FACILITATOR GUIDE

The Department of Agriculture, Trade and Consumer Protection's (DATCP) Bureau of Consumer Protection (BCP) created this guide to assist educators in providing information to students about Consumer Protection.

PRESENTATION: CONSUMER PROTECTION FOR YOUNG ADULTS

This Presenter Guide is a tool developed by the Bureau of Consumer Protection to assist presenters delivering the Consumer Protection for Young Adults presentation.

Audience: General public, community groups, young 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.

The **Consumer Protection Facilitator Guide** is to be used in conjunction with the delivery of the presentation developed by DATCP's Bureau of Consumer Protection (BCP). This presentation covers topics related to deceptive practices, common scams, identity theft, WI landlord tenant laws, and WI motor vehicle repair regulations.

Questions can be directed to the Consumer Protection Hotline at 1-800-422-7128 or DATCPHotline@wisconsin.gov. You will be connected to an Outreach Specialist. If there is a need for the guide to be used provided a PPT rather than a PDF, please submit requests to the hotline.

TABLE OF CONTENT

Slide	Content	Page
1	Cover page	3
2	Bureau of Consumer Protection	3
3	Topics covered today	4
4	Deceptive Practices - Explained	5
5	Deceptive advertising campaigns	6
6	Vaping and e-cigarettes	7
7	Deceptive advertising campaigns	8
8	Dark Patterns	9
9	Common scams – Explained	11
10	Scams - Statistics	12
11	Scams - Statistics	13
12	Scams - Statistics	13
13	Deceptive payment methods (red flags)	14
14	Social media scams - How they happen	15
15	Online shopping scams – How they happen	16
16	Friends and family (grandparent) scam	18
17	Scams involving Artificial intelligence (AI)	19
18	Student loan and financial aid scams	20
19	Identity theft - Explained	21
20	Identity theft - What they want?	22
21	How it happens - Online	23
22	How it happens - In-person	24
23	How it happens - Data breach	25
24	Identity theft – Social networking	26
25	Identity theft - Warning signs	27
26	Identity theft - Prevention	28
27	Identity theft - Prevention	29
28	Credit report security freeze	30
29	Landlord tenant basics – Explained	31
30	Types of lease	32
31	Disclosure requirements	33
32	Breaking a lease	34
33	Promises to repairs	35
34	Security deposits	36
35	Tenant's responsibilities	37
36	Motor vehicles - Explained	38
37	Buying a used car from a private seller	39
38	Motor vehicle repair shops	40
39	How to file a complaint	41
40	Learn more about DATCP	42
41	Thank you	42

1. Consumer Protection for Young Adults

2 MIN

Facilitator Notes/Questions

SLIDE



2. Bureau of Consumer Protection

2 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

Bureau Of Consumer Protection (BCP)

The bureau's mission is to ensure fair business practices for buyers and sellers alike by prohibiting fraud, deception, and unfair business practices in the marketplace.

- Consumer Protection Hotline: 1-800-422-7128
- ConsumerProtection.wi.gov

In 2024, DATCP responded to over 11,000 consumer complaints, returning over \$23 million to affected Wisconsin consumers.

These statistics represent the top consumer complaints received by DATCP's Bureau of Consumer Protection in 2024.

IMPORTANT CONSIDERATIONS

• Landlord-tenant issues topped the list of complaints, followed by telemarketing and home improvement concerns.

3. TOPICS COVERED TODAY

1 MIN

Facilitator Notes/Questions

SLIDE

TOPICS COVERED TODAY

1. Deceptive practices
2. Common Scams
3. Identify theft
4. Landford Tenant Law
5. Motor Vehicle Repair

NARRATIVE

It is crucial students learn how the following factors can affect them and affect their lives, even at the high school age, that's the reason we are covering these topics today.

Topics Covered Today:

- Deceptive Practices
- Common Scams
- Identify Theft
- Landlord Tenant
- Motor Vehicle

4. DECEPTIVE PRACTICES - EXPLAINED

2 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

Deceptive practices, also known as deceptive trade practices, are actions that mislead or deceive consumers, often with the intent to induce them into making a purchase or engaging in a transaction.

INSTRUCTIONS FOR PRESENTER

For young consumes it is worth highlighting the deceptive practices used by the vaping and e-cigarettes to engage younger audiences.

Emphasize that the vaping and E-cigarettes industry targets younger consumers to tap into the next generation as a market.

Learn how this industry uses deceptive practices to engage younger audiences:

- Why this is not the first time this has happened.
- How these businesses are using advertising campaigns to target young audiences.

SLIDE



NARRATIVE

- This has happened before with cigarettes.
- In the past, the tobacco industry used a variety of tactics to target youth, including advertising and promotion, celebrity endorsements, and even product placement in media programming intended for young audiences.

INSTRUCTIONS FOR PRESENTER

You may consider questions you can ask your audience to generate answers from audience.

- Why the vaping industry is marketing to children?
 Leads into indicating the following points:
 - o Industry calls young people "replacement smokers".
 - o When teens vape, they stress more so they vape more.
 - o Nicotine is highly addictive, and starting early makes it more difficult to quit later.

IMPORTANT CONSIDERATIONS

 Children and young people are particularly susceptible to marketing tactics and the influence of peers and advertising. They are also less likely to fully understand the long-term consequences of nicotine addiction.

RESOURCES

 Tobacco is Changing: E-Cigarettes | Wisconsin Department of Health Services https://www.dhs.wisconsin.gov/tobaccoischanging/e-cigarettes.htm

6. DECEPTIVE PRACTICES - VAPING AND E-CIGARETTES

3 MIN

Facilitator Notes/Questions

SLIDE



INSTRUCTIONS FOR PRESENTER

You may consider questions you can ask your audience to generate answers from audience.

• Do you know that the vaping industry has been known for producing flavors and packaging designed to resemble candy or fruit juice? Why do you think they do this?

NARRATIVE

As a deceptive practice, vaping companies are known for using child-friendly flavors and packaging designed to resemble candy or fruit juice to attract young users. For example: Trolli Sour Crawlers or Warheads.

Key points to highlight

- 80% of young e-cigarette users said they used e-cigarettes because they come in flavors they like.
- 89% of teens say they would not use unflavored tobacco.
- 96% of teens who have used e-cigs tried them before age 13.

RESOURCES

• Tobacco is Changing: E-Cigarettes | Wisconsin Department of Health Services https://www.dhs.wisconsin.gov/tobaccoischanging/e-cigarettes.htm

7. DECEPTIVE ADVERTISING CAMPAIGNS

3 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

Vaping companies often produce misleading health claims:

- Promoting as a "safe" alternative. E-cigarette companies present their products as safer than traditional cigarettes, despite the fact that e-cigarette vapor contains harmful chemicals.
- They also use words like "pure," "clean," or "tobacco-free."

Vaping industry disguises devices to conceal vaping habits:

- The vaping industry has engaged in the deceptive practice of intentionally disguising vaping devices to look like everyday objects, particularly to make it easier for minors to conceal their vaping habits from parents and teachers.
 - Some examples may include makeup, compact highlighters, pens, or USB drives, making them difficult to spot in schools or at home.

Vaping industry has also used covert shipping boxes and invoices as a deceptive practice to bypass age verification, and make it easier for unauthorized sales, particularly to minors. Here are some examples of how they employ these tactics:

- Using plain, unmarked boxes without any branding or indication of the contents.
- Using generic company names or abbreviations on shipping labels to avoid revealing the product's origin.
- Avoiding logos, graphics, or product information on the packaging to conceal the contents.
- Using vague language or generic terms on invoices to avoid explicitly stating that the products are vaping devices or e-liquids.

SLIDE



NARRATIVE

What are Dark Patterns?

- Dark patterns, also known as deceptive patterns, are design practices used to manipulate users into taking actions they might not otherwise choose, often to the benefit of the website or app.
- These techniques exploit users' cognitive biases and decision-making processes to achieve specific outcomes, such as making a purchase, subscribing to a service, or sharing personal data.

Key characteristics of Dark Patterns:

- Manipulative and Deceptive: They intentionally mislead or coerce users into actions like buying unwanted products or subscribing to unnecessary services.
- **Exploiting Cognitive Biases**: They capitalize on psychological tendencies like fear of missing out (FOMO) or the inclination to follow default options, prompting impulsive buying behavior.
- **Undermining User Autonomy:** They hinder a user's ability to make free and informed decisions, often leading to decisions they would not have made otherwise.
- Prioritizing Business Goals: These tactics are designed to increase conversion rates and profits, even if it means compromising the user experience.

Examples of Dark Patterns:

- Misleading Product Information: Using deceptive claims about product availability (e.g., "Only 3 items left in stock!", or "Limited time deal") or demand to pressure users into purchasing quickly, even if these claims are false.
- **Hidden Costs**: Presenting a lower price initially and then adding unexpected fees or charges during the checkout process.
- Forced Continuity: Automatically enrolling users into subscriptions after a free trial, making it
 making the cancellation process complicated and time-consuming.

NSTRUCTIONS FOR PRESENTER

You may consider doing an engagement activity to help students recognize manipulative design practices used to trick or pressure consumers.

1. Set the stage (say aloud):

"Have you ever tried to cancel a subscription and they made it really hard? Or maybe you were tricked into adding something to your cart without noticing? These tricks are called dark patterns. They're sneaky design choices meant to confuse or pressure you."

Option A - Homework Assignment: Spot the Dark Patterns Objective:

Learn to recognize "dark patterns" — sneaky design tricks websites use to influence your choices when shopping online.

Instructions:

- 1. Visit an online store or app you use or are familiar with (examples: Amazon, Shein, Temu, GameStop, DoorDash, etc.).
- 2. Find one example of a dark pattern. This could be:
 - A countdown timer
 - A pop-up that pressures you to stay or buy
 - Pre-checked boxes for add-ons
 - Hard-to-find "unsubscribe" or "cancel" options
 - Misleading labels like "only 2 left!" when it's not true
- 3. Take a screenshot or describe the example clearly.
- 4. Answer these questions in 1–2 paragraphs:
 - What is the dark pattern you found?
 - What does it try to make the user do?
 - Why do you think the company uses it?
 - How might it affect someone who is not paying close attention?

Option B - Scenario Analysis (no devices needed):

"I'm going to read a few dark pattern scenarios. Work in pairs to decide: Is this a dark pattern? Why or why not?"

• Scenario 1: The Vanishing Cancel Button

You signed up for a free trial of a streaming service. When you try to cancel before getting charged, you cannot find the "Cancel Subscription" button. It is buried in a long list of menus, and they keep showing you pop-ups begging you to stay.

o Ask: Is this a dark pattern? What is the trick?

Scenario 2: Countdown Pressure

You're browsing a shoe website and see a banner that says:

"Only 2 left! Sale ends in 5 minutes! Limited time deal!"

When you refresh the page 10 minutes later, it still says the same thing.

Ask: Is this a dark pattern? What is misleading here?

• Scenario 3: Pre-Checked Boxes

You are buying a concert ticket and notice there is a \$5 charge for "ticket insurance" already added. The box is checked by default, and you have to uncheck it manually to remove the fee.

Scenario 4: Confirm shaming

A popup asks if you want 10% off your order. The options are:

[Yes, give me the discount]

Or

[No thanks, I don't like saving money]

o Ask: Is this a dark pattern? What is the message behind that language?

• Scenario 5: The Illusion of Popularity

You are browsing the web and come across a Hoverboard with bold text that says:

"Over 2,000 bought in the past month!" and "#1 Top Rated on Our Site!"

But when you scroll down to check the reviews, there are only 3 actual reviews, all posted within the last two days. You also notice similar "#1" claims on several other products in totally different categories.

Ask: Is this a dark pattern? What is being implied—and is it trustworthy?

SLIDE



INSTRUCTIONS FOR PRESENTER

You may consider questions you can ask your audience to introduce the topic.

Have you ever received a weird text or DM from a stranger? What did it say?

NARRATIVE

Definition

A scam is a fraudulent activity carried out by an impersonator to gain your trust or play upon your fears to get:

- Your money
- Access to your personal information
- · Access to your financial information

NOTE FOR PRESENTER

No matter your age, learning about scams is important for everyone. By sharing what you know, you can help protect others in your community from scams.

RESOURCES

Imposter Scams | DATCP

https://datcp.wi.gov/Pages/Publications/ImposterScams214.aspx

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

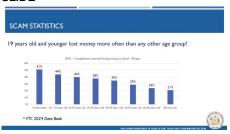
- FTC 2024 Data Book | Federal Trade Commission
 https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2024
- Global State of Scams Report 2024 | Global Anti-Scam Alliance https://www.feedzai.com/resource/global-state-of-scams-report-2024/

11. SCAMS - STATISTICS

2 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

Victims 19 years old and younger lost money more often than any other age group!

Federal Trade Commission 2024 Report

- Half of the complaints received by the FTC from consumers under age 19 reported losing money to scams.
- Total amount lost to fraud reported by consumers under age 19 was \$55 million.

SOURCE/RESOURCES

 Consumer Sentinel Network Data Book 2024 | Federal Trade Commission https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2024

12. SCAMS - STATISTICS

2 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

- 1. Scammers use all the communication methods used by students; this makes students a target for scams.
 - Phone calls is the method with highest per person reported losses, \$1,500 median loss.
 - Social media represents the method with the highest overall reported losses, \$1.9 billion total lost
 - o Email represents the method with the highest overall number of reports, 372,000 reports.

SOURCE/RESOURCES

 Consumer Sentinel Network Data Book 2024 | Federal Trade Commission https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2024

SLIDE



NARRATIVE

Scammers often use deceptive payment methods to make it difficult to trace or recover funds, as these methods offer limited protection for victims. Here are some common methods.

1. Cryptocurrency

- How it works: Scammers ask you to send money in cryptocurrency, often claiming it's a secure
 and untraceable method. Scammers increasingly use cryptocurrency ATMs to steal money by
 directing 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, and the volatility of the market can further complicate recovery efforts.

Gift cards

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

RESOURCES

- Consumer Guide | DATCP
 - https://datcp.wi.gov/Documents2/DATCPConsumerGuide.pdf
- Sure ways to spot a scammer | Federal Trade Commission https://consumer.ftc.gov/consumer-alerts/2024/03/sure-ways-spot-scammer

SLIDE



NARRATIVE

How they happen?

Scammers create a fake online identity to trick you into believing you are in a real online friendship or romance with them.

Once you trust them, they may:

- Scam you into sending them money
- Steal your identity using information you shared with them
- Ask you to lend them money or cryptocurrency
- Ask you to send them gaming credits
- Ask you to buy them gift cards

IMPORTANT CONSIDERATIONS

Teens spend plenty of their time online on social media. According to Pew Research, 95% of teenagers in the United States have access to a smartphone, with 45% saying they are online almost constantly. Unfortunately, their high level of engagement makes them easy targets for social media scams.

- Scammers are aware of this and deploy tactics to engage the younger generations.
- Scammers create fake online identities and engage teens often with grooming methods
- Scammers create fake social media profiles to impersonate friends, family members, or celebrities to gain trust and access personal information.
 - They may establish fake friendships or romantic relationships to manipulate teens into sharing personal information or sending money.
 - They may ask personal questions to get to know their victims and exploit their vulnerabilities.
 - Details about their family relationships.
 - Details about their private lives, like romantic relationships and friends.
 - Personal personally identifiable information, like your birthdate, home address and banking information.

To protect yourself

There is plenty you can do to protect yourself:

- Limit who can see your posts and information.
 - Set privacy settings on your social media accounts to limit who can see your posts and information.
- Be aware of online interactions with people you do not know.
 - Be cautious of accepting friend requests or engaging with accounts of people you do not know in real life.
- Be careful what you post and make public online.
 - Scammers can use details shared on social media to better understand and target you.
- Verify information before sharing it.
 - Do not share personal information or financial details with anyone you do not know or trust.

Never send money.

Do not send money, gift cards, or any other form of payment to someone you have not met in person.

Stop contact.

If you suspect you are dealing with a scammer, stop all contact with them immediately.

RESOURCES

• Screen time: US teens' and parents' experiences, approaches | Pew Research Center https://www.pewresearch.org/internet/2024/03/11/how-teens-and-parents-approach-screen-time/

15. ONLINE SHOPPING SCAMS - HOW THEY HAPPEN?

3 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

How they happen?

Online shopping scams involve scammers pretending to be legitimate sellers, either with fake websites or fake ads on real websites, often using tactics like offering unbelievably low prices or pressuring you to act quickly.

Risks associated with online shopping scams:

- Counterfeit goods. Consumers end up with imitations of popular brands.
- Non-delivery. Despite making a payment, the products never arrive, leaving consumers scammed and out of money.

IMPORTANT CONSIDERATIONS

Teens frequently shop online, particularly for fashion, electronics, and beauty products. However, the allure of great deals can lead them into the clutches of fraudulent online stores. These scammers set up fraudulent websites or social media accounts that advertise trendy items at low prices, only to deliver counterfeit goods or, more often, nothing at all.

According to Better Business Bureau (BBB) research, 80% of consumers aged 18-24 have encountered fraudulent online stores, with many teenagers reporting non-delivery after purchasing from ads on platforms such as Instagram or TikTok.

To protect yourself

Here are some recommendations for shopping online safely:

- Shop with trusted sites.
 - Shop with well-known and reputable online retailers.
- Verify the website.

Look for a physical address, phone number, and contact information on the website.

Be aware of unsolicited offers.

Be cautious of emails or messages that you did not ask for, especially if they offer something that seems too good to be true.

Use Strong Passwords.

Use strong, unique passwords for all your online accounts.

• Be mindful of payment methods.

Be cautious of unusual or specific payment methods, such as money orders or prepaid cards.

• Do not click suspicious links.

Avoid clicking on links in emails or messages, especially if you do not know the sender.

• If you've been scammed

Contact your bank or credit card company and dispute any fraudulent charges.

RESOURCES

• Protecting your personally identifiable information | eSafety Commissioner https://www.esafety.gov.au/young-people/protecting-your-identity

Targeting our youth full report | Better Business Bureau
 https://bbbmarketplacetrust.org/wp-content/uploads/2024/02/Targeting-our-youth-full-report.pdf

SLIDE



NARRATIVE

Grandparent scams involve scammers impersonating a grandchild or other family member to gain the trust of a family member and make them believe there is an emergency in the family and force them to pay money.

How students are involved

- · Scammers pretend to be the grandchild to trick their grandparents or another family member.
- If grandchild's social media accounts are public, scammers can grab photos, travel plans, and other personal details to make their story more believable.
- The grandchild will not know it is happening.

IMPORTANT CONSIDERATIONS

Note about Voice cloning

Scammers are becoming increasingly sophisticated, using technology like voice cloning to make their calls sound more authentic.

To protect yourself

Teens have an opportunity to safeguard their information and protect themselves and their families.

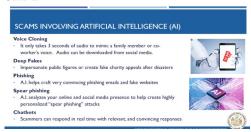
- Limit who can see your posts in social media.
- Be careful what you post and make public online.
- Do not give out personal information.
- Educate family members about these types of scams.
- Create a family passcode or phrase that only the inner circle of the family knows.

RESOURCES

• Imposter Scams | DATCP

https://datcp.wi.gov/Pages/Publications/ImposterScams214.aspx

SLIDE



NARRATIVE

The FBI concluded it only takes 3 seconds of voice audio to facilitate an AI scam. Businesses have been using AI 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.

Voice cloning:

One of the most alarming new scams uses AI 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.

Imagine a situation where a 'family member' calls from what appears to be their phone number and says they have been kidnapped, and then the 'kidnapper' gets on the line and gives urgent instructions," Schroeder explains. "Victims of these scams have said they were sure it was their family member's voice.

• Deepfakes:

Al 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:

Today, generative AI 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 and targeted "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.

SLIDE



NARRATIVE

Paying back student loans can be overwhelming. So called student loan debt relief companies promise to defer, lower, consolidate, or eliminate federal student debt, but end up costing you more money and may not reduce your federal student loan debt at all.

Signs of a student loan debt relief scam

- Promises of immediate loan forgiveness or cancellation.
 - Before they know the details of your situation, scammers might say they can quickly get rid of your loans through a loan forgiveness program programs most people will not qualify for. Scammers might also say they will wipe out your loans by disputing them. But they cannot do either.
- Requests for your Federal Student Aid (FSA) ID.
 Some scammers claim they need your FSA ID to help you. Do not share your FSA ID with anyone.
 Dishonest people could use that information to get into your account and take control of your
 - Dishonest people could use that information to get into your account and take c personal information.
- · Limited time offers.
 - To get you to act fast, scammers may tell you that you could miss qualifying for repayment plans, loan consolidation, or loan forgiveness programs if you do not sign up right away. Take your time and check it out.
- Requests to sign a third-party authorization form or a power of attorney.
 - These written agreements give a company legal permission to talk directly to your federal loan servicer and make decisions on your behalf. Scammers often want these authorizations so they can change your contact and payment information and then you do not know they stopped making payments on your student loan.
- Claims that the program has a special relationship with the government or Department of Education.
 - Scammers use official-looking names, seals and logos, and tell you they have special access to certain repayment plans, new federal loan consolidations, or loan forgiveness programs. They do not. If you have federal loans, go to the Department of Education directly at StudentAid.gov.

RESOURCES

- Student Loan Debt Relief | DATCP
 - https://datcp.wi.gov/Documents/StudentLoanDebtRelief504.pdf
- Wisconsin Coalition on Student Debt https://debtsmarts.org/

2 MIN

Facilitator Notes/Questions

SLIDE



INSTRUCTIONS FOR PRESENTER

You may consider questions you can ask your audience to introduce the topic.

Do you think young people like you get targeted for identity theft? Why or why not?

NARRATIVE

Identity theft is when someone uses your personal or financial information without your permission.

They could use your identity to:

- Buy things with your debit card.
- Get new credit cards in your name.
- Get a job.
- Pretend to be you if they are arrested.

IMPORTANT CONSIDERATIONS

Consumers should be mindful of the risk of identity theft because it can have a negative impact on important aspects of their lives, such as:

- Financial: Identity thieves can use stolen information to open new credit cards, take out loans, or make unauthorized purchases, leading to significant debt and difficulty obtaining credit in the future
- Legal: They might use their victim's identity to commit crimes, leading to false arrests, lawsuits, and legal issues for their victims.

RESOURCES

 Identity Theft and Privacy Protection | DATCP https://datcp.wi.gov/Pages/Programs_Services/IdentityTheft.aspx

20. IDENTIFY THEFT - WHAT THEY WANT?

2 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

Identify theft is attempting and/or obtaining key personal identifiers. These identifiers include the following:

Name in combination with:

- Social Security number
- · Date of birth
- Address
- Email
- Phone number
- School ID
- Passwords
- Debit card

IMPORTANT CONSIDERATIONS

There are key identifiers that never change in your entire life:

- Social Security number
- Date of birth

RESOURCES

- Identity Theft and Privacy Protection | DATCP https://datcp.wi.gov/Pages/Programs_Services/IdentityTheft.aspx
- Identity Theft Student Tips | DATCP https://datcp.wi.gov/Pages/Publications/IDTheftStudentTips637.aspx

SLIDE



NARRATIVE

Online: The digital world allows thieves to operate anonymously and access information from anywhere, making it difficult to track them down and prosecute them. There are some common methods used by identify thieves that consumers can anticipate and avoid:

- Phishing
 - **How it works:** Scammers use fraudulent emails, texts, or phone calls to trick you into revealing personal information.
- Social media
 - **How it works**: Identity thieves may look through your social media accounts for identifying information in posts or photos.
- Public Wi-Fi
 - How it works: Identity thieves can access your personal information when you use public Wi-Fi.
- Hacked accounts
 - **How it works**: Identity thieves can use your password or other login information to access your accounts and make purchases, pretend to be you on social media, or send spam emails.

RESOURCES

 Student Tips to Prevent Identity Theft | DATCP https://datcp.wi.gov/Pages/Publications/StudentTipsPreventIDTheft668.aspx

SLIDE



NARRATIVE

In-person: Thieves use in-person tactics because they offer opportunities for direct access to personal information and physical documents, bypassing online security measures.

- Wallet/Purse theft:
 - How it works: Scammers steal your wallet or purse to get access to ID, credit, or debit cards.
- Trash diving:
 - **How it works**: Identity thieves go through your trash to retrieve bank statements, tax documents, or other sensitive information.
- Intercepting mail:
 - How it works: Identity thieves intercept and redirect your mail to another location.
- Skimming:

How it works: A skimming device is a piece of equipment used by criminals to illegally capture credit or debit card data. These devices are often attached to card readers at ATMs, gas pumps, and point-of-sale (POS) terminals in gas stations, grocery or convenience stores. When a user swipes or inserts their card, the skimming device captures information from the card's magnetic stripe, including the card number, expiration date, and sometimes the cardholder's name.

SLIDE



NARRATIVE

Data Breach: A data breach is any incident involving the unauthorized acquisition, loss, or access to sensitive or confidential information, including personal data (like Social Security numbers, bank account numbers, or healthcare data) and corporate data (like customer records or financial information).

Data breaches can have multiple causes:

- Technical vulnerabilities
- Phishing attacks
- Malware attacks

- Human error
- Insider threats
- Physical security breaches

INSTRUCTION FOR PRESENTER

Describe the protection steps to protect yourself:

- Stay informed and take action:
- Stay vigilant: Be extra cautious about your online activity and monitor your accounts for any suspicious activity.
- Protect your accounts:
- Change passwords: Change passwords for all accounts, especially those that use the same password as the breached account, and consider using a password manager.
- Protect your credit:
- Place a fraud alert or security freeze: Consider placing a fraud alert or security freeze on your credit reports with the three major credit bureaus (Equifax, Experian, and Transunion).
- Check credit reports: review your credit reports for any suspicious activity or errors.
- · Report suspicious activity:
- Report to financial institutions: Contact your financial institutions immediately if you suspect any unauthorized activity on your accounts.
- Report to law enforcement: If you suspect identity theft or fraud.
- Enhance your online security:
- Use strong passwords: Create strong, unique passwords for all your accounts and avoid using the same password for multiple accounts.
- Be wary of phishing attempts: Be cautious of phishing emails or phone calls that resemble official correspondence from the company involved in the breach.

RESOURCES

 Data Breaches: What To Do If It Happens To You | DATCP https://datcp.wi.gov/Pages/Publications/IDTheftStepsForDataBreach640.aspx

24. IDENTIFY THEFT - SOCIAL NETWORKING

2 MIN

Facilitator Notes/Questions

SLIDE



INSTRUCTIONS FOR PRESENTER

You may consider questions you can ask your audience to introduce the topic.

- What kind of personal info do people share online without even realizing it?
- If someone posted a picture of their driver's license or student ID, what could go wrong?

NARRATIVE

Social media presents opportunities for identity theft because it facilitates the collection and misuse of personal information, enabling criminals to create fake profiles, impersonate others, and conduct scams

What are identity thieves looking for?

- Full name
- Hometown
- Employer
- Family member names & pictures
- Relationship status
- Past schools
- Pet names
- Hobbies & Affiliations
- Family tree
- Birthdays

25. IDENTIFY THEFT - WHAT ARE THE WARNING SIGNS?

2 MIN

Facilitator Notes/Questions

SLIDE

- Bills for items you did not buy
- Mail stops coming to or is missing from your mailbox
- Unauthorized debit and credit charges
 Unsolicited change of address





NARRATIVE

You may not know that you experienced ID theft immediately, nonetheless, take action if you notice any of these warning signs.

- Bills for items you did not buy.
- Mail stops coming to or is missing from your mailbox.
- Unauthorized debit and credit charges.
- Unsolicited change of address requests.

INSTRUCTION FOR PRESENTER

This is an opportunity to indicate that students may not know that they experienced identity theft immediately. Encourage them to take action if they notice any of these warning signs.

26. IDENTIFY THEFT - PREVENTION

1 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

When someone asks for your personal information, ask yourself:

- Why do they need it?
- Do I have to provide it?
- Did I contact them or did they contact me?
- What if I do not provide it?

INSTRUCTION FOR PRESENTER

Homework Assignment: Understanding Identity Theft Objective:

Learn what identity theft is, how it happens, and how to protect your personal information from being stolen or misused.

Instructions:

Answer the following questions in complete sentences. Be thoughtful and use your own words. You may handwrite or type your responses.

Part 1: Understanding the Basics

- What is identity theft? (Explain it in your own words.)
- 2. List at least three types of personal information that identity thieves often try to steal.
- 3. Why is it dangerous if someone steals your Social Security number, debit card, or login information?

Part 2: Real-World Awareness

4. Describe a situation where someone might accidentally share too much personal information online.

(Example: social media, a public computer, a phishing email, etc.)

Part 3: Protect Yourself

- 5. List at least three ways to protect your identity when using the internet or mobile apps.
- 6. Create a short "Safe Identity Checklist" with 3–5 tips that you would give to a friend or family member to help them stay safe.

SLIDE

IDENTITY THEFT PREVENTION Prevention steps Do not answer phone calls, texts, social media messages, or email from numbers or people you do not know. Do not share personal information like your bank account number, Social Security number or date of birth. Learn when it is safe to use a public Wi-Fi network. Store personal information, including your Social Security card, in a safe place. Do not carry it in your wallet. Enable Multi-factor authentication (MFA).

NARRATIVE

Identify theft can have devastating effects in your future, yet there are steps you can take to protect yourself from identity theft:

- Do not answer phone calls, texts, social media messages, or emails from numbers or people you do not know.
- Do not share personal information like your bank account number, Social Security number, or date
 of birth.
- Learn how to safely use public Wi-Fi networks.
- Store personal information, including your Social Security card, in a safe place. Do not carry it in your wallet.
- Enable multi-factor authentication (MFA).

RESOURCES

Identity Theft Student Tips | DATCP https://datcp.wi.gov/Pages/Publications/IDTheftStudentTips637.aspx

28. CREDIT REPORT SECURITY FREEZE

2 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

- Best way to protect you and your family.
- Parents or guardians can freeze their child's credit.
- Completely free.

NOTE FOR PRESENTER

• You may ask the students to share this information with their parents

RESOURCES

Credit Report Security Freeze | DATCP https://datcp.wi.gov/Pages/Publications/IDTheftCreditReportFreeze632.aspx

SLIDE



INSTRUCTIONS FOR PRESENTER

You may consider questions you can ask your audience to introduce the topic.

- Who here as ever toured an apartment?
- Who knows what a lease is?
- Who has heard of a security deposit?

Depending on the level of knowledge, you may continue by indicating that this presentation will cover these and more topics they need to know, before renting an apartment.

NARRATIVE

It is important for the next generation of tenants to be aware of landlord-tenant law. Learning about the specifics of the law is vital for your well-being, financial security, and ability to navigate the rental market effectively.

Important information that every tenant should know:

- Types of lease in Wisconsin
- Breaking a lease
- What you need to know before renting
- Promises to repair
- Your responsibilities as a tenant
- Security deposits
- Before submitting a complaint

RESOURCES

- Landlord Tenant Guide | DATCP https://datcp.wi.gov/Documents/LT-LandlordTenantGuide497.pdf
- Tenants' Rights and Responsibilities | DATCP https://datcp.wi.gov/Pages/Publications/LT-TenantsRights143.aspx

30. LANDLORD TENANT - TYPES OF LEASE IN WISCONSIN

2 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

Knowing the terms of a lease, including its length, rent, and other clauses, helps tenants and landlords navigate potential issues and ensure a fair tenancy.

One year lease

- The lease has a specific start and end date.
- Landlords cannot raise rent during the lease because of the protection afforded by the contract.

Month to month

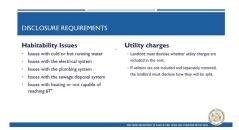
- Either party can end the tenancy with a 28-day notice prior to rent being due.
- Landlords can raise rent at any time with as little as a 28-day notice.

31. LANDLORD TENANT - DISCLOSURE REQUIREMENTS

2 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

The law requires landlords to disclose certain information.

Habitability Issues

- Issues with cold or hot running water.
- Issues with the electrical system.
- Issues with the plumbing system.
- Issues with the sewage disposal system.
- Issues with heating or not capable of reaching 67°.

Utility charges

The landlord must disclose whether utility charges are included in the rent. If utilities are not
included and separately metered, the landlord must disclose how they will be split.

IMPORTANT CONSIDERATIONS

Expanded description of the disclosure requirements.

1. Habitability Issues

Landlord must disclose to the prospective tenant if:

- The dwelling unit lacks hot or cold running water.
- Heating facilities serving the dwelling unit are not in safe operating condition or are not capable of maintaining at least 67° F during all seasons.
- Temperatures in living areas shall be measured at the approximate center of the room, midway between floor and ceiling.
- The dwelling unit is not served by electricity, or the electrical wiring, outlets or fixtures are not in safe operating condition.
- The dwelling unit is not served by plumbing facilities in good operating condition.
- The dwelling unit is not served by sewage disposal facilities in good operating condition.
- Any conditions which constitute a substantial hazard to the health or safety of the tenant or create an unreasonable risk of personal injury.

2. Utilities

• Landlord must disclose whether utility charges are included in the rent, If utilities are not included and separately metered, the landlord must disclose how they will be split.

3. Code violations (not included in the slide)

Landlord must disclose to the prospective tenant any building or housing code violations that
the landlord has actual knowledge of, that present a significant threat to the prospective
tenant's health or safety and which the landlord has not corrected.

4. Landlord or authorized agents (not included in the slide)

- Landlords must provide written disclosure of:
 - Name and address of the person collecting rent and able to receive legal service.
 - Name and address of the person managing and maintaining the premises.

32. LANDLORD TENANT - BREAKING A LEASE

2 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

If a tenant breaks a lease and vacates the premises before the end of the lease, the landlord may continue to charge them rent to the end of the lease.

If a tenant refuses to leave, the landlord can recover damages twice the rental value apportioned on a daily basis.

IMPORTANT CONSIDERATIONS

It is important that the students understand the importance of communicating with the landlord. This will often help them avoid additional fees or legal costs.

SLIDE



NARRATIVE

Some people agree to rent a unit based upon the landlord's promises to make certain repairs or improvements to the premises.

- 1. If a landlord indicates or promises to clean, fix, or improve something, they must indicate the date when it will be done.
- 2. Any promises made before signing a lease must be in writing, and the tenant must get a copy.
- 3. The landlord must complete the work on time unless something happens that they cannot control. If there is a delay, they must tell the tenant why and give a new completion date.

NOTE FOR PRESENTER

Expanded description from what was provided in the PowerPoint slide:

- (1) Every promise or representation made by a landlord to a tenant or prospective tenant *shall specify the date* or time period on or within which the cleaning, repairs or improvements are to be completed.
- (2) All promises made <u>before the initial rental agreement</u> shall be in writing with a copy furnished to the tenant.
- (3) Every promise or representation *shall be completed within the time period represented* unless the delay is beyond the landlord's control. The landlord shall give timely notice to the tenant of reasons beyond the landlord's control for any delay and when the cleaning, repairs or improvements will be completed.

34. LANDLORD TENANT - SECURITY DEPOSITS

3 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

Check-In procedures; pre-existing damages

- Landlords must provide new tenants with a check-in sheet to document the condition of the premises.
- Tenants have 7 days from move-in to complete the sheet and return it to the landlord.
- Tenants should carefully inspect the unit and document all defects or preexisting damages.
- Landlords must inform tenants of their right to receive a list of damages for which the landlord withheld money from the previous tenant's security deposit.

Returning security deposits and withholding rules

- Landlords must return security deposits, minus any proper withholdings, within 21 days after the rental agreement ends.
- Withholdings are limited to: Tenant damage, waste, or neglect, Unpaid rent and fees.

Statement of claims

- If withholdings are made, landlords must provide an itemized, written statement of accounting. Security deposit refund and change of address:
- Landlords must mail the security deposit refund and/or accounting to the tenant's last known address.
- Tenants should notify the postal service and landlord of their change of address to ensure timely receipt of the security deposit refund.

35. LANDLORD TENANT - TENANT RESPONSIBILITIES

2 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

Tenants should understand their responsibilities in Wisconsin to ensure a smooth and fair rental experience and to avoid potential legal issues. Knowing these responsibilities helps tenants protect their interests, maintain a good relationship with their landlord, and ensure they can exercise their rights effectively.

Key responsibilities of tenants in Wisconsin:

- Follow the rules in the lease.
- Pay your rent on time.
- Be respectful of neighbors.
- Do not damage property.
- Prior to a complaint do the following:
 - Communicate with the landlord and attempt to find a solution.
 - Become familiar with the terms of your contract and what sign.
 - o Document all issues and take issues as needed.

Homework Assignment: Renting in Wisconsin – Know Your Rights Objective:

Understand basic rights and responsibilities of landlords and tenants in Wisconsin.

Instructions:

Answer the following questions in complete sentences. Use your own words and think about how these issues affect real renters and landlords. You may use your notes, class materials, or the Wisconsin Department of Agriculture, Trade and Consumer Protection (DATCP) website: datcp.wi.gov

Part 1: Before you rent

- 1) What is a rental agreement or lease, and why is it important to read it carefully before signing?
- 2) What kinds of fees or deposits can a landlord legally charge a new tenant in Wisconsin? Name at least two.

Part 2: While you are living there

- 3) What are two things a landlord is required to do to maintain a safe and livable home?
- 4) What are two responsibilities a tenant has while renting?
- 5) If something in the unit breaks (for example, the heat stops working), what should a tenant do? What should a landlord do?

Part 3: Moving Out

- 6) What should a tenant do to make sure they get their security deposit back?
- 7) What can a tenant do if they believe their landlord kept their deposit unfairly?

36. MOTOR VEHICLES - EXPLAINED

3 MIN

Facilitator Notes/Questions

SLIDE



INSTRUCTIONS FOR PRESENTER

Consider some questions you can ask your audience to make the topic relatable and engaging:

• What do you think is more important to know as a car owner: where to buy a reliable vehicle or where to get it repaired when something goes wrong?

You can continue with a positive way to acknowledge their answers and lead into your presentation:

Great points from everyone! Whether you think, knowing where to buy a reliable car or
where to get it repaired is more important, the truth is — they are both equally important.
Buying smart sets you up for success and knowing how to care for and fix your car keeps
you safe and saves money down the road.

We are going to explore both sides in more detail, so you'll be better prepared whether you're buying your first car or dealing with repairs.

- Other questions for consideration, if time is an issue.
- Raise your hand if you dream of owning your own car one day!
- If you could have any car, regardless of price, what would it be and why?

IMPORTANT CONSIDERATIONS

While owning a car offers numerous benefits, younger consumers should be aware of the responsibilities, costs, and make informed decisions about car ownership and repairs.

Getting ready for the road

- What you should know about purchasing from a private seller.
- What you should know about motor vehicle repairs.

SLIDE



INSTRUCTIONS FOR PRESENTER

You may consider questions you can ask your audience to introduce the topic.

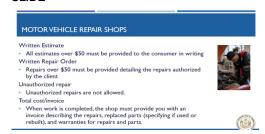
What do you think are some things to think about when buying a car, especially when it's not brand new?

NARRATIVE

Buying a used car, especially for the first time, can feel like a big deal, and maybe a little intimidating. There are so many things to consider, from figuring out your budget and finding the right car to navigating the buying process itself. Here are some things to consider:

- Be cautious of online marketplaces:
 - o Cars sold though social media and online boards.
 - o Inquiries from individuals in different countries, states, or cities.
 - Seller refusing to meet face-to-face before the transaction.
 - Requests for payment via wire transfers or cryptocurrency.
 - o Sellers paying more than agreed, and requesting the difference be returned.
 - Requests for payment before Inspection.
- Test drive
 - o Test-drive the vehicle. Drive it cold and warmed up. Test it at highway and city speeds.
- Ask the vehicle's former owner about its condition, mileage, and use.
- Keep copies of all documents and anything else you sign.
- Compare asking price with "vehicle value guide.
- Mechanical Inspection
 - Have a qualified mechanic inspect the vehicle to identify any underlying problems that might not be readily apparent.
- Ask to see the vehicle title. If the title is missing or is not in the seller's name, shop elsewhere.
- Never pay for a car without seeing it in person and verifying its condition.

SLIDE



NARRATIVE

While owning your first car is an exciting experience, vehicles require maintenance and repairs to function properly, this is a normal aspect of car ownership. Gaining knowledge of car maintenance and repairs can lead to cost savings, increased confidence, and the prevention of more significant issues. Here are some things to consider:

Written estimates

 Wisconsin car repair shops must get your authorization for any repair and must offer you an estimate, or firm price quote, if repairs will cost \$50 or more.

Written repair order

- Before a shop starts any repairs whose total price may exceed \$50 a shop representative shall prepare a written repair order that clearly and legibly describes the repairs authorized by the customer.
- The repair order shall be dated and signed by the shop representative.
- When requesting additional authorization, the shop must tell you both the cost for the additional repairs and the new total cost of the complete job. Make sure you leave a telephone number where the shop can reach you.
- If you need expensive or complicated repairs, or if you have questions about their recommended repairs, consider getting a second opinion.

Unauthorized repair

- Unauthorized repairs are not allowed.
- o However, if you drop off your car before the shop opens with a note to repair something and you do not ask them to call you with an estimate the shop can charge what it wants.

Total cost/invoice

 When work is completed, the shop must provide you with an invoice describing the repairs, replaced parts (specifying if used or rebuilt), and warranties for repairs and parts.

RESOURCES:

Motor Vehicle Repair Tips | DATPC

https://datcp.wi.gov/Pages/Publications/MV-RepairTips456.aspx

INSTRUCTIONS FOR PRESENTER

Homework Assignment: Buying and Repairing a Vehicle in Wisconsin

Objective:

Learn key protections and smart practices for purchasing and repairing a motor vehicle in Wisconsin.

Instructions:

Answer the questions below in your own words. You may use your class notes or explore the Wisconsin DATCP website for help:

datcp.wi.gov

You may handwrite or type your answers.

Part 1: Buying a Vehicle

1) Why is it important to get a vehicle history report before buying a used car? What information can it tell you?

Part 2: Vehicle Repairs

- 2) If you take your car to a repair shop, what are your rights before the mechanic begins the work? (Hint: cost estimate? approval?)
- 3) What should you do if a repair shop does work you did not authorize—or charges more than expected?
- 4) What information should always appear on your written repair invoice or receipt? Name at least two things.

Part 3: Avoiding Problems

- 5) What are two red flags that might mean a car ad or repair shop is a scam?
- 6) Imagine a friend wants to buy a used car but the seller refuses a test drive and wants to be paid in gift cards. What would you tell your friend?

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

40. 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.

41. THANK YOU

0 MIN

Facilitator Notes/Questions

SLIDE



INSTRUCTIONS FOR PRESENTER Closing