

PRESENTER GUIDE: IDENTITY THEFT – PROTECT AND PREVENT

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

This Presenter Guide is a tool developed by the Bureau of Consumer Protection to assist presenters delivering the Identity Theft presentation.

Audience: General public, community groups, adult learners.

Presentation Length: Approximately 45 - 60 minutes

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

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

INDEX OF CONTENT

Slide #	Content	Page
1	Cover Page	3
2	What is Identity Theft?	3
3	What do they want?	4
4	Identity Theft by Age	5
5	How it Happens	6
6	Skimming Devices	7
7	Imposter Scams Phone calls / Texts / emails	8
8	Data breaches	9
9	Social Networking	10
10	Prevention Basics – Social media	11
11	Prevention Basics - Smartphone Safety	12
12	Public WI-FI Networks	13
13	Prevention Basics – Computer Use	14
14	Prevention Basics – Identity Theft	15
15	Credit Report	16
16	Credit Freeze	17
17	Identity theft protection insurance	18
18	Home Title theft	19
19	Identity Theft Warning Signs	20
20	Identity Theft victim response	21
21	How to file a complaint	22
22	Learn more about DATCP	23
23	Thank you	23

1. COVER PAGE

0.5 MIN

Facilitator Notes/Questions

NARRATIVE

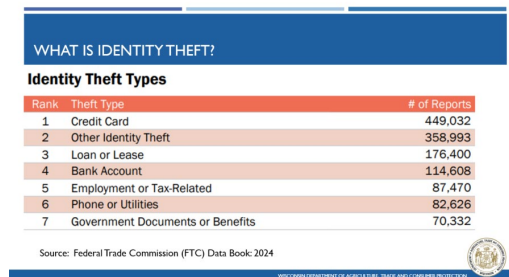
- Welcome.

2. WHAT IS IDENTITY THEFT?

2 MIN

Facilitator Notes/Questions

SLIDE



INSTRUCTIONS FOR PRESENTERS

- Presenters may consider asking the audience about who has experienced credit card fraud to get audience engaged in the presentation.
- If questions from the audience about what is included under category #2 *Other Identify Theft*. This subcategory includes email or social media, insurance, online shopping, payment account, security accounts, and other.

NARRATIVE

Identity theft is real. Thousands of consumers are impacted by it every day.

What is Identity Theft?

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

According to the FTC, in 2024, the most frequently reported types of identity theft include the following categories:

1. Credit Card
2. Other Identity Theft
3. Loan or Lease
4. Bank Account
5. Employment or Tax-Related
6. Phone or Utilities
7. Government Documents or Benefits

RESOURCES

- **Consumer Sentinel Network | Federal Trade Commission**
<https://www.ftc.gov/enforcement/consumer-sentinel-network>

3. WHAT DO THEY WANT?

2 MIN


Facilitator Notes/Questions

SLIDE

WHAT DO THEY WANT?

Name in combination with:

- **Social Security number**
- **Date of birth**
- Address (email & physical)
- Driver's license number
- Passport number
- Credit card numbers & PINs
- Passwords
- Bank account numbers



The slide displays two identification documents. The top document is a Wisconsin Driver License for John O. Public, showing his photo, name, date of birth, and license number. The bottom document is a Social Security card for John O. Public, showing his name and Social Security number (123-45-6789).

NARRATIVE

Criminals are interested in everything.

In conclusion, these criminals are after:

- **Name**, in combination with:
- **Social Security number**
- **Date of birth**
- Address (email and physical)
- Driver license number
- Passport number
- Credit card numbers and PINs
- Passwords
- Bank account numbers

IMPORTANT CONSIDERATIONS

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

- Social Security number
- Date of birth

The combination of name, Social Security number (SSN), and date of birth (DOB) is crucial for identity theft because it allows thieves to establish a new identity, open accounts, apply for loans, and commit other financial crimes using the stolen information.

How criminals take advantage of your information:

- All that is needed to open a credit card is a person's name, Social Security number, date of birth, and average annual salary. It only takes one minute to be approved.

RESOURCES

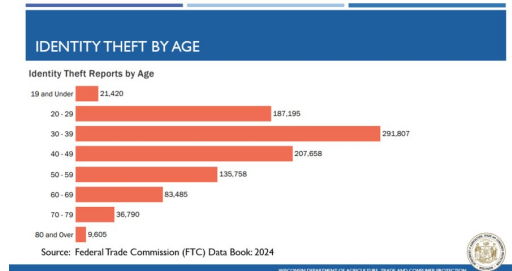
- **Safeguarding Your Information | Department of Agriculture, Trade and Consumer Protection**
<https://datcp.wi.gov/Pages/Publications/IDTheftSafeguards603.aspx>

4. IDENTITY THEFT BY AGE

2 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

- Although this report indicates, the majority of the reports submitted are between the ages of 20 and 50.
- Anyone's identity can be stolen, from the youngest to the oldest individual.
- If you have a name, DOB, and SSN, you can be victimized through no fault of your own.
- While the FTC's data shows lower reported cases for those under 19, the true extent of identity theft among this age group is likely higher due to underreporting or delayed discovery by victims.

INSTRUCTIONS FOR PRESENTERS

- Highlight that everyone can be victimized, regardless of their age.

RESOURCES

- **Consumer Sentinel Network | Federal Trade Commission**
<https://www.ftc.gov/enforcement/consumer-sentinel-network>

5. HOW IT HAPPENS

2 MIN

Facilitator Notes/Questions

SLIDE

HOW IT HAPPENS

Identity thieves are looking to steal:

- Mail & Packages
- Documents
- Wallets
- ID, SS card, Credit, & Debit
- Phones



NARRATIVE

There are several ways that scammers can steal your identity, including in person, online, through social media, and by phone. Scammers may:

- Steal your mail, including bank statements, credit card offers, personal checks, and tax documents.
- Go through your trash to retrieve bank statements or tax documents.
- Steal your wallet or purse to get your ID, credit cards, or debit cards.
- Get personal information from your phone when you connect to a public Wi-Fi network, or steal your unlocked device to obtain data stored on it.

IMPORTANT CONSIDERATIONS

- These are some of the ways identity thieves steal from their victims.

RESOURCES

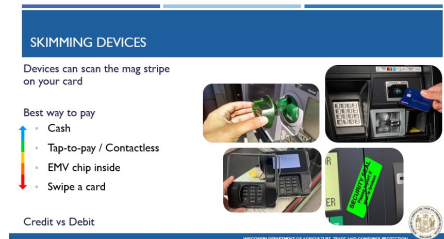
- **Identity Theft Consumer Tips and Info | Department of Agriculture, Trade and Consumer Protection**
<https://datcp.wi.gov/Pages/Publications/IDTheftPrivacyProtectionFactSheets.aspx>

6. SKIMMING DEVICES

2 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

Skimming occurs when a device is illegally installed on or inside ATMs, point-of-sale (POS) terminals, or fuel pumps. Skimmers capture data and record cardholders' PIN entries. Criminals use the data to create fake payment cards, which are used to make unauthorized purchases or steal from victims' accounts.

TO PROTECT YOURSELF

- **Inspect card readers:** Look for anything loose, crooked, damaged, or scratched before use. Avoid using suspicious readers that seem to have been tampered with.
- **Check the keypad:** Gently pull at the edges before entering your PIN.
- **Cover your PIN:** Shield the keypad fully while entering your PIN to prevent camera recording. Be aware of potential pinhole camera locations.
- **Use secure ATMs:** Opt for ATMs in well-lit, indoor locations when possible. Be extra cautious in tourist areas.
- **Use chip cards:** While chips are more secure, remember the magnetic stripe is still vulnerable while using one.
- **Avoid debit cards:** If compromised, criminals can access all accounts linked to a debit card. Use credit cards instead.
- **Monitor accounts regularly:** Check for unauthorized transactions frequently and set up transaction alerts if possible.
- **Report stuck cards immediately:** If an ATM does not return your card, contact your bank right away.

RESOURCES

- **Skimming | Federal Bureau of Investigation**
<https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/skimming>

7. IMPOSTER SCAMS PHONE CALLS / TEXTS / EMAILS

2 MIN

Facilitator Notes/Questions

SLIDE

IMPOSTER SCAMS PHONE CALLS / TEXTS / EMAILS

- Government imposters
- IRS / Law enforcement / SS
- Family & Friends Impostors
- Tech support
- Charities
- Utilities
- Student Loans
- Auto Warranties
- And Many more!

SCAM ALERT

WISCONSIN DEPARTMENT OF AGRICULTURE, TRADE AND CONSUMER PROTECTION

NARRATIVE

Identity thieves use imposter scams. The impersonator attempts to gain the trust of their victims or play upon their fears to steal:

- Money
- Personal information
- Financial information

To achieve this, imposters use “phishing” to get information about you through fraudulent email, texts, or phone calls.

The term “Phishing,” was intentionally coined as a play on “fishing.” Fishing is exactly what the scam artists are doing – throwing you deceptive bait to see if you will bite and give up your personal information. Once they have that, scammers can make unauthorized charges to your bank account or credit card, or even open fraudulent accounts in your name.

Examples of people and organizations scammers might impersonate include:

- Government agencies (IRS / law enforcement / Social Security Administration)
- Family and friends
- Tech support
- Charities
- Utility companies
- Student loans servicers
- Auto warranty companies
- Many more

IMPORTANT CONSIDERATIONS

- BCP offers a separate presentation and presenter guide specifically tailored to discuss each of these in detail. It is called Common Scams and Frauds.

RESOURCES

- **Phishing, Vishing and Smishing | Department of Agriculture, Trade and Consumer Protection**
<https://datcp.wi.gov/Pages/Publications/Phishing402.aspx>
- **Imposter Scams | Department of Agriculture, Trade and Consumer Protection**
<https://datcp.wi.gov/Pages/Publications/ImposterScams214.aspx>

8. DATA BREACHES

2 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

Data Breach: A data breach is an 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

TO PROTECT YOURSELF

- **Stay informed and take action:** Be extra cautious about your online activity and monitor your accounts for any suspicious activity.
- **Protect your accounts:** Change passwords for all accounts regularly, and immediately if notified of a breach. Especially those that use the same password as the breached account, and consider using a password manager.
- **Protect your credit:** Consider placing a fraud alert or security freeze on your credit reports with the three major credit bureaus (Equifax, Experian, and TransUnion). Review your credit reports often for any suspicious activity or errors.
- **Report suspicious activity:** Contact your financial institutions immediately if you suspect any unauthorized activity on your financial accounts. Report to law enforcement if you suspect identity theft or fraud.
- **Enhance your online security:** Create strong, unique passwords for all your accounts and avoid using the same password for multiple accounts. Use MFA when available. 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>
- **Wisconsin's Data Breach Notification Law | DATCP**
<https://datcp.wi.gov/Pages/Publications/IDTheftDataBreach607.aspx>

9. SOCIAL NETWORKING

2 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

Social networking presents opportunities for identity theft because it facilitates the collection of personal information.

What are identity thieves looking for?

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

IMPORTANT CONSIDERATIONS

- **What others post about you:** Even if you are not on social media, you likely have friends and family who are, and they could be posting about you with or without your knowledge.
- **Artificial intelligence used for the wrong purpose:** A.I. is being used to aggregate profiles of a person to use in a scam, or to create profiles to target specific individuals. A.I. is also used to enhance social media 'spear phishing' scams.
- **Passwords:** Many seemingly innocuous pieces of information about you can be useful to scammers. For example, past schools, pet names, and birthdays are often used in passwords and security questions.

RESOURCES

- **Social Networking | DATCP**
<https://datcp.wi.gov/Pages/Publications/SocialNetworking473.aspx>

10. PREVENTION BASICS – SOCIAL MEDIA

2 MIN

Facilitator Notes/Questions

SLIDE

PREVENTION BASICS – SOCIAL MEDIA

- Imposter accounts
 - Just because you recognize the profile pic doesn't mean this is your friend
 - Will often send a message with a link
 - "Too good to be true" investment offers and business opportunities in messages
 - Set your "Friends" list to PRIVATE



NARRATIVE

The world of social media is constantly evolving and attracting audiences who seek connection with friends and family. This interconnection provides criminals with opportunities to create fake profiles, impersonate others, and conduct scams. Identity thieves may look through your social media accounts to find identifying information in posts or photos. On the other hand, they may ask you for personal information in 'fun' online quizzes and surveys.

Imposter accounts

- Nothing stops a criminal from taking a screenshot of your profile picture and creating a new account with your name. After doing this, identity thieves will send messages to your friends while pretending to be you.
- Once trust is gained, thieves will attempt to mislead targets into sending them personal information or money for fake emergencies.
- Identity thieves also use social media to promote "too good to be true" investment offers and business opportunities.

TO PROTECT YOURSELF

- **Set profiles to private:** Limit who can see your posts, photos, and personal information. Adjust settings to only allow friends or followers you trust.
- **Think before you post:** Consider how information you share online could be used by criminals. Avoid posting sensitive information like your full name, birthdate, address, phone number, or financial details.
- **Be cautious of friend requests and messages:** Only accept friend requests from people you know, and be wary of unsolicited messages, especially those containing links or asking for personal information.
- **Use strong, unique passwords:** Use long, complex passwords that include uppercase and lowercase letters, numbers, and symbols. Avoid reusing passwords across different accounts.
- **Be alert for phishing scams:** Be wary of emails, messages, or links that ask for personal information or direct you to fake login pages. Check web addresses carefully, and verify messages really came from the sender by contacting them through a different, verified communication method.

RESOURCES

- **Social Networking | DATCP**
<https://datcp.wi.gov/Pages/Publications/SocialNetworking473.aspx>

11. PREVENTION BASICS - SMARTPHONE SAFETY

2 MIN

Facilitator Notes/Questions

SLIDE

PREVENTION BASICS - SMARTPHONE SAFETY

- Keep your phone locked
 - Facial recognition, fingerprint, etc...
- Keep operating system updated
- Don't click links in unknown or unsolicited texts & emails
- Only install apps from major app stores

Google Play App Store SAMSUNG Galaxy Store

The slide features a blue header with the title 'PREVENTION BASICS - SMARTPHONE SAFETY'. Below the header is a bulleted list of four security recommendations. To the right of the list is a graphic of a smartphone with a padlock icon and various security-related icons. At the bottom left are logos for Google Play, the App Store, and the Samsung Galaxy Store. At the bottom right is a small circular seal.

NARRATIVE

Smartphone safety is necessary to prevent identity theft. The following recommendations can help ensure safety:

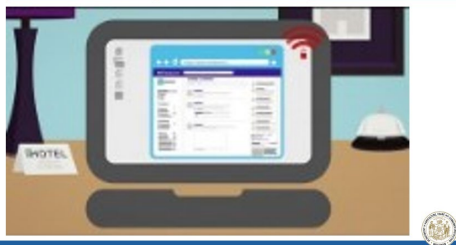
- **Keep the phone locked with strong passwords/biometrics:** Use unique, complex passwords for your device and accounts, or utilize biometric authentication like fingerprint or face recognition at all times when the device is not in use.
- **Keep operating system updated:** Keep your operating system and apps up-to-date to patch security vulnerabilities.
- **Be mindful of phishing:** Do not click links or open attachments in unsolicited emails or text messages.
- **Download apps from trusted sources:** Only download apps from official app stores like the Google Play Store or Apple App Store.

12. PUBLIC WI-FI NETWORKS

4 MIN

Facilitator Notes/Questions

SLIDE



INSTRUCTIONS FOR PRESENTERS

- Play video for audience. Duration: 3:12 minutes. Internet connection is required for playing video.
- Mention recap of the important considerations as time allows.

IMPORTANT CONSIDERATIONS – AFTER WATCHING THE VIDEO

Wi-Fi is a wireless technology used to conveniently connect computers, tablets, smartphones and other devices to the internet. Nonetheless, they can also be used by identity thieves to get ahold of your information.

- People often use free Wi-Fi hotspots provided through hotels, airports, coffee shops, etc.
- Although they are convenient, they often are not secure. These networks do not use encryption to protect user data.
- That could make it easy for someone else to access your online accounts or steal your personal information, like:
 - Private documents
 - Contacts
 - Photos
 - Login information
 - Financial information, Social Security numbers, and credit card details
- **To reduce your risk, consider these tips:**
 - Do not assume that a public Wi-Fi network uses encryption.
 - If necessary, be sure to send any sensitive information using a secure website. A secure site will encrypt your information even if the network does not. If the web address starts with “https,” (not just “http”) your information is encrypted before it is sent. The “s” stands for “secure.” Look for the “https” on every page you visit, not just when you log in.
 - Do not use the same username and password for different sites. It could give someone who gains access to one of your accounts access to many of your accounts.
 - Never email financial information, including credit card, Social Security, and checking account numbers, even if the network and website are secure.
 - Do not stay permanently signed into accounts.
 - When you have finished using a site, log out.

RESOURCES

- **Public Wi-Fi Networks - Security Tips | Federal Trade Commission**
<https://www.youtube.com/watch?v=bzoEy-t8Y-8>
- **Tips for Using Public Wi-Fi | Department of Agriculture, Trade and Consumer Protection**
<https://datcp.wi.gov/Pages/Publications/IDTheftWi-FiTips659.aspx>

13. PREVENTION BASICS – COMPUTER USE

2 MIN

Facilitator Notes/Questions

SLIDE

PREVENTION BASICS – COMPUTER USE

- Enable Auto update
- Don't click links or trust phone numbers on suspicious emails & pop-ups
- Install: Anti-virus, Anti-Malware, Anti-Pop-up & Firewall protection
- Only use secure Wi-Fi



NARRATIVE

To prevent identity theft, computer use must be supplemented with safety practices, including:

- **Keep software updated:** Regularly update your operating system, web browser, and antivirus software. Enable auto updates.
- **Be cautious of phishing attempts:** Be aware of phishing emails or pop-ups trying to trick you into revealing personal information. These can also be malicious and lead to virus or malware infection.
- **Use a firewall and install antivirus software:** Protect your computer from unauthorized access, and regularly scan your computer for viruses and malware.
- **Only use secure Wi-Fi:** Ensure information is encrypted and secure. If unsure, do not transmit sensitive data (online banking and shopping).

IMPORTANT CONSIDERATIONS

- **Be careful when online shopping:** Always use secure websites for your transactions. Be aware of scammers impersonating legitimate online sellers. Research the site and check that the web address is correct before shopping.

RESOURCES

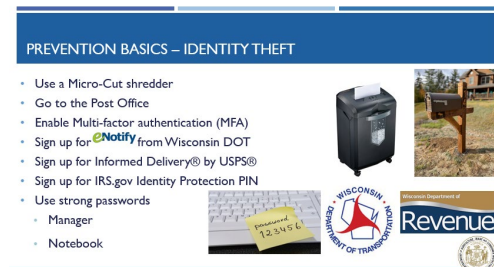
- **Computer Protection Tips | DATCP**
<https://datcp.wi.gov/Pages/Publications/IDTheftComputerProtection643.aspx>

14. PREVENTION BASICS – IDENTITY THEFT

2 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

- **Shred sensitive documents:** Shred documents containing personal information before disposing of them. It is highly recommended to use a micro-cut shredder.
- **Reduce the risk of mail theft:** Prioritize delivering outgoing mail with sensitive information to a post office, rather than leaving it in your mailbox.
- **Enable multi-factor authentication (MFA):** Adds an extra layer of security to your accounts.
- **Sign up for eNotify from Wisconsin DOT:** Empowers you to manage your account, stay informed about important notifications, protect your personal information, and alerts you of any unauthorized changes or transactions.
- **Sign up for informed delivery by USPS:** Offers several benefits, including a free service that sends you digital images of your letter-sized mail each morning. This allows you to preview your mail, manage your packages, and receive tracking updates. It also enhances convenience and security by helping you track deliveries and manage your mail logistics.
- **Sign up for an IRS.gov Identity Protection PIN:** The IRS IP PIN is a 6-digit number assigned to eligible taxpayers to help prevent the misuse of their Social Security number (SSN) on fraudulent federal income tax returns.
- **Use strong passwords:** Take advantage of password managers that some smartphones incorporate in their devices or offer as downloadable apps. You can also write down passwords in a personal notebook stored in a secure location.

INSTRUCTIONS FOR PRESENTERS

- Explain the benefits of real-time notifications with eNotify and informed delivery.
- Explain how the IP PIN works to protect tax returns (IRS and WI DOR).
- Explain how MFA works.
- Talk about password managers and personal notebooks stored in a secure location.
- Ask participants if they check their credit reports and emphasize that they should check their credit reports regularly.

RESOURCES

- **Safeguarding your information | Department of Agriculture, Trade and Consumer Protection**
<https://datcp.wi.gov/Pages/Publications/IDTheftSafeguards603.aspx>
- **Mail goes digital with informed delivery | United States Postal Service**
<https://www.usps.com/manage/informed-delivery.htm>
- **eNotify: Get renewal notifications by email/text | Wisconsin Department of Transportation**
<https://wisconsindot.gov/Pages/online-srvcs/renew-licens/enotify-default.aspx>
- **FAQs about the identity protection personal identification number (IP PIN) | Internal Revenue Service**
<https://www.irs.gov/identity-theft-fraud-scams/frequently-asked-questions-about-the-identity-protection-personal-identification-number-ip-pin>

15. CREDIT REPORT

2 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

A credit report is a summary of your personal credit history. Your credit report includes identifying information, (like your address and date of birth), and information about your credit history, (like how you pay your bills or if you have filed for bankruptcy). Three nationwide credit bureaus (Equifax, Experian, and TransUnion) collect and update this information.

Checking your credit report is crucial for monitoring your financial health, protecting against identity theft, and ensuring accurate financial information. It allows you to identify errors, dispute inaccuracies, and understand how your credit history is viewed by lenders and other entities.

Some factors to consider:

- **Free to check online every week:** The federal government lets you check your credit report from each nationwide credit bureau once a week for free at AnnualCreditReport.com.
- **Helps you catch signs of identity theft early:** Regularly reviewing your credit report helps you detect signs of identity theft early, such as unauthorized accounts or inquiries, so you can take prompt action.
- **Request from each credit-reporting agency:** The three nationwide credit bureaus have a centralized website, toll-free telephone number, and mailing address so you can order your free annual reports in one place. Do not contact the three credit bureaus individually.
- **Does not include your credit score:** Your credit report and your credit score are not the same thing. Your credit report contains information that a credit reporting has received about you. Your credit score is calculated by plugging the information in your credit report into a credit score formula.

IMPORTANT CONSIDERATIONS

- Federal law gives you the right to ask for a copy of your credit report from each nationwide credit reporting company every year for free or weekly, if you do it yourself online.
- The information in your credit report can affect your chance to get a job, rent or buy a place to live, and buy insurance. Credit bureaus sell the information in your report to businesses that use it to decide whether to loan you money, give you credit, offer you insurance, or rent you a home. Some employers use credit reports in hiring decisions. The strength of your credit history also affects how much you will have to pay to borrow money.

RESOURCES

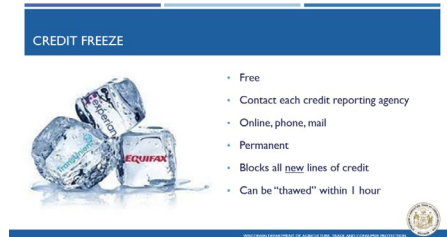
- **Free credit reports | Department of Agriculture, Trade and Consumer Protection**
<https://datcp.wi.gov/Pages/Publications/CreditReportFree409.aspx>
- **All about credit reports | Annual Credit Reports**
<https://www.annualcreditreport.com/whatIsCreditReport.action>
- **Free credit reports | Federal Trade Commission**
<https://consumer.ftc.gov/articles/free-credit-reports>.

16. CREDIT FREEZE

2 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

Freezing your credit helps prevent identity theft and fraud by restricting access to your credit reports, making it harder for scammers to open new accounts in your name. It is a proactive measure, especially helpful if you are concerned about potential identity theft.

- Free
- Contact each credit reporting agency
- Online, phone, mail
- Does not expire
- Blocks all new lines of credit
- Can be "thawed" within one hour
- Freezing your credit is a free service offered by all three major credit bureaus (Equifax, Experian, and TransUnion).
- You can do it online, by phone, or by mail.
- When a credit freeze is in place, it restricts access to your credit report, preventing lenders from opening new accounts in your name.
- A credit freeze stays active until you either lift it permanently or temporarily.
- Quick and easy to unfreeze. When you are ready to apply for a new credit card or loan, you can easily unfreeze your credit temporarily for the duration of the application.
- Freezing your credit will not affect your credit score.
- Freezing your credit only impacts future loans – not current ones.

RESOURCES

- **Credit report security freeze | Department of Agriculture, Trade and Consumer Protection**
<https://datcp.wi.gov/Pages/Publications/IDTheftCreditReportFreeze632.aspx>
- **Credit Freeze or Fraud Alert: What's Right for Your Credit Report? | Federal Trade Commission**
<https://consumer.ftc.gov/articles/credit-freeze-or-fraud-alert-whats-right-your-credit-report>

17. IDENTITY THEFT PROTECTION INSURANCE

2 MIN

Facilitator Notes/Questions

SLIDE

IDENTITY THEFT PROTECTION INSURANCE

There are many businesses that now offer:

- Credit report monitoring services
- “Dark web” scans
- Identity theft protection
- Identity theft insurance

Is it worth it?

What does it cover?



NARRATIVE

There are many businesses that now offer:

- Credit report monitoring services
- “Dark web” scans
- Identity theft protection
- Identity theft insurance

IMPORTANT CONSIDERATIONS

- Identity theft insurance cannot prevent the theft from happening in the first place.
- Many types of identity theft can be recovered from at little to no cost to the victim. Like all insurance, the consumer must look at the coverage, deductibles, and cost, before deciding to purchase or not.
- Consumers should evaluate the company, learn if there are complaints against them, and learn about their data privacy policies and practices.
- Before doing business, be aware that they may need your personal information to “do the job”.

RESOURCES

- Identity theft protection, insurance and credit monitoring services | Department of Agriculture, Trade and Consumer Protection
<https://datcp.wi.gov/Pages/Publications/IDTheftInsurance617.aspx>

18. HOME TITLE THEFT

2 MIN

Facilitator Notes/Questions

SLIDE



HOME TITLE THEFT

- Often starts with identity theft
- Target empty homes
 - Vacation or rental properties
- Target homes high in equity
- Owner's title insurance
- Obtain fraudulent deeds
- Open home equity line of credit
- Monitor county register of deeds

NARRATIVE

Home title theft, also known as deed fraud, involves someone illegally transferring a property title without the homeowner's consent, effectively stealing ownership rights. It is a type of real estate fraud where criminals forge documents or use false identities to steal a property deed and transfer it to their own name. This allows them to sell the property or take out loans against it without the homeowner's knowledge or permission.

Here are some factors to consider:

While rare in Wisconsin, it is worth highlighting, because:

- Often starts with identity theft
- Targets empty homes
 - Vacation or rental properties
- Targets homes high in equity
- Owner's title insurance
- Obtain fraudulent deeds
- Open home equity line of credit

IMPORTANT CONSIDERATIONS

- Criminals may steal personal information like Social Security numbers or use false IDs to forge documents. They then register the fraudulent transfer at the county recorder's office, allowing them to sell the property or take out loans.
- Check with your county to see if there is a way to "lock/freeze" your title/deed.
- Home title theft often requires the owner's identity to be stolen or compromised beforehand.
- Open any letters you receive from a mortgage company, even if your name is not on it. Find out what it says and follow up to get more information.
- Homeowners should monitor their property records regularly (this can be done for free or for a small fee), be cautious about suspicious activity related to their property, and consider protecting their identity. They should also be wary of anyone offering to buy their property for below market value or asking for overly detailed financial information.

19. IDENTITY THEFT WARNING SIGNS

2 MIN

Facilitator Notes/Questions

SLIDE

IDENTITY THEFT WARNING SIGNS

- Unauthorized debit and credit charges
- Unsolicited credit cards in the mail
- Unsolicited change of address
- Earning Statement / W-2
- Unknown claims in medical explanation of benefits
- Bill collectors are calling

The slide features a word cloud graphic with the words 'stealing', 'security', 'identity', and 'theft' prominently displayed. Other words in the cloud include 'information', 'fraud', 'credit', 'card', 'debit', 'charge', 'change', 'address', 'statement', 'W-2', 'medical', 'explanation', 'benefits', 'bill', 'collectors', 'calls', 'unknown', 'debts', 'notice', 'receive', 'notice', 'change', 'address', 'requests', 'forms', 'do', 'not', 'recognize', 'claims', 'in', 'a', 'medical', 'explanation', 'of', 'benefits', 'receive', 'calls', 'from', 'bill', 'collectors', 'for', 'unknown', 'debts', 'notice', 'any', 'of', 'these', 'warning', 'signs', 'it', 'is', 'crucial', 'to', 'take', 'action', 'promptly', 'you', 'can', 'place', 'a', 'fraud', 'alert', 'or', 'security', 'freeze', 'on', 'your', 'credit', 'report', 'and', 'you', 'should', 'check', 'your', 'credit', 'report', 'and', 'bank', 'statements', 'regularly', 'be', 'sure', 'to', 'examine', 'your', 'W-2', 'and', 'Explanation', 'of', 'Benefits', 'EOB', 'when', 'they', 'arrive', 'identity', 'theft', 'and', 'privacy', 'protection', 'Department', 'of', 'Agriculture', 'Trade', 'and', 'Consumer', 'Protection', 'https://datcp.wi.gov/Pages/Programs_Services/IdentityTheft.aspx'.

NARRATIVE

There are several warning signs that you might be experiencing identity theft:

- You notice unauthorized debit and credit charges.
- You receive unsolicited credit cards in the mail.
- You notice unsolicited change of address requests.
- You receive earning statements or W-2 forms you do not recognize.
- You receive unknown claims in a medical explanation of benefits.
- You receive calls from bill collectors for unknown debts.

IMPORTANT CONSIDERATIONS

- If you notice any of these warning signs, it is crucial to take action promptly. You can place a fraud alert or security freeze on your credit report, and you should check your credit report and bank statements regularly. Be sure to examine your W-2 and Explanation of Benefits (EOB) when they arrive.

RESOURCES

- **Identity theft and privacy protection | Department of Agriculture, Trade and Consumer Protection**
https://datcp.wi.gov/Pages/Programs_Services/IdentityTheft.aspx

20. IDENTITY THEFT VICTIM RESPONSE

2 MIN

Facilitator Notes/Questions

SLIDE

IDENTITY THEFT VICTIM RESPONSE

- Report to:
 - Law Enforcement – (police report)
 - Bureau of Consumer Protection at DATCP (complaint packet)
 - Federal Trade Commission (resources)
- Contact financial institutions and CRAs to contest fraudulent charges or accounts
- Obtain copy of credit report to determine how widespread the ID Theft is

The slide also includes a screenshot of the DATCP website, showing a form for reporting identity theft and a list of resources.

NARRATIVE

Identity theft is a complicated and personal problem. It is normal for this crime to have an emotional impact on you and your family. Nonetheless, you should take action.

Here are some steps you should take as soon as possible:

1. File a report with law enforcement (police report) and ask for a copy for your records.
2. Visit datcp.wi.gov to get a complaint packet.
3. Visit ftc.gov – the website of the Federal Trade Commission, for additional resources on identify theft.
4. Contact financial institutions and credit reporting agencies (CRAs) to see how widespread the situation could be and contest any inaccurate information.
5. Obtain copy of credit report to determine how widespread the identity theft is.

RESOURCES

- **Identity theft and privacy protection | Department of Agriculture, Trade and Consumer Protection**
https://datcp.wi.gov/Pages/Programs_Services/IdentityTheft.aspx

21. HOW TO FILE A COMPLAINT

1 MIN

Facilitator Notes/Questions

SLIDE

FILING A COMPLAINT WITH DATCP

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



NARRATIVE

Consumers have several options to submit a complaint:

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

INSTRUCTIONS FOR PRESENTER

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

RESOURCES

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

22. 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.

23. THANK YOU

0 MIN

Facilitator Notes/Questions

SLIDE

