FINANCIAL CRIMES
ELDER ABUSE UNIT

PRESENTERS

Detective John Overstreet

Detective Paul Hill

FinancialCrimes@fresno.gov

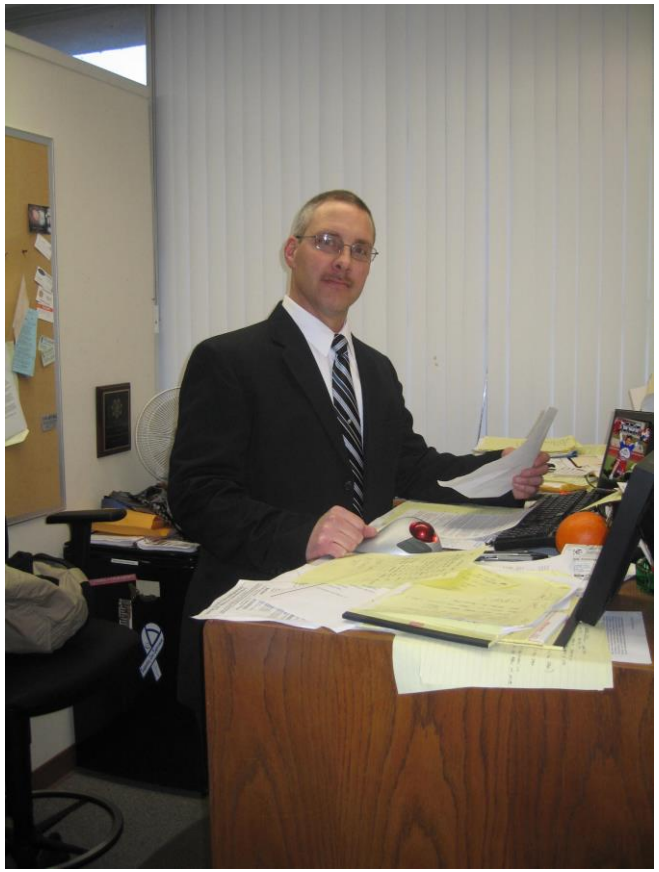
BEST PRACTICES TO STAY SAFE FROM FINANCIAL ABUSE

REDUCING THE RISK

Disclaimer:

All information discussed today is meant to be generic guidelines and not legal or procedural advise. Please contact your legal advisor or administration for specific incidents..

Sgt Martin Van Overbeek
Financial Crimes Supervisor



Financial Crimes & Elder Abuse

TRUE STORY
JEFF BEZOS – OWNER OF AMAZON AND WASHINGTON POST IPHONE HACK

September 2017 – Washing Post published critical article of Saudi Arabia and Crown Prince – Mohammad bin Salman – published by journalist Jamal Khashoggi. Self imposed exile in USA 2017.

April 2018 – Bezos and the Crown Prince were at a dinner together; they exchanged WHATSAPP and phone numbers.

October 2018 – Khashoggi was murdered (Saudi Consulate in Istanbul, Turkey). The Washington Post increasingly wrote critically of Saudi Arabia and of the Crown Prince – Mohammed bin Salman. Bad for national business, so discredit campaign scam against Bezos.

January 2019 – The National Inquirer released details of Bezos involved in an affair including text messages and graphic photos.

February 2019 - FTI consulting group investigates and learns video from Saudi Arabia Crown Prince – Mohammad bin Salman – sent WHATSAPP video with Malware to infect Jeff Bezos phone.

Movie about Khashoggi assassination: The Dissident

Current Scams

- **Fake Computer Blue Screen of Death, "Call Microsoft at 1-800-ImA-Scammer"**
- **Grandchild in Trouble (Arrested, involved in a crash, kidnapped).**
- **Sweetheart Scams - Relationships Groomed Over Time like a Child Predator**
- **Work From Home Scams (Money Mules / Product Repackaging)**
- **Online Pet Purchases / Animal Shipment (Air-conditioned crate / Hold at Customs)**
- **Arrest Warrant / Missed Court Summons**
- **PG&E Utility Shutoff for Late Payment**
- **IRS Delinquent Taxes Phone Call**
- **Fake Text/Email saying Bank Account Locked/Compromised**
- **Fake Text/Email Confirming Amazon Purchase or Antivirus Renewal for $$$**
- **Rental vehicle linked to you pulled over in Texas, drugs/blood in trunk, accounts linked to you.**

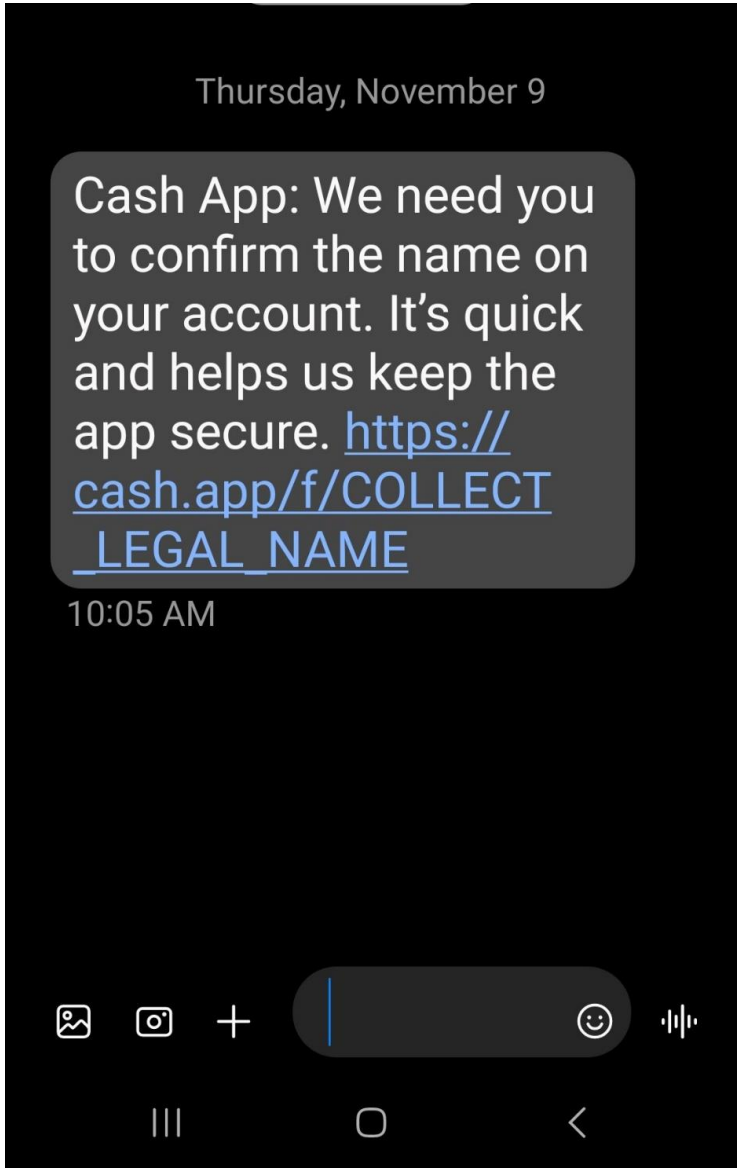
Scammer Tactics Used

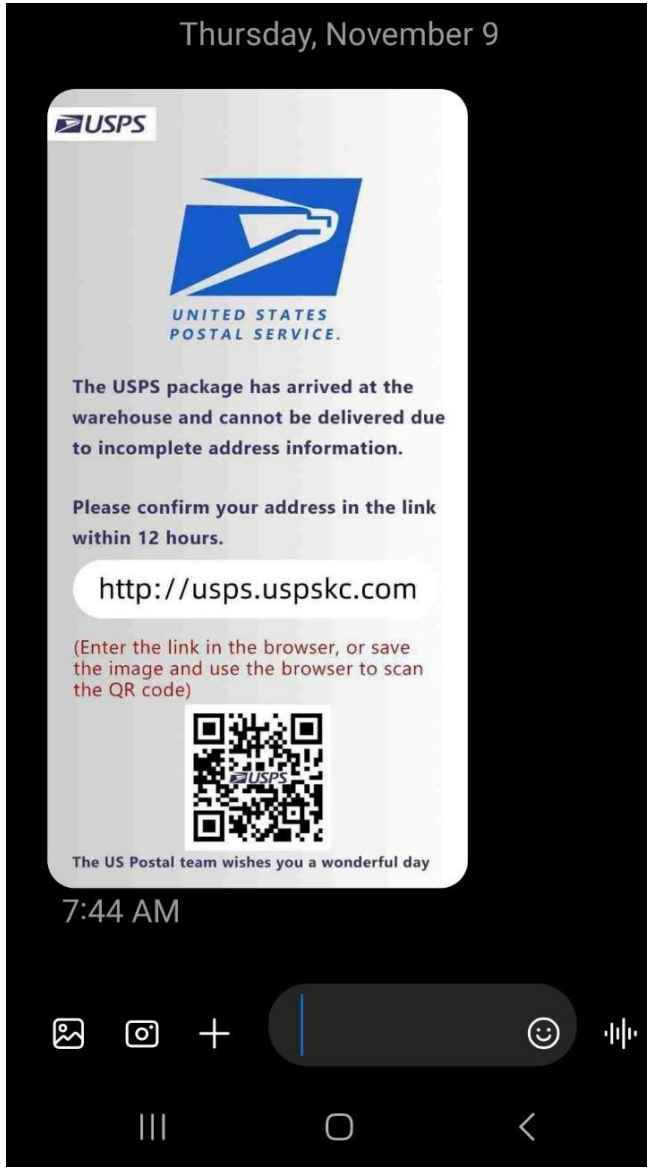
- **Groom a Friendship for weeks/months, then introduce need for money**
- **Gain your trust using believable explanations (They're using a script)**
- **Create Fear with a consequence (i.e. Arrest, Utilities Shut-Off, Lien on your House, Loss of job, etc.)**
- **Keep you on the Phone to prevent from checking with Family (1-2 hours not uncommon)**
- **Instruct you to Lie o Bank Tellers, Store Clerks, Family, Friends**
- **Tell you not to tell anyone or that will show you're a suspect not cooperating**
- **Use other Scammers to make it more believable (e.g. Supervisor, Special Agent, Officer, etc.)**
- **Call from "Spoofed" numbers for the Police/Sheriff's Department, IRS, or Bank**
- **Threaten and become overbearing to try and bully you**

How to Prevent Being Scammed

- **Be selective on what Calls You Answer, Don't always trust Caller ID**
- **IRS/PG&E/Fresno Sheriff will NOT call for money**
- **NEVER click on links sent to your text messages/emails**
- **Call Customer Service # from back of your ATM/Credit Card, NOT the one in the link**
- **Scammers will also list FAKE Customer Support #s in Google searches**
- **NEVER give out personal info (Name/Birthdate/SSN/Address) to Unverified People**
- **NEVER buy gift cards to pay a bill (Will ask you to take a picture and send it)**
- **NEVER pay a bill or "Safeguard" money using a Bitcoin ATM**
- **If Scammer instructs you to withdraw money and keep it secret or you'll be arrested -HANG UP!!!**
- **Be selective on what Calls You Answer, Don't always trust Caller ID**
- **If you get an email requesting you to change account info, verify via phone w/ known number for requestor**

Text Scams


Thursday, November 9
Cash App: We need you to confirm the name on your account. It's quick and helps us keep the app secure. https://cash.app/f/COLLECT_LEGAL_NAME
10:05 AM


Thursday, November 9
USPS
UNITED STATES POSTAL SERVICE.
The USPS package has arrived at the warehouse and cannot be delivered due to incomplete address information.
Please confirm your address in the link within 12 hours.
http://usps.uspskc.com
(Enter the link in the browser, or save the image and use the browser to scan the QR code)
The US Postal team wishes you a wonderful day
7:44 AM

How to Prevent Being Scammed

- **Sign Up for Informed Delivery through the US Post Office**
- **Setup account alerts (Text & Email with low % threshold**
- **Retrieve mail close to delivery time when possible, DO NOT leave in box overnight**
- **NEVER carry your Social Security Card in Your Wallet/Purse**
- **NEVER hide your Wallet/Purse in your vehicle while Shopping**
- **Pull up on Point-Of-Sale devices to make sure they don't have a skimmer**
- **Use ATMs <u>inside</u> the Bank whenever possible**
- **Trust your conscience warning you when something doesn't seem RIGHT**
- **Ask for help when unsure from a trusted friend/family member**

What Do I Do If I Was Scammed

- **Phone Calls - HANG UP and DO NOT answer their Call Back Attempts**
- **Computers - Un-Plug Internet/Turn Off WiFi/Un-Plug Computer**
- **Report to your local Law Enforcement Agency immediately**
- **Tell a trusted family member and ask for help**
- **If Banking information given, notify the Bank and consider changing accounts**
- **Change your passwords to accounts**
- **Monitor your credit (Free copy of credit report www.annualcreditreport.com)**

BEST PRACTICES

Informed Delivery with USPS

Computer antivirus program (Norton, avast, McAfee, TREND, etc…)

- **VPN Protection**
- **App Locking**
- **Password vault**

Freeze all three Credit Bureaus (Equifax, Transunion, Experian)

Never respond to email with personal information

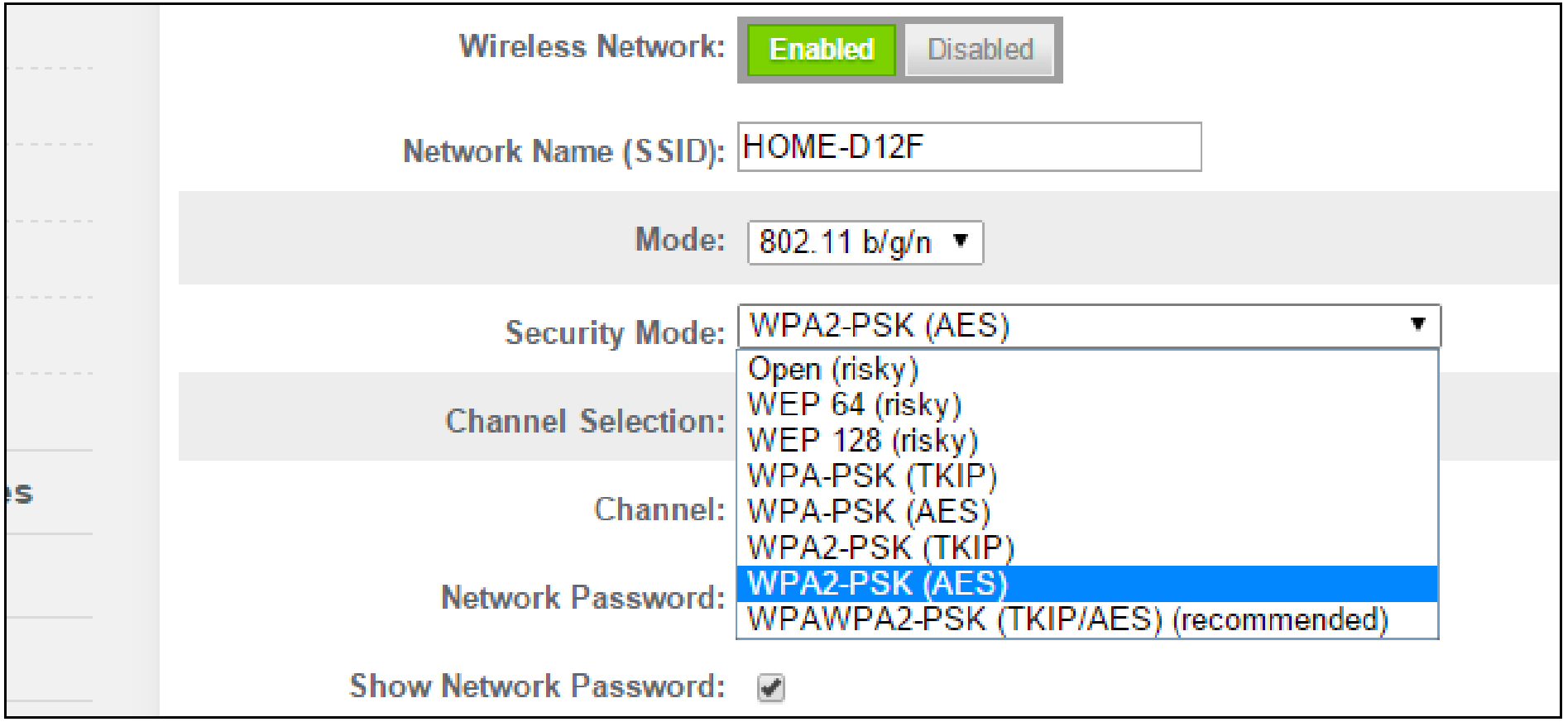
- **Social Security**
- **Bank Account information**

Can report to Internet Crime Complaint Center (IC3)

- **https://www.ic3.gov**

Secure WiFi with encryption

WI-FI ENCRYPTION



Example of Wifi encryption protocols

Recommended: at least <u>WPA2-PSK (AES)</u>

IN HOME CARE PROVIDERS

Families/Elder:

- **Keep valuables in secure place**
- **Don’t lend out credit or debit cards. If necessary, have a specific card for groceries, etc, and limit the amount available**
- **Use security cameras where legally available (Nest, Ring, etc..)**
- **Have emergency numbers easily available**
- **Conduct unannounced visits**

Care givers:

- **Don’t take or use property from the home or elder for yourself**
- **Keep a journal of care, use of money/credit cards, property**
- **Don’t ask for loans, money, property**
- **Don’t accept loans, money, property**

BANKING AND FINANCES

- Keep track of all spending and deposits
- Check your statement every month, report discrepancies immediately
- Use online banking and auto pays if possible
- Use online bank notifications to stay informed
- Limit amount of funds in accounts used by others
- Set up passwords (software encryption) with your bank or credit union
- Check your credit history often, better yet, use a monitoring service (LifeLock, Privacy Guard, etc…)
- Get to know your banker