

The Current Landscape of Fraud Schemes and Cybercrimes

SSA Kevin Cooke, CFE
United States Secret Service
New York Field Office
Financial Crimes and Cyber Fraud Task Force

WHAT IS OUR GREATEST THREAT IN REGARDS TO FRAUD AND/OR CYBERCRIME?

Immunity

"It won't happen to me"

Mis-prioritization

"I'll install that update later"



"I don't have anything important on my computer"

Undervaluing of potential

"I don't have any money"

Undervaluing of assets

COMMON FRAUDS



Identity Theft

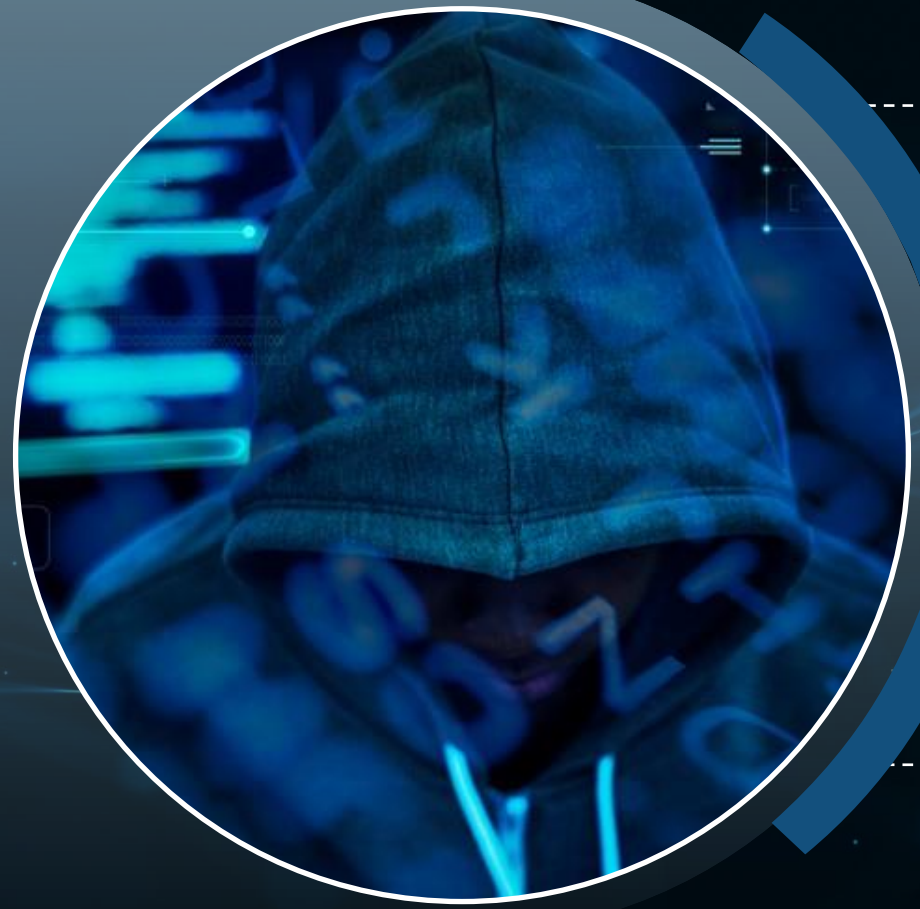
Business Email Compromise

(BEC)

Cryptocurrency Scams

(Pig Butchering)

IDENTITY THEFT



Crime of our Generation

An Identity is stolen every **22 seconds** worldwide

Fraud losses total over **$5.8 billion** per year

TYPES OF IDENTITY THEFT



- Financial Identity Theft
- Medical Identity Theft
- Child Identity Theft
- Synthetic Identity Theft

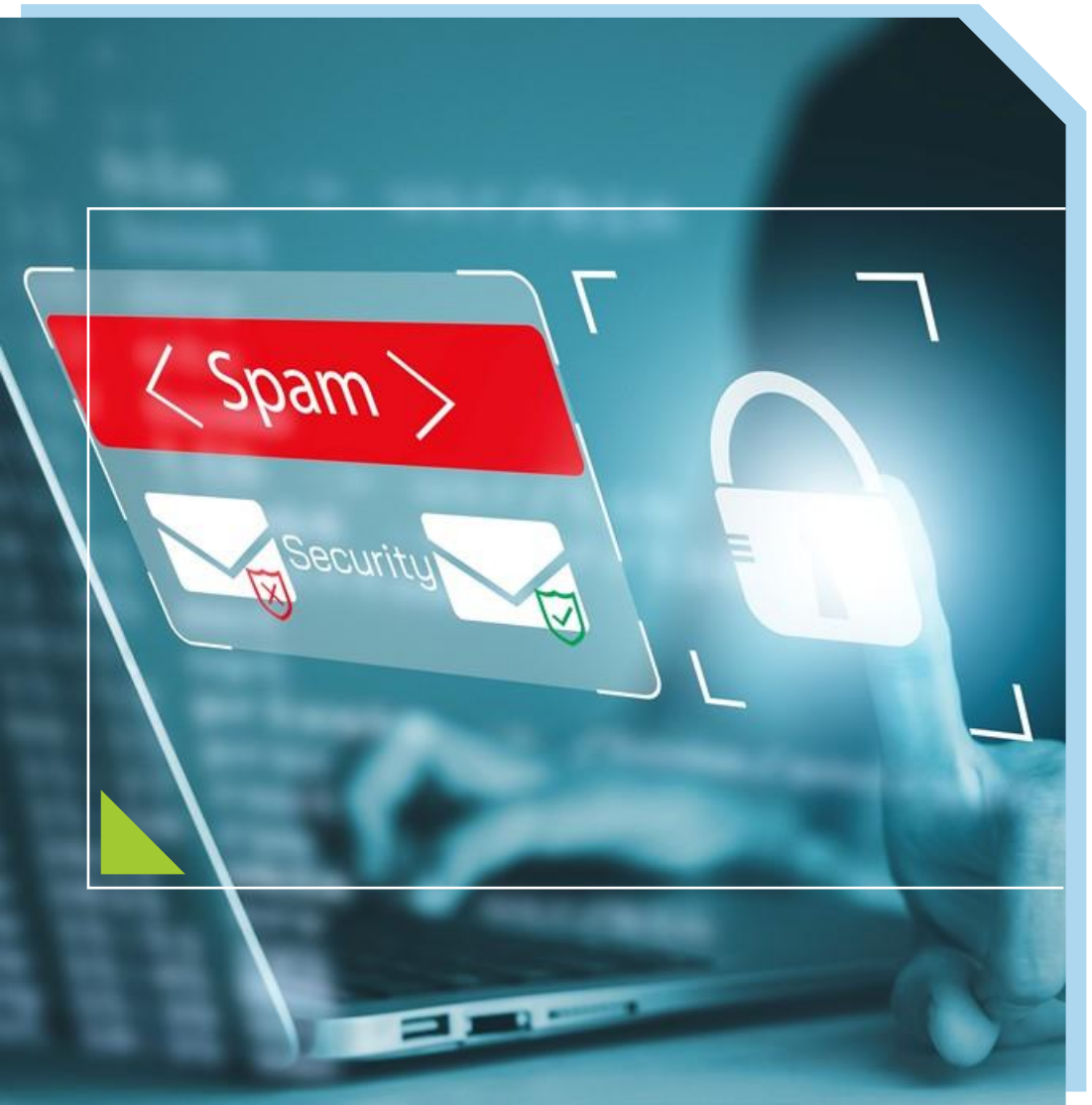
BUSINESS EMAIL COMPROMISE

Most profitable form of cybercrime

Over $43 billion in loss between June 2016 and December 2021, FBI IC3

Multiple Tactics Utilized

UNIDENTIFIED BEC GROUP PHISHING EMAILS UTILIZING (AiTM) ADVERSARY IN THE MIDDLE



- Since September 2021 – over 10,000 victims and billions in loss globally
- Scours emails for companies, also learns correct syntax of victim
- Spoof’s victim’s email and requests payments to new bank account etc.

LILAC WOLVERINE
CENTRAL NIGERIAN BASED BEC GROUP



Targets personal accounts via phishing emails

Spoofs the hacked account and request gift cards playing on emotions

For example, a friend or colleague is undergoing cancer treatment

CRIMSON KINGSNAKE – BEC GROUP

Utilizes Blind Third Party attacks (supply chain attack)

Spoofs law firms and targets companies they represent

Requests payment of overdue fake invoices



CRYPTOCURRENCY SCAMS (PIG BUTCHERING)

01

Most begin with SMS phishing (smishing); dating apps; and WhatsApp



02

In 2021 the FBI IC3 received over 4,300 complaints $429 million in losses

03

Gamification of the process preys on greed and promises of riches

COMMON TACTICS



Most investments go into mainstream crypto accounts

Often will allow for early withdrawals of profits

Which often leads to people investing more, (Fattening the Pig)

Request tax payment if they attempt to withdraw all the funds, “sunk cost fallacy”



CASE STUDY

Invest with us and let us invest for you. Let's think, explore and dominate the market, all for you! you don't have to consider the risk of investing in capital market. Choose any investment plan and let us manage all the risk for you and please note that each investment (deposit) lasts for the said number of days as depicted on each investment plan.

STARTER PLAN

WEEKLY 15.7% FOR 4 TIMES

For 4 times

15.7% ROI each time

CLASSIC PLAN

MONTHLY 39% FOR 4 TIMES

For 4 times

39% ROI each time

PREMIUM PLAN

MONTHLY40.5% FOR 8 TIMES

For 8 times

40.5% ROI each time

PREMIUM PLAN

MONTHLY45% FOR 6 TIMES

For 6 times

45% ROI each time

IT’S ABOUT THE DATA



Business data – vendor lists, bank accounts, trade secret, etc.

Personal data – PII (personal identifying information)

- Name, DOB, SS#, Phone #, Account info, etc.

PASSWORD HYGIENE

01 Inventory accounts

02 Example: (banking, Netflix, Facebook, etc.)

03 Use a strong, different password for each

04 Combination of letters, numbers & symbols

05 8+ characters

06 Use sentences or acronyms instead of words

07 Example: My dog Fido is great! = Mid0gF1d01sGr8!

08 Use multi-factor authentication when possible

09 Close all unused accounts

10 Consider using an encrypted password manager

OPERATING SYSTEMS



Phones, computers, and all electronics should all be kept current



Skipping updates prolongs vulnerability and eases unauthorized access to private information, putting you at risk for identity theft, loss of money, credit, etc.

INSTALL AND USE A VPN

Virtual Private Networks (“VPNs”) create an encrypted connection between your device and the network



Prevents data from being hacked on a public Wi-Fi network

Hides information from ISPs

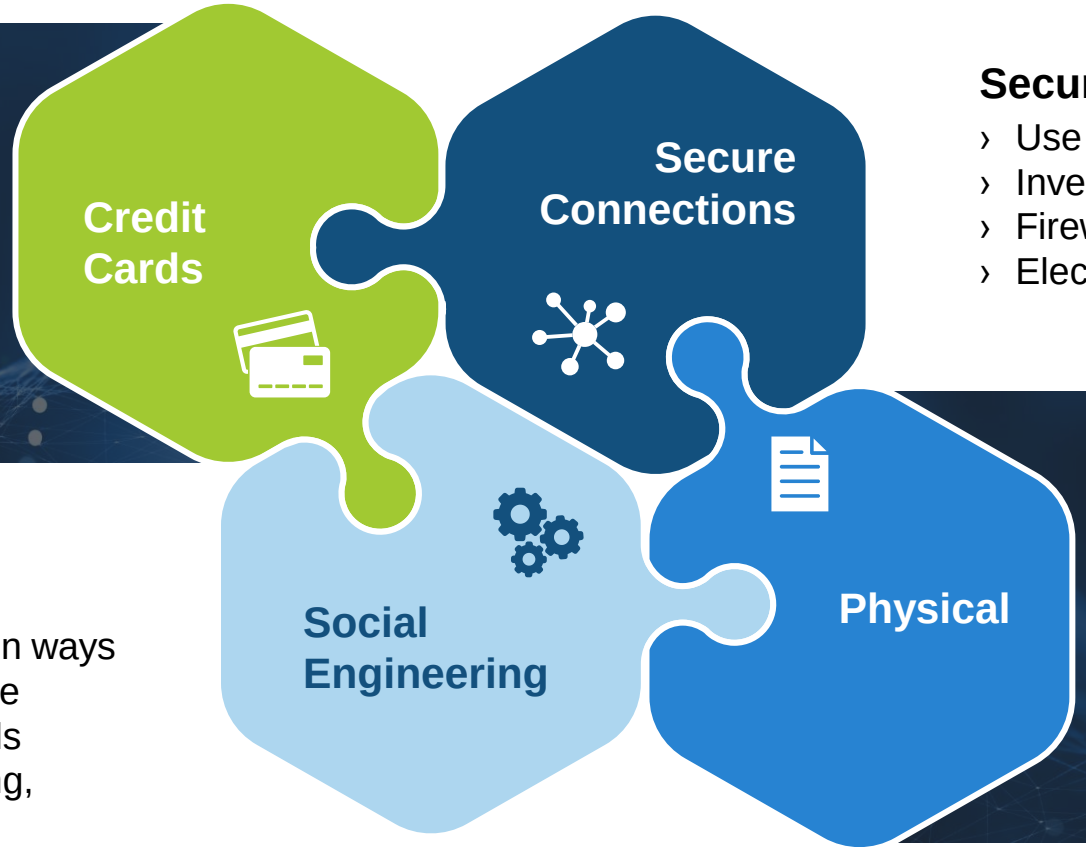
Mirror another location to access websites only available in a certain geographic location

ADDITIONAL EDUCATION AND ACTIONS

Key knowledge components and best practices to keep you ahead of the curve

Credit Cards

- Set up recurring payments for regular bills
- Online purchases
- POS purchases
- Practice caution around ATMs



Secure Connections

- Use HTTPS vs. HTTP URLs when possible
- Inventory of connected devices
- Firewalls / Encryption
- Electronic banking

Social Engineering

- Know the most common ways in which scammers take advantage of individuals
- Phishing, spam, whaling, phone calls, SMS

Physical

- Shred unneeded documents
- Opt out of mailers
- Be aware of immediate surroundings
- Social media
- Monitor credit score at least annually

SAVE YOURSELF

STOP: Everything you are doing

ASK: Is there urgency; is this out of the ordinary?

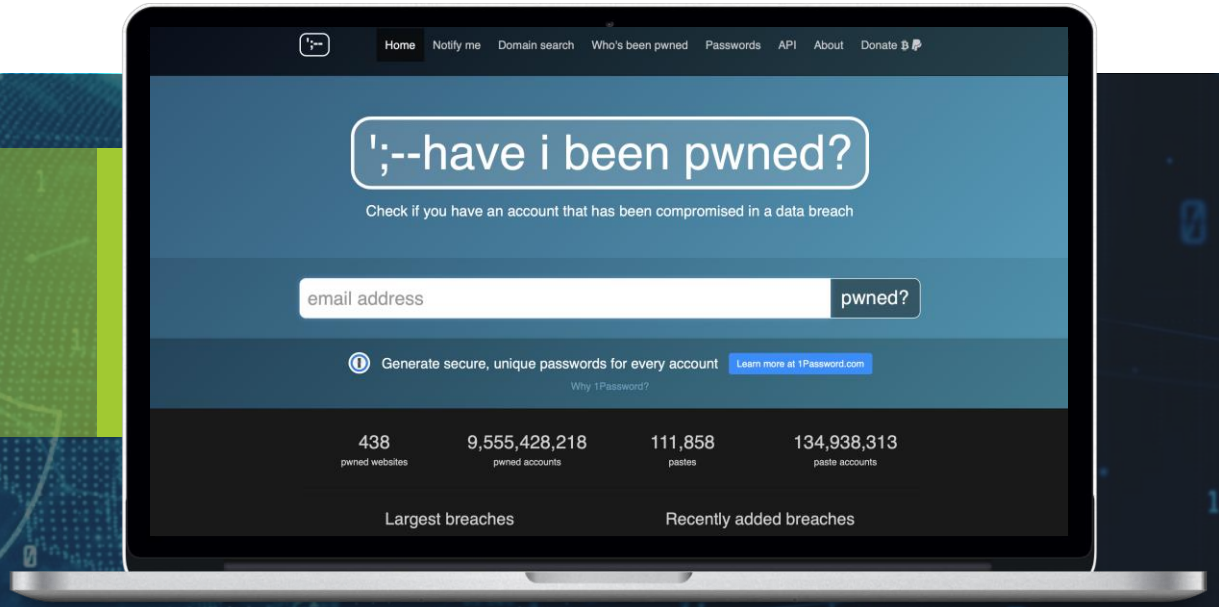
VERIFY: Pick up the phone and verify!!

ELEVATE: Security department, authorities. IC3 –Internet Crime Complaint Center (FBI)



RESOURCES

www.haveibeenpwned.com
checks email addresses to determine if it is associated with an account that has been compromised in a data breach





www.ic3.gov
the mission of the Internet Crime Complaint Center, also known as IC3, is to provide the public with a reliable and convenient reporting mechanism to submit information to the FBI

United States Secret Service

SSA Kevin W. Cooke, CFE
New York Field Office

DISCLAIMER:

The views and opinions in this document are those of the individual presenter and should not be attributed to the United States Secret Service and/or the Department of Homeland Security.

This document is the intellectual property of the individual presenter and may not be redistributed or repurposed without prior written consent from the author.