

PRESENTER GUIDE: COMMON SCAMS AND FRAUD

Department of Agriculture, Trade and Consumer Protection, Bureau of Consumer Protection

This Presenter Guide is a tool developed by the Bureau of Consumer Protection to assist presenters delivering the Common Scams and Fraud presentation.

Audience: General public, community groups, adult learners.

Presentation Length: Approximately 60 minutes

Purpose: This guide provides facilitators with the resources needed to deliver the presentation effectively. It includes content, discussion prompts, talking points, and timed instructions for each slide, enabling flexible and adaptable delivery based on audience needs and time constraints.

The guide it is not intended for distribution among session participants.

INDEX OF CONTENT

Slide #	Content	Page
1	Bureau of Consumer Protection	3
2	Scam Statistics	3
3	Scam Statistics	4
4	Scam Statistics	5
5	Scam Statistics	6
6	Scam Trends: Text/Email	7
7	Social Media	8
8	Scam Trends: Phone	9
9	Scams involving Artificial intelligence (AI)	10
10	Deceptive payment methods (red flags)	11
11	Government imposter Scams	12
12	Utility imposter Scams	13
13	Tech support	14
14	Tech support	15
15	Romance / relationship / sweetheart Scams	16
16	Lottery, Contests & Sweepstakes scams	17
17	Grandparent Scam - Video	18
18	Grandparent Scam	19
19	Auto Warranty Scam	20
20	Charity Scams	21
21	Investment scams – FTC 2024	22
22	Cryptocurrency	24
23	How to avoid being scammed	25
24	How to avoid being scammed (cont.)	25
25	What you can do?	26
26	How to stop some unwanted calls	26
27	Victim of A Scam	27
28	How to file a complaint	28
29	Learn more about DATCP	29
30	Thank you	29

1. COVER PAGE

0.5 MIN

Facilitator Notes/Questions

INSTRUCTIONS FOR PRESENTERS

- Introduce yourself and welcome everyone.
- As an ice breaker, you may ask audience the following question:
 - Using a scale of 1 to 10, with 1 being not confident at all, and 10 being very confident, how confident are you in your ability to recognize a scam?
- Indicate that is the purpose of this presentation is to equip the audience with information so they can be ready to recognize a scam and protect themselves and their families.

2. SCAM STATISTICS

2 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

In 2024:

- 2.6 million fraud reports.
- \$12.5 billion reported lost.
- More than 1 in 3 people who reported a scam also reported losing money.
- Almost half of the world encounters a scam at least once a week.
- Estimated that only 30% of victims report being scammed.
- Worldwide losses are estimated to be \$1.03 trillion.*

IMPORTANT CONSIDERATIONS

- The amount lost to scams is difficult to estimate considering only 30% of victims report being scammed, according to data provided by the Federal Trade Commission.

RESOURCES

- **FTC 2024 Data Book | Federal Trade Commission**
<https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2024>
- **Global State of Scams Report 2024 | Global Anti-Scam Alliance**
<https://www.feedzai.com/resource/global-state-of-scams-report-2024/>

3. SCAM STATISTICS

2 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

- Younger people reported losing money to fraud more often than older people did.

INSTRUCTIONS FOR PRESENTERS

- You may consider asking the audience if they can explain why this disparity exists.
 - One possibility is that younger generations typically have a wider digital presence, which gives scammers more access to them.
- When presenting to younger audiences, emphasize how they are targeted and why they need to be aware of scams.
- When presenting to older consumers, use this slide as a transition to the next one.

RESOURCES

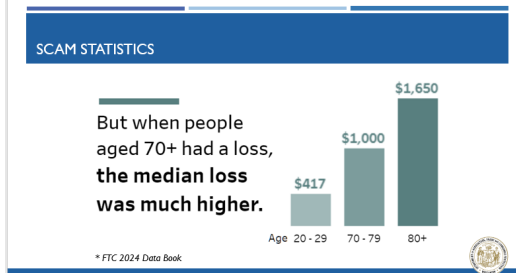
- **FTC 2024 Data Book | Federal Trade Commission**
<https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2024>

4. SCAM STATISTICS

2 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

- We showed younger audiences reported losing money more often but the older generations lost two to three times as much.

INSTRUCTIONS FOR PRESENTERS

- You may consider asking audience why this might be.
 - Some probable factors can include:
 - Older consumers have had more time to build wealth and scammers know this.
 - There may be confusion due to medications or medical conditions, which may impair reasoning.
 - Older consumers may be experiencing social isolation or loneliness, which may make them more vulnerable to scammers.
- Emphasize: No matter how high or low the loss, this can be devastating for the victim.

RESOURCES

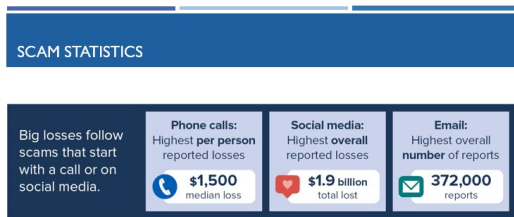
- **FTC 2024 Data Book | Federal Trade Commission**
<https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2024>

5. SCAM STATISTICS

1 MIN

Facilitator Notes/Questions

SLIDE



* FTC 2024 Data Book



NARRATIVE

- Scammers will always find a way to get their message through to potential victims.

RESOURCES

- FTC 2024 Data Book | Federal Trade Commission
<https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2024>

6. SCAM TRENDS: TEXT/EMAIL

3 MIN

Facilitator Notes/Questions

SLIDE

The slide features a blue header with the title 'SCAM TRENDS: TEXT/EMAIL'. Below the header, there are three images: a text message from a 'Post Office' asking for a security code, a smartphone screen displaying a 'USPS Tracking' page, and a text message from a 'Tracking Number' asking for a security code. To the right of these images is a bulleted list titled 'Text/Email' with the following items: Malicious Links, Hidden Sender, Hacked Accounts, and Fake Phone Numbers. At the bottom right of the slide is a small circular seal of the Department of Agriculture, Trade and Consumer Protection.

NARRATIVE

Victims will typically receive a deceptive text message or email intended to lure the recipient into providing their personal or financial information. These scammers often attempt to disguise themselves as a government agency, bank, or other company to lend legitimacy to their claims. These scammers are called imposters.

HOW TO PROTECT YOURSELF

- **Do not open unsolicited texts and do not click suspicious links.**
If you suspect the text message you have received is suspicious but are expecting a parcel, please do not click on any links. Rather, report it and visit USPS.com from your mobile device or computer for tracking and additional resources.
- **Be mindful of hidden sender.**
Hidden senders might try to trick you into clicking on links that lead to fake websites designed to make you disclose personal information or provide payments to scammers.
- **Be cautious of hacked accounts.**
Scammers often send deceptive texts from compromised accounts to trick recipients into revealing personal information or downloading malicious software.
- **Be aware of fake phone numbers**
Scammers may alter the sender ID in the SMS header, making the message appear to be from a legitimate number, like your bank or a well-known company.

IMPORTANT CONSIDERATIONS

Scammers want to steal personally identifiable information from their victims, which includes the following: account usernames and passwords, Social Security number, date of birth, credit and debit card numbers, personal identification numbers or other sensitive information. This information is used to carry out other crimes, such as financial fraud or identity theft.

RESOURCES

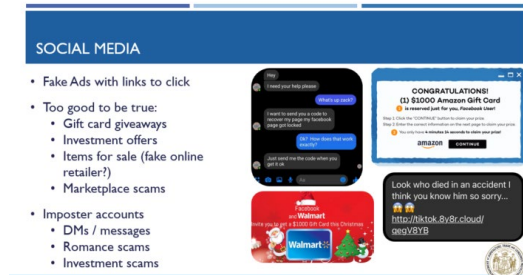
- **Phishing, Vishing and Smishing | Department of Agriculture, Trade and Consumer Protection**
<https://datcp.wi.gov/Pages/Publications/Phishing402.aspx>

7. SOCIAL MEDIA

3 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

Social media scams have some common denominators:

- 1) Fake ads with links to click.
Example: Message indicating the consumer won a gift card or prize, or messages to spark the curiosity of the consumer.
- 2) Too good to be true offers, such as:
 - a. Gift card giveaways.
 - b. Investment offers.
 - c. Items for sale (fake online retailer).
 - d. Marketplace scams.
- 3) Imposter accounts
 - a. DMs / messages.
 - b. Romance scams.
 - c. Investment scams.

INSTRUCTIONS FOR PRESENTERS

- Asking about fake ads can be a good way to engage your audience and assess their current awareness of scams. Here are some ideas to promote participation and gather insights:
 - How many of you have seen a suspicious ad in social media?"
Ask for a show of hands.
 - "Can anyone share an experience where you saw an ad and immediately recognized it as a scam? What were the red flags?"

RESOURCES

- Imposter Scams | Department of Agriculture, Trade and Consumer Protection (DATCP)
<https://datcp.wi.gov/Pages/Publications/ImposterScams214.aspx>

8. SCAM TRENDS: PHONE

3 MIN

Facilitator Notes/Questions

SLIDE

SCAM TRENDS: PHONE



Don't trust Caller ID (Spoofing)

Robocalls

- Don't press any buttons
- Do not say "yes"

Incoming phone calls = unknown caller

NARRATIVE

Scammers use various methods to engage consumers.

- **Spoofing:**
Scammers often "spoof" the sender's name on caller ID to make it look like the call is coming from a legitimate source, like your bank or a well-known company.
- **Robocalls**
Automated calls request some victims to press buttons, or say "yes" or "no" to prompt questions.

How to protect yourself

- Do not answer calls from unknown callers.
- If you receive unsolicited calls, do not press any buttons or respond to questions, even if it is a simple "yes."
 - Saying "yes" may be recorded and used to confirm acceptance for subscription, payment, calls, etc.
- If in doubt whether the call is legitimate, hang up, verify the real phone number of the business or organization that called you, and initiate a call to confirm the authenticity of the first call.

9. ARTIFICIAL INTELLIGENCE AND SCAMS




3 MIN

Facilitator Notes/Questions

SLIDE

ARTIFICIAL INTELLIGENCE AND SCAMS

- Voice Cloning**
 - It only takes 3 seconds of audio to mimic a family member or co-worker's voice. Audio can be downloaded from social media.
- Deep Fakes**
 - Impersonate public figures or create fake charity appeals after disasters
- Phishing**
 - A.I. helps craft very convincing phishing emails and fake websites
- Spear phishing**
 - A.I. analyzes your online and social media presence to help create highly personalized "spear phishing" attacks
- Chatbots**
 - Scammers can respond in real time with relevant, and convincing responses



NARRATIVE

- **Voice cloning:** One of the most alarming new scams uses A.I. to clone voices. Scammers only need a short audio clip of someone's voice to create a convincing fake. They then use the cloned voice to impersonate a family member in distress, claiming they need money urgently.
- **Deepfakes:** A.I. can also create fake photos or videos that prey on your emotions and can look incredibly real. Scammers may use these to impersonate public figures or create fake charity appeals after disasters.
- **Phishing:** The days of the classic "Nigerian Scam"—relatively easy-to-spot emails riddled with misspellings and grammar mistakes—are mostly over. Today, generative A.I. helps scammers craft much more convincing phishing emails and fake websites. These might appear to be from your bank, your favorite shopping site, or even your friendly neighborhood Help Desk.
- **Spear phishing:** Scammers can use A.I. tools to analyze your online and social media presence to help them create highly personalized "spear phishing" attacks. They use your personal information for sophisticated social engineering, including romance scams.
- **Chatbots:** Scammers can respond in real time with relevant, and convincing responses

IMPORTANT CONSIDERATIONS

- The FBI concluded it only takes 3 seconds of voice audio to facilitate an A.I. scam. Businesses have been using A.I. in chatbots for a while, so we are used to seeing them. Think about the little chat boxes that pop up on websites. Many of those have been automated for years.

10. DECEPTIVE PAYMENT METHODS (RED FLAGS)

3 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

1) Cryptocurrency

How it works: Scammers ask you to send them cryptocurrency, often claiming it is a secure method. Scammers increasingly use cryptocurrency ATMs to steal money by directing their victims to deposit cash, which is then converted to cryptocurrency and sent to the scammer's wallet, making recovery difficult.

Why they use it: Cryptocurrency transactions are difficult to trace. Cryptocurrency is not regulated by the government.

2) Gift cards

How it works: Scammers instruct you to buy gift cards from a specific retailer and then send them the codes and card numbers.

Why they use it: Gift cards are difficult to trace, and once the codes are used, the money is gone.

3) Prepaid Visa / MasterCard gift cards

How it works: Scammers trick victims into purchasing and providing information from prepaid Visa and MasterCard gift cards.

Why they use it: Scammers ask for these cards because they offer a fast and untraceable way to steal money.

4) Wire Transfer

How it works: Scammers request you send money to them under false pretenses, often through email scams, phishing, or social engineering.

Why they use it: Wire transfers are difficult to reverse, making it hard for victims to get their money back.

5) Mailing cash

How it works: Scammers trick victims into physically mailing cash to a physical address or P.O. Box. It often targets older adults. Scammers instruct victims to hide cash inside magazines and demand overnight delivery using various carriers including UPS, FedEx, and the U.S. Postal Service.

Why they use it: Cash mailing is untraceable, avoids law enforcement and banking oversight, and is harder to detect in transit. Once the scammers receive the cash, they disappear.

6) Courier pickup at your residence

How it works: This is not a payment method, but rather a delivery method, by which, scammers convince victims to hand over cash, prepaid cards or even gold bars as a form of payment to a fake courier.

Why they use it: This method avoids digital fraud detection, allows for instant theft, and keeps transactions untraceable.

11. GOVERNMENT IMPOSTER SCAMS

3 MIN

Facilitator Notes/Questions

SLIDE


GOVERNMENT IMPOSTER SCAMS

- Social Security**
 - Change in benefits
- IRS**
 - Unpaid taxes
 - Threaten intercept
- Medicare**
 - Expiring benefits
 - Try to obtain Medicare #
- Law Enforcement/FBI**
 - Warrant for arrest
 - Demand payment for fines

Transcription Note: "Please call to share the Department of Social Security representative the reason you have called from our department is to inform you that we are reviewing your Social Security number because we found some suspicious activity and if you want to know about this case and events we thank you."

Speaker Call Back Delete

INSTRUCTIONS FOR PRESENTERS

- You may consider playing the 35-seconds audio files included in the slide. To play click on symbol . This slide contains two audio files.

NARRATIVE

Government imposter scams are when fraudsters pretend to work for the government and use that false authority to trick consumers out of their money, or to disclose their personal or financial information.

Tactics used by scammers

- Social engineering:**

Scammers may use persuasive language or play on emotions like fear to manipulate the recipient into providing personal information, and providing payment for unpaid taxes, expired benefits, or warrant for arrests.
- Urgency:**

They create a sense of urgency by claiming an issue with your Social Security account, benefits or fear of intimidation with arrests warrants. They may ask you to disclose personal information to confirm your identity:

 - Example: Press a number to speak to an operator or government official.
 - Example: Produce payment or risk being arrested.
- Urgent payment demands:**

Scammers will often threaten a consumer with arrest or fines, unless payment is made, creating a sense of urgency to prevent victims from verifying the information.

How to protect yourself

- Do not disclose personal information if you did not initiate the call.
- If in doubt whether the call is legitimate, hang up, verify the real number of the business or organization that called you. Initiate a call to confirm the authenticity of the first call.

IMPORTANT CONSIDERATIONS


- The federal government does not make unsolicited phone calls.
- Government agencies rarely work at night – therefore they would not be calling you after 5 p.m.
- Social Security will never ask for your Social Security number.
- Social Security/Medicare/IRS will not call you unexpectedly. You can make appointments for phone calls – but initial correspondence comes in the mail.

12. UTILITY IMPOSTER SCAMS

2 MIN



Facilitator Notes/Questions

SLIDE

UTILITY IMPOSTER SCAMS 

Water, Gas, Electric, Telecommunications:

- Threaten to cut off service
 - "Crew is on the way"
- Ask victim to "verify" account information
 - Personal info
 - Payment/Banking info
- Rebate or discount promotion



INSTRUCTIONS FOR PRESENTERS

- You may consider playing the 15-second audio file included in the slide. To play click on symbol



NARRATIVE

Utility imposter scams involve individuals pretending to be utility company representatives to deceive customers into paying fraudulent bills or providing personal information. Scammers often use phone calls, claiming payment is overdue and service will be cut off if payment is not made immediately.

TACTICS USED BY SCAMMERS

- **Social engineering:**
Scammers may use persuasive language or play on emotions like fear to manipulate the recipient into providing personal information, and providing payment for fake unpaid bills.
- **Urgency:**
They create a sense of urgency by claiming an issue with payment of your bill.
- **Threats:**
Scammers will often threaten immediate disconnection unless payment is made, creating a sense of urgency to prevent victims from verifying the information. They also claim it will take several days to restore the connection along with a reconnection fee.
- **Requests for personal information:**
Scammers may ask for personal information like bank account details or Social Security numbers with the excuse of verifying the account or initiating a payment.
- **Unusual payment methods:**
They may request payment through prepaid cards, gift cards, wired money or digital payment apps, which are not legitimate methods for utility payments.

HOW TO PROTECT YOURSELF

- **Contact your utility company directly:** Hang up and call your utility company directly using the phone number on your bill or their official website to verify any information or payment requests.
- **Be suspicious of unusual payment methods:** Never provide payment via prepaid cards, gift cards, or payment apps.
- **Do not trust your caller ID:** Do not assume a call is legitimate just because the caller ID displays a utility company number. Call the utility company directly using the number on your bill or their website to confirm any inquiries.

RESOURCES

- **Imposter Scam: Fake Utility Calls | DATCP**
https://datcp.wi.gov/Pages/News_Media/20180823CA_UtilityScams.aspx

13. TECH SUPPORT

3 MIN

Facilitator Notes/Questions

SLIDE



INSTRUCTIONS FOR PRESENTERS

- You may consider playing the YouTube 3:06-minute video hyperlinked in the slide. Internet connection is required for playing video.
- Otherwise, this content is also examined in the next slide.

KEY CONSIDERATIONS AFTER WATCHING VIDEO

- Tech support scams can happen to anyone.
- Victims are manipulated into giving scammers access to their computers.
- Victims often feel ashamed to seek help.

RESOURCES

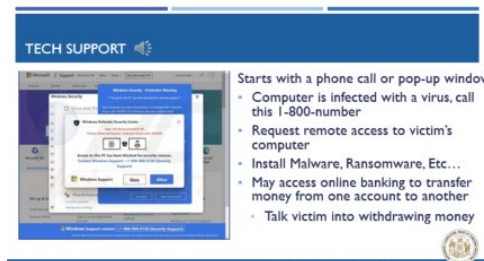
- **How to Avoid a Tech Support Scam | Federal Trade Commission**
<https://www.youtube.com/watch?v=wuj5tvnbJwg>

14. TECH SUPPORT

2 MIN

Facilitator Notes/Questions

SLIDE



INSTRUCTIONS FOR PRESENTERS

- You may consider playing the 13-second audio file included in the slide. To play click on symbol



NARRATIVE

Tech support scams involve fraudsters posing as legitimate technical support, often claiming a computer problem exists and offering to fix it if you pay. Scammers often use fake pop-ups or unsolicited calls/emails to scare victims into granting remote access, installing malware, or providing personal/financial information.

TACTICS USED BY SCAMMERS

- Unsolicited contact and fake security alert:**
 - Starts with a phone call or pop-up window.
 - A computer pop-up indicates the device is infected with a virus, and instructs users to call a 800 number.
- Remote access:**
 - The scammer requests remote access to the victim's computer.
 - Scammer may install malware or ransomware.
 - Scammer may access online banking to transfer money from one account to another.
- Requests for payment:**
 - Scammers may ask for payment in unconventional ways like gift cards, reloadable debit cards, or wire transfers, which are difficult to reverse.

HOW TO PROTECT YOURSELF

- Hang up or ignore:** If you receive an unsolicited call or message, hang up or ignore it.
- Verify the source:**

If you are unsure about the legitimacy of a contact, verify it with the company you are dealing with by contacting them through their official website or phone number. Software companies do not contact consumers through pop-ups in your computer or through unsolicited phone calls.
- Don't click on links or download attachments:**

Be careful clicking on links or downloading attachments from unknown sources, especially if they appear to be from tech support. If someone is pressuring you to take action quickly or is using scare tactics, it is a good sign that something is wrong.
- Requests for remote access:**

Never give remote access to your computer to someone you did not initiate contact with.

RESOURCES

- Consumer Guide | DATCP**
<https://datcp.wi.gov/Documents2/DATCPConsumerGuide.pdf>

15. ROMANCE / RELATIONSHIP / SWEETHEART SCAMS


3 MIN

Facilitator Notes/Questions

SLIDE

ROMANCE / RELATIONSHIP / SWEETHEART SCAMS

- Can start through texting, social media, online gaming, dating sites, etc....
- Profess their love for you early in the "relationship"
- Refuse to meet face to face
 - Travel expenses needed to meet
 - Serving overseas in military
- Encounter major problem, needs money
 - Medical/family emergency



NARRATIVE

Romance scams are deceptive schemes where fraudsters build fake online relationships to gain trust and then manipulate their victims into sending money or personal information. They often use fake profiles and romantic enticements to extract funds or gain access to sensitive data.

TACTICS USED BY SCAMMERS

In romance scams, a criminal uses a fake online identity to gain a victim's affection and trust. The scammer then uses the illusion of a romantic or close relationship to manipulate and/or steal from the victim.

- **Methods of engagement:**
Communications can start through texting, social media, or dating sites. Scammers will pressure victims to move the conversation to a messenger platform such as WhatsApp or Telegram.
- **Building a fake relationship:**
The scammer establishes a relationship as quickly as possible. The scammer then uses the illusion of a romantic or close relationship to manipulate and/or steal from the victim.
- **False promises:**
Scammers may propose marriage and make plans to meet in person; they will use affectionate language and shared interests to create a strong emotional connection.
- **Too quick to love:**
Scammers often express strong feelings and commitment very early in the relationship. They use a manipulation tactic known as "love bombing", where someone manipulates another person with excessive affection and attention to gain control and develop dependency.
- **Requests for money:**
Once trust is built, they invent stories about emergencies, financial difficulties, or the need for help with travel or other expenses to get the victim to send money or provide financial information.

HOW TO PROTECT YOURSELF

Do not ignore the red flags even though you may want to.

- **Be cautious if someone requests that you send money:**
Never send money to anyone you have only communicated with online or by phone.
- **Don't give in to pressure:**
Scammers often use emotional manipulation, so trust your instincts and do not send money or provide personal information.

IMPORTANT CONSIDERATIONS

- If the person refuses to meet in person or always has excuses for not doing so, it could be a red flag.
- Scammers often pose as soldiers, doctors, or other professions to appear trustworthy and explain their inability to meet in person.
- Scammers may lure victims to invest in cryptocurrency scams, or pig butchering scams. (This is addressed in slide #21.)

RESOURCES

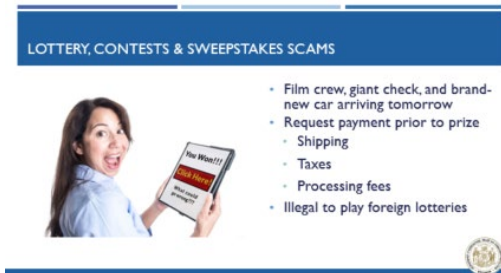
- **Consumer Guide | DATCP**
<https://datcp.wi.gov/Documents2/DATCPConsumerGuide.pdf>

16. LOTTERY, CONTESTS & SWEEPSTAKES SCAMS

3 MIN

Facilitator Notes/Questions

SLIDE



LOTTERY, CONTESTS & SWEEPSTAKES SCAMS

- Film crew, giant check, and brand-new car arriving tomorrow
- Request payment prior to prize
 - Shipping
 - Taxes
 - Processing fees
- Illegal to play foreign lotteries

NARRATIVE

Lottery and sweepstakes scams are fraudulent schemes in which scammers contact individuals, typically via email or phone, to falsely claim the victim has won a lottery or sweepstakes prize. The victim is asked to pay fees or taxes upfront to claim their supposed winnings. These scams are designed to deceive individuals into providing money or personal information under the false promise of a substantial prize.

TACTICS USED BY SCAMMERS

- **Scammers use names of organizations you might recognize to gain your trust:**
Scammers might pretend to be from well-known companies that run real sweepstakes. However, no real sweepstakes company will contact you asking for money to claim a prize.
- **Promises of huge prizes:**
Scammers call you by phone or send you a message (via text, email, or social media) to get your personal information. They might say you won a gift card, or something expensive like an iPad or a new car from your local dealership. They may say the film crew with giant check, or brand-new car will be arriving tomorrow.
- **Requests for money:**
Scammers pressure you to act now to get a prize. They will request payment prior to sending your prize for things such as shipping, taxes, and processing fees.

IMPORTANT CONSIDERATIONS

- It is illegal for U.S. citizens to play a foreign lottery. Don't trust someone who asks you to break the law.
- Scammers make it seem like you are the only person who won a prize. However, the same text, call, email, or letter went to lots of people.
- If you have to pay to get your prize, it is a scam.
- If you have to pay to increase your odds of winning, it is a scam.
- If you have to give your financial or personal information, it is a scam.
- If you never entered a contest, you cannot win.

RESOURCES

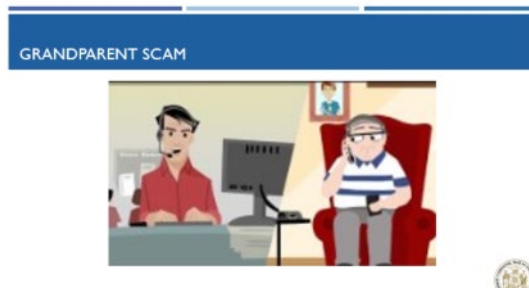
- **United States Postal Service | Foreign Lotteries**
<https://about.usps.com/publications/pub300a>.

17. GRANDPARENT SCAM

1 MIN

Facilitator Notes/Questions

SLIDE



INSTRUCTIONS FOR PRESENTER

- You may consider playing the YouTube 40-second video hyperlinked in the slide. Internet connection is required for playing video.

KEY CONSIDERATIONS AFTER WATCHING VIDEO

- Grandparent scams can happen to anyone.
- Victims of grandparent scams are made to believe that their family members, usually a grandchild, are in trouble and need urgent financial assistance.

RESOURCES

- **Family Emergency Imposter Scams | Federal Trade Commission**
https://www.youtube.com/watch?v=QEPdo_DvakY&t=1s

18. GRANDPARENT SCAM

3 MIN

Facilitator Notes/Questions

SLIDE

GRANDPARENT SCAM

- Grandchild has been arrested or involved in a crash
 - “crash” may involve a broken nose, why?
- May use A.I. to mimic a grandchild’s voice
- Trick you into saying a name
- Get information from social media
- “Shhhh” don’t tell anyone
- May impersonate law enforcement or lawyer
- Family password

The slide includes two images: a woman on a phone and a sign that says “Billy, is that you?”.

NARRATIVE

Grandparent scams target older adults by impersonating a family member in distress and requesting immediate financial help.

INSTRUCTIONS FOR PRESENTERS

- If presenting to older consumers, this is a good time to engage the audience by asking if anyone has received this call.

TACTICS USED BY SCAMMERS

- **Impersonation:**
Scammers pretend to be a grandchild, often using information from social media to make the story seem real. Scammers may use A.I. to mimic a grandchild’s voice, via voice cloning.
- **Emergency situation:**
They may indicate the grandchild has been arrested or involved in a crash. They may impersonate a doctor, law enforcement or a lawyer.
- **Urgency, pressure and secrecy:**
Scammers rush victims into making a decision before they can think clearly, sometimes instructing them to keep the situation secret.
- **Method of payment:**
Scammers request money through wire transfers, gift cards, or other methods that are difficult to recover and track.

HOW TO PROTECT YOURSELF

- **Verify the caller’s identity:**
Ask specific questions that only your grandchild would know the answer to. Create a family passcode that only the inner circle of the family knows.
- **Don’t give in to pressure:**
Scammers often use emotional manipulation. Pause and think before acting, especially if you are feeling emotional distress.
- **Contact family members:**
Call your grandchild or another trusted family member to confirm the story and the caller’s identity.
- **Avoid sending money:**
Be cautious about sending money through methods that are difficult to trace or recover.

RESOURCES

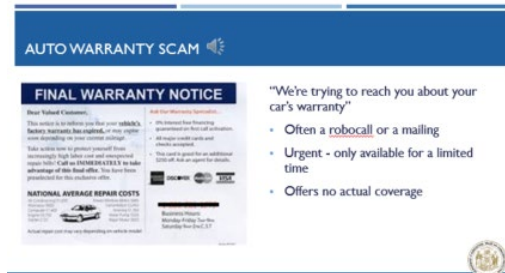
- **Senior phone scams | DATCP**
<https://datcp.wi.gov/Pages/Publications/SeniorsPhoneScams283.aspx>

19. AUTO WARRANTY SCAM

2 MIN

Facilitator Notes/Questions

SLIDE



INSTRUCTIONS FOR PRESENTERS

- You may consider playing the 23-second audio file included in the slide. To play click on symbol



NARRATIVE

Auto warranty scams often involve unsolicited calls, texts, or emails claiming your car's warranty is expiring or that you need to extend it. These scams frequently use pre-recorded messages or fake warranty notices to pressure you into purchasing an extended warranty. Scammers may even spoof their caller ID to make the call appear legitimate.

TACTICS USED BY SCAMMERS

- Unsolicited contact:**
Scammers use various methods to reach potential victims, including mail, robocalls, texts, and emails.
- Fake notifications:**
They may send fake warranty expiration notices or claim your warranty is about to expire. However, their extended warranty offers no actual coverage.
- Fake company appearances:**
They may claim to represent your car dealer or manufacturer, but they are often unrelated.
- High-pressure tactics:**
Scammers often use urgency and scare tactics to encourage immediate action, such as extending your warranty or paying for a service contract. "Urgent – only available for a limited time."
- Personal information requests:**
They may ask for personal or financial information, which they can use for fraudulent purposes.

HOW TO PROTECT YOURSELF

- Be skeptical:** Do not trust unsolicited offers or those that use high-pressure tactics.
- Verify legitimate offers:** Contact your car manufacturer or dealership directly to verify warranty status.
- Do not provide personal information:** Never give out personal or financial details to an unsolicited message or call.

IMPORTANT CONSIDERATIONS

- Consider your needs:** If you want a warranty for your vehicle, shop for it with intention. Do not accept a call allegedly from a warranty firm.

20. CHARITY SCAMS

2 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

Charity scams are deceptive practices where fraudsters pretend to be a charity or associated with one to solicit donations. Scammers may use false information, mimic legitimate charities, or exploit current events to trick donors into parting with their money.

TACTICS USED BY SCAMMERS

- **Charity misrepresentations:**
Scammers create fake charities that appear legitimate by using names similar to well-known organizations, using professional-looking graphics, and crafting convincing stories. It is almost impossible to tell a real call from a fake call.
- **Exploiting current events:**
Scammers often latch onto current events like natural disasters or crises to take advantage of people's desire to help.
- **High-pressure tactics:**
Scammers may pressure you to donate immediately, refusing to provide details about the charity or its mission.
- **Soliciting donations:**
Scammers may reach out through phone calls, emails, text messages, social media, or even door-to-door. Note: Under the law, charities are allowed to call consumers on the Do Not Call Registry.

HOW TO PROTECT YOURSELF

- **Research the charity:**
Before donating, verify the charity's by checking with organizations like Better Business Bureau's (BBB) Wise Giving Alliance, www.CharityNavigator.org or www.Give.org. You can also verify if a charity is registered with the Department of Financial Institutions at <https://dfi.wi.gov>.
- **Be skeptical of pressure:**
Do not fall for high-pressure tactics or requests to donate immediately. Searching the name of the organization online – especially with the word "complaint(s)" or "scam" – is another way to check its reputation.
- **Don't give on impulse:**
Take your time to research the charity before making a donation.
- **Watch out for payment method red flags:**
Avoid donating via cash, gift cards, cryptocurrency, or wire transfers, and always use a secure method like credit card. Do not provide your credit or check card number, bank account number or any personal information until you have thoroughly researched the charity.
- **Check with the charity:**
If you receive a solicitation, contact the charity directly to confirm the request is legitimate.

IMPORTANT CONSIDERATIONS

- Be wary of charities that spring up suddenly in response to current events and natural disasters. Even if they are legitimate, they probably do not have the infrastructure to get the donations to the affected area or people.
- If a donation request comes from a group claiming to help your local community (for example, local police or firefighters), ask the local agency if they have heard of the group and are getting financial support.

RESOURCES

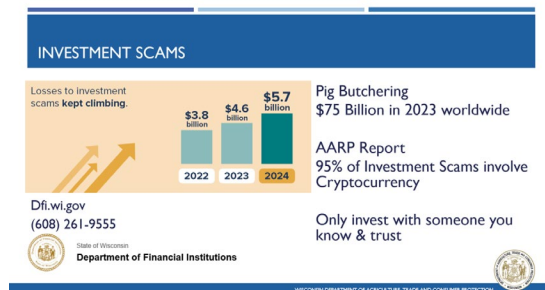
- **Charity Requests | DATCP**
<https://datcp.wi.gov/Pages/Publications/CharityRequests120.aspx>
- **Charity and Disaster Fraud | Federal Bureau of Investigation (FBI)**
<https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/charity-and-disaster-fraud>

21. INVESTMENT SCAMS

3 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

This slide focuses on “pig butchering” as a trending investment scam that is affecting consumers. Pig butchering scams are investment frauds where scammers build relationships with victims online, often using romance scams, and then lure them into investing in fake cryptocurrency or working with a fraudulent financial advisor. These scams can lead to significant financial losses, and victims are often left with no way to recover their funds.

- Losses to pig butchering:
 - \$75 billion in 2023 worldwide.
- AARP Report:
 - 95% of investment scams involve cryptocurrency.
- FTC Statistics:
 - 4% of all fraud reports.
 - 30% of total losses to fraud.
 - \$7,000 average loss.

INSTRUCTIONS FOR PRESENTERS

- Asking about investment scams can be a good way to engage the audience and assess their current awareness of this type of scam. Some ways to phrase questions to promote participation and gather insights are:
 - How many of you have seen an apparently innocent “wrong number” text message? Ask for a show of hands to get a quick visual estimate.
 - “Can anyone share an experience where you received this type of text and immediately recognized it as a scam? What were the red flags?” - This can encourage deeper sharing and discussion.

TACTICS USED BY SCAMMERS

- **Building trust:**
Scammers often begin by creating a fake online persona, often using stolen or A.I. generated photos and conveying a glamorous lifestyle to attract victims. They may also use a deceptive "wrong number" text message to initiate contact. Scammers will pressure victims to move the conversation to a messenger platform such as WhatsApp or Telegram.
- **Establishing a relationship:**
Scammers engage in extensive conversation, often mimicking the victim's interests and building emotional connections to gain trust. They may feign romantic interest to deepen the bond.
- **Luring into investments:**
Once trust is established, the scammer will introduce the victim to a fake investment opportunity, often promising high returns. They may use fake charts or "withdrawals" to convince the victim of the legitimacy of the investment.
- **Collecting money (Butchering):**
After persuading the victim to invest, scammers collect funds, often through digital payment platforms or cryptocurrencies, to complicate tracking and tracing of the transactions. When victims attempt to collect their supposed gains, scammers present them with taxes and fees that are presumably required.
- **Disappearance of the scammer:**
Once a substantial amount has been collected, or when victims attempt to withdraw funds, scammers become unreachable, delete their online presence, or create new identities; leaving the victims with no way to recover their funds.

HOW TO PROTECT YOURSELF

- **Be wary of unexpected messages or texts:**
Especially those from "wrong numbers" or unknown individuals.
- **Be suspicious of promises of unrealistic returns:**
If something seems too good to be true, it probably is.
- **Don't rush into investing:**
Take your time to research and verify any investment opportunity before making any decisions.
- **Don't send money to strangers online:**
Never send money to someone you have not met in person or whose identity you have not verified.

RESOURCES

- **Investment Scam Tracker | Wisconsin Department of Financial Institutions**
<https://dfi.wi.gov/Pages/Securities/InvestorResources/InvestmentScamTracker.aspx>

22. CRYPTOCURRENCY

2 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

- 2023 IC3 Report & 2024 Chain Analysis Crime Report:
 - 2023 – \$5.6 billion in losses.
 - 45% increase from 2022.
 - Victims over 60 years old account for 30% of losses.
 - 2024 – Total loss expected to exceed \$7 billion.
 - Wisconsin overall loss – \$92,084,459.
- Consumers should be wary of the use of cryptocurrency for fraudulent purposes.
- Getting money back from a crypto fraud is difficult, as cryptocurrency transactions are generally irreversible.

RESOURCES

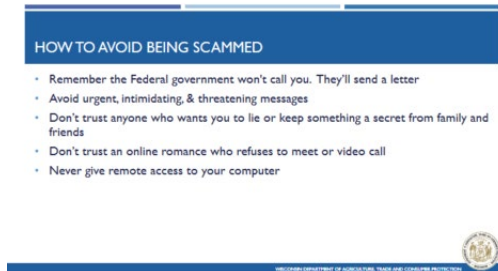
- Investment Fraud | DATCP
<https://datcp.wi.gov/Pages/Publications/InvestmentFraud495.aspx>

23. HOW TO AVOID BEING SCAMMED

2 MIN

Facilitator Notes/Questions

SLIDE



HOW TO AVOID BEING SCAMMED

- Remember the Federal government won't call you. They'll send a letter
- Avoid urgent, intimidating, & threatening messages
- Don't trust anyone who wants you to lie or keep something a secret from family and friends
- Don't trust an online romance who refuses to meet or video call
- Never give remote access to your computer

WISCONSIN DEPARTMENT OF EDUCATION, TRAINING AND CONSUMER PROTECTION

NARRATIVE

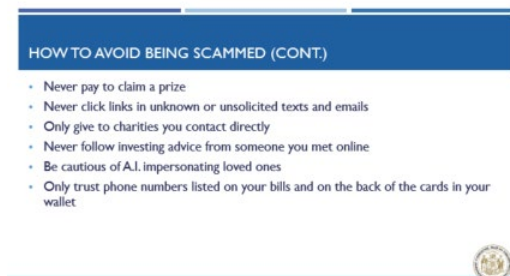
- Remember, the federal government will not call you. They will send a letter.
- Avoid urgent, intimidating, and threatening messages.
- Don't trust anyone who wants you to lie or keep something a secret from family and friends.
- Don't trust an online romance who refuses to meet or video call.
- Never give remote access to your computer.

24. HOW TO AVOID BEING SCAMMED

2 MIN

Facilitator Notes/Questions

SLIDE



HOW TO AVOID BEING SCAMMED (CONT.)

- Never pay to claim a prize
- Never click links in unknown or unsolicited texts and emails
- Only give to charities you contact directly
- Never follow investing advice from someone you met online
- Be cautious of A.I. impersonating loved ones
- Only trust phone numbers listed on your bills and on the back of the cards in your wallet

WISCONSIN DEPARTMENT OF EDUCATION, TRAINING AND CONSUMER PROTECTION

NARRATIVE

- Never pay to claim a prize.
- Never click links in unknown or unsolicited texts and emails.
- Only give to charities you contact directly.
- Never follow investing advice from someone you met online.
- Be cautious of A.I. impersonating loved ones.
- Only trust phone numbers listed on your bills and on the back of the cards in your wallet.

25. WHAT CAN YOU DO?

2 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

As a consumer, there are steps you can take to stop unwanted calls on a cell phone.

- Contact your phone's service provider and request scam call blocking.
- Use apps/built in services to block scam calls on smartphones.
- Register for the WI Do Not Call Registry.

RESOURCES

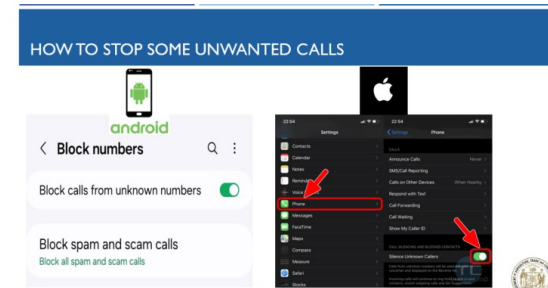
- **Wisconsin Do Not Call Registry | DATCP**
https://datcp.wi.gov/Pages/Online_Services/DoNotCall.aspx
- **Unwanted Junk: Mail, Calls, Emails, Texts, Faxes | DATCP**
<https://datcp.wi.gov/Pages/Publications/JunkMailUnwantedCalls140.aspx>

26. HOW TO STOP SOME UNWANTED CALLS

2 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

Some smartphones have built-in systems that allow users to stop some unwanted calls.

- Set your phone to block unknown and private numbers, depending on the system:
 - Android
 - iPhone

27. VICTIM OF A SCAM

2 MIN

Facilitator Notes/Questions

SLIDE

VICTIM OF A SCAM

- Report to local law enforcement and www.ic3.gov as quickly as possible
- Notify financial institution(s) to stop the transaction
- If you mailed money or gift cards, contact USPS as soon as possible to stop shipment
- File a complaint w/ WI Bureau of Consumer Protection



NARRATIVE

Consumers can take action if they have been victims of a scam.

- Report to local law enforcement and www.ic3.gov as quickly as possible.
- Notify financial institution(s) to stop the transaction.
- If you mailed money or gift cards, contact USPS as soon as possible to stop shipment.
- File a complaint with Wisconsin's Bureau of Consumer Protection.

IMPORTANT CONSIDERATIONS

- Do not be ashamed if you are scammed; allow yourself to ask for help.
- Support others and encourage them to file a complaint.
- Remember that ANYONE can fall victim to a scam.

28. HOW TO FILE A COMPLAINT


1 MIN

Facilitator Notes/Questions

SLIDE

FILING A COMPLAINT WITH DATCP

- Consumers have several options to submit a complaint:
 - File online at ConsumerProtection.wi.gov.
 - Download the form on DATCP's website.
 - Contact DATCP's Consumer Protection Hotline and have a complaint mailed to you.
- Completed complaints and copies of relevant documents should be mailed to:
DATCP Bureau of Consumer Protection
PO Box 8911
Madison, WI 53708-8911
- Hotline staff can schedule onsite appointments to assist with submitting a complaint.
- Video tutorials on DATCP's website explain how to submit a complaint and what to expect afterwards.



NARRATIVE

Consumers have several options to submit a complaint:

- Consumers can file complaints online by visiting: ConsumerProtection.wi.gov.
- Consumers can submit a complaint by mail by downloading the form on DATCP's website, or contacting DATCP's Consumer Protection Hotline and requesting a complaint be sent to them.
- Completed complaints and copies of relevant documents should be mailed to:
DATCP Bureau of Consumer Protection
PO Box 8911
Madison, WI 53708-8911
- Hotline staff can schedule onsite appointments to assist consumers with submitting a complaint.
- Video tutorials on DATCP's website explain how to submit a complaint and what to expect afterwards.

INSTRUCTIONS FOR PRESENTER

- Encourage the audience to omit or mark out any confidential or personal information (e.g., checking account number, credit card number, Social Security Number, date of birth, etc.) if it is not relevant to the complaint.

RESOURCES

- **File a Consumer Complaint | DATCP**
https://datcp.wi.gov/Pages/Programs_Services/FileConsumerComplaint.aspx

29. LEARN MORE ABOUT DATCP

1 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

- DATCP runs social media accounts to keep consumers up to date on scams, consumer issues, and other topics the Department is involved in.
- DATCP offers free presentations on the topics listed here to community groups, organizations, and businesses all over Wisconsin. In-person or virtual options are available. Anyone can request a presentation at datcp.wi.gov.

30. THANK YOU

0.5 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

- Thank you.