

# Phishing, Smishing, & Scamming...

**Let's Learn How to Prevent Fraud**



Presented By: Maureen Richard-Saltman

# Introduction & Welcome

**Maureen Richard-Saltman**

**Owner & Artist**

**Former “Fraud Fighter” for...**

**Nextel Communications 1995 - 2005**

*Sr. Operations Analyst, Credit Manager, Fraud Manager*

**Sprint 2005 - 2020**

*Risk Mitigation & National Fraud Prevention Manager*



***The Perfectly Imperfect  
Gift Shoppe***

30 Main Street, Topsfield, MA 01983  
[www.theperfectlyimperfectgiftshoppe.com](http://www.theperfectlyimperfectgiftshoppe.com)

**NEXTEL**

**Sprint**



# Fraud Statistics



The Federal Trade Commission (FTC) reported in 2022:

- ID theft scams were UP by 30% over 2021 with more than \$8.8B lost to fraudsters!
- Top Scams:
  - Investment Scams - \$3.8B
  - Imposter Scam - \$2.6B
  - Online Shopping, “Free” prizes, Sweepstakes, Lotteries, Job Opportunities, and more!
- The age group most frequently reporting ID Theft: 30-39 (26% of all reports to FTC.gov)
- The age group reporting the greatest dollar loss per scam: 40-49 (\$840M)

# Fraud Statistics

Identity theft type

**Most Commonly Reported Fraud:** Credit card

Other

Bank

Loan or lease

Employment or tax-related

Phone or utilities

Government documents or benefits



441,822

326,590

156,099

153,547

103,402

77,284

57,877

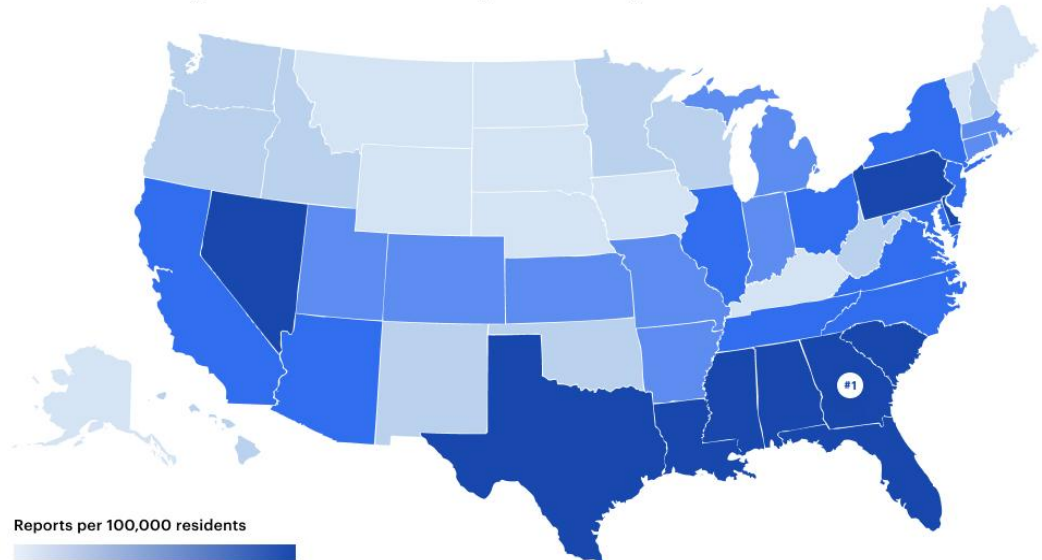
# Fraud Statistics

Consumer Affairs reports:

## ID Fraud Ranking by State (Top 5):

1. Georgia
2. Louisiana
3. Florida
4. Delaware
5. Nevada

## Reports of identity theft by state in 2022



## Driven by multiple factors including:

- Population
- Socio-economics
- Age
- Ethnicity.



# How Does Fraud Happen?

Many Ways!

We will focus on 3 of the primary methods used by fraudsters.



Then we will chat about how to protect ourselves against the common mistakes we make that make us vulnerable to fraud.



Phish·ing *noun*

The **fraudulent** practice of sending emails or other messages **purporting** to be from **reputable** companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

- Emails appear to be from legitimate businesses, medical offices, government agencies, friends, or banking institutions.
- Often ask for verification of personal information: address, DOB, SSN, credit card information, account number, password, user name.
- Might ask you to download software or a link to your computer.

**PHISHING**




**FAKE!**



service@amazon.com  
 Message: Need action signin from amazon service  
 To: maureen richard

Details ID : #FKOT-18082023



Your Amazon account has been put on hold, therefore any pending order, and subscriptions will be temporary on hold.

We took this action, because the billing information you provided did not match with the information of the card issuer data. which is **violating our terms of service**.

Please update your information as soon as possible so you can continue using your card with Amazon.

[Update Information](#)

In order to maintain the safety of your account, your account will be on hold until you fulfill the required forms.

You might want to do this sooner, any locked account will be deleted in order to protect the data from being leaked.

We hope to see you again soon,  
 Sincerely,  
 Amazon Team Support

no-reply@amazon.com

- ✓ noreplymail-qUNyCuRqu@lord.andrecestaroli.com.br
- Edit Address
- Remove Address
- Copy Address
- Add to VIPs
- Block Contact
- Add to Contacts
- Search for "service@amazon.com"

To: **no-reply@amazon.com**

**The REAL Amazon**

Subject: Re: Your Amazon.com order #112-8695067-7385051 has shipped

On Aug 17, 2023, at 7:31 PM, Amazon.com <shipment-tracking@amazon.com> wrote:



Hi Maureen, your package will arrive:  
**Friday, August 18**

[Track package](#)

help@amazon.com <noreplymail-tlntsgu@pt.mibspirit...> Inbox - Msn August 10, 2023 at 6:57 PM

An important Message: Account Locked [#Case ID-708849945619]

To: maureen richard

Electronic-Message ID 169517801279884 Document-Signat...20.doc



**Don't Fall for the Download!**





Smish·ing *noun*

The **fraudulent** practice of sending text messages **purporting** to be from **reputable** companies in order to induce individuals to reveal personal information, such as passwords or credit card numbers.

Not restricted to pretending to be businesses.

- Can pretend to be someone on Facebook or Instagram DM pretending to be someone you know using an account that's already been hacked.
- Could ask for credit card or other information under guise of friendship or help in an emergency situation (see "Scamming").

# SMISHING



Text Message  
Today 8:55 AM

█, urgent notification regarding the USPS delivery S46K5 from 04/04/2020. Go to: [m9sxx.info/lbJOnVq6Ft](http://m9sxx.info/lbJOnVq6Ft)

4:55

+1 (646) 706-3017

Text Message  
Mon, Aug 24, 10:04 PM

Walter, we came across a package from February owed to you. Kindly assume ownership and confirm for delivery here: [1ismc.info/i4B8uioBPO](http://1ismc.info/i4B8uioBPO)

8:38 PM 48%

+1 (951) 314-1717

Text Message  
Today 8:38 PM

Congrats Kelli! Your code L6R-K8X7 printed on your last receipt is among 7 we randomly picked for \$1000 Walmart gift card promotion [k3xvc.info/p/1Llr3N5GNM](http://k3xvc.info/p/1Llr3N5GNM)

From Google Security: We have detected a rogue sign-in to your [goodguy@gmail.com](mailto:goodguy@gmail.com) account credentials. In order to determine the legitimate login we're going to send a verification code to your previously registered phone number from another Google support number. Please re-type the sent verification code in response to this message or your account will be permanently locked.

954327

Sent

Text Message  
Today 08:58

We have identified some unusual activity on your online banking. Please log in via <http://bit.do/dq3WJ> to secure your account.

Messages Facebooksupport Details

Your Facebook account has been suspended. Contact us now to unlock it now. Go to [www.█.com](http://www.█.com)

Today 07:25

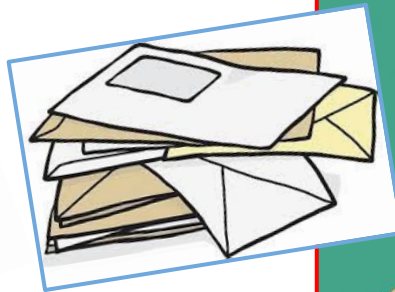
Your Santander Bank Account has been blocked. All services have been withdrawn. Go to <http://santander.onlineupdatesecures.he.net.pk> to reactivate now.

1 (410) 200-500

Text Message  
Today 1:54 PM

FRM: [18443693848](tel:18443693848)  
MSG: Your card has been put on hold. CALL now free : [1-844-369-3848](tel:1-844-369-3848) and follow instructions to resolve this issue.

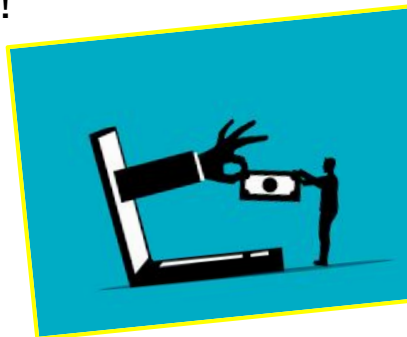
# SCAMMING



## Scam noun

: a fraudulent or deceptive act or operation

- LOTS of scams happening ALL the time!
- Social media.
- Telephone.
- Email.
- USPS.



# SCAMMING

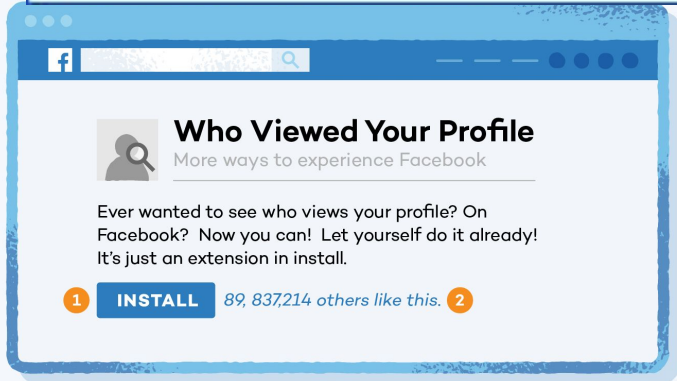


12:40

From Saturday morning facebook will become chargeable. If you have at least 10 contacts send them this message. In this way we will see that you are an avid user and your logo will become blue (🔵) and will remain free. (As discussed in the paper today. Facebook will cost 0.01ps per message. Send this message to 10 people. When you do the light will turn blue otherwise facebook will activate billing.

Melanie Sue · 2h · 🧑

Hello,my family is planning on moving out soon, and we are finding it difficult to move all our items with us. We have thus decided to dispose of the items below but at less prices. Incase anyone is interested, please p.m me. Thank you



- 1 Requires installation
- 2 Large number of strangers like the app

# SCAMMING



Call. Dad someone has kidnapped brie

brie picked up and she's fine

she's calling you

she's fine for now at least idk what that ransom thing was about

Fri, Jan 20 at 7:22 PM

Listen, he was kidnapped by myself and my men and i demand a ransom payment of \$7,000 before i release him back to you alive. You are warned not to tell anyone or the Cops about this Or HE DIES. Do not act smart.

Is he okay

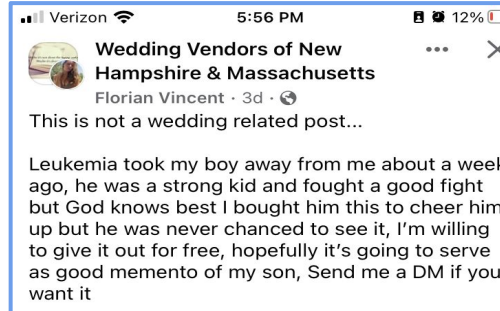
Your fast response is needed

## Facebook Romance Scammers



For sale or swap or for free holywell, Flint and Mold

Hello. If anyone is looking for this sweet boy, found him lying on the side road in #Holywell He was hit by a car in a hit and run incident. I took him to the ve... See more

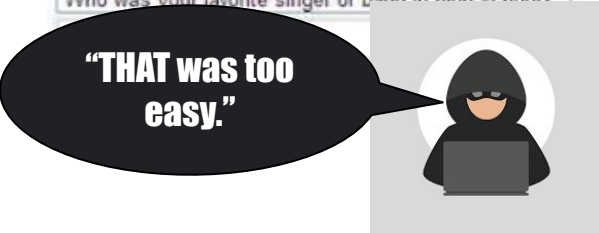
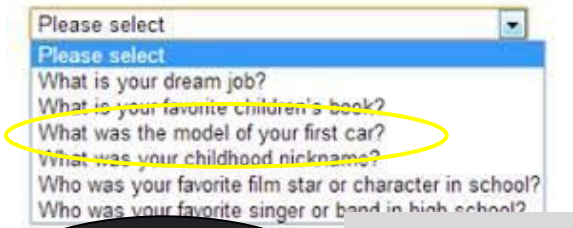
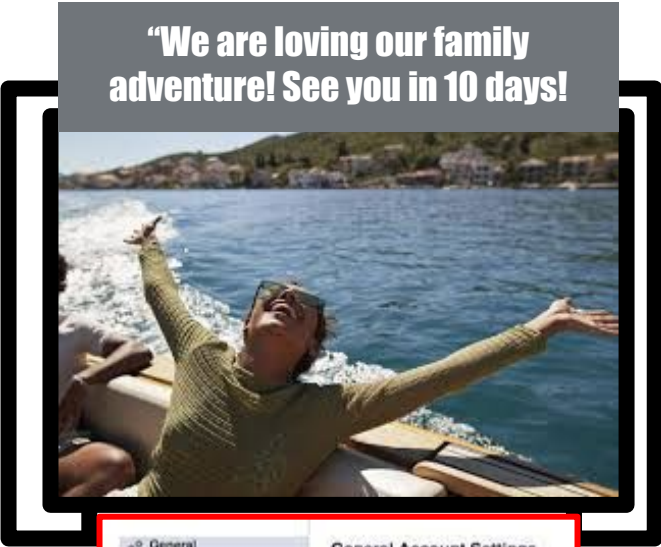


# THE HEART-STRINGS SCAMS

# Social Media



The #1 song on May 4, 1977  
**Hotel California**  
By Eagles



**THE ONLY ONES THAT CARE TO KNOW THAT  
INFORMATION ARE...**

**SCAMMERS!**



# Telephone

**2am Call:**

**“Grampy! It’s Annie I got in an accident and they won’t tow my car. I don’t have any money. I’m stuck. I need help. OMG! I’m so scared! I’m so sorry. {crying} I need to give these guys a credit card or something. I don’t have one. OMG! They won’t let me leave. Please don’t call Mom & Dad....”**

**This is National Grid. Your service is about to be shut-off. Our crew is on route to your location now. This is your last opportunity to pay the balance due. I need your account number and a credit card to process the balance of \$350.00.**

**This is the IRS. You are being immediately audited for unpaid taxes. If you don’t pay today, you will be arrested for unpaid IRS debt. You must remit the full payment over the phone.**



**“Hello. We are pleased to let you know that your doctor has approved your knee brace. We just need to process your paperwork to get it shipped to you. Would you please provide your Medicare number to us for confirmation. Also your credit card for shipping costs that Medicare doesn’t cover. Also please confirm your DOB and address. Thank you.**



# Email

Exclusively for: | VALUED CUSTOMER  
Online Banking



## Your Bank of America accounts has been locked!

There are a number of invalid login attempts on your account. We had to believe that, there might be some security problems on your account. So we have decided to put an extra verification process to ensure your identity and your account security.



Please [click here](#) to continue the verification process and ensure your account security.

### Email Preferences

This is a service email. If you receive a suspicious email with a link to update your account information, do not click on the link—instead, report the email to Amazon for investigation.

Dear Sir,  
I am prince [redacted] from Nigeria. Your help would be very appreciated. I want to transfer all of my fortune outside of Nigeria due to a frozen account. If you could be so kind and transfer small sum of 3 500 USD to my account, I would be able to unfreeze my account and transfer my money outside of Nigeria. To repay your kindness, I will send 1 000 000 USD to your account.

Please contact me to provide more details.

Prince [redacted]

Amazon <ofvial@amazon.com>  
November 24, 2017 at 12:39 PM  
Alert  
To:  
Reply-To: Amazon <ofvial@amazon.com>

**amazon** Password assistance

Someone tried to reset your password from Dayton, Ohio, if you have not requested this code  
Please Call Us on 1-800-801-5811  
Please provide below mentioned code with your Email address to verify

**161145**

Amazon takes your account security very seriously. Amazon will never ask you to disclose or verify your Amazon password, credit card, or banking account number. If you receive a suspicious email with a link to update your account information, do not click on the link—instead, report the email to Amazon for investigation.



Michael Neu was charged with 269 counts of wire fraud and money laundering.

**They do this all day , every day.  
They aren't regulated.  
They don't care about "DO NOT CALL" registries.  
They bypass your "Junk" email filters.  
They WANT you to let your guard down because that's when you make mistakes. They make \$\$\$.**



# What Can You Do?



- Do NOT respond directly to unsolicited emails that are sent to you.
  - Always go to the source's verifiable website.
- Don't shop on sites that aren't secure.
  - Use sites that have "https" - the "S" means "SECURE".
  - If it's not a secure site, use a "throw-away" password, not one that you use normally.
- Always use a credit card, as opposed to a debit card when making online purchases.
  - This is also a good rule when paying anyplace that your card leaves your possession (restaurant, bar, etc.).
  - You have more protection from your credit card company AND it's their money! They'll WANT to get it back.
- NEVER give out information to unsolicited callers or via emails.
- Use COMMON SENSE! If it seems too good to be true, then it probably is!

## What Can You Do?



Use passwords that aren't easy to guess.

- Don't use the same passwords for ALL of your important sites (banking, credit cards, social media).
- Use alpha-numeric and symbols when possible.

We ALL love our pets, but don't use their names as your passwords.

- How many times have you posted your pet's name on your social media??

Choose Security Questions & Answers that aren't easy to guess.

- If the SQA asks what was your "first car", answer can be "red mustang".

## What Can You Do?



Don't take action on a text without calling the business/bank directly or going directly to their website.

- “Spoofing” of telephone numbers is a real thing. Don't be fooled.

Never assume that the person on the other end of the text is legitimate.

- ALWAYS go to the source! See above.

Again...Use your COMMON SENSE! If it seems too good to be true OR if it would be strange for the business/bank to be contacting you using that method of communication, then it's probably **FRAUD**.

## What Can You Do?



Don't fall for the phishing scams on social media. Think first!

- Many of these “fun” social media quizzes funnel back to China, Russia, N. Korea, and other countries that farm your data.
- Artificial Intelligence can use your image, voice, and other attributes to defraud you. (example: The popular “Here’s what you’ll look like in 40 years”)
- Know who you’re sharing your information with on social media.
- Check your privacy settings to make sure that you are only sharing with your friends list and that your posts are not open to the public.

# What Can You Do?



**Be careful of what you're sharing in your photos too.**

- ★ **First Day of School Photos**
  - Child's Name, Age, School, Grade, & Teacher. **\*\*\*NO!!!!**
  - If you haven't checked your privacy settings OR if you're sharing with friends/family who haven't got their privacy settings tightened, then your child's information is now PUBLIC!
  - Keep it simple!



## What Can You Do?



Fraudsters Need You to Act Fast! It's All About Pressure!

- Take a minute. Think. Don't allow them to pull the strings!
- If it's a fake utility shut-off call, tell them that you'll check your invoices and call them back.
- Hang-up and call the utility company or go online to check your account status.
- The IRS is NEVER going to call you to demand that you pay your taxes.
- They will send you notification by mail. You can check it on your IRS.gov account to verify it.

## What Can You Do?



If you receive a late night call from a relative for an “emergency” situation, take their information - Where are you located? What number are you on? Who are you with? What do you need?

- Write down the information.
- Call your local police department and provide them with this information ASAP.
- Let them check out the situation.
- You should NOT be handling this yourself.
- This is one of the most commonly reported forms of financial fraud committed against the elderly. It’s often reported by banks or places that sell money orders.





## What Can You Do?



### Lonely Hearts...

- Meeting people online is fine, but not if they are asking you for money.
- Don't allow your heart to permit a scammer to empty your bank account.
- Love doesn't cost \$\$\$ no matter the excuses.

### Heart-String Scammers...

- There are many wonderful agencies and rescues out there that assist people with caring for injured animals.
- There's no need for someone to keep an injured stray at their home and request money from YOU. It's a SCAM.

## What Can You Do?



### Heart-String Scammers...(continued)

- If you had a child that just passed-away, would you be giving-away their items on FB? Probably not. This is a scam.
- You will start a DM with this person. They will tug on your heart-strings and eventually the subject of money will be raised. They are a scammer.

### The “I’m Selling Everything” Scammer”...

- How many rooms can this person possibly have in their dwelling?
- All high end furniture, appliances, yard equipment, etc.
- SCAM! SCAM! SCAM! They’ll take your money and RUN!

## What Can You Do?

Report ALL of them to the admins for the social media platform EVERY single time that you encounter them!

Yes, it's like "Whack-A-Mole", but you'll help to stop them that one time.



# Your Best Source for Help...



FEDERAL TRADE COMMISSION  
PROTECTING AMERICA'S CONSUMERS



## Fair Credit Reporting Act

Do you use credit reports to make eligibility decisions about consumers?  
Learn about the Fair Credit Reporting Act and how to responsibly use, report  
and dispose of information in those reports.

Learn More

The Federal Trade Commission!

[www.ftc.gov](http://www.ftc.gov)

- Information on consumer rights
- Information on The Fair Credit reporting Act
- Get your FREE Credit Report
- File information to report fraud attempts or if you've been a victim of fraud
- It's FREE. Don't PAY for help until you utilize what's available here first!



FEDERAL TRADE COMMISSION  
PROTECTING AMERICA'S CONSUMERS

# Your Best Source for Help...

reportfraud.ftc.gov/#/assistant

Start  Submit FTC's Cl

### Is your report about any of these common problems?

Choose the best fit. If you don't see your problem, choose "Something else."

|   |  |
|---|--|
| <input type="radio"/> An impersonator<br>(ex. fake government, business, love interest, grandchild) | <input type="radio"/> Online shopping  |
| <input type="radio"/> Job, investment, money-making opportunity, franchise                          | <input type="radio"/> Sweepstakes, prize, lottery  |
| <input type="radio"/> Phone, internet, TV service   | <input type="radio"/> Auto sale, repair  |
| <input type="radio"/> Health<br>(ex. weight loss, eye care, treatment)                              | <input type="radio"/> Credit, debt, loan<br>(ex. debt collection, credit report, student loan debt relief) |
| <input type="radio"/> Just an annoying call   | <input type="radio"/> Something else<br>(we'll get it to the right place)                                  |

reportfraud.ftc.gov/#/form/main

### Report details

Please share as much as you know. The details help law enforcement investigations.

Did you send the scammer payment of any kind?  Yes  No

How much money did you pay the scammer in total? \$

How did you pay or send the money?

When did you most recently pay or send money (mm/dd/yyyy)?

How did you first learn about the scam?

There is A LOT of information here to assist you. It's FREE!

# Wrapping-Up

- Fraud is NEVER going to go away.
- Use COMMON SENSE.
- If it seems too good to be true, it probably is!
- STOP. THINK. GO TO THE SOURCE.
- Maintain good passwords.
- Maintain good privacy settings on social media.
- Don't be afraid to report fraud if you've been a victim (it's an under-reported crime).
- Use credit cards, NOT debit cards for online and out-of-possession purchases.
- I'm here if you need me. You know where to find me.



**THANK YOU!**