FACILITATOR GUIDE

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

Presentation: Holidays Presentation

The **Holidays presentation** is to be used in conjunction with the delivery of the presentation developed by the Bureau of Consumer Protection.

Audience: General public, community groups, adult learners.

Presentation Length: Approximately 45 minutes.

Purpose: This guide provides presenters 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 is not intended for distribution among session participants.

TABLE OF CONTENT

Slide #	Content	Page
1	Cover Page	3
2	What to Look Out For this Holiday Season	3
3	FTC Data 2024 - Wisconsin	4
4	Practice Safe Online Shopping	5
5	Return, Refund and Shipping Policies	7
6	Payment Methods	8
7	Door Buster and In-Store Deals	10
8	Holiday Credit Card Offers	11
9	Gift cards	12
10	Social Media	13
11	"Giving Tuesday" and Charity Scams	14
12	Holiday Shipping Scams	15
13	Deceptive Payment Methods	16
14	Holiday Refund Scam	17
15	Toy Safety	18
16	Filing a Complaint with BCP	19
17	Learn More About DATCP	20
18	Thank You	20

1. COVER PAGE

0.5 MIN

Facilitator Notes/Questions

SLIDE



2. WHAT TO LOOK OUT FOR THIS HOLIDAY SEASON

0.5 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

The holiday season is a time for giving, celebration and connection with family and friends. However, consumers need to be aware of scams and other shopping considerations to ensure a positive holiday experience. This presentation will cover the following aspects associated with the holidays:

- Online shopping risks and best practices
- In-store considerations
- Credit card offers
- Surveys and games
- · Gift cards
- Charitable giving
- Common holiday scams
- Toy safety

2 MIN

3. FTC DATA 2024 - WISCONSIN

Facilitator Notes/Questions

SLIDE



INSTRUCTIONS FOR PRESENTER

Consider asking the audience if they have shopped online lately to get a sense of how familiar audience members are with the online shopping experience.

NARRATIVE

The FTC's Consumer Sentinel Data Book showed online shopping fraud was the most reported fraud type in 2024 in Wisconsin, with 5,024 reported cases.

Online Shopping

This category includes: undisclosed costs, failure to deliver on time, non-delivery, and refusal to honor a guarantee on purchases made online; internet auctions; and businesses trying to prevent people from giving honest reviews about products or services they purchased.

RESOURCES

 Consumer Sentinel Network Data Book, 2024 | Federal Trade Commission https://www.ftc.gov/system/files/ftc_gov/pdf/csn-annual-data-book-2024.pdf

SLIDE



INSTRUCTIONS FOR PRESENTER

Consider asking the audience a prompt question for engagement.

Here are two prompt questions to introduce the topic:

- Do you usually shop online from your phone, tablet, or computer?
- Why do you choose that device?

NARRATIVE

Is your device up to date?

As the word "online" indicates, this is not a brick-and-mortar shopping experience. In order to shop online, you need a device to connect you to the internet.

Electronic devices such as phones, tablets, laptops and computers are the most common ways consumers connect to the Internet.

The following safety tips are important to achieve a safe online experience:

- Use reputable antivirus and anti-malware software: Keep your devices protected against viruses and malware by using legitimate security software.
- Keep software updated: Install software updates promptly to patch security vulnerabilities and update protection.
- Ensure you have the latest versions of your operating system, browsers, apps, and protection software.

How did you end up on the website?

There is a big difference between going to a known online retailer where you have shopped in the past, compared to seeing an advertisement on social media and clicking a link to a website you have never done business with before.

- Be wary of phishing attempts. Do not click on links in suspicious emails, texts from unknown senders, or online ads in social media. Always access websites directly by typing the address into your browser.
- Be mindful of how you use search engines for online shopping; they can generate poor results such as imposter websites and fake reviews.

(Continued on next page)

Is the checkout encrypted?

Have you ever noticed the "https" at the beginning of a web address?

'HTTPS' at the beginning of a website address adds a layer of security to 'HTTP' by encrypting the data transmitted between your browser and the website. The "S" indicates that the connection between your browser and a website is encrypted.

- Ensure the website URL begins with "https://" indicating a secure connection and encrypted data transmission. You may also see a padlock, however, a padlock alone does not indicate security.
- o Never send payment card info or personal info on an unencrypted website (HTTP).
- Keep in mind that while HTTPS ensures a secure connection, it does not guarantee a website's legitimacy or trustworthiness.

• Are you connected using secure Wi-Fi?

Shoppers need to ensure they have a secure connection to the web. While, accessing the internet using a public Wi-Fi hotspot is convenient and often free for users, hotspots typically are not secure.

- o Be aware of fake Wi-Fi networks that may closely resemble the real one.
 - For example: 'StarbucksWiFi' is not the same as 'Starbucks', which is why you need to pay attention to the network name.
- Connect to the web through 5G on your phone. Phone carriers incorporate enhanced security features with encryption algorithms and improved authentication protocols.
- Use a VPN (Virtual Private Network) to make private any data sent across a network. VPNs are designed to be used on computers and mobile devices.

Where is the product being delivered?

Be aware of porch pirates. These are individuals that steal packages delivered to homes, which are typically left on porches or near front doors. This form of theft has become increasingly prevalent with the rise of online shopping and package deliveries.

How to protect yourself from mail and package theft:

- o Consider installing a security camera or video doorbell.
- Request signature confirmation for deliveries.
- o Consider package lockers or pickup locations.
- o Request delivery to a neighbor or friend.
- Utilize delivery tracking and notifications.

RESOURCES

- Computer security tips | Federal Trade Commission https://www.ftc.gov/media/70875
- Safe Online Shopping Tips | Department of Agriculture, Trade and Consumer Protection https://datcp.wi.gov/Pages/Programs_Services/SafeOnlineShoppingTips.aspx
- Tips for Using Public Wi-Fi | Department of Agriculture, Trade and Consumer Protection https://datcp.wi.gov/Pages/Publications/IDTheftWi-FiTips659.aspx
- Mail & Package Theft | United States Postal Inspection Service https://www.uspis.gov/tips-prevention/mail-theft

5. RETURN, REFUND, AND SHIPPING POLICIES

3 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

A return policy outlines the conditions and process for returns, exchanges, and refunds. Consumers should read the return policy before making a purchase. Understanding the return policy helps manage customer expectations and prevents misunderstandings or frustration later.

When reviewing a return policy, consider the following factors to ensure it meets your needs and expectations before making a purchase.

- Third-party surcharge: A business that uses a third-party warehouse to store and process returns may add a surcharge to cover the warehouse storage and handling fees.
- **Restocking fees:** Some retailers may charge restocking fees for returns, and knowing about these beforehand can prevent surprises.

For example: A retailer may charge a restocking fee for items returned outside of their return policy, in used or damaged condition, or for specific product types like opened software or video games.

• Shipping and handling fees: Understand whether you or the retailer is responsible for return shipping fees. Some retailers may offer free return shipping, while others offer different options with varying costs.

For example: A company indicates that the seller pays for return shipping if they offer a free return policy or if the item was damaged, faulty, or doesn't match the listing description. However, the buyer may be responsible for return shipping if they changed their mind or the product does not fit.

- Return window/timeframe: Search for the number of days after purchase or delivery that returns are allowed.
- Refund options: These specify whether a full refund, store credit, or exchange is offered for returned items.
- Return method and process: Check if returns are initiated online, in-store, or by contacting customer service. Some retailers may provide prepaid return shipping labels, while others may require you to purchase them yourself.

RESOURCES

 Shopping Tips | Department of Agriculture, Trade and Consumer Protection https://datcp.wi.gov/Pages/Publications/ShoppingTips212.aspx

SLIDE



NARRATIVE

Shoppers have different options for payment methods. Selecting the appropriate payment for your purchases is important.

Using payment apps

Payment apps are digital wallets that allow users to make instant payments, send and receive money, and manage their financial information through a smartphone or other device. They offer a convenient alternative to cash or traditional payment methods. Popular payment apps include Venmo, Cash App, Zelle, PayPal, Apple Pay, Google Pay, and Samsung Pay.

Although payment apps can be a convenient way to send and receive money with your smartphone, scammers may try to use them to steal your money.

Tips for using payment apps safely:

- Be cautious of any unexpected or suspicious payment requests, regardless of the method used. Verify the legitimacy of the request and the identity of the sender before making any payments, especially through payment apps.
- Generally, recovering money sent to a scammer through a payment app is difficult and often impossible, especially if the transaction is completed.

Using Friends and Family (F&F) option on payment apps:

This type of payment is intended for personal transfers between people who know and trust each other, like splitting a bill or sending a gift.

- F&F payments typically do not come with buyer protection, leaving you vulnerable if you pay for a product or service and do not receive it or it is not as described.
- Scammers often try to trick consumers into using F&F for purchases, knowing they will have no recourse if they do not deliver.

Difference between credit cards, debit cards and gift cards as it relates to buyer protection

Credit cards:

- Strongest buyer protection: Credit cards generally offer the most comprehensive buyer protection.
- Purchase protection: Many credit cards offer purchase protection, which can reimburse you for damaged, stolen, or lost items purchased with the card within a specific timeframe (typically 90-120 days).
- Fraudulent activity: If your credit card information is stolen and used fraudulently, the impact on your personal finances may be less immediate, as the money is not directly withdrawn from your bank account.

(Continued on next page)

Debit cards:

- Limited buyer protection: Debit cards offer less robust buyer protection compared to credit cards.
- Purchase protection: Debit cards typically do not offer purchase protection or other similar benefits.
- Fraudulent activity: Your liability for unauthorized debit card transactions can vary depending on how quickly you report the issue and the specific bank's policies.

· Gift cards:

- Limited buyer protection: Gift cards offer the least amount of buyer protection, often with no recourse if lost or stolen.
- Fraudulent activity: Gift cards are often used, requested, or sold by scammers, making it
 essential to purchase them from reputable sources and avoid suspicious offers. If a gift
 card is lost or stolen, you typically cannot recover the funds. However, you should report it
 immediately.

Virtual card numbers:

Virtual card numbers, also known as temporary or anonymous card numbers, are a security feature offered by some credit card issuers. They are 16-digit numbers, expiration dates, and CVV codes that can be used for online purchases, but they are not associated with the physical card's actual number. These virtual numbers are linked to your credit card account and can be used to make purchases, but they are not stored on your physical card or with the merchant.

RESOURCES

 Shopping Tips | Department of Agriculture, Trade and Consumer Protection https://datcp.wi.gov/Pages/Publications/ShoppingTips212.aspx

SLIDE



INSTRUCTIONS FOR PRESENTER

Consider asking a prompt question to introduce the topic.

- When you see a big "door buster" or limited-time deal advertised, how do you decide whether it's truly a good bargain or just clever marketing?
- Have you ever felt pressured to buy something in-store because of a countdown, limited quantity, or crowd excitement? How do those strategies influence your decisions?

NARRATIVE

Every holiday season, shoppers are drawn to "door busters" and flashy in-store deals promising huge savings on popular gifts. These promotions can be exciting, but they are also designed to generate store traffic and encourage people to act fast.

Understand how to spot real bargains and avoid high-pressure sales tactics.

- Read the fine print before you shop.
 - Some door buster deals can start early, even before normal store hours, so it is worth checking the advertised times carefully. These deals are often available in extremely limited quantities, sometimes with no rainchecks offered, and may be limited to the first few customers.
- Review the seller's return and exchange policy.
 - Most retailers accept returns. Some even extend their return policies during the holiday season. However, there may be final sales, exclusions or conditions on "deal" items. Make sure to read the terms carefully before buying.
- Remember, sellers must honor the lowest posted price.
 - In Wisconsin, if a customer is charged more than the lowest advertised or displayed price for an item, they must be refunded the difference.
- Save all receipts and packaging in case a purchase needs to be returned.

RESOURCES

- The Basics of Price Accuracy | Department of Agriculture, Trade and Consumer Protection https://datcp.wi.gov/Documents/BasicsPriceAccuracyFAQ.pdf
- Price Refund: Price Information Requirements | Department of Agriculture, Trade and Consumer Protection
 - https://datcp.wi.gov/Documents/PriceRefundPricePostingFactSheet.pdf

SLIDE



NARRATIVE

Some consumers may be tempted by holiday credit card offers. When considering this, know what to look for in a new card and what to watch out for.

"Save a certain percentage off today's bill".

Store credit card offers like "Save a certain percentage off today's bill" are a trade-off: a one-time discount in exchange for opening a new credit card account. These offers often come with significant drawbacks, including high interest rates and potential harm to your credit score.

Store cards often have a higher APR.

The discount often comes with a store card that has a much higher Annual Percentage Rate (APR) than a regular credit card. Some store card APRs can be as high as 30% or more, compared to the current average of around 20% for regular cards. If you carry a balance, the interest charges will quickly erase any savings from the initial discount.

Require entering your Social Security number and date of birth to apply.

A store credit card is not the same as a store's free loyalty program, which often just requires your email or phone number to provide special discounts. If you are offered a "save today" deal at the register, it is likely a credit application, and you will be asked for your personal identifying information.

Does your credit freeze need to be lifted?

If you have a credit freeze, you must lift it before applying for a store credit card or any other form of new credit. A credit freeze prevents any lender, including the bank that issues the store card, from performing a "hard inquiry" to check your credit report.

9. GIFT CARDS 3 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

During the holidays, gift cards offer a blend of thoughtful personalization and practical convenience for both the giver and the recipient. When shopping for gift cards during the holidays, consumers should keep a few considerations in mind:

When giving:

Purchase as close to the holiday as possible

It is easy to misplace a physical gift card or lose track of an e-gift card that has been sent to your email. If the company that issued the gift card goes out of business, your card could become worthless.

Check for tampered packaging

Before buying, check for any signs that a card's packaging has been opened, peeled, or resealed.

Examine for bar code stickers covering the real bar code on the packaging

Scammers can place fraudulent barcode stickers over the card's real one. When scanned, the money you pay is loaded onto a different account controlled by the scammer.

Ensure the receipt data matches the card you just purchased

It is critical to ensure the gift card number on your receipt matches the card itself to protect against tampering and fraud. By checking the numbers at the point of sales, you can confirm you are leaving with the correct, newly activated card.

When receiving:

Use it right away

To maximize the card's value, you should use a gift card as soon as possible after receiving it. Putting it off increases your risk of losing the physical card, forgetting about an e-gift card, or having the value stolen by scammers who are specifically targeting activated cards.

Never give the numbers to a stranger

Once you provide the numbers and PIN, the funds are essentially untraceable and often gone instantly.

SLIDE



NARRATIVE

During the holidays, friends and families share joyful moments and connect across distances using social media. However, scammers take advantage of this opportunity to target consumers through multiple tactics:

- Fake ads with links to click: These appear to be from trusted brands or friends and contain
 malicious links. When clicked, the links can lead to websites designed to steal personal data or
 install malware.
- "Free" giveaways: Be highly skeptical of "free giveaways" on social media, especially during the
 holidays, as many are scams designed to steal your money and personal information. Legitimate
 businesses do run giveaways, but scammers often impersonate well-known brands to appear
 trustworthy.
- Imposter websites: Fraudulent ads for deeply discounted or hard-to-find items are common on social media. These ads link to fake shopping sites that either sell counterfeit goods or take your payment without shipping anything.
- Marketplace scams: Scammers heavily use online social media marketplaces and classified ads
 during the holidays, exploiting the high volume of buying and selling to steal money from both
 buyers and sellers.
- Too good to be true deals: Scammers deceive consumers with high-value items, like luxury
 vacations, expensive electronics, or large sums of cash, to make the offer irresistible. Real
 giveaways are usually more modest.
- **Surveys:** Never share personal or financial information in response to a survey, especially if you were not expecting it.
- Holiday games: Harmless-seeming social media games like "What's your elf name?" are a common tactic used by scammers to collect your personal data. These quizzes are designed to collect key pieces of information that scammers can use for identity theft or to hack into your online accounts.
- Pay it forward / Gift exchange: These scams, which sometimes use names like "Secret Sister,"
 "Wine Exchange," or "Secret Santa Dog," rely on recruiting new participants to send money or gifts to the people at the top of the pyramid. You are promised a significant number of gifts in return, but this never materializes.

Tips for consumers

- Do your research before making any purchases or clicking on links from social media ads.
- Always be skeptical of unsolicited messages, or ads from unfamiliar sources.

SLIDE



INSTRUCTIONS FOR PRESENTER

Consider asking a prompt question to introduce the topic:

- When you see a charity request during the holidays, what is the most important factor you consider when deciding to donate?
- Do you consider if the charity is a legitimate organization?

NARRATIVE

During the holidays, many people feel inspired to give back and support causes that make a difference, especially on Giving Tuesday. This global generosity movement occurs on the first Tuesday after Thanksgiving. On this day, millions of people come together to give back to their communities through acts of kindness, donating, volunteering, and advocating for their favorite causes.

Unfortunately, scammers know this too, and they often take advantage of our generosity through email, social media, text message, or phone call scams.

Understanding how to verify a legitimate charity and spot red flags of a scam is key to ensuring that your donations truly reach the people and causes you care about.

- Real charities are allowed to call you and request donations.
 Real charities are exempt from the Wisconsin Do Not Call Registry, which applies to telephone solicitations or telemarketing calls.
- However, there is nothing stopping a criminal from impersonating a charity.
 Charity scams increase around Giving Tuesday, as criminals seek to exploit people's generosity during the holiday season. They often use deceptive tactics to pose as legitimate organizations and steal donations.
- It may be impossible to tell the difference between the two calls.

 It is not easy to tell the difference between scam calls and legitimate charity calls, as scammers have become adept at imitating real organizations. They intentionally use deceptive tactics to make their calls seem convincing, making it essential to be vigilant and verify any donation request you receive.
- **Solution**: Never give money to an unexpected phone call, email, or text. Research the organization at www.CharityNavigator.org or www.Give.org and then donate on the organization's legitimate website or by writing a check to the organization not to an individual solicitor.

SLIDE



NARRATIVE

Scammers exploit the holiday season by creating fake delivery notifications or fake account alerts. Holiday shipping scams often involve fake texts or emails claiming there's an issue with a delivery, like a "failed delivery" or a request to "pay a small fee" to complete the delivery. These messages contain phishing links that lead to fake websites designed to steal your personal information, login credentials, or financial details.

Common tactics used by scammers

"Problem" with your order.

These texts often create a false sense of urgency about a missed delivery or unpaid fee to trick you into clicking a malicious link.

- Additional postage/fee.
- o Verify delivery address.
- o Missed delivery.
- · Click here for tracking or to confirm delivery.

The link in the text leads you to a fake website designed to appear like a legitimate carrier's tracking page.

Call this number to report any problems.

Some delivery text scams ask you to call a number to resolve a problem. In these cases, calling the number connects you directly to a scammer, who uses social engineering to steal your personal and financial information. For example:

- The scammer will claim they need to verify your identity or delivery details and will ask for personal information such as your full name and address, credit card and other financial information, or Social Security number.
- The scammer will claim you need to pay a small fee to get your package released, such as a "customs fee" or a "redelivery fee." They will take your payment information and disappear with the funds.

IMPORTANT CONSIDERATIONS

Phishing: Phishing is an online scam where criminals pretend to be a trusted person or company to trick people into giving them sensitive information, like passwords, credit card numbers, or bank account details.

Smishing: Smishing is a form of cybercrime that uses deceptive text messages to trick people into revealing sensitive personal or financial information. The term is a mashup of "SMS" (for Short Message Service, or text messaging) and "phishing."

RESOURCES

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

13. DECEPTIVE PAYMENT METHODS (RED FLAGS)

3 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

Scammers leverage the busy atmosphere and festive emotions to create a "perfect storm" by impersonating a trustworthy person or organization to trick you into sending money. You might receive a call, email, text, or social media message that appears to be from a legitimate source. The message usually states there is a problem with your account, you have a prize, or you are connected to criminal activity to make you panic. Next, they will ask for payment.

Deceptive payment methods (red flags)

Scammers frequently demand payment using methods that are hard to trace and recover.

Scammers take advantage of the evolution from wire transfers to prepaid cards, gift cards, and cryptocurrency by exploiting the vulnerabilities inherent to each payment method. They have adapted their tactics to leverage features like speed, convenience, and anonymity, while capitalizing on consumer lack of awareness and a false sense of security.

A request for payment using any of the deceptive methods listed below is a major red flag for a scam.

SLIDE



INSTRUCTIONS FOR PRESENTER

Consider asking a prompt question to introduce the topic:

 Have you ever received an unexpected message or email saying you are owed a refund for a recent purchase or delivery, what made you trust or doubt it?

NARRATIVE

In a holiday refund scam, scammers impersonate retailers or service providers to trick you into giving up personal information or money. These scams often appear as fake refund notifications.

Examples of the language scammers use to lure their victims:

- A "routine quality inspection" determined a recent purchase doesn't meet quality standards or has been recalled.
 - o Click here to request refund.
 - o Call this number to report fraud.

How the scam works

The message often creates a sense of urgency, telling you to act quickly to claim the refund. The notification comes by email or text and contains a link to a fake website to "claim" the refund. The website is designed to steal your personal information, login credentials, or financial details.

How to protect yourself

- Never click on links in emails or texts about refunds unless you initiated the transaction and are sure of the source.
- Independently verify any refund notice by contacting the company directly through their official website or phone number.
- Monitor your bank accounts for unauthorized activity.

15. Toy Safety 2 MIN

Facilitator Notes/Questions

SLIDE



INSTRUCTIONS FOR PRESENTER

Consider asking a prompt question to introduce the topic:

- Why is it important to follow the age recommendations on toy packaging?
- When buying toys for children, what safety features do you check for first?

NARRATIVE

Holidays are one of the most exciting times of the year for children—and one of the busiest for toy shopping. Some toys may contain parts not appropriate for all ages that pose choking hazards and other risks.

- Always check for hazards.
- Take a few moments to review labels and inspect the packaging to identify:
 - Suggested age range for using the product.
 - Small parts, sharp edges, magnets, choking hazards.
- Ask yourself if a younger child who also lives in the household might access the toy or parts.
- Consider including safety gear with your gift, like a helmet with a bike or scooter.

Understanding how to choose safe, age-appropriate toys helps ensure that holiday surprises bring joy and not injuries.

RESOURCES

 Child Care Safety | Department of Agriculture, Trade and Consumer Protection https://datcp.wi.gov/Pages/Publications/ChildCareSafety230.aspx

16. How to FILE A COMPLAINT

1 MIN

Facilitator Notes/Questions

SLIDE



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

17. 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.

18. THANK YOU

0.5 MIN

Facilitator Notes/Questions

SLIDE

