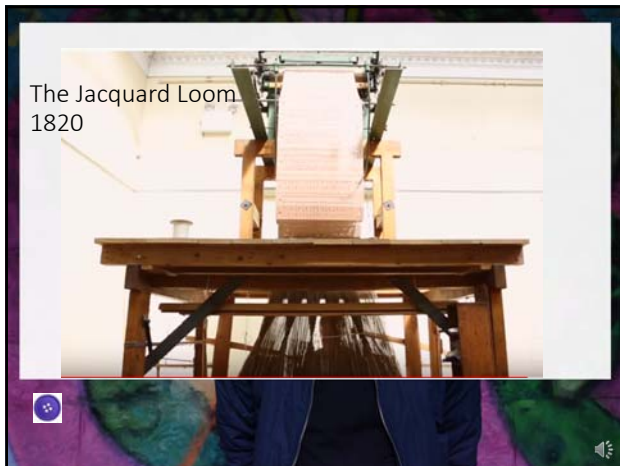
---

---

---

---

---



44

---

---

---

---

---

---

---

---



45

---

---

---

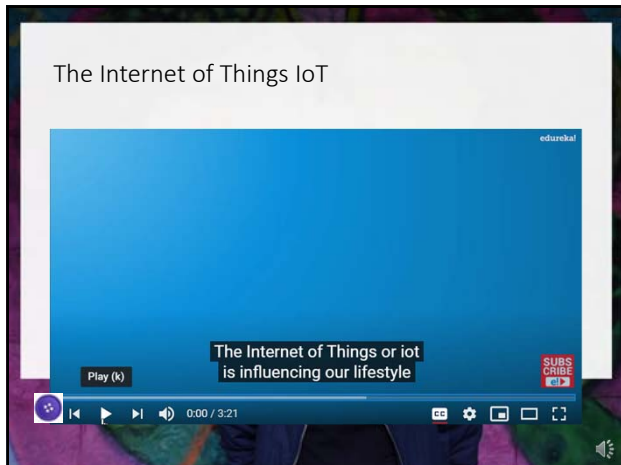
---

---

---

---

---



46



47



48



49

---

---

---

---

---

---

---

---



50

---

---

---

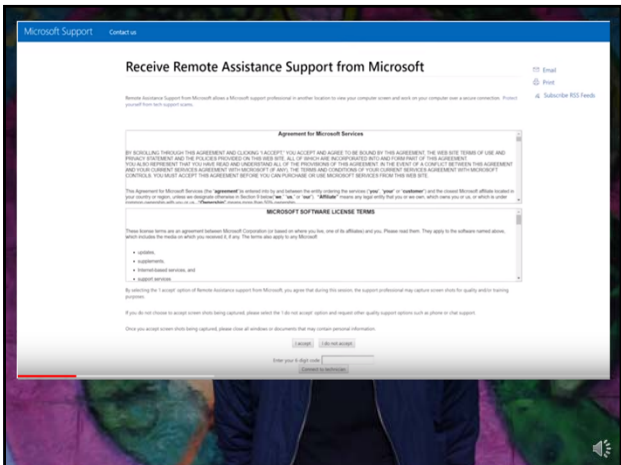
---

---

---

---

---



51

---

---

---

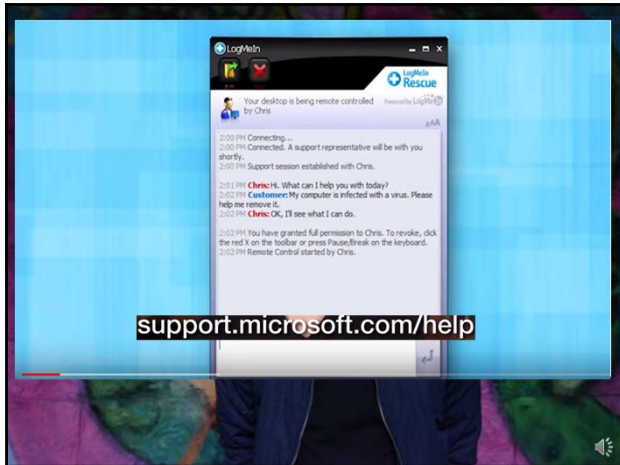
---

---

---

---

---



52

---

---

---

---

---

---

---

---



53

---

---

---

---

---

---

---

---



54

---

---

---

---

---

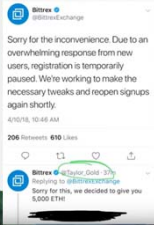
---

---

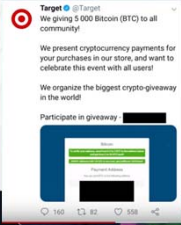
---

# Twitter Scams (Spoofing)

Real Profile responds with fake profile



Real Profile Hacked



55

---

---

---

---

---

---

---

---

# Questions

Eric Rodriguez, **CFCS, CFE, CCS, CBAO**  
President, ACFE Heartland Chapter  
Enterprise Compliance  
Financial Crimes Risk Management  
Suite-900 / Wells Fargo Center  
Lincoln, NE 68508  
O: 402-458-2754  
C: 402-617-9331  
[eric.rodriguez@neinet.net](mailto:eric.rodriguez@neinet.net)

Office of Corporate Investigations, BSA, AML, OFAC, KYC, CIP, Privacy, GDPR

*"Helping you to protect our customers."*

*"Greatness is not measured by what a man or woman accomplishes, but by the opposition, he or she has overcome to reach his goals."*



56

---

---

---

---

---

---

---

---