PRESENTER GUIDE

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

PRESENTATION: CYBERSECURITY FOR CONSUMERS

The **Cybersecurity for Consumers presenter guide** is to be used in conjunction with the delivery of the presentation developed by the Bureau of Consumer Protection.

Audience: General public and community groups.

Presentation Length: Approximately 60 minutes.

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

The guide is not intended for distribution among session participants.

TABLE OF CONTENT

1. Cover Page

0.5 MIN

Facilitator Notes/Questions

SLIDE

2. What is Cybersecurity?

0.5 MIN

Facilitator Notes/Questions

SLIDE

INSTRUCTIONS FOR PRESENTER

Consider using a prompt question: What is cybersecurity?

NARRATIVE

Cybersecurity is the practice of protecting networks, devices, and data from unauthorized access or criminal use, while ensuring confidentiality, integrity, and availability. — Cybersecurity and Infrastructure Security Agency (CISA)

- This official definition establishes digital safety as a comprehensive shield that keeps your personal devices, connected home systems, and private data protected from exploitation while ensuring your financial records remain completely unaltered and your online accounts stay fully accessible to you whenever you need them.

RESOURCES

- **Online Privacy and Security | Federal Trade Commission (FTC)**
  https://consumer.ftc.gov/identity-theft-and-online-security/online-privacy-and-security
- **Cybersecurity Basics and Core Definition| Cybersecurity and Infrastructure Security Agency (CISA)**
  https://www.cisa.gov/topics/cybersecurity-best-practices

3. WHY SHOULD I CARE ABOUT CYBERSECURITY? | 2 MIN

Facilitator Notes/Questions

SLIDE

INSTRUCTIONS FOR PRESENTER

Consider using a prompt question: Why should I care about cybersecurity?

NARRATIVE

Cybersecurity affects nearly everyone—not just technology professionals.

- Every individual who interacts with a digital screen or an internet-connected service is an active participant in today's modern security landscape.

Smartphones, email, online banking, shopping, and social media are part of daily life.

- Because our daily routines rely completely on the convenience of handling sensitive personal records and private communications right from our pockets, protecting these platforms is essential to preventing identity theft.

Today's online scams target consumers more often than computer systems.

- Modern cybercriminals rarely spend time trying to crack sophisticated firewalls when they can simply use phishing emails or deceptive text messages to trick an individual instead.

Small changes in everyday habits can greatly reduce your risk.

- Simple actions, such as turning on multi-factor authentication or setting up automatic software updates, create an immediate roadblock against automated online scams.

Cybersecurity is an important part of protecting yourself and your family.

- Just as you would lock your physical front door at night to protect your household, practicing good cyber hygiene preserves your (and your family's) real-world financial safety and privacy.

RESOURCES

- **Online Privacy and Security | Federal Trade Commission (FTC)**
  https://consumer.ftc.gov/identity-theft-and-online-security/online-privacy-and-security
- **Secure Our World Consumer Initiative | Cybersecurity and Infrastructure Security Agency (CISA)**
  https://www.cisa.gov/secure-our-world

4. ISN'T CYBERSECURITY JUST FOR IT PROFESSIONALS? | 2 MIN

Facilitator Notes/Questions

SLIDE

INSTRUCTIONS FOR PRESENTER
Consider using a prompt question: Isn't cybersecurity just for IT professionals?

NARRATIVE
The ultimate shield against cyber fraud rests in the hands of the individual consumer. Taking personal responsibility for your digital habits builds a safer internet environment for yourself, your family, and your entire community.

Cybersecurity is no longer just an IT issue.

- While network defense was once considered a complex task reserved exclusively for corporate programmers, our hyper-connected modern lives have transformed digital safety into a mainstream consumer protection priority for every household.

Anyone using a phone, computer, or the internet can become a target.

- Cybercriminals deploy automated campaigns that do not discriminate based on your age or income, meaning that simply owning a smartphone or email address automatically puts you within their reach.

Online safety is about protecting your identity, finances, and personal information.

- Implementing a strong digital defense serves as your primary shield against devastating real-world consequences like drained bank accounts, stolen Social Security numbers, and long-term identity theft.

Good security habits help prevent scams before they happen.

- By proactively adopting basic protective habits like verifying unexpected alerts and using strong credentials, you can successfully block online threats before they ever gain access to your private data.

Everyone plays a role in protecting themselves online.

- Government consumer protection agencies can issue warnings, but the ultimate shield against digital fraud relies on individual consumers taking personal responsibility for their own cyber hygiene.

RESOURCES

- **How to Recognize and Avoid Phishing Scams | Federal Trade Commission (FTC)**
  https://consumer.ftc.gov/articles/how-recognize-avoid-phishing-scams
- **Cybersecurity Best Practices Guide | Cybersecurity and Infrastructure Security Agency (CISA)**
  https://www.cisa.gov/topics/cybersecurity-best-practices

5. How Does Cybersecurity Relate to Consumer Protection? 2 MIN

Facilitator Notes/Questions

SLIDE

NARRATIVE

Many modern scams happen online.

- Traditional con artists have largely shifted their operations away from physical tactics into digital spaces like email, social media, and text messaging, allowing them to target thousands of unsuspecting consumers simultaneously with minimal overhead cost.

Criminals use technology to steal money and personal information.

- Threat actors deploy deceptive tools like malicious links and automated scripts to compromise consumer devices, rapidly draining financial accounts or harvesting private credentials to sell to underground data brokers

Identity theft

- This occurs when bad actors illegally acquire your sensitive data, such as your Social Security number or bank routing details, to open fraudulent accounts and lines of credit under your name.

Fake online stores

- Scammers build highly convincing e-commerce websites featuring deeply discounted, non-existent products to steal consumers' money and harvest their credit card details for automated fraud rings.

Investment scams

- Deceptive online schemes leverage messaging platforms and social media to trick victims into depositing funds into fraudulent cryptocurrency applications or fake stock portfolios by promising guaranteed, high-return payouts with zero risk.

Bank impersonation scams

- Fraudsters send urgent text alerts or place spoofed calls pretending to be from your bank's security department, using fear tactics to trick you into revealing access codes or transferring funds directly into accounts they control.

Consumer protection now includes digital safety.

- Government agencies have significantly expanded traditional fair-trading safeguards to aggressively combat online fraud networks, making digital hygiene just as essential to household security as understanding your fundamental consumer rights.

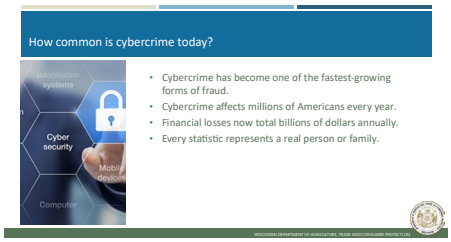
RESOURCES

- **How to Recognize and Avoid Phishing Scams | Federal Trade Commission (FTC)**
  https://consumer.ftc.gov/articles/how-recognize-avoid-phishing-scams
- **Online Privacy and Security| Federal Trade Commission (FTC)**
  https://consumer.ftc.gov/identity-theft-and-online-security/online-privacy-and-security

6. How Common is Cybercrime Today? | 2 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

Cybercrime has become one of the fastest-growing forms of fraud.

- As our reliance on digital connectivity accelerates, malicious actors are continuously developing automated and highly sophisticated methods to exploit everyday consumers on a massive scale.

Cybercrime affects millions of Americans every year.

- From deceptive text messages to identity theft rings, digital scams now successfully penetrate the households of over a million citizens annually across the nation.

Financial losses now total billions of dollars annually.

- According to official federal reporting data, internet-related fraud stripped nearly $21 billion from the American economy in 2025 alone.

Every statistic represents a real person or family.

- Beyond the overwhelming numbers and dollar figures, a single digital security compromise can completely disrupt a household's financial stability, emotional well-being, and long-term peace of mind.

RESOURCES

- **Internet Crime Complaint Center (IC3) Annual Report | Federal Bureau of Investigation (FBI)**
  https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf
- **Online Privacy and Security| Federal Trade Commission (FTC)**
  https://consumer.ftc.gov/identity-theft-and-online-security/online-privacy-and-security

7. WHY DO CRIMINALS TARGET EVERYDAY PEOPLE? | 2 MIN

Facilitator Notes/Questions

SLIDE

NARRATIVE

Victims come from every age group and background.

- Scammers deliberately customize their deceptive tactics to target everyone from teenagers scrolling on social media to retirees protecting their lifelong savings.

Criminals are not just looking for wealthy victims; they're looking for opportunity.

- Automated cyberattack tools constantly sweep the internet to exploit unlocked digital doors and weak security settings without any regard for the victim's actual income level.

Your information has value even if you don't think it does.

- Even if your bank account balance is modest, your basic email logins, utility account numbers, and personal identifiers are highly prized on the dark web for building identity theft profiles.

Anyone with email, online banking, credit cards, smartphones, etc. can become a target.

- Using even a single modern digital convenience automatically places your daily lifestyle within the operational reach of global scam networks and automated phishing scripts.

Cybercrime is ultimately about people, not technology.

- While threat actors rely on digital tools to distribute their scams, their structural success entirely depends on manipulating normal human emotions like trust, panic, or curiosity.

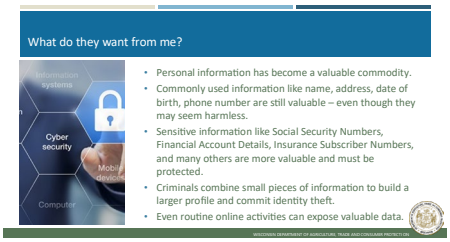
RESOURCES

- **Internet Crime Complaint Center (IC3) Annual Report | Federal Bureau of Investigation (FBI)**
  https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf
- **Online Privacy and Security| Federal Trade Commission (FTC)**
  https://consumer.ftc.gov/identity-theft-and-online-security/online-privacy-and-security

8. WHAT DO THEY WANT FROM ME? | 2 MIN

Facilitator Notes/Questions

SLIDE



INSTRUCTIONS FOR PRESENTER

Consider using a prompt question: What do they want from me?

NARRATIVE

Personal information has become a valuable commodity.

- In the modern digital economy, your personal data functions as a high-value currency that cybercriminals actively steal, trade, and monetize on dark web marketplaces.

Commonly used information like name, address, date of birth, phone number are still valuable – even though they may seem harmless.

- Although basic details like your phone number or home address might seem completely insignificant on their own, scammers prize this data because it allows them to target you with highly customized phishing schemes.

Sensitive information like Social Security numbers, financial account details, insurance subscriber numbers, and many others, are more valuable and must be protected.

- High-value identifiers like your Social Security number or banking credentials require the absolute highest level of protection because threat actors can immediately weaponize them to drain your bank accounts or file fraudulent tax returns.

Criminals combine small pieces of information to build a larger profile and commit identity theft.

- Sophisticated identity thieves carefully piece together minor fragments of public and private data collected from various sources to construct a complete profile, enabling them to open fraudulent lines of credit in your name.

Even routine online activities can expose valuable data.

- Seemingly harmless daily habits, such as connecting to unencrypted public Wi-Fi networks or taking viral social media quizzes, can inadvertently leak personal files directly to opportunistic hackers.

RESOURCES

- **Identity Theft Consumer Tips and Info | Department of Agriculture, Trade and Consumer Protection**
  https://datcp.wi.gov/Pages/Publications/IDTheftPrivacyProtectionFactSheets.aspx
- **Identity Theft Tips for Consumers| Department of Agriculture, Trade and Consumer Protection**
  https://datcp.wi.gov/Pages/Publications/IDTheftConsumerTips636.aspx
- **What to Know About Identity Theft | Federal Trade Commission (FTC)**
  https://consumer.ftc.gov/articles/what-know-about-identity-theft
- **Preventing and Responding to Identity Theft | Cybersecurity and Infrastructure Security Agency**
  https://www.cisa.gov/news-events/news/preventing-and-responding-identity-theft

9. How Do Criminals Exploit Weak Cybersecurity? | 2 MIN

Facilitator Notes/Questions

SLIDE

NARRATIVE

Most cybercriminals don't "hack" computers like in the movies.

- Real-world cyber threats rarely involve highly sophisticated programmers breaking through complex enterprise security firewalls, but instead rely on automated scripts designed to scan for completely unguarded devices and weak credentials.

They manipulate people into giving away information voluntarily. This is called social engineering.

- Social engineering is a deceptive psychological methodology where scammers deliberately build fake scenarios to trick you into bypassing your own safety protocols and handing over private access keys.

Criminals rely on trust, urgency, and emotion.

- By triggering artificial emergencies—such as an alleged fraud alert on your bank account or a fabricated problem with a package delivery—fraudsters manipulate your anxiety so you react impulsively before you have time to think clearly.

The easiest target is often a distracted or unsuspecting person.

- Threat actors specifically design their schemes to catch consumers while they are multi-tasking or rushing through their day, knowing that a busy individual is significantly more likely to overlook a suspicious link or a spoofed sender address.

Common methods include; fake emails (phishing), fraudulent text messages (smishing), phone scams (vishing), fake websites, and many more.

- These pervasive multi-channel scams exploit our everyday communication tools to cast an incredibly wide net, hunting for any consumer who will inadvertently click a malicious link or answer a fraudulent caller.

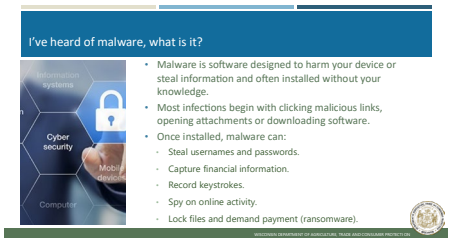
RESOURCES

- **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
- **Avoid Social Engineering and Phishing Attacks | Cybersecurity and Infrastructure Security Agency**
  https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks
- **How to Recognize and Avoid Phishing Scams | Federal Trade Commission (FTC)**
  https://consumer.ftc.gov/articles/how-recognize-avoid-phishing-scams

10. I'VE HEARD OF MALWARE, WHAT IS IT? | 2 MIN

Facilitator Notes/Questions

SLIDE



INSTRUCTIONS FOR PRESENTER

Consider using a prompt question: Have you heard of malware, and if so, do you know what it is?

NARRATIVE

Malware is software designed to harm your device or steal information, and it is often installed without your knowledge.

- Malware stands for "malicious software" and represents any unauthorized program that slips onto your computer or phone to secretly disrupt your system, monitor your behavior, or harvest your data.

Most infections begin with clicking malicious links, opening attachments or downloading software.

- Cybercriminals rarely force their way into a clean device; instead, they trick consumers into downloading the infection themselves by hiding it behind urgent fake delivery alerts, suspicious email attachments, or deceptive pop-up windows.

Once installed, malware can…

- Run silently in the background to compromise your digital safety in several specific ways.

Steal usernames and passwords.

- The software can scan your device's saved data or web browser memory to harvest account credentials and send them directly to identity theft networks.

Capture financial information.

- Malware can actively monitor your online shopping sessions or extract stored bank details to allow scammers to execute unauthorized transfers under your name.

Record keystrokes.

- Specialized tracking programs known as keyloggers can register every individual button you press on your screen or keyboard, allowing thieves to secretly record your private messages and security PINs.

Spy on online activity.

- Spyware variants can silently track your web browsing history, monitor your physical location, or even access your device's camera to severely violate your personal privacy.

Lock files and demand payment (ransomware).

- Extortion software known as ransomware can completely encrypt your family photos, tax forms, and vital files, holding your digital life hostage until an expensive ransom fee is paid.

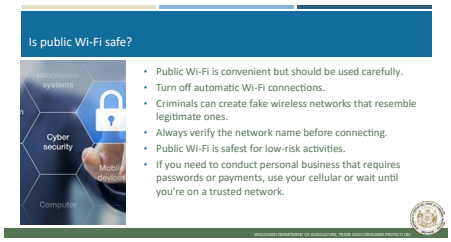
RESOURCES

- **Malware: How To Protect Against, Detect, and Remove It | Federal Trade Commission (FTC)**
  https://consumer.ftc.gov/articles/malware-how-protect-against-detect-and-remove-it
- **Recognizing and Avoiding Malware | Cybersecurity and Infrastructure Security Agency**
  https://www.cisa.gov/news-events/news/recognizing-and-avoiding-spyware

11. Is Public Wi-Fi Safe? 2 MIN

Facilitator Notes/Questions

SLIDE



INSTRUCTIONS FOR PRESENTER

Consider using a prompt question: By a show of hands, how many of you think public Wi-Fi is safe?

NARRATIVE

Public Wi-Fi is convenient but should be used carefully.

- Free wireless internet access in public spaces makes staying connected effortless, but these shared networks lack the basic security encryption necessary to keep your private data secure from nearby snoops.

Turn off automatic Wi-Fi connections.

- Leaving your smartphone or tablet set to auto-connect allows your device to silently join unsecured local networks without your explicit knowledge or permission.

Criminals can create fake wireless networks that resemble legitimate ones.

- Scammers frequently deploy rogue wireless routers to broadcast deceptive "evil twin" network names that trick consumers into routing their traffic directly through a criminal's system.

Always verify the network name before connecting.

- You should always double-check the exact spelling of a wireless network with the establishment's staff to ensure you are not joining a fraudulent look-alike hotspot.

Public Wi-Fi is safest for low-risk activities.

- Shared public connections are perfectly fine for casual browsing, checking the weather, or reading public articles where no account login is required.

If you need to conduct personal business that requires passwords or payments, use your cellular data or wait until you can use a trusted network.

- When managing financial balances, making online purchases, or accessing sensitive accounts, you should completely disconnect from public Wi-Fi and switch to your encrypted mobile data hotspot for safety.

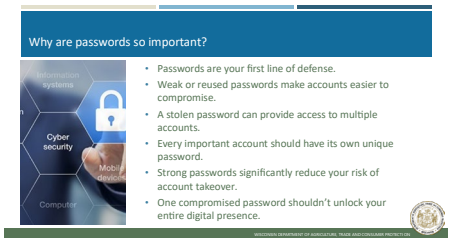
RESOURCES

- **Tips for Using Public Wi-Fi | Department of Agriculture, Trade and Consumer Protection**
  https://datcp.wi.gov/Pages/Publications/IDTheftWi-FiTips659.aspx
- **Tips for Using Public Wireless Networks Safely | Federal Trade Commission (FTC)**
  https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know
- **Securing Wireless Devices in Public Settings | Cybersecurity and Infrastructure Security Agency**
  https://www.cisa.gov/news-events/news/securing-wireless-networks

12. WHY ARE PASSWORDS SO IMPORTANT? | 2 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

Passwords are your first line of defense.

- A password acts as the primary digital padlock protecting your private life, serving as the baseline boundary that keeps unauthorized individuals away from your personal accounts.

Weak or reused passwords make accounts easier to compromise.

- When you choose simple words or repeat the same phrase across multiple websites, cybercriminals can use automated software to guess your credentials almost instantly.

A stolen password can provide access to multiple accounts.

- If a scammer successfully compromises a single password that you have duplicated, they will immediately try to use it to break into your other profiles across the internet.

Every important account should have its own unique password.

- Creating a distinct password for each individual platform ensures that a security problem at one minor website does not expose your highly sensitive financial files.

Strong passwords significantly reduce your risk of account takeover.

- Upgrading to a long and complex passphrase makes it mathematically impossible for automated hacking tools to crack your profile during a mass credential attack.

One compromised password should not unlock your entire digital presence.

- Isolating your online profiles with independent keys ensures that a single data leak remains completely contained rather than turning into a total identity crisis.

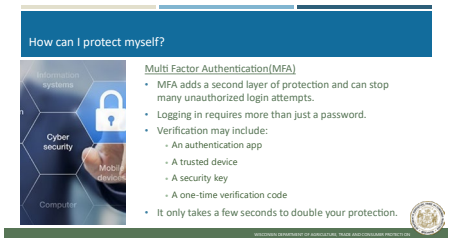
RESOURCES

- **Creating Strong Passwords| Department of Agriculture, Trade and Consumer Protection**
  https://datcp.wi.gov/Pages/Publications/IDTheftPasswordsCreating658.aspx
- **Advice on Creating Unique Passwords | Cybersecurity and Infrastructure Security Agency**
  https://www.cisa.gov/secure-our-world/use-strong-passwords
- **Creating Strong Passwords and Securing Accounts | Federal Trade Commission (FTC)**
  https://consumer.ftc.gov/articles/creating-strong-passwords-and-other-ways-protect-your-accounts

13. How Can I Protect Myself? 2 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

Multi-Factor Authentication (MFA)

- Multi-factor authentication is an essential, multi-layered security setup that acts as an advanced digital checkpoint to protect your accounts from remote exploitation.

MFA adds a second layer of protection and can stop many unauthorized login attempts.

- This secondary verification layer successfully blocks cybercriminals from entering your private profiles even if they have already stolen your correct username and password string.

Logging in requires more than just a password.

- Enabling this feature means that gaining entry to your data relies on combining a traditional password with a live validation step that only you can complete.

Verification may include: An authentication app

- A dedicated application on your smartphone can generate temporary, rolling numeric codes that provide superior defense against modern identity thieves.

Verification may include: A trusted device

- A pre-registered personal smartphone or tablet can receive a direct security prompt requiring you to tap a notification to approve a login.

Verification may include: A security key

- A physical USB or wireless hardware token offers uncopyable protection by requiring a direct physical touch to verify access.

Verification may include: A one-time verification code

- A temporary code sent immediately to your phone number or backup email address sets up a quick secondary barrier against automated remote hackers.

It only takes a few seconds to double your protection.

- Turning this feature on across your primary email and banking platforms takes minimal effort but instantly eliminates the vast majority of automated account takeover threats.

RESOURCES

- **Multi-Factor Authentication Consumer Guide | Cybersecurity and Infrastructure Security Agency** https://www.cisa.gov/topics/cybersecurity-best-practices/multifactor-authentication
- **Protect Your Personal Information From Hackers and Scammers| Federal Trade Commission (FTC)** https://consumer.ftc.gov/articles/protect-your-personal-information-hackers-and-scammers

14. How Can I Protect Myself? 2 MIN

Facilitator Notes/Questions

SLIDE

NARRATIVE

Software Updates

Updates fix known security vulnerabilities.

- Software manufacturers routinely issue these digital patches to repair hidden programming flaws and close off entries that could allow malicious code to compromise your operating system.

Criminals often target devices with outdated software.

- Cybercriminals actively scan the internet for unpatched phones and computers because older software versions provide an easy, unguarded pathway to execute automated data-harvesting attacks.

Updates improve both security and performance.

- In addition to deploying critical safety defenses, regular software updates optimize your device's processing speed, resolve system bugs, and introduce helpful new features.

Delaying updates increases your exposure to risk.

- Every time you choose to postpone a software notification, you prolong the window of opportunity for an opportunistic scammer to exploit a known flaw on your device.

Enable automatic updates whenever possible.

- Turning on automatic updates within your device settings ensures that your smartphone, apps, and web browsers receive immediate, hands-free protection against emerging online fraud networks.

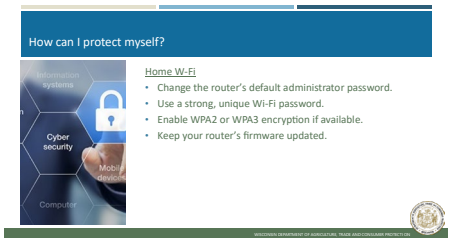
RESOURCES

- **Computer Protection Tips| Department of Agriculture, Trade and Consumer Protection**
  https://datcp.wi.gov/Pages/Publications/IDTheftComputerProtection643.aspx
- **Protect Your Computer from Malware | Federal Trade Commission (FTC)**
  https://www.ftc.gov/media/79889
- **Secure Our World Consumer Initiative | Cybersecurity and Infrastructure Security Agency (CISA)**
  https://www.cisa.gov/secure-our-world

15. How Can I Protect Myself? 2 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

Home Wi-Fi

Change the router's default administrator password.

- Most internet routers come pre-configured with generic, factory-default administrative credentials that cybercriminals can easily look up online to gain total control of your network.

Use a strong, unique Wi-Fi password.

- Replacing your default wireless password with a long, distinct passphrase blocks unauthorized strangers and automated hacking tools from piggybacking on your connection.

Enable WPA2 or WPA3 encryption if available.

- Activating WPA3 or WPA2 wireless security in your settings scrambles the information moving across your network, ensuring that nearby threat actors cannot intercept or read your private online activities.

Keep your router's firmware updated.

- Regularly updating your router's internal firmware by checking the manufacturer's website or application repairs critical software vulnerabilities before automated exploit scripts can target your household.

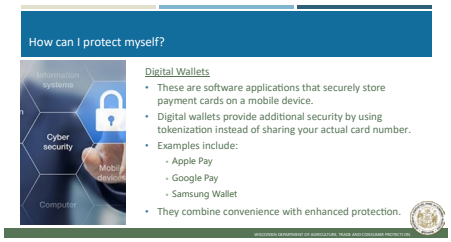
RESOURCES

- **Protect Your Computer from Malware | Federal Trade Commission (FTC)**
  https://www.ftc.gov/media/79889
- **Secure Our World Consumer Initiative | Cybersecurity and Infrastructure Security Agency (CISA)**
  https://www.cisa.gov/secure-our-world

16. How Can I Protect Myself? 2 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

Digital Wallets

These are software applications that securely store payment cards on a mobile device.

- A digital wallet acts as an encrypted virtual vault on your smartphone or smartwatch, safely holding your payment credentials so you do not have to carry or expose physical plastic cards during transactions.

Digital wallets provide additional security by using tokenization instead of sharing your actual card number.

- Instead of broadcasting your real account details to a merchant's card reader, these applications substitute your sensitive data with a randomized, single-use code called a token to validate the transaction.

Examples include: Apple Pay, Google Pay, Samsung Wallet.

- These mainstream, highly regulated mobile payment services come built into modern devices to provide everyday consumers with an instantly accessible layer of transaction security.

They combine convenience with enhanced protection.

- Because these applications require a local biometric check—like a fingerprint scan or facial recognition—to authorize a payment, your financial accounts remain completely inaccessible to thieves even if your physical phone is lost or stolen.

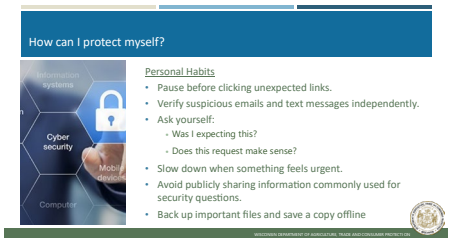
RESOURCES

- **Mobile Payment Apps: How To Avoid a Scam When You Use One| Federal Trade Commission (FTC)** https://consumer.ftc.gov/articles/mobile-payment-apps-how-avoid-scam-when-you-use-one

17. How Can I Protect Myself? 2 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

Personal Habits

Pause before clicking unexpected links.

- Taking a intentional moment to pause before clicking on any unsolicited web link disrupts the automated traps used by cybercriminals to deploy malicious software.

Verify suspicious emails and text messages independently.

- You should always use an official customer service website or a known phone number to confirm an alert rather than using the contact details provided in a questionable message.

Ask yourself: Was I expecting this?

- Evaluating whether an incoming communication aligns with your real-world activities helps you instantly flag unsolicited phishing messages.

Ask yourself: Does this request make sense?

- Questioning why an established agency or business would suddenly demand sensitive personal credentials or odd payment methods reveals the logical flaws common to online scams.

Slow down when something feels urgent.

- Cybercriminals deliberately manufacture high-pressure emergencies to induce fear, so forcing yourself to slow down gives you the time needed to think clearly before reacting impulsively.

Avoid publicly sharing information commonly used for security questions.

- Refraining from answering viral social media quizzes or posting specific personal milestones online prevents scammers from gathering the answers required to reset your account passwords.

Back up important files and save a copy offline.

- Maintaining a detached, offline backup copy of your family files on an external hard drive ensures you can safely restore your data without paying an extortionist if ransomware infects your computer.

RESOURCES

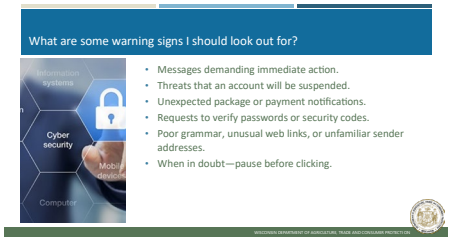
- **Phishing, Vishing and Smishing | Department of Agriculture, Trade and Consumer Protection**
  https://datcp.wi.gov/Pages/Publications/Phishing402.aspx
- **Imposter Scams| Department of Agriculture, Trade and Consumer Protection**
  https://datcp.wi.gov/Pages/Publications/ImposterScams214.aspx
- **Spotting and Reporting Scams | Federal Trade Commission (FTC)**
  https://consumer.ftc.gov/scams
- **Secure Our World Consumer Initiative | Cybersecurity and Infrastructure Security Agency (CISA)**
  https://www.cisa.gov/secure-our-world

18. What Are Some Warning Signs I Should Look Out For?

2 MIN

Facilitator Notes/Questions

SLIDE



INSTRUCTIONS FOR PRESENTER

Consider using a prompt question: What are some warning signs we should look out for?

NARRATIVE

Messages demanding immediate action.

- Phishing attempts deliberately use high-pressure scare tactics to make you panic so that you will act quickly before taking the time to verify if the alert is real.

Threats that an account will be suspended.

- Scammers frequently send fake notifications claiming your bank account, streaming service, or tax profile will be permanently locked unless you click their link immediately.

Unexpected package or payment notifications.

- Deceptive text messages and emails often claim you have a missing delivery or an unpaid invoice to trick you into downloading malware or entering your credit card details.

Requests to verify passwords or security codes.

- Legitimate organizations will never contact you out of the blue to demand your private passwords, full Social Security number, or temporary two-factor authentication codes.

Poor grammar, unusual web links, or unfamiliar sender addresses.

- While some modern scams look highly professional, many phishing attempts still contain subtle spelling errors, strange email extensions, or mismatched website addresses that expose them as fakes.

When in doubt, pause.

- Taking an intentional, calm moment to step away from a suspicious message completely breaks the sense of urgency that cybercriminals rely on to steal your information.

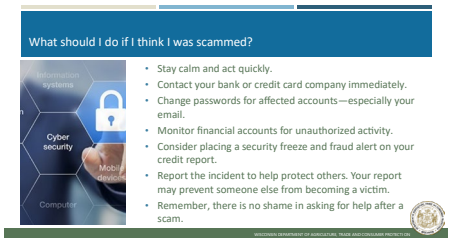
RESOURCES

- **Spotting and Reporting Scams | Federal Trade Commission (FTC)**
  https://consumer.ftc.gov/scams
- **Secure Our World Consumer Initiative | Cybersecurity and Infrastructure Security Agency (CISA)**
  https://www.cisa.gov/secure-our-world

19. WHAT SHOULD I DO IF I THINK I WAS SCAMMED? | 2 MIN

Facilitator Notes/Questions

SLIDE



NARRATIVE

Stay calm and act quickly.

- Taking immediate control of the situation right after a scam occurs is essential to minimizing your overall financial and personal data exposure.

Contact your bank or credit card company immediately.

- Notifying your financial institution right away allows them to freeze compromised accounts, dispute fraudulent charges, and legally shield your remaining funds.

Change passwords for affected accounts—especially your email.

- Updating your passwords immediately prevents scammers from maintaining a persistent foothold in your profiles and completely cuts off their access to your private recovery options.

Monitor financial accounts for unauthorized activity.

- Reviewing your bank statements and credit card history daily over the following weeks helps you catch and report any secondary or delayed fraudulent transactions early.

Consider placing a security freeze and fraud alert on your credit report.

- Requesting a security freeze on a credit report completely blocks bad actors from illegally opening new credit cards or utility accounts in your name using your stolen personal identifiers.

Report the incident to help protect others. Your report may prevent someone else from becoming a victim.

- Filing an official report with federal consumer defense networks helps law enforcement aggregate data to track down global fraud rings and shut down malicious websites.

Remember, there is no shame in asking for help after a scam.

- Modern online fraudsters use sophisticated psychological manipulation designed to trick anyone. Reaching out to trusted family members or official agencies is a vital step toward recovery.

RESOURCES

- **Identity Theft Consumer Tips and Info | Department of Agriculture, Trade and Consumer Protection**
  https://datcp.wi.gov/Pages/Publications/IDTheftPrivacyProtectionFactSheets.aspx
- **What To Do If It Happens to You | Department of Agriculture, Trade and Consumer Protection**
  https://datcp.wi.gov/Pages/Publications/IDTheftWhatToDo602.aspx
- **Identity Theft Recovery and Reporting Portal | Federal Trade Commission (FTC)**
  https://www.identitytheft.gov/
- **What To Do if You Were Scammed| Federal Trade Commission (FTC)**
  https://consumer.ftc.gov/articles/what-do-if-you-were-scammed

20. What Are Some Things I Can Start Doing Today?

2 MIN

Facilitator Notes/Questions

SLIDE

NARRATIVE

Use strong, unique passwords and change them regularly.

- Replacing short, predictable credentials with long passphrases creates an unyielding digital padlock that automated cracking scripts cannot easily decipher.

Enable multi-factor authentication wherever possible.

- Activating multi-factor authentication creates a vital secondary security checkpoint that completely blocks unauthorized remote logins even if a scammer manages to steal your password.

Keep devices and software updated.

- Regularly updating your operating systems ensures that hidden digital pathways are repaired before opportunistic hackers can locate them.

Verify unexpected communications.

- You should always independently look up an official customer service number to verify a suspicious alert rather than trusting the links or contact info sent in an unexpected message.

Turn on automatic software updates for all devices.

- Switching your phone, web browsers, and apps to update automatically gives your household hands-free, real-time defense against emerging cyber threats.

Review your social media privacy settings.

- Locking down your public profiles prevents bad actors from harvesting the personal details and life events frequently used to bypass account security verification questions.

Talk with a family member about online scams.

- Sharing these practical safety baselines with your loved ones builds an open, supportive household defense network that actively shields vulnerable relatives from predatory fraud rings.

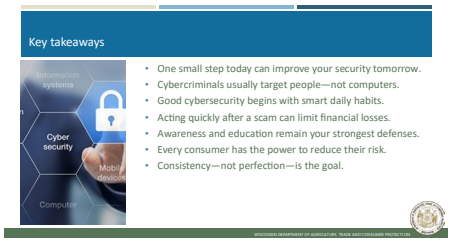
RESOURCES

- **Secure Our World Consumer Initiative | Cybersecurity and Infrastructure Security Agency (CISA)** https://www.cisa.gov/secure-our-world

21. KEY TAKEAWAYS | 2 MIN

Facilitator Notes/Questions

SLIDE



INSTRUCTIONS FOR PRESENTER

- Use this final slide to summarize the entire presentation. Remind them that they do not need to be tech experts to protect their households, they just need to remain mindful as they go about their everyday digital routines.

NARRATIVE

One small step today can improve your security tomorrow.

- Taking immediate action to secure just one critical asset, like your primary email address, sets up a powerful barrier that completely disrupts a hacker's automated strategy.

Cybercriminals usually target people—not computers.

- Because modern consumer fraud relies almost entirely on social engineering and emotional manipulation, your personal skepticism is your single most effective defense against online scams.

Good cybersecurity begins with smart daily habits.

- Achieving a safe online environment does not require an advanced computer science degree, but simply the willingness to stick to secure personal habits as you browse, shop, and communicate.

Acting quickly after a scam can limit financial losses.

- If an incident does occur, moving past the initial shock immediately to contact your bank and freeze your credit files will dramatically reduce the scammer's ability to cause long-term damage.

Awareness and education remain your strongest defenses.

- Staying updated on the latest deceptive trends allows you to easily spot digital red flags before clicking a malicious link or responding to a fraudulent caller.

Every consumer has the power to reduce their risk.

- You are never entirely helpless against internet threat networks, because activating standard security settings puts the ultimate control of your data back into your own hands.

Consistency—not perfection—is the goal.

- Safeguarding your identity is a continuous practice of building up small operational boundaries over time rather than a flawless, all-or-nothing technical configuration.

RESOURCES

- **Computer and Internet Consumer Tips| Department of Agriculture, Trade and Consumer Protection**
  https://datcp.wi.gov/Pages/Publications/ComputersInternetFactSheets.aspx
- **Secure Our World Consumer Initiative | Cybersecurity and Infrastructure Security Agency (CISA)**
  https://www.cisa.gov/secure-our-world

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.
- DATCP offers free presentations on the topics listed 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! — 2 MIN

Facilitator Notes/Questions

SLIDE