Cybersecurity for Consumers

WISCONSIN DEPARTMENT OF AGRICULTURE TRADE AND CONSUMER PROTECTION

PresentationGuideCybersecurityConsumers761b(09/2026)

What is Cybersecurity?

Cybersecurity is the practice of protecting networks, devices, and data from unauthorized access or criminal use, while ensuring confidentiality, integrity, and availability.

- CISA (Cybersecurity and Infrastructure Security Agency)

Why Should I Care About Cybersecurity?

- Cybersecurity affects nearly everyone—not just technology professionals.
- Smartphones, email, online banking, shopping, and social media are part of daily life.
- Today's online scams target consumers more often than computer systems.
- Small changes in everyday habits can greatly reduce your risk.
- Cybersecurity is an important part of protecting yourself and your family.

Isn’t Cybersecurity Just For IT Professionals?

- Cybersecurity is no longer just an IT issue.
- Anyone using a phone, computer, or the internet can become a target.
- Online safety is about protecting your identity, finances, and personal information.
- Good security habits help prevent scams before they happen.
- Everyone plays a role in protecting themselves online.

How Does Cybersecurity Relate To Consumer Protection?

- Many modern scams now happen online.
- Criminals use technology to steal money and personal information.
- Common scams include:
  - Identity theft
  - Fake online stores
  - Investment scams
  - Bank impersonation scams
- Consumer protection now includes digital safety.

How Common Is Cybercrime Today?

- Cybercrime has become one of the fastest-growing forms of fraud.
- Cybercrime affects millions of Americans every year.
- Financial losses now total billions of dollars annually.
- Every statistic represents a real person or family.

Why Do Criminals Target Everyday People?

- Victims come from every age group and background.
- Criminals aren't just looking for wealthy victims; they're looking for opportunity.
- Your information has value even if you don't think it does.
- Anyone with email, online banking, credit cards, smartphones, etc. can become a target.
- Cybercrime is ultimately about people, not technology.

What Do They Want From Me?

- Personal information has become a valuable commodity.
- Commonly used information like a name, address, date of birth, or phone number are still valuable – even though they may seem harmless.
- Sensitive information like Social Security numbers, financial account details, insurance subscriber numbers, and many others are more valuable and must be protected.
- Criminals combine small pieces of information to build a larger profile and commit identity theft.
- Even routine online activities can expose valuable data.

How Do Criminals Exploit Weak Cybersecurity?

- Most cybercriminals don’t “hack” computers like in the movies.
- They manipulate people into giving away information voluntarily. This tactic is called social engineering.
- Criminals rely on trust, urgency, and emotion.
- The easiest target is often a distracted or unsuspecting person.
- Common methods include; fake emails (phishing), fraudulent text messages (smishing), phone scams (vishing), fake websites, and many more.

I’ve Heard of Malware, What Is It?

- Malware is software designed to harm your device or steal information, and is often installed without your knowledge.
- Most infections begin with clicking malicious links, opening attachments or downloading software.
- Once installed, malware can:
  - Steal usernames and passwords.
  - Capture financial information.
  - Record keystrokes.
  - Spy on online activity.
  - Lock files and demand payment (ransomware).

Is Public Wi-Fi Safe?

- Public Wi-Fi is convenient but should be used carefully.
- Turn off automatic Wi-Fi connections.
- Criminals can create fake wireless networks that resemble legitimate ones.
- Always verify the network name before connecting.
- Public Wi-Fi is safest for low-risk activities.
- If you need to conduct personal business that requires passwords or payments, use your cellular data or wait until you are on a trusted network.

Why Are Passwords So Important?

- Passwords are your first line of defense.
- Weak or reused passwords make accounts easier to compromise.
- A stolen password can provide access to multiple accounts.
- Every important account should have its own unique password.
- Strong passwords significantly reduce your risk of account takeover.
- One compromised password should not unlock your entire digital presence.

How Can I Protect Myself?

Multi Factor Authentication (MFA)

- MFA adds a second layer of protection and can stop many unauthorized login attempts.
- Logging in requires more than just a password.
- Verification may include:
  - An authentication app
  - A trusted device
  - A security key
  - A one-time verification code
- It only takes a few seconds to double your protection.

How Can I Protect Myself?

Software Updates

- Updates fix known security vulnerabilities.
- Criminals often target devices with outdated software.
- Updates improve both security and performance.
- Delaying updates increases your exposure to risk.
- Enable automatic updates whenever possible.

How Can I Protect Myself?

Home Wi-Fi

- Change the router's default administrator password.
- Use a strong, unique Wi-Fi password.
- Enable WPA2 or WPA3 encryption if available.
- Keep your router's firmware updated.

How Can I Protect Myself?

Digital Wallets

- These are software applications that securely store payment cards on a mobile device.
- Digital wallets provide additional security by using tokenization instead of sharing your actual card number.
- Examples include:
  - Apple Pay
  - Google Pay
  - Samsung Wallet
- They combine convenience with enhanced protection.

How Can I Protect Myself?

Personal Habits

- Pause before clicking unexpected links.
- Verify suspicious emails and text messages independently.
- Ask yourself:
  - Was I expecting this?
  - Does this request make sense?
- Slow down when something feels urgent.
- Avoid publicly sharing information commonly used for security questions.
- Back up important files and save a copy offline.

What Are Some Warning Signs I Should Look Out For?

- Messages demanding immediate action.
- Threats that an account will be suspended.
- Unexpected package or payment notifications.
- Requests to verify passwords or security codes.
- Poor grammar, unusual web links, or unfamiliar sender addresses.
- When in doubt—pause before clicking.

What Should I Do If I Think I Was Scammed?

- Stay calm and act quickly.
- Contact your bank or credit card company immediately.
- Change passwords for affected accounts—especially your email.
- Monitor financial accounts for unauthorized activity.
- Consider placing a security freeze and fraud alert on your credit report.
- Report the incident to help protect others. Your report may prevent someone else from becoming a victim.
- Remember, there is no shame in asking for help after a scam.

What Are Some Things I Can Start Doing Today?

- Use strong, unique passwords and change them regularly.
- Enable multi-factor authentication wherever possible.
- Keep devices and software updated.
- Verify unexpected communications.
- Turn on automatic software updates for all devices.
- Review your social media privacy settings.
- Talk with a family member about online scams.

Key Takeaways

- One small step today can improve your security tomorrow.
- Cybercriminals usually target people—not computers.
- Good cybersecurity begins with smart daily habits.
- Acting quickly after a scam can limit financial losses.
- Awareness and education remain your strongest defenses.
- Every consumer has the power to reduce their risk.
- Consistency—not perfection—is the goal.

Learn More About DATCP

Linked In

Facebook

Instagram

X (Twitter)

Consumer Protection

REQUEST A PRESENTATION @ DATCP.WI.GOV

- Common Scams and Fraud
- Identity Theft and Privacy Protection
- Landlord and Tenant - Rights and Responsibilities
- Safe Online Shopping
- Home Improvement Contracts
- Cryptocurrency
- Artificial Intelligence (AI) for Consumer Protection
- Consumer Protection for Young Adults
- Scams and Fraud Targeting Small Businesses
- Business Identity Theft
- And many more!

Thank you!


DEPARTMENT OF AGRICULTURE, TRADE AND CONSUMER PROTECTION
FORWARD
WISCONSIN
FOR RENT