External Fraud: How Criminals Socially Engineer Us and How to Avoid Getting Fooled

© Financial Operations Networks LLC

VIMCOE
VENDOR INFORMATION MANAGEMENT CENTER OF EXCELLENCE

Lesson Sections

- Global Fraud
- What is Social Engineering?
- Social Engineering Scams - Phishing
- Social Engineering Scams – BEC
- How to Combat Social Engineering Scams
- Summary

VIMCOE
VENDOR INFORMATION MANAGEMENT CENTER OF EXCELLENCE

Global Fraud

VIMCOE
VENDOR INFORMATION MANAGEMENT CENTER OF EXCELLENCE

Fraud in Accounts Payable - US

FBI Internet Crime Complaint Center: FBI 2021 Report of IC3 Complaints

Total Complaints

847,376

Average of 2,300 per day

Business Email Compromise (BEC) Scams

19,954

$2.4 Billion in Losses

Victim per State*

Rank	State	Victims
1	California	67,095
2	Florida	15,855
3	Texas	41,148
4	New York	29,065
5	Illinois	17,999
6	Nevada	17,706
7	Ohio	17,510
8	Pennsylvania	17,262
9	Washington	13,903
	New Jersey	12,817

Total Victim Losses by State*

Rank	State	Loss
1	California	$1,227,989,139
2	Texas	$606,179,646
3	New York	$559,965,598
4	Florida	$528,573,929
5	Pennsylvania	$206,982,032
6	New Jersey	$203,510,341
7	Illinois	$184,860,704
8	Michigan	$181,622,993
9	Virginia	$172,767,012
	Washington	$157,454,331

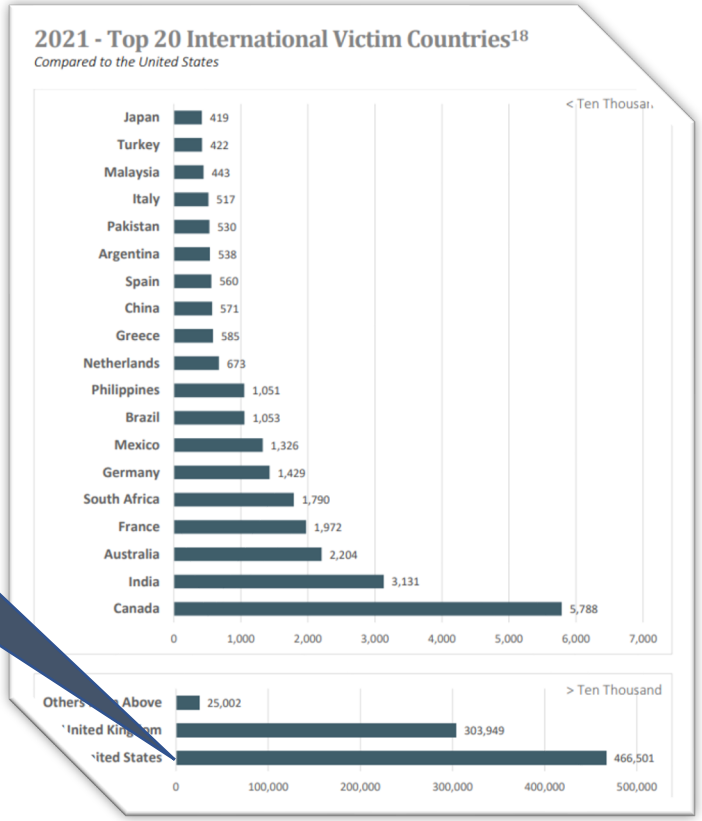
VIMCOE
VENDOR INFORMATION MANAGEMENT CENTER OF EXCELLENCE

Fraud in Accounts Payable - Global

FBI Internet Crime Complaint Center: FBI 2021 Report of IC3 Complaints

#BECareful

UK – 301,949



VIMCOE
VENDOR INFORMATION MANAGEMENT CENTER OF EXCELLENCE

What is Social Engineering?

VIMCOE
VENDOR INFORMATION MANAGEMENT CENTER OF EXCELLENCE

What is Social Engineering?

Definition: A fraudulent practice of communication purporting to be from reputable senders in order to induce individuals to reveal sensitive information or make unauthorized changes. **Business Email Compromise (BEC)** and **Phishing** are forms of social engineering.

For Vendor Maintenance Teams fraudsters target sensitive information on the vendor master record in order to submit changes that **divert payments** for legitimate invoices or for fictitious invoices that they have created - also using that sensitive data.

VIMCOE
VENDOR INFORMATION MANAGEMENT CENTER OF EXCELLENCE

What is SPI in the Vendor Master File?

Tax ID – For US vendors, it can either be the Employer Identification Number (EIN), the Social Security Number (SSN) or an Individual Taxpayer Identification Number (ITIN). Both the SSN and the ITIN can be assigned to an individual, and as such, they are considered sensitive personal information. Since some accounting systems have one field for either tax identification number, the Tax ID should still be considered sensitive personal information.

Banking Details – Many companies include banking details on their invoices (especially International vendors) because the accounts that AP uses is a "deposit only" account or a Universal Payment Identification Code (UPIC). That is not always the case. Many Individuals, Single Member LLCs do not have "deposit only" accounts, so banking details are considered sensitive personal information.

Birth Date – In specific scenarios, the IRS and some Countries (Italy) requires the collection of a birthdate for Foreign Individuals. Birthdates are considered sensitive personal data that should only be collected for regulatory requirements.

Social Engineering Scams - Phishing

VIMCOE
VENDOR INFORMATION MANAGEMENT CENTER OF EXCELLENCE

General Types of Phishing Emails

Phishing

Mass emails

Spear Phishing

Targets a Specific Person or Group

Whaling

Highly Targeted to Senior Executives

- **May or May Not Have Grammatical Errors**
- **Sense of Urgency**
- **Emotional Cues**

VIMCOE
VENDOR INFORMATION MANAGEMENT CENTER OF EXCELLENCE

What is Vishing and SMSishing?

- **Vishing –** Attempts to obtain sensitive personal information via live voice.

- **“SMSishing” or Smishing** – Attempts to obtain sensitive personal information via text message.

Phishing Goals

1. **Obtain login credentials**
   - Create spoofed sites that look legitimate to get users to enter their username and password
   - Get into company email and company systems

2. **Obtain sensitive data**
   - Submit requests to divert vendor payments or create fictitious invoices

3. **Get Users to click on attached file or malicious link to download ransomware**
   - Block access to files
   - Demand ransom be paid in order regain access to files

Fraudsters are IN Legitimate Emails

- **Successful phishing/vishing/smishing attacks**

- **Internal Employee AND Vendor Email**
  - Requesting Change of Banking
  - Requesting Wire Transfer
  - Sending Request from Historical Email String

VIMCOE
VENDOR INFORMATION MANAGEMENT CENTER OF EXCELLENCE

Social Engineering Scams – Business Email Compromise (BEC)

VIMCOE
VENDOR INFORMATION MANAGEMENT CENTER OF EXCELLENCE

What is Business Email Compromise (BEC)?

Image Credit: https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise

BEC Scams – fraudulent requests that results in diverting vendor payments or company funds to a fraudulent account

These scams typically involve a criminal spoofing or mimicking a legitimate email address. For example, an AP Team Member will receive a message that appears to be from an executive within their company or a vendor with which the company has a relationship. The email will request a vendor banking change, wire transfer, or gift card purchase that seems legitimate but funnels money directly to a criminal.

VIMCOE
VENDOR INFORMATION MANAGEMENT CENTER OF EXCELLENCE

Email Issues

- IT Team blocks 85%, leaving 15% of Fraudulent Emails getting through to your inbox
- Fraudsters are constantly evolving
  - Can remove External Email Indicators
  - Can obtain “https” to appear as a secure site
  - Grammatical & Context Errors – disappearing by using native English speakers

Changing Vendor's Remittance Details

- **Divert** legitimate vendor payments
  - Can be request to change **vendor banking** for electronic payments
  - Can be request to change **vendor remit** address for check payments
- Banks differ in their threshold to **recover fraudulent funds**
- Fraudsters use **personal victims** to move funds to multiple accounts

Gift Card Scams

- Fraudsters will **spoof your leaderships' email** (or they are in the real email account) and request you to purchase gift cards urgently while they become unreachable

- They then reach back out and **ask you for the numbers** from the back of the gift cards

VIMCOE
VENDOR INFORMATION MANAGEMENT CENTER OF EXCELLENCE

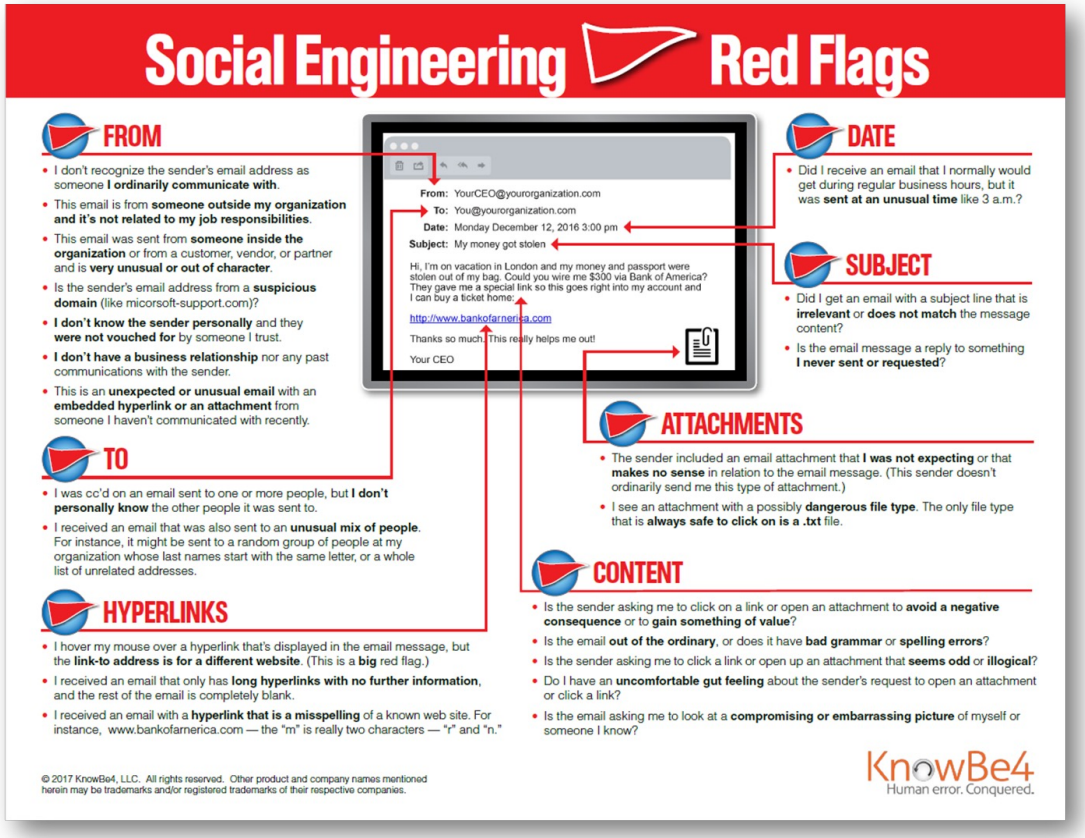
Deep Fake Scams

- Uses artificial intelligence and machine learning algorithms to imitate the work and characteristics of real humans
- According to the FBI, Deep Fake Scams are evolution of “Business **Email** Compromise” to “Business **Identity** Compromise”
  - Fraudsters are **applying for real jobs** to get access to sensitive personal information
  - Fraudsters are **interviewing real candidates** for fake jobs then sending a fake offer letter to their company email, and when opened, downloads ransomware

How to Combat Social Engineering Scams

VIMCOE
VENDOR INFORMATION MANAGEMENT CENTER OF EXCELLENCE

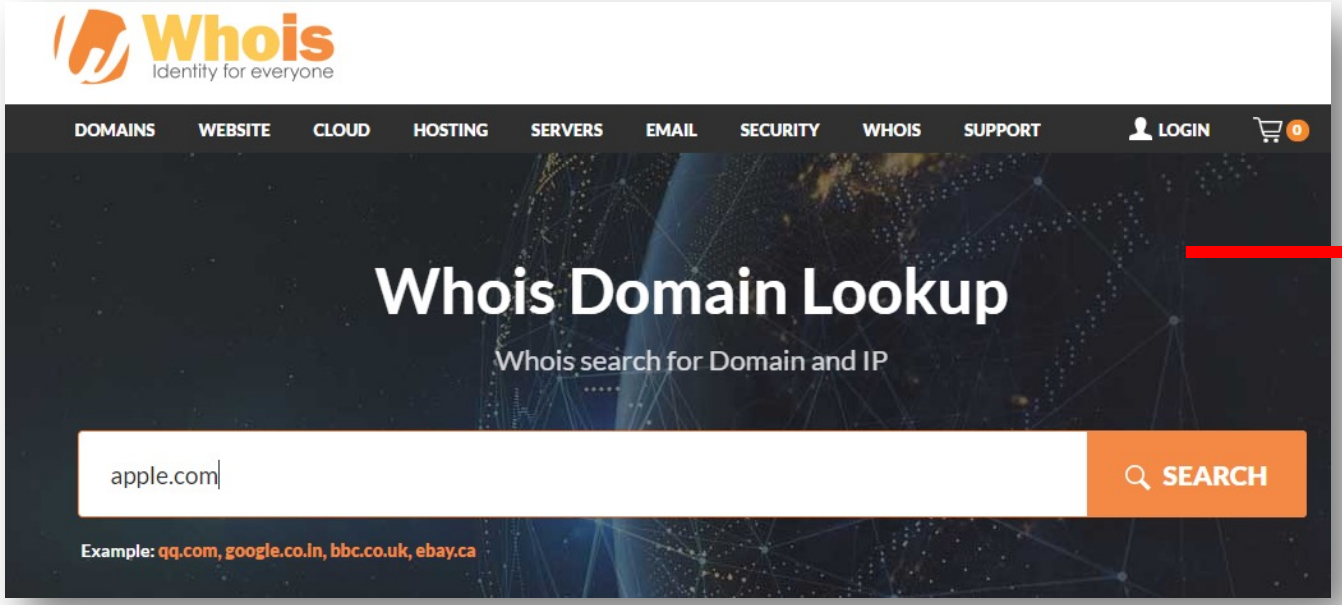
BEC & Phishing – Validate Email



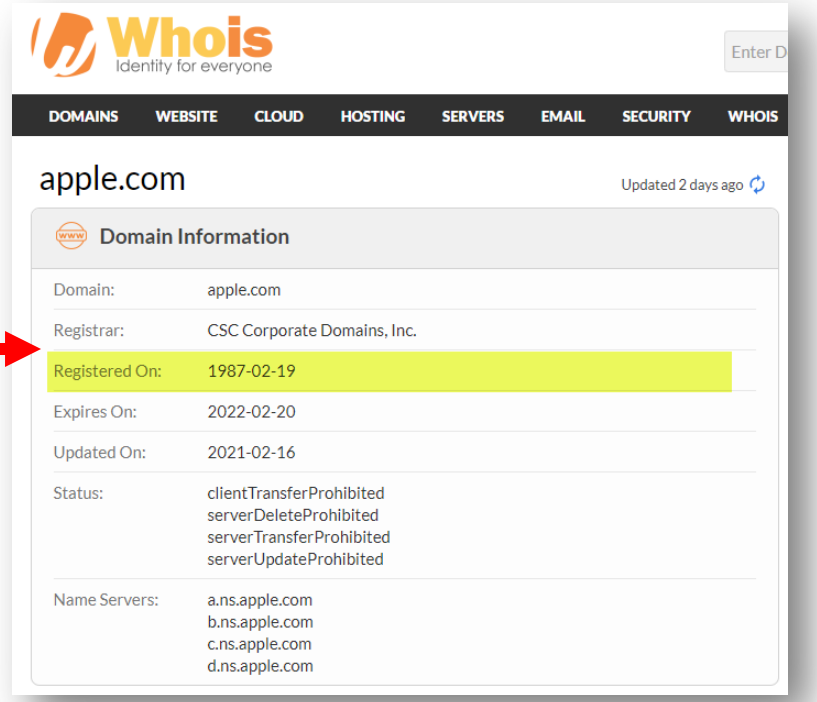
VIMCOE
VENDOR INFORMATION MANAGEMENT CENTER OF EXCELLENCE

BEC & Phishing – Validate Email Domain

1 https://www.whois.com/whois



2 Does the Registration Date Match Expectations?



VIMCOE
VENDOR INFORMATION MANAGEMENT CENTER OF EXCELLENCE

Add Authentication & Internal Controls

Authenticate the Data

Require Existing Banking to Change Banking

Check Payments Before Sending

Payments > $K with Remittance

Change Within 90 Days

Authenticate the Requestor

Only Way to Get Required Forms

Forms Sent/Collected Directly to Vendor

Vendor Communication Before/After Change

Added Scripts to Ensure Valid Confirmation

Added Send Vendor Notification After Change

Confirm with the Vendor They Received the Payment

Audit Process / Vendor Data

Vendor Add/Change Process Audit

VMF Data Review and Revalidation

VIMCOE

VENDOR INFORMATION MANAGEMENT CENTER OF EXCELLENCE

Add Best Practices

- Use a Password Manager
- STOP C-Suite Level requesting payments via email
- Train the staff

VIMCOE
VENDOR INFORMATION MANAGEMENT CENTER OF EXCELLENCE

Stay Up To Date on New Frauds

FBI Internet Crime Complaint Center Alerts

IRS Tax Scams/Consumer Alerts

Better Business Bureau (BBB) Scam Tracker

Google Alerts

VIMCOE
VENDOR INFORMATION MANAGEMENT CENTER OF EXCELLENCE

Victim of Fraud? Report It Internally And…

IRS

phishing@IRS.gov

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

FTC.gov/Complaint
Identitytheft.gov

FEDERAL BUREAU OF INVESTIGATION
Internet Crime Complaint Center IC3

ic3.gov/Home/BEC

VIMCOE
VENDOR INFORMATION MANAGEMENT CENTER OF EXCELLENCE

Summary

VIMCOE
VENDOR INFORMATION MANAGEMENT CENTER OF EXCELLENCE

What You Learned

In this lesson, you learned:

- FBI reported complaints on Phishing and BEC scams
- Definition of Social Engineering and what is considered SPI for vendors
- Phishing and BEC: what information is targeted and the fraudsters' ultimate goals
- Authentication steps, internal controls and best practices to combat social engineering scams

Be sure to seek leadership and/or audit approval on any new processes or tools prior to implementation.

That concludes this lesson

Send questions to: questions@vimcoe.com

VIMCOE
VENDOR INFORMATION MANAGEMENT CENTER OF EXCELLENCE