SCAMS COMING TO YOU!

HOWARD COUNTY OFFICE OF CONSUMER PROTECTION

CONSUMER@HOWARDCOUNTYMD.GOV

(410) 313-6420
WHAT WE DO

• Handle disputes between merchants and consumers & between landlords and tenants
• Provide consumer specialists by phone or in-person
• Enforce the County’s consumer protection law
• Education and Outreach to the Community
• License and Regulate certain businesses
STATISTICS

• 2019 World Economic Forum Report on Cybercrime: 0.05% caught

• In 2019, estimate 50% of all calls to cell phones are from robocallers.

• In 2020, econsumer.gov had 60,835 reports of international scams, with reported losses exceeding $211.6 million.

• In 2021, FTC received 2.8M fraud reports, losses more than $2.3B

• Americans field about 5B spam calls per month
  • 40% drop in April/May 2020 due to pandemic (empty call centers)

• In 2021, 25% of all reported losses started on social media.
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” are a rapidly increasing fraud target because:
• Too comfortable online
• Trust websites too easily
• Lack of financial literacy education in formative years
WHO’S TARGETTED TODAY? #Scamdemic
Common Scams

- Medicare ID theft
- Invest in bogus cures & preventatives
- Imposter Scams
- Work-from-home scams
- Grandparent Scams
- VA Benefits
- Funeral / Cemetery
- Financial Exploitation
- Woodchucks
- SSN "inactivation"
- Mortgage assistance fraud
- PEPCO Cut-off Notices
Overconfidence Bias

71% CLAIM THEY CAN SPOT SCAMS

69% DIDN'T SPOT THE SCAM

[Graph showing the confidence levels of individuals in identifying scams]

[Pie chart showing the reasons for not identifying scams]

Greed (14%) and "Taking a Gamble" (17%) play a minor role.
TELEPHONE
SCAMS
JUST HANG UP!
$30B lost to phone scams in 2021

Average Money Lost to Scam Calls
(Among those who were affected)

Source: Truecaller Insights/Harris Poll
Who’s at Risk?

Scam Victims by Gender and Age Bracket in the past 12 months

- 18-34: 31% Female, 40% Male
- 35-44: 25% Female, 46% Male
- 45-54: 12% Female, 28% Male
- 55-64: 13% Female, 16% Male
- 65+: 3% Female, 10% Male

Source: Truecaller Insights/Harris Poll
KNOW THE TRICKS

• Spoofing/Cloning
  • With VoIP, callers can disguise their true number
  • Calls from IRS, Sherriff’s Office, PEPCO, bank, your neighborhood
  • Hide: private, unavailable or unknown

• Turn off your brain, turn on your emotions
  • Phantom riches
  • Source credibility
  • Social consensus
  • Reciprocity
  • Scarcity
  • Fear
AVOIDANCE TIPS: Trust your instincts!

• Screen your calls
  • If you don’t recognize the number, let the voicemail or machine pick up
  • Beware of cloned telephone numbers
  • Report to FTC and FCC

• Just hang up!
  • Empty air = machine calling you.
  • Hang up as soon as you know it’s a solicitation, a threat, or possible harassment
    • Remember IT support never called you when there was a problem.

• Don’t close the deal
  • If you haven’t hung up yet and you think this might be legitimate, hang up and call back on a number you had before the call.
  • Do your own research. No offer is truly off the table if it came to you.
  • Avoid saying “yes” because they could record your voice and “slam” you
WHAT IS IDENTITY THEFT?

- Identity theft happens when somebody steals your personal information and then USES IT without your permission.
- It’s just the opposite of a Power-of Attorney
- Identity theft can disrupt your finances, medical care, credit history and take substantial time and money to resolve.
Don’t Overshare!

- Grocery Stores
- Work
- Restaurants
- Gas Station
- Online
- Doctor’s Office
- Pharmacy
- School

Who or Where?
Phishing, Smishing Vishing, & Hacking

Phishing: Phony + Fishing
- You give access through emails
- Charity, “sextortion” & tech support schemes

Smishing: SMS + Fishing
- You give access through text and social media messaging
- ~88B spam texts, $10B in losses (Robokiller 2021)
- STIR/SHAKEN not working

Vishing: Voice + Fishing
- You give access through phone engagement
- 72B spam calls, $30B in losses (Robokiller 2021)
- Google Voice verification scam

Hacking: Misuse of system to steal data
- Access is taken without your permission
Trojans, Malware and Bots Oh My!

**Trojans**: innocent looking programs which launch other programs like...

**Virus**: code injected into programs causing malfunction and spread

**Spyware**: watches actions, keystrokes and searches for PII and reports back.

**Ransomware**: pop-up on your screen, preventing any further access to your device until you pay for the unlocking key.

**Netbot**: spam and malware-infected emails, or use infected links on web pages, to recruit your computer into an automated network to do their dirty work

**Worms**: worms copy themselves over and over again, spreading across your home network and attaching themselves to messages you send out

**Root kits**: programs that bury deep into your system, hard to remove

**Subscription Bombs**: hiding new account notices in a blizzard of emails
Deter

- Shred documents: cross-, micro-, or diamond-cut shredder
- Protect your information
  - Don’t carry your SSN card
  - Keep security software updated
  - Passcode your smartphone (biometrics or numerical)
- Don’t give out personal data
  - Especially to unsolicited messages
- Beware of unsolicited emails
  - Before you link, stop and think!
  - Don’t download anything unknown to your computer
- Passphrases with symbols and numbers (12 characters)
  - IL0v3Kumqu@t$ (I love kumquats)
  - Use different passphrases for each account
  - Password manager
- Don’t put checks or gift cards in the mail
  - Check washing/mail theft
- Use strong passwords w/ Wi-Fi and WPA2 encryption
  - Use public Wi-Fi with VPN only
- Forward smish to 7726
QR Codes

- Restaurant Menus
- Payment Apps
- Company websites
- Package tracking

Risks:
- QR code takes you to a phishing website, where you are prompted to enter your personal information or login credentials for scammers to steal.
- Con artists use QR codes to automatically launch payment apps or follow a malicious social media account.

Tips: check for layered sticker, don’t open links sent by strangers, use QR app with additional security
Payment Options

- **Credit Cards**
  - not linked to a bank account
  - build credit
  - legal protections of the Fair Credit Billing Act
    - Chip safest from skimmers
    - Tap does not transmit name, card number or 3-digit security

- **Debit Cards**
  - linked to a bank account
  - no protection under the Fair Credit Billing Act
  - some protection under the Electronic Fund Transfer Act

- **Money Transfer Services** – Western Union and MoneyGram
  - Escrow/Earnest Money Scams

- **Mobile Pay (P2P)** – PayPal, Venmo, Zelle, Apple Pay, CashApp, etc.
  - App linked to a bank account or card
  - Transactions treated like cash
  - No statutory protections
  - Potential for malware to infect
  - Privacy and security concerns

- **Buy Now, Pay Later**
  - FCBA/EFTA does not apply
Peer-to-Peer (P2P) Payment Apps

Quick Facts

→ Designed to be a quick and easy way to give money to someone you know

→ Not recommended for online shopping and should not be used to accept/send payment to people you don’t know or trust

→ Managed by third-party companies (e.g. not your bank who may be advertising them)

→ Don’t offer the same consumer protections as other payments (e.g. credit card)

→ Scams: Use Venmo account with public transactions; pick prior transaction, create an account with a similar name, ask for more money.
How to Protect Yourself from App Scams

- Don’t use them to purchase products
- Double- and triple-check the: address, username or phone number of the person you are trying to send money to
- Opt-in for stronger security- create a personal identification number (PIN) for extra layer of security
Fake Social Media Accounts

Goals:
1. Ads for fake websites & fake products
   a. Counterfeit
   b. Non-existent
2. Steal money or PII
3. Romance scams
4. Spread false information
5. AI generated images for profiles

Tips:
1. Check for stock photos on Google Images
2. Examine the follower-to-engagement ratio
3. Research the owner and see if there's any reviews or scam complaints
4. Do the reviews match the product specifically or are they generic?
5. How old is the account?
ROMANCE SCAMS
MORE THAN A BROKEN HEART
“Catfishing” or “Love Bombing”

Con-Game

• Use social media, dating websites/apps, or other venues to create a false identity.

• Use public data to find the hook to reel you in
  • Your interests, faith, etc.

• Ultimate goal is money or personal information

• 2021 alone over $1B stolen

• CryptoRom: use replica e-wallet sites for investment; fake returns

• Money Mule
DOOR-TO-DOOR SCAMS

WHEN SCAMMERS COME KNOCKING
SCAM vs LEGITIMATE

Scam Types
- Magazine, candy, etc.
  - Underpaid child labor
  - May never get the magazine
- Home improvement claims
  - Your neighbors have already used them
  - They have extra material to offer a good deal
  - Slow schedule
- Energy Scam
  - Competing suppliers pretend to be PEPCO or Washington Gas wanting to save you money
- Parking Lot Pirates

Legitimate Knocks
- Home Accessories
  - Windows/Doors/Siding
  - Solar
- Religious
- Census takers
  - **Always** ask the merchant’s rep to see the Peddler’s License issued by Dep’t of Permitting Services
  - If no license, say goodbye and shut the door!
- Report scams to OCP for future alerts.
WOODCHUCKS: Not just cute & furry

Q: How much wood would a woodchuck chuck if a woodchuck could chuck wood?

A: A woodchuck would chuck all the wood he could, if a woodchuck could chuck wood!

- Unlicensed home improvement contractors
  - Landscapers
  - Stormchasers

- The Con
  - Take the deposit and never return
  - Take insurance money and never return
  - Substandard work, often unpermitted
MAIL SCAMS

IT’S NOT JUST ABOUT JUNK MAIL
<table>
<thead>
<tr>
<th>SCAMS USING YOUR MAILBOX</th>
<th>SCAMS BEING MAILED TO YOU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail Marauders steal your mail looking for checks in your mailbox</td>
<td>Beware of invitations to free lunches</td>
</tr>
<tr>
<td>Porch Pirates steal your shipments</td>
<td>▪ MLM,</td>
</tr>
<tr>
<td>New age shoplifters open accounts in your name, ship products to your house, and steal it from your mailbox or front door</td>
<td>▪ pyramid</td>
</tr>
<tr>
<td>Scammers can change your address to divert mail</td>
<td>▪ “Amazing Deals” on investment schemes</td>
</tr>
<tr>
<td>Report mail scams to the U.S. Postal Inspection Service or to OCP</td>
<td>Checks/money orders – overpayment scam</td>
</tr>
<tr>
<td></td>
<td>Lottery/sweepstakes scams</td>
</tr>
<tr>
<td></td>
<td>Work from home scams/Jobfishing</td>
</tr>
<tr>
<td></td>
<td>Psychics, foreign political figures</td>
</tr>
</tbody>
</table>