Anatomy of a Scam

How to Spot the Red Flags

Howard County Office of Consumer Protection
Department of Community Resources and Services

1

WHAT WE DO

- Handle disputes between merchants and consumers & between landlords and tenant
- Provide consumer specialists by phone or in person
- Enforce the County's consumer protection laws
- Education and Outreach to the Community
- License and Regulate certain businesses

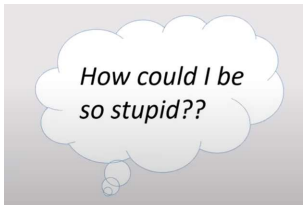
HOWARD COUNTY OFFICE OF CONSUMER PROTECTION

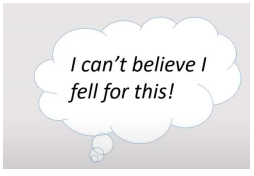
2

SCAM STATISTICS

- 2019 World Economic Forum Report on Cybercrime: 0.05% caught
- 2021: Americans field about 5B spam calls *per month;* 25% of all reported losses started on social media; online fraud tripled. Business imposter scams up 134%, investment scams up 213%, government imposter scams up 109%
- 2023: 23% of Americans lost $159B to scams.

3





Survivors of Crime not Dupes or Victims

- Violent or Property Crimes
  - Oh that poor family!
  - Bring them food
- Financial Crimes
  - You'd have to be an idiot
  - How'd you fall for that?
  - How much money did you *give* them?

4

WHO'S TYPICALLY TARGETED?

Seniors have historically been targeted because:

- Seniors have a "nest egg"
- Seniors were raised to be polite and trusting
- Seniors are less likely to report a fraud
- Seniors are more likely to live alone

"Millennials" and Gen Z are increasing fraud target because:

- Too comfortable online
- Trust websites too easily
- Lack of financial literacy education in formative years

5

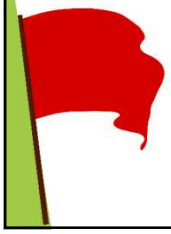
How Scams Work

- Scammers are looking to separate you from your money or your personal information. They try to exploit your fears and emotions so you will act before you think.

6

Imposter Scams

- Most scams are called "imposter scams." The scammer will assume the identity of others to gain your trust, create a sense of urgency and/or exert authority.
- For example, a scammer will pretend to be an IRS agent, a bank, a major corporation, or even a friend.



7

Phishing

- Phishing refers to emails that claim to be from your bank, a reputable business or charity.
- You are told information is needed to "verify your account" or to protect you from fraud.
- The email provides a link to a legitimate looking site where you are told to enter the information.
- The email asks for personal information, such as your Social Security number, and bank account number.

8

Phishing Red Flags

- Check out the email address of the sender – is it from the actual business it says it's from or it is from somewhere unrecognizable?
- How is the email addressed – to your email name or to you personally?
- Is the email grammatically correct, or does it sound suspicious?
- Does it give a link asking for your SSN and other personal information?

9

FWD: USPS Parcel Recovery

USPS <chandler.007@hotmail.com>

Fri 1/29/2021 9:57 AM

To:

Hi (email address)

Due to a lack of complete address information, we have been unable to deliver your parcel 1700800752215642*

Currently your parcel is being stored in our local depot,

RESCHEDULE DELIVERY

10

10

You must pay immediately

- For example, the IRS scam.
- The caller claims to be from the IRS and tells you that you owe money for back taxes.
- Caller threatens that if you don't pay up immediately, you'll be arrested or deported.
- You will be told to send your money to the caller, not the IRS.

11

Don't tell anyone!

- The grandparent scam is a good example.
- The caller poses as a loved-one, police officer or ER nurse.
- You are told that your loved-one has been arrested, mugged, or injured, often while outside of the country.
- You are asked not to call parents or others because they are embarrassed or "will get in trouble."
- Only by wiring money or sending pre-paid card will the person get out of trouble.

12

I Need You to Buy A Gift Card

- You get an email from a friend, boss or religious leader, asking for help.
- The email instructs you to buy a certain amount of gift cards and then respond to the number in the email.
- You later find out the email account was hacked and the scammers have the money you spent on gift cards.

13

13

Its your lucky day!

- The check that just arrives in your mail.
- A letter informs you have won a sweepstakes or lottery (that you never entered).
- The letter includes a check to cover your “taxes and fees,” which must be paid immediately by wire transfer or money card, before you can get your winnings.
- You later find out that the check is no good, but there’s no way to get back the money you paid.
- Any check that comes unannounced and requires you to send back money is a scam!

14

Tech Scams

- Caller claims to be from Microsoft and says that during routine monitoring they noticed that your computer has a problem that will lead to a crash or security breach.
- Caller requests remote access to your computer to fix the problem.
- Once the scammer has access, s/he can download all information stored on the computer, i.e. bank records, tax information.
- Remember: Computer manufacturers are unable to monitor your computer.

15

Sales Scams

- You are contacted by a well-known company such as Amazon, Apple, or Best Buy's Geek Squad
- You are told a purchase was made in your name, on your account, or have agreed to a service plan, and are asked to verify, or let them know if you did not make it.
- As you did not agree to or make the purchase, you click on the link provided, or if it's a caller, you give access to your computer to the caller to fix the problem.

16

16

I just happen to be in your neighborhood

- Tree Service Scam – a solicitor comes to your door claiming that your trees are infested with pests or disease, and even shows you a "sample." He offers to fix the problem before it spreads.
- Driveway Paving Scam – a solicitor states he can give you a reduced rate to seal your driveway because he has left over sealant. The sealant turns out to be oil paint that runs off in the next rain.
- In both cases, the claims are untrue, the cost is high, and the work is inferior.

17

Solicitor's Must Be Licensed

- Check to see if the solicitor is licensed by the Howard County Office of Consumer Protection

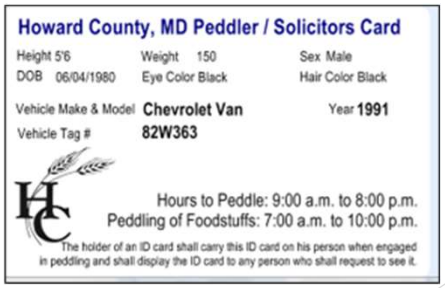

Howard County MD Peddler / Solicitors Card

Registration No. #D-1356 Expiration Date: 06/30/2015

Card Holder Curtis Dorsey
1032 St Michaels Rd TEL 301-781-2391
Mt Airy MD 21721

Business Smokey Meadows Grill
1032 St Michaels Rd TEL 301-787-2391
Mt Airy MD 21771

This ID Card has been issued by the Howard County Office of Consumer Affairs 410-313-6420
Possession of this ID does not constitute endorsement by the County.


Howard County, MD Peddler / Solicitors Card

Height 5'6 Weight 150 Sex Male
DOB 06/04/1980 Eye Color Black Hair Color Black

Vehicle Make & Model Chevrolet Van Year 1991
Vehicle Tag # 82W363

Hours to Peddle: 9:00 a.m. to 8:00 p.m.
Peddling of Foodstuffs: 7:00 a.m. to 10:00 p.m.

The holder of an ID card shall carry this ID card on his person when engaged in peddling and shall display the ID card to any person who shall request to see it.

18

18

Common Scams Targeting Veterans

Military Romance Scams

- Here's how military romance scams typically work:

1. Fraudsters create fake profiles on dating apps, websites, and social media. They'll use real photos and research real service members to create a believable persona.
2. Next, they identify vulnerable targets. The usual victims are people who show support for the military either through their profiles or by joining Facebook groups or donating to veterans charities.
3. Once you're in an online relationship, they escalate quickly. Scammers will "love bomb" their victims or even propose in a matter of weeks. Many scammers operate as groups and share scripts and formulas that pull on your emotions and cloud your judgment.
4. Once you're hooked, they ask for favors. This could be in the form of money, gift cards, or sensitive information they can use for identity theft and extortion.
5. When you realize they're a scammer, they disappear. You're left embarrassed and out the money they stole from you.

19

More Military Related Scams

1. Phishing scams from fake government agencies
2. Charging for free military records
3. Investment and military pension fraud
4. Offering "secret" government funding
5. Demanding security deposits on veteran-discounted properties
6. Posing as veteran-friendly employers and schools
7. Targeting veterans getting benefits under the PACT Act

20

VA Related Scams

- Veterans and their benefits are the target of many types of fraud. Here are some tips about being contacted by the VA:
  - VA will never charge you for processing a claim
  - VA will never ask you for your personal information via email.
  - VA will not threaten claimants with jail or lawsuits.
  - VA may check in with you by phone, email or text. If you are unsure about any contact, confirm details with VA directly at 1-800-827-1000.

21

21

Strategies to Safeguard Yourself

Take your time.

When talking to someone you don't know, always take a break before agreeing to anything. Hang up, talk to someone else about the offer.

Never click on links that are from a sending you don't know; or fill out forms that come with an attachment.

Any offer that is legitimate will be available later.

22


Strategies to Safeguard Yourself
Verify that the caller is from the organization they claim to be from.
Never wire money, or send prepaid cards or gifts cards to people you don't know. No legitimate business will ask for payment this way.
When buying on-line, look for the https to show that it is a secure website
Don't give out your personal information to someone you don't know or reply to emails or open attachments.
If it sounds too good to be true, it is too good to be true.

23


For more information on scams or other consumer topics, please contact:
Howard County
Office of Consumer Protection
410-313-6420
Consumer@howardcountymd.gov
www.howardcountymd.gov/consumer

24