FACILITATOR GUIDE

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

PRESENTATION: SAFE ONLINE SHOPPING

The **Safe Online Shopping Guide** 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 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.

TABLE OF CONTENT

1. COVER PAGE	0.5 MIN

Facilitator Notes/Questions

SLIDE

2. FTC DATA 2024	2 MIN

Facilitator Notes/Questions

SLIDE

INSTRUCTIONS FOR PRESENTER
You may consider asking the audience about who has shopped online lately to get a sense of how familiar audience members are with the online shopping experience.

NARRATIVE
The FTC's Consumer Sentinel Network data, specifically the Consumer Sentinel Network Data Book, provides insights into online shopping fraud, including trends and reported losses. Online shopping fraud was the second most reported fraud type in 2024, with 11,515 reported cases.

Online Shopping and Negative Reviews:
This category includes the following subcategories: undisclosed costs, failure to deliver on time, non-delivery, and refusal to honor a guarantee on purchases made online; internet auctions; 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

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? (*Encourages personal reflection and opens discussion about convenience vs. safety.)*
- Do you think it is safer to shop from a phone or a laptop?

NARRATIVE

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 primary way most consumers connect to the web, and as users we need to make sure they are our first line of protection.

 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 improve protection.
    - o Ensure you have the latest versions of your operating system, browsers, apps, and protection software.
- **Be mindful of how you send sensitive information:** Never email sensitive data (credit card numbers or personal information). Only share this information through trusted payment systems or websites.

RESOURCES

- **Protect Your Personal Information From Hackers and Scammers | Federal Trade Commission**
  https://consumer.ftc.gov/articles/protect-your-personal-information-hackers-and-scammers

Facilitator Notes/Questions

SLIDE

INSTRUCTIONS FOR PRESENTER
You may consider asking the audience about their experience connecting to the web through a public Wi-Fi connection. Here are some ways to phrase questions to promote participation and gather insights:
- Have you ever connected to Wi-Fi at a coffee shop, airport or store? What made you trust that connection?
- What do you some think someone could see or do if they were in the same public Wi-Fi network as you?

NARRATIVE
In addition to the device, online shoppers also need a connection to the internet. More importantly, shoppers need to ensure they have a secure connection to the web.

Connecting to the web with Wi-Fi connections:
- Accessing the internet using a public Wi-Fi hotspot is convenient and often free for mobile users, but hotspots typically are not secure. If you are not required to enter a password provided by the Wi-Fi host (e.g., a coffee shop or hotel) before gaining access to the network, another Wi-Fi user could hack into your electronic device to access your personal information and what you are sending.
- Scammers also create Wi-Fi networks that may closely resemble the real one.
    - For example: 'StarbucksWiFi' is not the same as 'starbuckswifi' or 'Starbucks,' which is why you need to pay attention to the network name.

Connecting to the web through 4G or 5G on your phone:
- Generally, it is reasonably safe to use a 4G or 5G data connection provided by your phone carrier. This is because they incorporate enhanced security features with encryption algorithms and improved authentication protocols.

Using a VPN (Virtual Private Network):
- A Virtual Private Network (VPN) secures and makes private any data sent across a network, usually the internet, by building an "encrypted tunnel." Data passes through this tunnel, protecting it from anyone who tries to intercept it. Even if the data is intercepted, it is hopelessly scrambled and useless to anyone without the key to decrypt it.
- VPNs are designed to be used on computers and mobile devices, and they can be installed and used on both Android and iOS devices.
- Keep in mind that you will have to purchase a VPN to use it.

RESOURCES
- **Tips for Using Public Wi-Fi | Department of Agriculture, Trade and Consumer Protection** https://datcp.wi.gov/Pages/Publications/IDTheftWi-FiTips659.aspx

Facilitator Notes/Questions

SLIDE

NARRATIVE

Online shopping offers convenience and a vast selection, but it is crucial to be aware of potential risks and take precautions to choose trusted online retailers.

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 malicious links and phishing attempts:
- Be wary of phishing attempts. Do not click on links in suspicious emails or texts from unknown senders. Always access websites directly by typing the address into your browser.

Using search engines for online shopping can lead to fake or deceptive sellers:
- Using search engines for online shopping can generate poor results that carry risks such as fake stores, data breaches, fake reviews, and identity theft.
- Online search and social media suggestions may lead you to a fake/malicious website.
  - *Note: Slide #9 further explores social media advertisements.*

Shop on reputable sites:
- Stick to well-known and trusted online retailers.
- Research unfamiliar businesses. If you decide to shop with a new online store, check reviews on platforms like Trustpilot and Google.
  - *Note: Slide #7 expands on this topic.*
- Beware of "too good to be true" deals. Exceptionally low prices may indicate a scam or fraudulent website.

RESOURCES
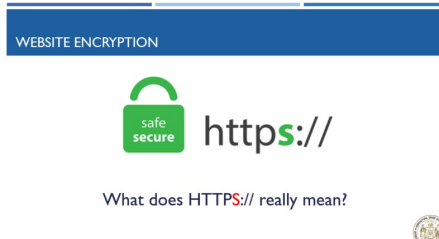- **Online Shopping - Security Tips | Federal Trade Commission**
  https://consumer.ftc.gov/media/79929
- **Safe Online Shopping Tips | Department of Agriculture, Trade and Consumer Protection**
  https://datcp.wi.gov/Pages/Programs_Services/SafeOnlineShoppingTips.aspx

6. WEBSITE ENCRYPTION   3 MIN

SLIDE

WEBSITE ENCRYPTION

https:// safe secure

What does HTTPS:// really mean?

INSTRUCTIONS FOR PRESENTER
You may consider asking the audience a prompt question to introduce the topic of the importance of HTTPS:
- Have you ever noticed a little padlock icon or the "https" at the beginning of a web address?
- Would you feel safe entering your credit card information on a website without the lock icon? Why or why not?

NARRATIVE

How HTTPS works:
'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; ensuring that data transmitted between the two is <u>secure</u> (hence the added 'S') and protected from eavesdropping or tampering.

How data encryption works:
HTTPS uses encryption to scramble data, making it unreadable to anyone who might be trying to intercept it during transmission.

IMPORTANT CONSIDERATIONS
- Look for "HTTPS" and a padlock icon. Ensure the website URL begins with "https://" and has a padlock symbol 🔒 in the address bar, indicating a secure connection and encrypted data transmission. A deadlock alone does not indicate security.
- Never send payment card info or personal info on an unencrypted website (HTTP).
- While HTTPS ensures a secure connection, it does not guarantee a website's legitimacy or trustworthiness. Any website can use HTTPS, including those that might be trying to deceive you. HTTPS primarily protects the data transmitted between your browser and the server, but it does not protect you from phishing or other scams.
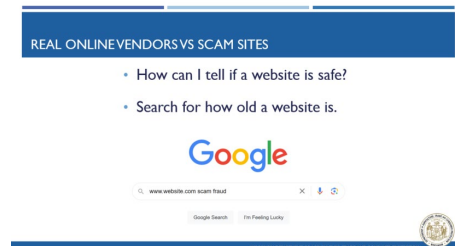
RESOURCES
- **Tips for Using Public Wi-Fi| Department of Agriculture, Trade and Consumer Protection**
https://datcp.wi.gov/Pages/Publications/IDTheftWi-FiTips659.aspx

Facilitator Notes/Questions

SLIDE

INSTRUCTIONS FOR PRESENTER
Here are two prompt questions to introduce the topic of real online vendors vs. scam sites.
- When you shop online, how can you tell if a website is trustworthy or sketchy?
- Have you or someone you know ever ordered something online and it never arrived? Was it what you expected?

NARRATIVE
Just because a website looks real and appealing, it does not mean it is legitimate website.
How can you tell if a website is safe and legitimate? Here are a few tips to help you identify red flags that should alert you to navigate away.

Tips for spotting a potentially unsafe website:
1. **Search engine check:** Search the website's URL with terms like "scam" or "fraud" to see if others have reported problems.
2. **Website checkers:** Use tools like Google Safe Browsing or Norton Safe Web to assess the site's security status.
3. **Domain name**: Be cautious of domains ending in .biz or .info, as they are less common for legitimate organizations.
4. **Contact information:** A legitimate website should have a contact page with a physical address, phone number, and email address. The absence of this information is a red flag.
5. **Website red flags:** Evaluate website design, content, contact info, and security features for potential signs of fraud.
6. **Hover over links**: Mouse over links to see where they truly lead before clicking, to avoid deceptive URLs.
7. **Domain age:** Check how long the website has been active, using a WHOIS lookup or similar tool, as older domains are generally more trustworthy.

RESOURCES
- **Google Transparency Report | Google**
  https://transparencyreport.google.com/safe-browsing/search
- **Norton SafeWeb | Norton**
  https://safeweb.norton.com/
- **Domain Name Age Checker | What's my DNS**
  https://www.whatsmydns.net/domain-age
- **Trustpilot**
  https://www.trustpilot.com/
- **Better Business Bureau**
  https://www.bbb.org/

8. COMPUTER SECURITY TIPS	6 MIN

SLIDE
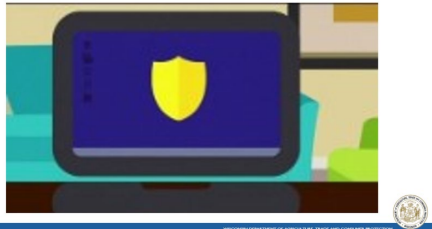
INSTRUCTIONS FOR PRESENTER
If possible, play the video for the audience. Duration 3:32 minutes.

You may consider asking some prompt questions to generate comments after the video.
- What are some things you do, or should do to keep your computer safe from viruses or hackers?
- Why do you think it is important to update your software or run antivirus scans?

IMPORTANT CONSIDERATIONS – AFTER WATCHING VIDEO
Key ways to protect yourself online:
1. **Install and update security software.**
    - Use reputable security software (many free options are available).
    - Ensure it is set to update automatically to handle new threats.
    - Also set your operating system and web browser to automatically update.
    - Be wary of unsolicited messages claiming your computer is infected, as they could be scams trying to sell you fake software.
2. **Protect your financial information.**
    - Treat financial information (Social Security number, credit card numbers, bank account details) like cash.
    If asked for financial information, verify the reason and security measures in place when requested for financial information.
3. **Research unfamiliar online companies.**
    - If you find a deal from a company you do not know, investigate before buying.
4. **Create strong passwords.**
    - Make passwords at least 10 characters long.
    - Use a mix of letters, numbers, and special characters.
    - Avoid using easily guessable information, like your name.

RESOURCES
- **Computer security tips | Federal Trade Commission**
  https://www.ftc.gov/media/70875
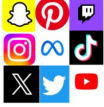
Facilitator Notes/Questions

SLIDE

INSTRUCTIONS FOR PRESENTER
Here are two prompt questions to introduce the topic of social media advertisements:
- Have you ever clicked on ad while scrolling through Instagram, Facebook, or TikTok? What made you click, or ignore it?"
- "Do you think all ads on social media are from real companies? Should you click on the links from your social media feed?

NARRATIVE
Fake ads on social media are a growing concern, leading to scams and misleading consumers. These ads often exploit the platform's reach, targeting, and user trust to deceive individuals. They can appear legitimate but offer poor quality products or services, or even lead to scams and fraud.
By being aware of red flags and taking preventive measures, consumers can protect themselves from scams and deceptive practices.

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.
- Be suspicious if a company lacks verifiable reviews, testimonials, or a professional website.
- Avoid making rushed decisions; legitimate businesses rarely require immediate action.
- Remember the adage: "If it seems too good to be true, it probably is."

RESOURCES
- **Advertising and Marketing Basics | Federal Trade Commission**
  https://www.ftc.gov/business-guidance/advertising-marketing/advertising-marketing-basics

SLIDE

INSTRUCTIONS FOR PRESENTER

Here are two prompt questions to introduce the topic of shopping with international or overseas retailers:

- Have you ever ordered something online and later realized it was coming from another country? What happened?
- What do you think are the risks associated with buying from an international seller?

NARRATIVE

Consumers may be attracted by "apparent" lower prices from international and overseas retailers. Nonetheless, there are potential risks to consider.

Tips for shopping with international or oversea retailers:

- **Review your order summary**: Carefully check all the product details, conditions, shipping costs, and the delivery address before making a purchase. Keep copies of all documentation and order confirmation emails.
- **Review the return policies:** Carefully review the retailer's return policy before making a purchase, as this can help mitigate the risk of receiving a product that does not meet your expectations.
- **Confirm shipping details with seller.** This will clarify delivery time expectations and avoid additional costs for faster delivery or incorrect addresses.
- **Check size charts thoroughly:** Compare the retailer's size chart with your own measurements, and if possible, compare it with size charts from brands you are familiar with.
- **Clarify product details**: If you have any doubts about the product description or features, contact the seller directly to ask for clarification.
- **Ensure accurate delivery with tracking**: If provided, track the delivery and contact the retailer if you have any questions.

RESOURCES

- **eConsumer.gov | International Consumer Protection and Enforcement Network.** https://econsumer.gov/#crnt?lang=en-US

11. ONLINE MARKETPLACE	**3 MIN**

SLIDE

NARRATIVE

An online marketplace is a digital space or platform that connects buyers and sellers, facilitating transactions for goods and services without the marketplace owner necessarily holding any inventory themselves. Examples of product marketplaces include Facebook, eBay, Etsy, and Pinterest.

How this type of marketplace operates?

Sellers on a marketplace platform range from individual users selling pre-owned items to small businesses. Some platform allows for simpler product listings, often without the need for extensive product descriptions or professional photography.

Risks associated with this type of marketplace platform:

- **Counterfeit goods:** Sellers may list fake or imitation items as authentic, especially for branded or high-value goods.
- **Faulty or damaged items:** Products may not function as described, or have hidden defects not disclosed by the seller.
- **Non-delivery:** Sellers may take payment without ever shipping the item, or provide fake shipping information.
- **Phishing and social engineering:** Scammers may try to trick buyers into clicking malicious links or revealing personal information.
- **Lack of formal seller verification:** Unlike dedicated e-commerce platforms, some online marketplace may not have strict seller verification processes, increasing the risk of encountering dishonest individuals.
- **Limited buyer/seller protection**: While some platforms offer some tools for reporting issues, it is not as robust as dedicated buyer protection programs on e-commerce platforms.
- **Privacy concerns.** Buyers may unintentionally reveal personal information that could be used for identity theft or other malicious purposes.

Tips for staying safe on online marketplaces:

- **Research buyers and sellers**: Check seller's profiles for authenticity, reviews, and any red flags.
- **Communicate with seller through the platform:** Avoid communicating outside of the platform.
- **Use secure payment methods:** Cash or built-in payment system are generally safer.
- **Inspect items thoroughly:** When possible, carefully inspect items before purchasing them.
- **Be mindful of overpayment scams:** Where buyers pretend to overpay for a product, then request a refund, and walk away with your money, when the original payment is reversed due to fraud.
- **Report suspicious activity**: Report scams and suspicious users to the platform, and submit a complaint with the Bureau of Consumer Protection.

RESOURCES

- Buying From an Online Marketplace | Federal Trade Commission
  https://consumer.ftc.gov/articles/buying-online-marketplace

SLIDE

NARRATIVE

Consumers should read the return policy before making a purchase. Understanding the seller's return policy is crucial for making informed purchases. A return policy outlines the conditions and process for returns, exchanges, and refunds. This 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's 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 fees**: Understand whether you or the retailer is responsible for return shipping fees. Some retailers may offer free return shipping, while others may offer different options with varying costs.
  - For example: A company indicates that the seller pays for return shipping if they offer a free returns policy or if the item was damaged, faulty, or doesn't match the listing description. The buyer pays for return shipping if they are returning the item because they changed their mind, and the seller's return policy states that buyers are responsible for return shipping.
- **Return window/timeframe**: Look 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
- **Amazon Return Policy | Amazon**
  https://www.amazon.com/gp/help/customer/display.html?ref_=hp_bc_nav&nodeId=GNW5VKFXMF72FFMR
- **Return shipping for buyers | eBay**
  https://www.ebay.com/help/buying/returns-items-not-received-refunds-buyers/returning-item/return-shipping?id=4066

13. Payment Methods	4 MIN

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:**
    - o 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.
    - o 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) as a payment option
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.

- **Tips for using F&F safely:**
    - o 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.
    - o Scammers often try to trick consumers into using F&F for purchases, knowing they will have no recourse if they do not deliver or the item is faulty.

Difference between credit cards, debit cards and gift cards as it relates to buyer protection
- **Credit cards:**
    - o **Strongest buyer protection:** Credit cards generally offer the most comprehensive buyer protection.
    - o **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).
    - o **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.

- **Debit cards:**
    - o **Limited buyer protection:** Debit cards offer less robust buyer protection compared to credit cards.
    - o **Purchase protection:** Debit cards typically do not offer purchase protection or other similar benefits.
    - o **Fraudulent activity:** Federal law and bank policies offer some protection, but 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:**
    - o **Limited buyer protection:** Gift cards offer the least amount of buyer protection, often with no recourse if lost or stolen.
    - o **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.
- **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

14.	WHERE WILL THE PACKAGE BE DELIVERED?	2 MIN

SLIDE

INSTRUCTIONS FOR PRESENTER

Here are two prompt questions to introduce the topic of porch pirates (package theft):

- Have you or someone you know ever had a package stolen from the front porch or mailbox? What did you do?"
- What are some ways people can protect their deliveries from being stolen?

NARRATIVE

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:

- **Install a package lockbox or delivery box:** A lockable box on your porch can provide a secure location for packages to be placed
- **Install a security camera or video doorbell:** These devices can deter potential thieves and capture valuable evidence if a theft occurs.
- **Request signature confirmation for deliveries:** This ensures packages are not left unattended and can only be delivered to the intended recipient.
- **Use package lockers or pickup locations:** Many delivery services offer secure package lockers or allow you to have packages delivered to designated pickup locations, minimizing the risk of theft.
- **Request delivery to a neighbor or friend:** If you know someone who is home during the day, you can have your packages delivered to their address for safekeeping.
- **Utilize delivery tracking and notifications:** Stay informed about the expected delivery time and quickly retrieve your package upon arrival to minimize the time it sits unattended.

RESOURCES

- Mail & Package Theft | United States Postal Inspection Service
  https://www.uspis.gov/tips-prevention/mail-theft

15.	SHIPPING SCAMS AND HOW TO SPOT THEM	2 MIN

SLIDE

INSTRUCTIONS FOR PRESENTER

Here are two prompt questions to introduce the topic of delivery/shipping text scams:

- Have you ever received a text or email saying your package is delayed or needs a delivery fee, but you weren't expecting anything?
- What would you do if you got a message asking you to click a link to 'reschedule a delivery'? How do you know if it's real?

NARRATIVE

Fake shipping scams are considered "smishing" scams. In the case of fake delivery/shipping texts, scammers pretend to be from the Postal Service (USPS) or FedEx, and try to trick you into clicking a malicious link and providing personal or financial information.

Smishing: Smishing, a combination of "SMS" and "phishing," is a cybercrime that uses deceptive text messages to trick people into revealing sensitive information, such as passwords, credit card numbers, or Social Security numbers. It relies on social engineering tactics like urgency, fear, and curiosity to manipulate victims into taking immediate action, often by clicking a malicious link.

How to protect yourself from postal delivery scams

- **Be cautious of unsolicited messages:** Do not click on links or provide personal information unless you are certain the message is legitimate.
- **Verify tracking information:** Use the official delivery company's website to track packages, not links in messages.

IMPORTANT CONSIDERATIONS

- USPS utilizes the 5-digit short codes to send and receive SMS to and from mobile phones.
- Smishing: The word is a blend of SMS + phishing. Other modalities of smishing include Bank or Credit Card Alerts Fake Messages, Government or IRS Scams, Prize or Giveaway Scams, and Account Suspension Scams.

RESOURCES

- **Smishing: Package Tracking Text Scams | United States Postal Inspection Service**
  https://www.uspis.gov/news/scam-article/smishing-package-tracking-text-scams

16.	INFORM CONSUMERS ACT	2 MIN

SLIDE

INFORM CONSUMERS ACT

The goal of the INFORM Consumers Act is to add more transparency to online transactions and to deter criminals from acquiring stolen, counterfeit, or unsafe items and selling them through those marketplaces.

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

How does this act protect me as a consumer?

Can I file a complaint?

INSTRUCTIONS FOR PRESENTER
Consider this to introduce the topic of the Inform Consumers Act:
- "When you buy something from a seller on Amazon, eBay, or Facebook Marketplace, do you ever wonder who's really behind the sale, and whether you can trust them?"
  (Gets the audience thinking about transparency and online marketplaces.)

NARRATIVE
What is the purpose of the law?
- When consumers buy products from online marketplaces, the identity of the seller is often unclear.
- The goal of the INFORM Consumers Act is to add more transparency to online transactions and to deter criminals from acquiring stolen, counterfeit, or unsafe items and selling them through those marketplaces.
- Online marketplace must provide a way to file a complaint if stolen, counterfeit, or unsafe items are received.
- Disclosure requirements apply to high-volume third-party sellers with annual gross revenues of $20,000 or more on a particular online marketplace. If they meet that threshold, the marketplace must clearly disclose the above information on each of the seller's product listing pages.
- The law went into effect June 2023.

RESOURCES
- [Informing Businesses about the INFORM Consumers Act | Federal Trade Commission](https://www.ftc.gov/business-guidance/resources/INFORMAct)
  https://www.ftc.gov/business-guidance/resources/INFORMAct

SLIDE

NARRATIVE

Online marketplaces must collect, verify and disclose certain information about high-volume third-party sellers.

- **Collect:**
  - Bank account, tax ID and contact information.
- **Disclose:**
  - The seller's full name.
  - The seller's physical address.
  - Contact information that will allow "direct, unhindered communication" with the seller.

IMPORTANT CONSIDERATIONS

Additionally, the online marketplace must take additional steps, which includes the following.

- **Verification:**
  - Online marketplaces must verify the information they get from these sellers. They also must require sellers to keep their information current and to certify it is accurate at least once a year.
- **Suspension of non-compliant sellers:**
  - Online marketplaces must suspend high-volume third-party sellers that do not provide information the law requires.
- **Reporting mechanism.**
  - Online marketplaces must provide a clear way for consumers to report suspicious conduct on high-volume third-party sellers' product listings.

RESOURCES

- [Informing Businesses about the INFORM Consumers Act | Federal Trade Commission](https://www.ftc.gov/business-guidance/resources/INFORMAct)
  https://www.ftc.gov/business-guidance/resources/INFORMAct

18. HOW TO FILE A COMPLAINT	2 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

19.	LEARN MORE ABOUT DATCP	1 MIN

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.

RESOURCES
- Consumer Protection Presentations| Department of Agriculture, Trade and Consumer Protection
https://datcp.wi.gov/Pages/Publications/RequestPresentation.aspx

20.	THANK YOU	MIN

Facilitator Notes/Questions

SLIDE