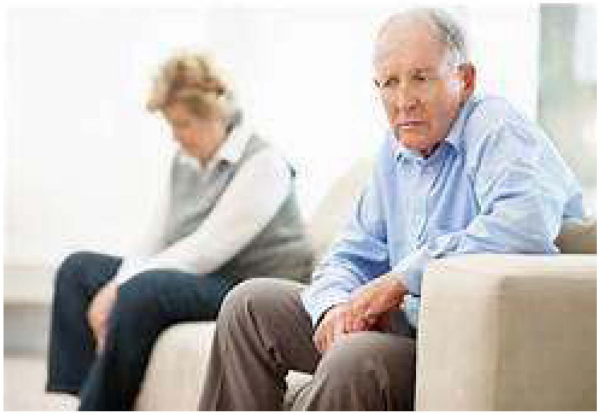
Beware of Senior scams!



Introduction

- Staff Sergeant Eric Calendine
- Beaufort County Sheriff Office
- Currently assigned a supervisor for Southern Investigations
- 20 year experience in Law Enforcement
- Bachelor of Arts Criminology and Criminal Justice 1999 The University of Maryland
- Former Defensive End for Maryland Terrapins 1995-1999.
- Claim to fame: I once delivered a baby on the side of the road.

Elder Abuse and Exploitation

- How you, your loved ones, clients, and your neighbors are being preyed upon by local, national, and international criminals.

- In this lecture, I will discuss the trends in scams used to defraud victims of their money, identity, and financial peace. These scams are becoming big business for criminals. It is estimated that last year alone criminals stole over 37 Billion dollars from victims and financial institutions. The total number of victims is increasing as baby boomers retire and their ability to manage trillions of dollars in personal assets diminishes.

- (please hold questions to the end of the presentation)

Elder Abuse Statistics

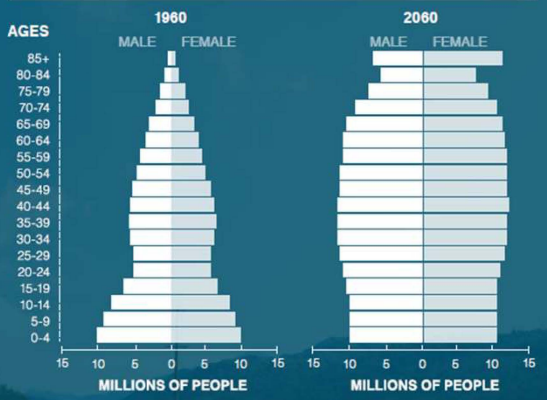
Population of Older Adults

Older adults age 65 or older comprise 14.9% of the total population in the USA.

Projections anticipate the percentage of the population age 65 and older to continue to grow in the coming decades.

From Pyramid to Pillar: A Century of Change

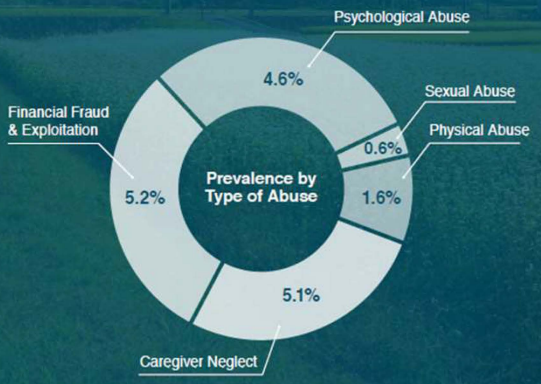
Population of the United States



Definition and Prevalence of Elder Abuse

Elder abuse is "An intentional act or failure to act by a caregiver or another person in a relationship involving an expectation of trust that causes or creates a risk of harm to an older adult"[i]. It is a term under which five types of abuse are reflected[ii]:

- Caregiver Neglect
- Financial Fraud & Exploitation
- Pyschological Abuse
- Sexual Abuse
- Physical Abuse



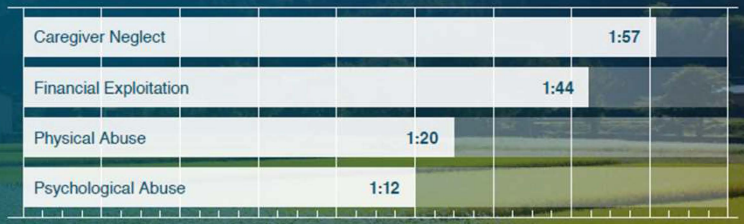
Prevalence of Elder Abuse

At least 10% of adults age 65 and older will experience some form of elder abuse in a given year, with some older adults simultaneously experiencing more than one type of abuse.

The Majority of Older Adults Live in the Community

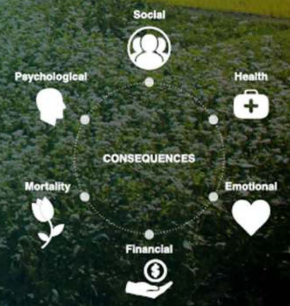
As over 90% of older adults reside in the community (as opposed to various forms of congregate living situations), most elder abuse is occurring among older adults living in the community.

Rate of Underreported by Type of Elder Abuse



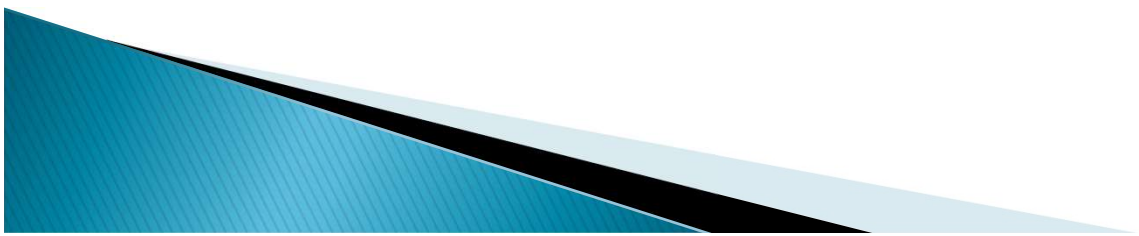
The Consequences of Elder Abuse

The trauma of elder abuse may result in health issues such as a deterioration in health, hospitalization and increased mortality, clinical issues such as depression and suicide, social issues such as disrupted relationships, and financial loss, all leading to diminished independence and quality of life.



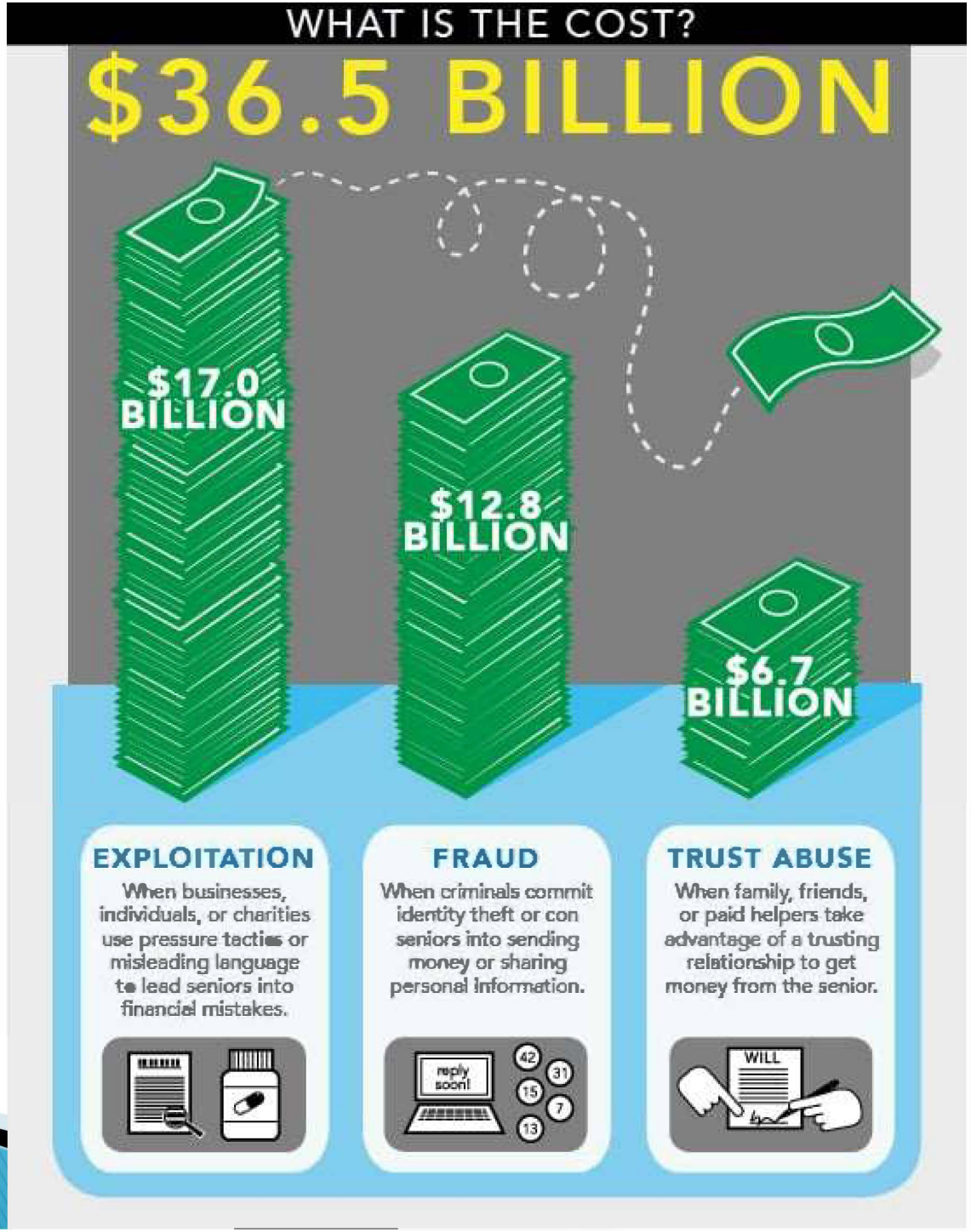
Financial exploitation means the misuse or withholding of an older adult's resources by another.

- In a given year, 1 in 18 "cognitively intact" older adults is victim to financial scams, fraud or abuse, according to a new study in the American Journal of Public Health.
- It's easier to try to exploit a senior citizen with cognitive or other impairments in financial issues, who are alone, than it is to rob a bank. So they are the targets.



Elder Exploitation is a 37 Billion dollar industry

- Some 5 million older Americans are financially exploited every year by scammers
- In 2015, Dr. Lachs (Weill Cornell Medicine) coined the term "Age-Associated Financial Vulnerability," or AAFV.
- He defined it as a "pattern of imprudent financial decision-making that begins at a late age and puts older adults at risk for material losses that could decimate their quality of life." Financial judgment can start to falter before normal cognition does, regardless of whether the person was savvy with money when they were younger. In other words, it can happen even when the person seems normal.


WHAT IS THE COST?
$36.5 BILLION
$17.0 BILLION
$12.8 BILLION
$6.7 BILLION
EXPLOITATION
When businesses, individuals, or charities use pressure tactics or misleading language to lead seniors into financial mistakes.
FRAUD
When criminals commit identity theft or con seniors into sending money or sharing personal information.
reply soon!
42
31
15
7
13
TRUST ABUSE
When family, friends, or paid helpers take advantage of a trusting relationship to get money from the senior.
WILL

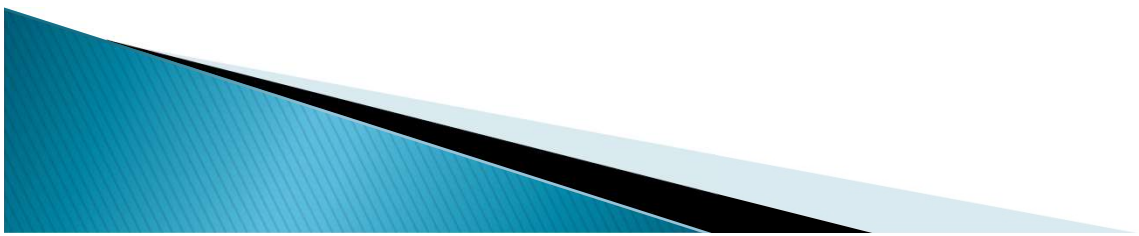

CYBER EXTORTION SCAM
LOAN SCAM
JOB SCAM
INVESTMENT SCAM
PENSION SCAM
HOME/ROOM RENTAL SCAM
INVESTMENT SCAM
INHERITANCE SCAM
LET'S FIGHT SCAMS
Scams are designed to trick people into giving away their money or personal information.

Types of scams

Lottery
Government or local official
Charity
Family member in need
Mortgage assistance
Debt relief
Construction
Computer or
Phone issues
Romance
Medical

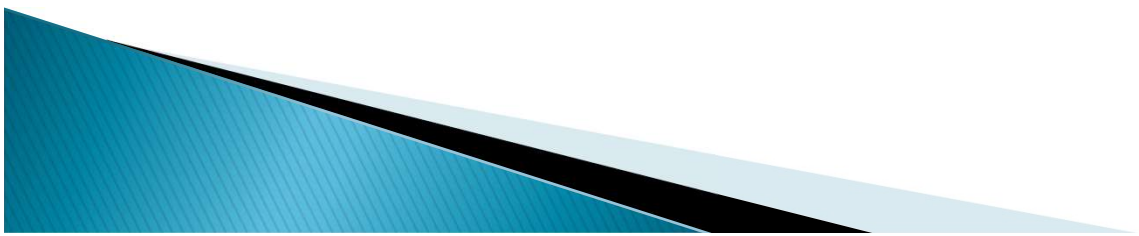
Investigate before you act!

- DO NOT GIVE OUT PERSONAL INFORMATION!
- Don’t pay up front for a promise!
- Don’t let the caller rush or put pressure on you to act quickly.
- Ask a friend or family member to look at the situation.
- Google the situation, for example “IRS call for money”.



Tools criminal use to get your money!

- Criminals will ask you to pay them in the most common forms;
  - Money gram
  - Western Union
  - ITunes card
  - Ebay cards
  - Green Dot card
  - Reloadit card or Moneypak
  - Cash, PayPal, Venmo, or Zelle




green dot
5412 7512 3456 7890
MasterCard
VISA
YOUR NAME GOES HERE

Green Dot


$100
$50
$25
$15
iTunes
Apps, games, music, movies, TV shows, books, and more.


PayPal


venmo

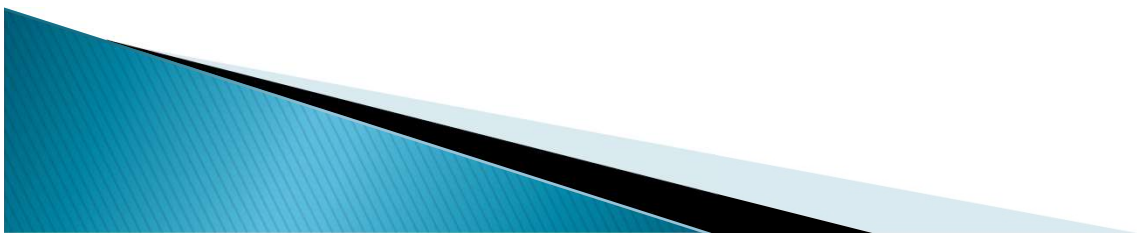

MoneyPak
Send cash quickly and conveniently to almost anyone


WESTERN UNION
MONEY TRANSFER


MoneyGram
money transfer


Zelle
Zelle

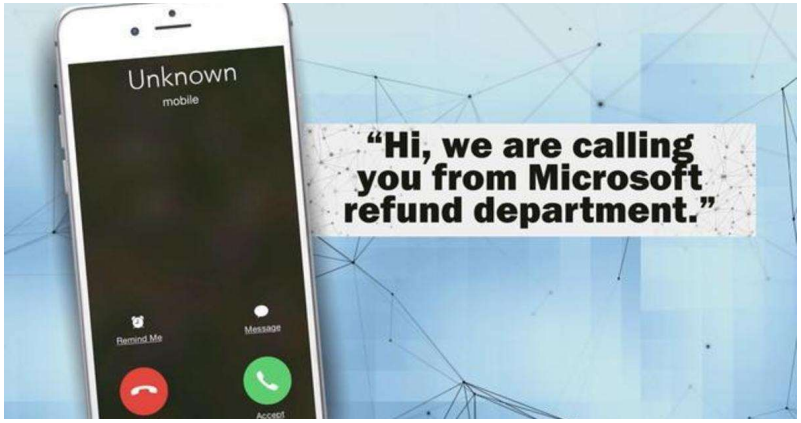
Government offices and honest companies wont require you to use these types of payment methods!



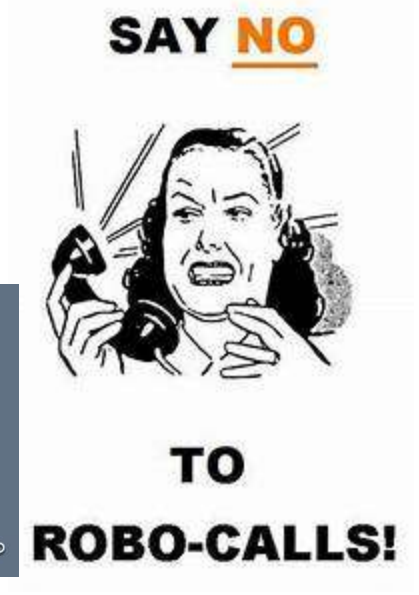
Question the caller

- Most criminal callers will answer basic questions but will become irritated when you do not follow their instructions.
- Anyone who will not let you think about the offer or let you research the situation has something to hide. Be careful!!!!

ROBO Calls



- Hang up!!!!
- Pressing numbers to be put on the no call list allows the ROBO call system to see that you have answered the call.
- This will potentially lead to additional automated or even live calls.



What to do?

- In todays world, criminals use technology to deceive your caller id. Don't trust the number listed as the number calling.
- Ask questions.
- Block ROBO call and scam call numbers.
- If you don't recognize the phone number let it go to voice mail. You can always call the person back it if is a legitimate call.
- FTC 877-382-4357

Account takeovers

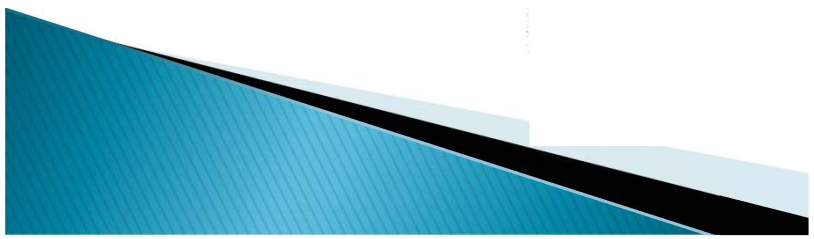
- Banks, Credit unions, HELOC, Mortgages, Auto loans, Medical loans, Pensions, Money Markets, 401K, Retirement accounts, etc.

Bank of America

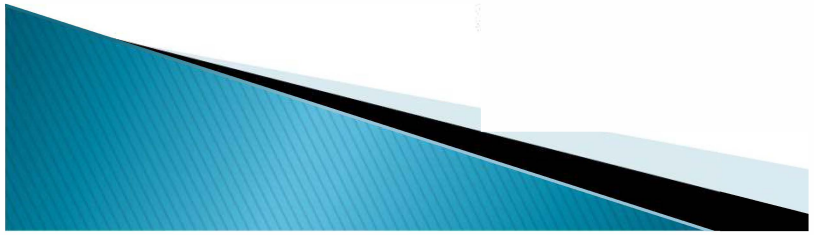
TD Bank

SunTrust

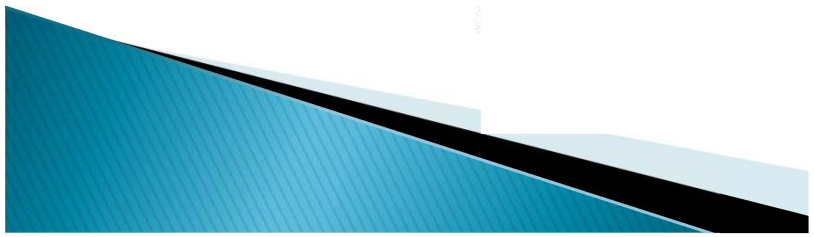
Impersonator in NC victim lives in FL.



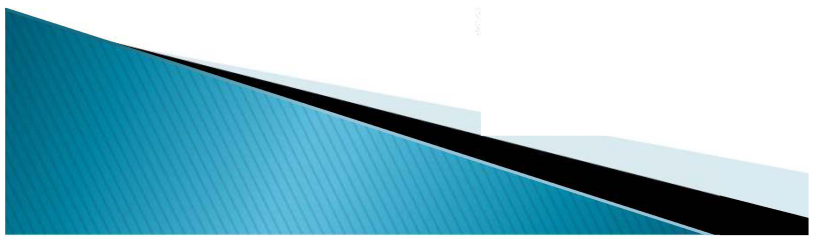
Suspect deposits check in victim's account, then requests cashier check in lower amount. Then suspect accessed victims HELOC and withdrew $26,000.



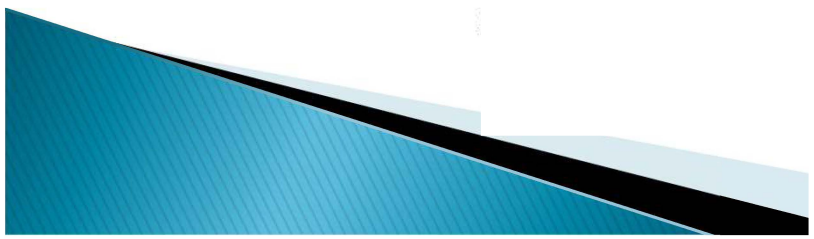
Suspect in Georgia impersonated victim in Florida. Significant losses.



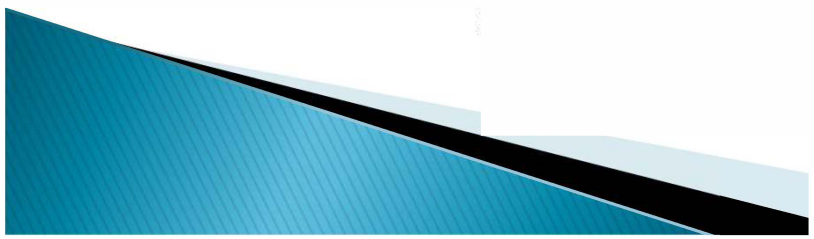
Customer impersonation $4,000



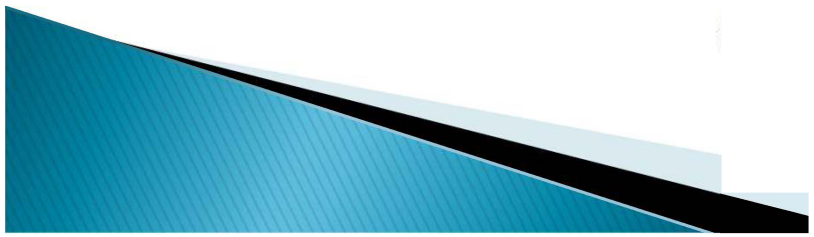
Multiple withdrawals at various branches.



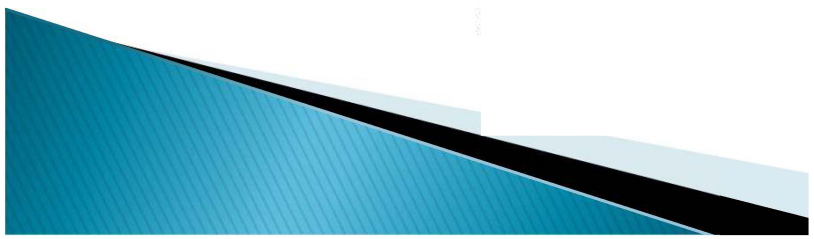
2018-2019 suspects have been impersonating clients throughout the southeast. Over $765,000 stolen.



Posed as victim and cashed checks against account.



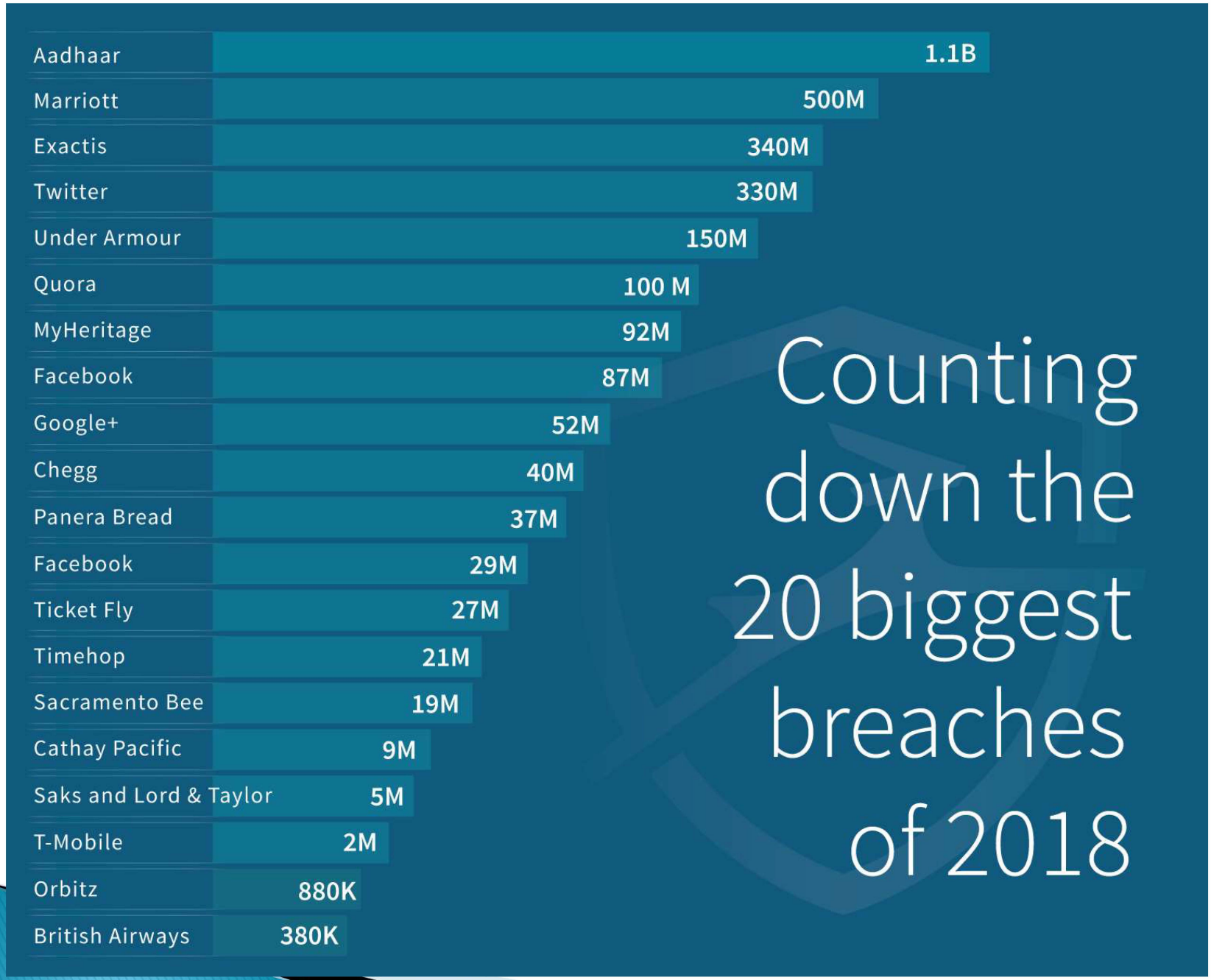
Cashing checks in NY, CT, and Florida. Victim lives in Florida.



How Does Digital Identity Theft Happen?

Data Breaches in 2018

Company	Breached	Content
Aadhar	1.1 Billion	Names, ID number, bank accounts, etc.
Marriott Starwood Hotels	500 Million	Phone, email, passport #, CC #
Exactis	340 Million	Phone, address, personal interests, character
State of SC Income Tax Records (2012 – everyone since 1998)		
Quora	100 Million	Names, email addresses, passwords, linked info
MyHeritage	92 Million	Email addresses, passwords

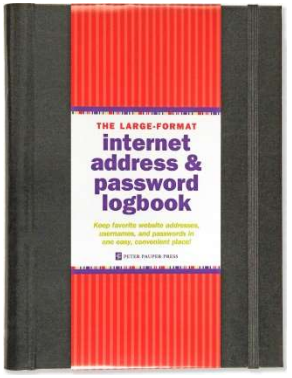

Aadhaar 1.1B
Marriott 500M
Exactis 340M
Twitter 330M
Under Armour 150M
Quora 100 M
MyHeritage 92M
Facebook 87M
Google+ 52M
Chegg 40M
Panera Bread 37M
Facebook 29M
Ticket Fly 27M
Timehop 21M
Sacramento Bee 19M
Cathay Pacific 9M
Saks and Lord & Taylor 5M
T-Mobile 2M
Orbitz 880K
British Airways 380K
Counting down the 20 biggest breaches of 2018

Preventing Identity Theft –Digital Actions

- Remember that every online service you have has a sign in requirement
  - **Username** which is your email address
  - **Password** which you select yourself
- Since you can be pretty sure that one of your accounts has been included in a major breach, **You <u>should not</u> use the same password on multiple accounts**!
- You **MUST** use an organized way to remember passwords – manual or automated or system like Last Pass
  - Password booklet from the computer club available at the Volunteer Table
- Enable Two Step Authorization on important accounts
- Consider Purchasing Identity Theft Insurance

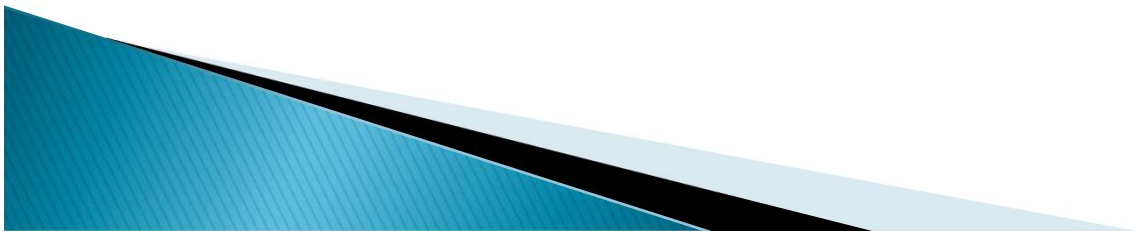
LastPass •••|

1Password



How Do I Know If It Has Happened To Me?

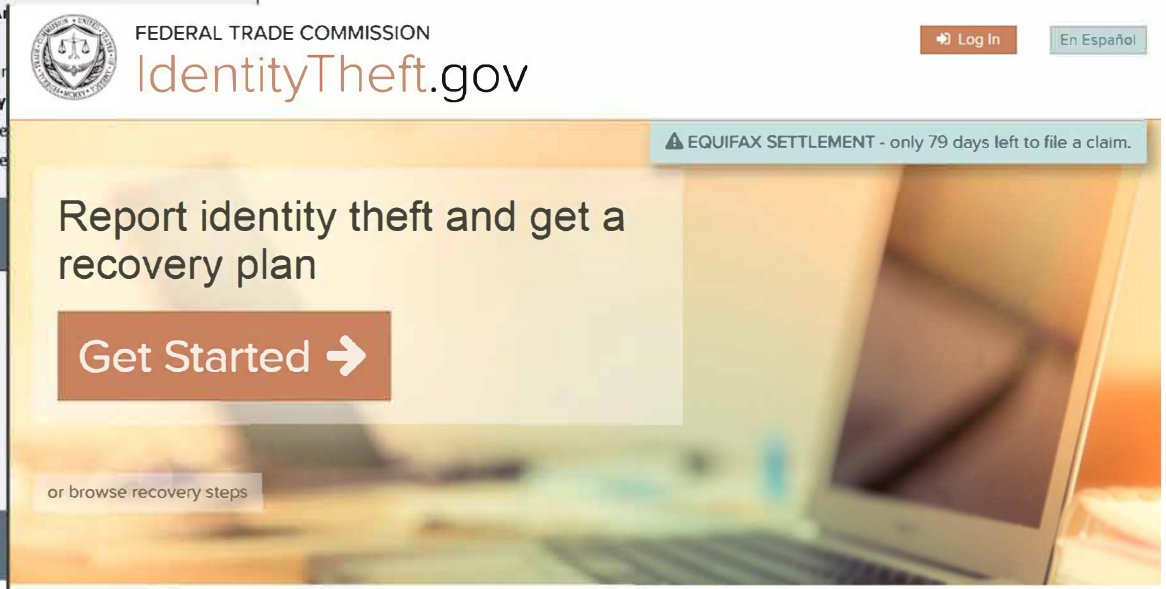
- Balance Your Bank Account
- Verify Your Credit Card Purchases
- Review Your Credit Report Quarterly
  - Loans or accounts you don't know about
  - Drop in credit score for unknown reason
- Take Immediate Action IF
  - Your mail is held or forwarded
  - You receive a statement or bill from an organization you don't do business with
  - Other indicators of financial activity you didn't initiate

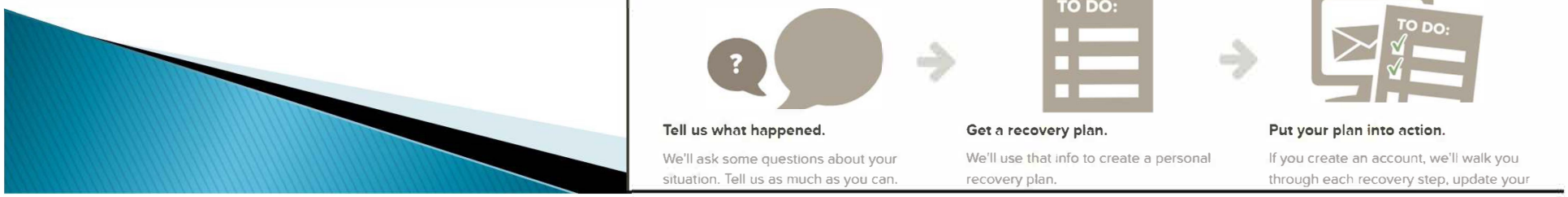


What Do I Do If It Happens To Me

- www.identityTheft.gov
  - Social Security Administration automatically notified.
  - WWW.IC3.gov
    FBI internet computer crime center
- File a Police Report
- Contact Your ID Protector
- Develop a Recovery Plan


Federal Bureau of Investigation
Internet Crime Complaint Center(IC3)
Home
File a Complaint
Press Room
News
About IC3
Filing a Complaint with the IC3
The IC3 accepts online Internet crime complaints from either the actual victim or from a third party to the complainant. We can best process your complaint if we receive accurate and complete information from you. Therefore, we request you provide the following information when filing a complaint:
Victim's name, address, telephone, and email
Financial transaction information (e.g., account information, transaction date and amount, who received the money)
Subject's name, address, telephone, email, website, and IP address
Specific details on how you were victimized
Email header(s)
Any other relevant information you believe is necessary to support your complaint
File a Complaint
Welcome to the IC3
Site Navigation
FAQs
Privacy


FEDERAL TRADE COMMISSION
IdentityTheft.gov
Log In
En Español
EQUIFAX SETTLEMENT - only 79 days left to file a claim.
Report identity theft and get a recovery plan
Get Started
or browse recovery steps


IdentityTheft.gov can help you report and recover from identity theft.
HERE'S HOW IT WORKS:
TO DO:
TO DO:
Tell us what happened.
We'll ask some questions about your situation. Tell us as much as you can.
Get a recovery plan.
We'll use that info to create a personal recovery plan.
Put your plan into action.
If you create an account, we'll walk you through each recovery step, update your

Cases in the Low Country of Elder Exploitation

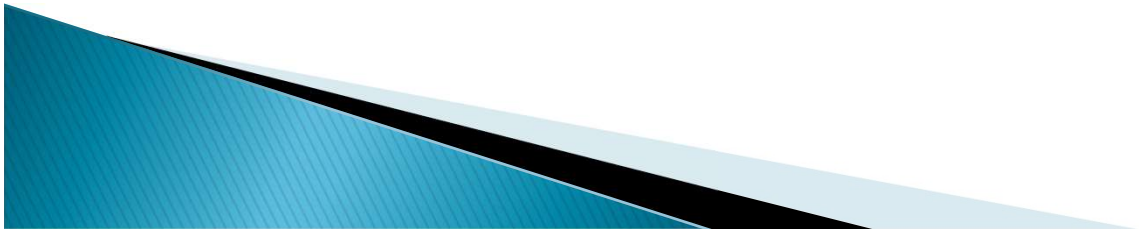
- Sun City Man with high medical bills
  Online Grant scam to cover bills. 70K

Bluffton Couple lottery scam
  received checks and sent money to Jamaica over 20K

Rose Hill Man thought he won Lottery sent money via mail for taxes over 100K.

Bluffton Man over 100k in sent in scam

Westbury Park
  Female victim of lottery scam, sent money and even obtained a reverse mortgage. Lost home



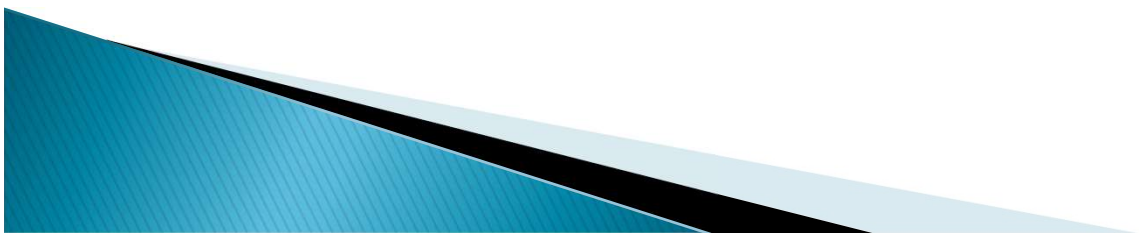
- Hilton Head Island
  - Dementia Patient with Stage 6 Alzheimer's new BF trying to get married. Went to Dr and Probate court.

Cypress marsh assisted living

92 Yr old male scam to lottery attempted to mail 30K. Bold new scheme Pizza Delivery

Spa at Port Royal

Mule sent checks throughout the world and wire transfers.

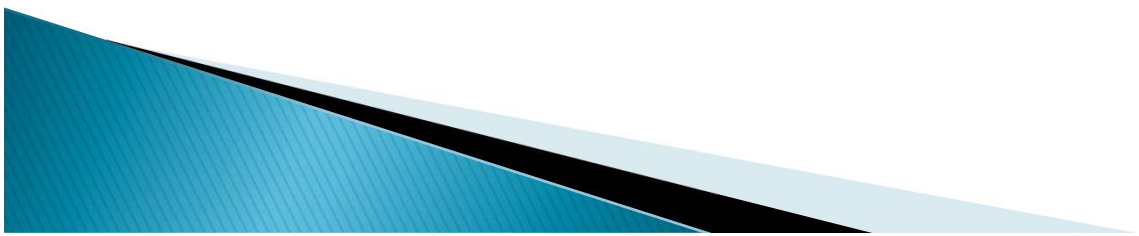


Green Dot Scam

- Green dot scam: IRS or Sherriff warrant for arrest

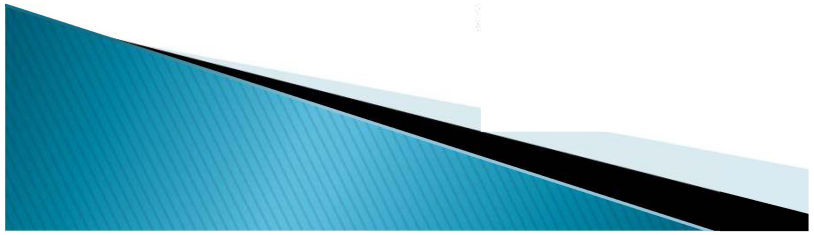
2015 thousand of dollars scammed out of the low country:

Follow the money and calls. Georgia Prisons. Gangs and guard involved. Arrests made



- **URGENT Green Dot card scam run from behind bars – Augusta to Aiken and ripping off**

  Oregonians : Feds allege Augusta prison inmate and his family ran a debit card like scam involved Green Dot cards



Construction Scams

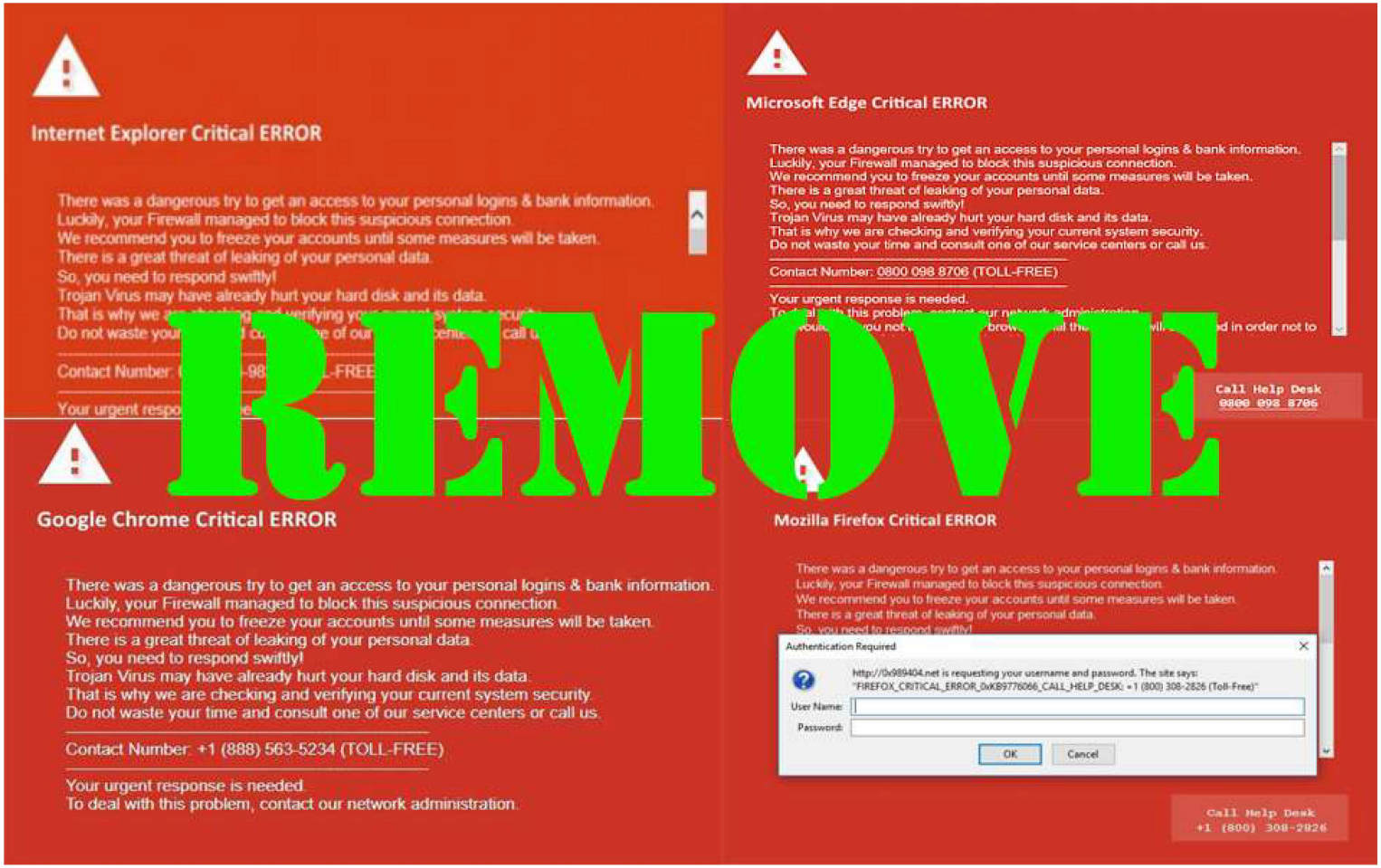
Contractor scams

- Check references
- Never pay total cost up front
- Check with the South Carolina Department of Labor, Licensing, and Regulation (SCDLLR)
- Make sure they obtain permits
- Use the internet to search the name of the company or owner
- https://llr.sc.gov/

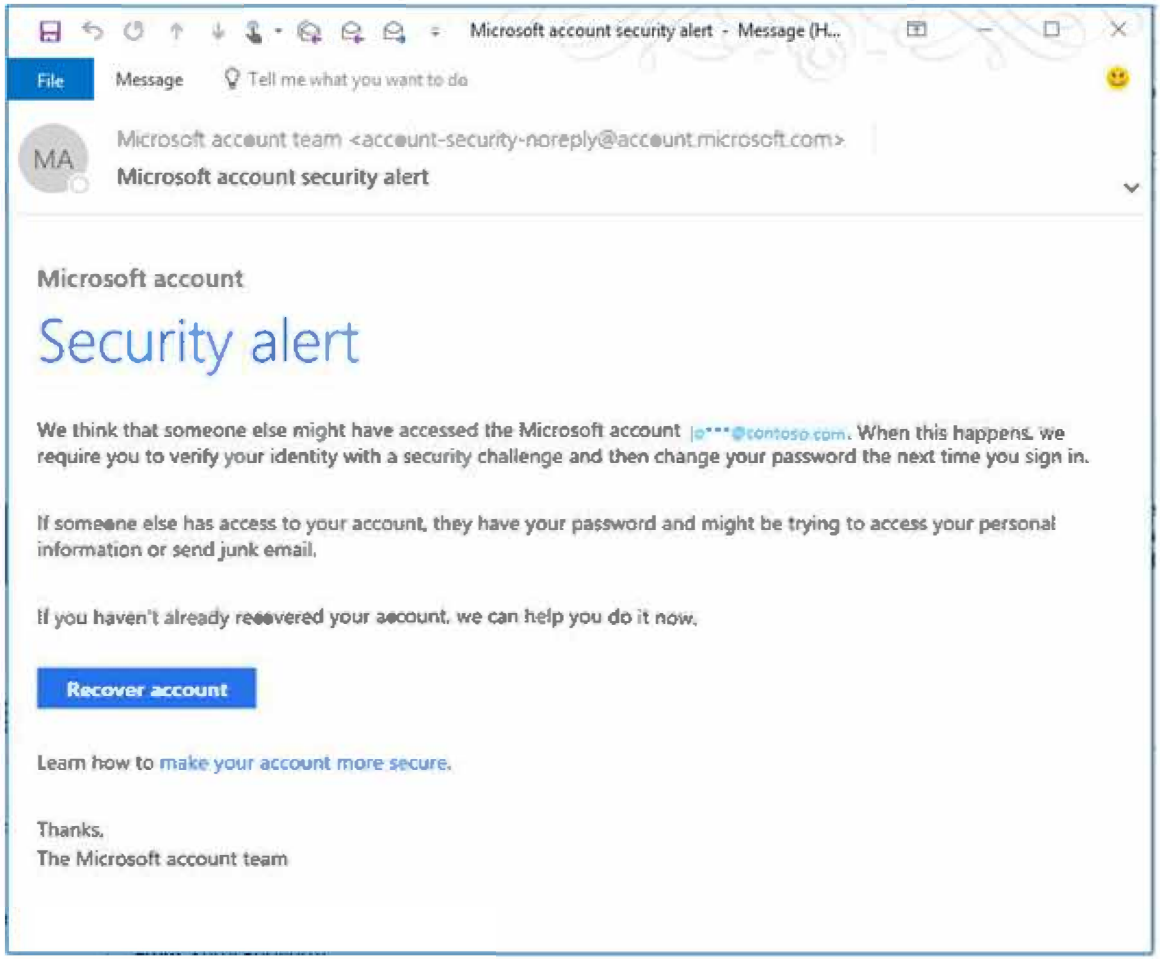
Romance Scam

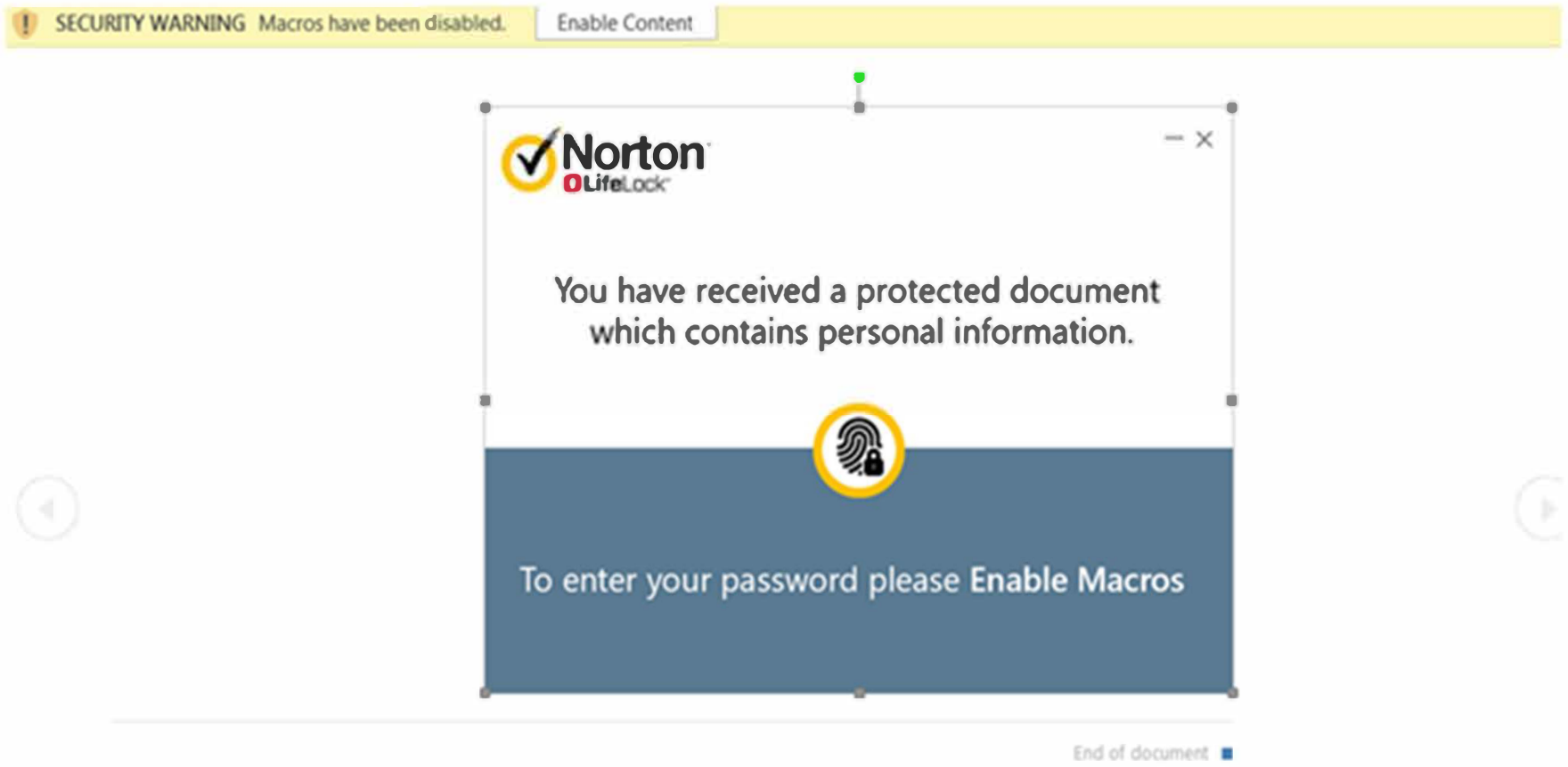
- Sun City
- For over 2 years lady was being scammed by “boyfriend”. Once the first scammer was identified as a fraudster, a “lawyer” calls the victim advising he knows the real “boyfriend” and he would love to meet her. Scam continues. Over 100K wire transferred. Reverse Mortgage obtained. Thought she was protected.

Computer Scams



Fake emails that appear legitimate




SECURITY WARNING Macros have been disabled.
Enable Content
Norton
LifeLock
You have received a protected document which contains personal information.
To enter your password please Enable Macros
End of document

Norton 360 LifeLock Scam Infects Inboxes With Malware

NATASHA DEENEY MARCH 6, 2020 CYBER SECURITY SCAMS

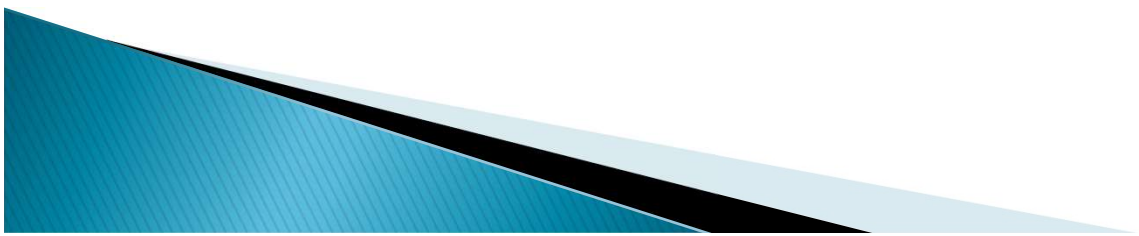
Cybercriminals have launched a clever Norton 360 LifeLock scam, which is disguised as a fake document, in order to trick victims into installing a remote access trojan (RAT).

RATs have the potential to cause significant damage. Their ability to remotely control PCs and capture screens, keystrokes, audio, and video makes them far more dangerous than typical viruses and worms.

The scam begins with a phishing email, which appears to be from the anti-virus and software security

Defending Yourself

- Defending yourself starts with acknowledging you or a loved one are a target. Be aware of the many different forms elder financial abuse can take including phone and email scams and bad actors within your social media circle. That can help you deflect attempts and spot issues before they have a substantial financial impact.



- Beaufort County Sheriff's Office

- Staff Sergeant Eric Calendine
  - ecalendine@bcgov.net
  - 843-255-3427