Mankato Computer Technology Internet, Email, and AI Safety

- Simple tips to stay safe, confident, and connected online
- https://mankatotechs.com/
- **OFFICE**
- 11 Civic Center Plaza #300
  Mankato, MN 56001
- 507.625.8324

Why Online Safety Matters

Online safety matters because it protects your personal identity, finances, and mental well-being from pervasive digital threats like malware, scams, and cyberbullying.

Practicing good cyber hygiene ensures you can navigate the internet securely without compromising sensitive information or falling victim to malicious attacks.

Understanding and applying internet safety principles is essential for several critical reasons:

1. Protect personal information
2. Avoid scams and fraud
3. Stay connected safely with family and friends

Financial and Data Protection:

Cybercriminals heavily rely on phishing and malware to steal identities, banking details, or login credentials.

Being cautious prevents unauthorized access to your funds and personal information.

Protection from Malicious Content:

The internet contains unregulated spaces where users—especially children and teens—can encounter inappropriate materials, violence, or hate speech.

Safety measures provide a shield against exposure to distressing content.

Preventing Harassment and Bullying:

Cyberbullying can cause severe emotional distress, isolation, and anxiety.

Promoting a secure and respectful digital environment reduces the likelihood of these devastating mental health impacts.

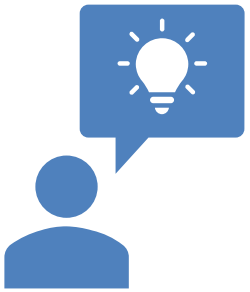
Avoiding Online Predators:

Anonymity online allows predators to easily target vulnerable individuals.

Awareness and education help users identify manipulative behaviors (grooming) and know exactly how to block and report them.

Combating Misinformation

Digital platforms are frequently used to spread unverified claims, conspiracy theories, and disinformation.



Practicing online safety helps you develop critical thinking to evaluate what is real and trustworthy.

To explore actionable tips on protecting your identity and devices, visit the Department of Homeland Security Online Safety Overview

https://www.dhs.gov/blue-campaign/online-safety

Creating Strong Passwords

- Use long passwords (12+ characters)

- Mix letters, numbers, symbols

- Don’t reuse passwords

- Consider a password notebook or manager

1. Use a Random Password Generator

The most secure way to create complex, uncrackable passwords is by letting a tool generate them for you.

- **Built-in tools:** Use your browser's built-in password generator.
- **Dedicated tools:** Generate a random string using the
- 1Password Generator or the
- Avast Password Generator

2. Create a Memorable Passphrase

If you need to remember the password yourself, combine 4 or more unrelated words into a long passphrase.

Example: Battery-Horse-Staple-Correct or Purple~Flying~Turtle~99

Add numbers or special characters to increase complexity.

3. Best Practices

Never reuse passwords: Use a completely unique password for every website and app.

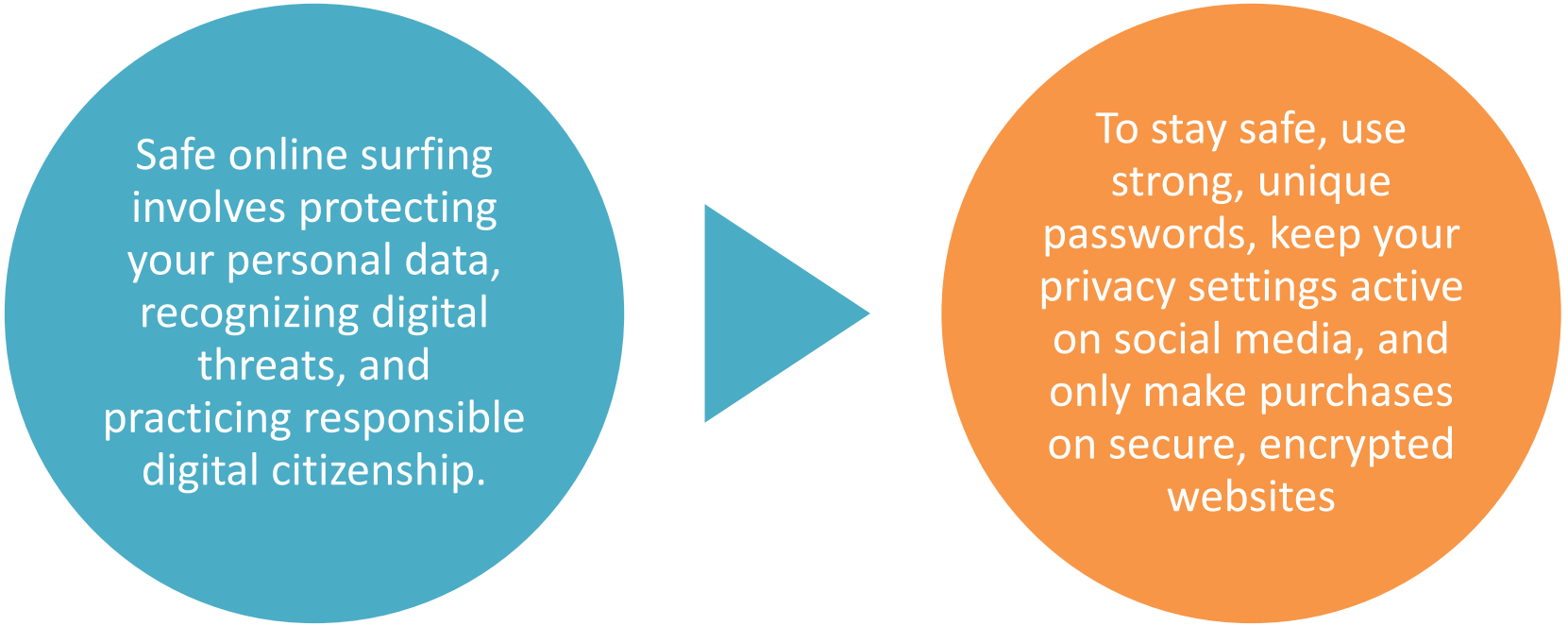
Avoid personal info: Never use names of pets, birthdays, or street addresses.

Use a password manager: Consider a password manager like Bitwarden to safely store and auto-fill all your unique credentials.

Safe Internet Browsing

- Look for https and lock icon
- Avoid unfamiliar pop-ups
- Don’t download from unknown sites
- Keep your device updated

Safe Online Surfing



Essential Internet Safety Rules

Limit Personal Info: Keep details like your address, phone number, and date of birth private.

Use Strong Passwords: Utilize a combination of letters, numbers, and symbols, or use a password manager.

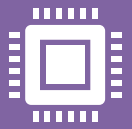
Watch Out for Phishing: Never click on suspicious links from unknown senders or download unexpected attachments.

Secure Your Connections: Avoid logging into sensitive accounts on public Wi-Fi networks unless using a Virtual Private Network (VPN).

Safeguarding Devices

Update Software: Ensure your operating system and web browsers are regularly updated with the latest security patches.

Enable 2FA: Set up two-factor authentication (2FA) across your accounts to add a crucial layer of security.



Install Antivirus: Use trusted security software to scan for malware and viruses.

Email Safety Tips

• Only open emails from people you trust

• Don’t click links in suspicious emails

• Watch for spelling errors or urgency

• When unsure, call the sender

https://www.youtube.com/watch?v=veSumPzip0w&t=7s

Protect your email by enabling multi-factor authentication (MFA), using unique and complex passwords, and avoiding suspicious attachments.

Never click unsolicited links or share sensitive information like passwords or financial details via email. Stay vigilant against phishing attempts.

Account & Password Security

Enable MFA: Add a layer of security so even if your password is stolen, hackers cannot access your account.

Use a Password Manager: Never reuse passwords across sites. Use a trusted password manager like Bitwarden or 1Password to generate and store secure, complex credentials.

Keep Recovery Info Updated: Ensure your recovery email and phone number are accurate so you can regain access if locked out.

Spotting Phishing & Scams

1

Verify the Sender: Double-check the actual email address (not just the display name). Spoofed domains often alter a single letter (e.g., @microsoft-support.com instead of @microsoft.com).

2

Confirm Before You Click: Hover over links before clicking them to view the actual destination URL. If an email asks for login details, do not click the provided link; instead, navigate directly to the official website.

3

Watch for Warning Signs: Urgent requests (like an "expiring subscription"), poor grammar, and generic greetings are major red flags.

Handling Attachments & Data

- **Be Skeptical:** Never open attachments you weren't expecting, even if they come from someone you know.
- **Avoid Executable Files:** Be extremely cautious with files ending in `.exe`, `.scr`, `.bat`, or even zipped files, as they can contain malware.
- **Encrypt Sensitive Info:** Never send confidential details like Social Security or bank account numbers via unencrypted regular email. [1,

🧹 Inbox Hygiene & Privacy

- **Use Email Aliases:** Avoid giving out your main email address to untrusted sites. Use a "throwaway" email or an alias service like SimpleLogin for online shopping or newsletters.
- **Limit Signature Details:** Keep personal information (like your home address, personal phone number, or job title) out of your email signature to prevent it from being forwarded to strangers.
- **Use BCC for Group Emails:** When emailing multiple people who don't know each other, use the Blind Carbon Copy (BCC) field to protect everyone's privacy and avoid chaotic "reply-all" chains

Common Scams to Watch

- ‘Urgent’ messages asking for money
- Fake tech support calls
- Prize or lottery scams
- Requests for personal information

To protect yourself, watch out for high-pressure tactics demanding immediate payment via wire transfers, cryptocurrency, gift cards, or courier.

Common scams currently include AI-driven phishing, fake government imposter alerts, social media marketplace traps, and recovery scams

Stay vigilant by being on the lookout for the following prevalent schemes:

AI Phishing & Deepfakes: Scammers use AI to generate convincing emails, texts, and voice clones—often impersonating bosses, family members in distress, or bank officials to steal your login credentials or money.

Imposter Scams: Callers or messagers pretend to be from the IRS, Medicare, the Social Security Administration, or local law enforcement, threatening immediate arrest or fines if you do not pay them immediately.

Social Media & Marketplace Scams: Fake listings on community boards or social media platforms offer items at unbelievable discounts or ask for upfront deposits for housing. Scammers frequently ask for non-refundable payment apps like Zelle or Venmo.

Job & Investment Scams: Unsolicited job offers where you are sent a check to buy "equipment" (which bounces later) or high-yield, no-risk cryptocurrency investment schemes designed to drain your digital wallet.

Recovery Scams: Criminals target previous scam victims, promising to help recover lost funds for an upfront fee

How to Protect Yourself

Verify before trusting: Independently contact the organization or person using an official phone number or website rather than clicking links in unsolicited messages.

Do your research: Review guidelines and report suspicious activities directly through the FBI Common Scams and Safety.

Pause and evaluate: Scammers thrive on urgency and fear. If someone is aggressively demanding fast action or specific, untraceable payment methods, stop and think.

AI Safety Basics

- Don’t share private or financial info

- Double-check AI answers

- Use well-known tools

- Ask someone if unsure

Key Risks and Dangers

- **Bias and Discrimination:** AI systems learn from historical data, which can perpetuate or amplify societal biases in critical decisions like hiring or lending.
- **Hallucinations:** AI can confidently generate false or entirely fabricated information, which can cause severe operational issues if not verified by humans.
- **Data Privacy:** Feeding sensitive personal or corporate data into public AI models can result in data leaks and unauthorized access.
- **Misuse:** Generative AI can be used maliciously to automate scams, deepfakes, and targeted disinformation campaigns.
- https://www.youtube.com/watch?v=UiFBU8Aoq3I&t=85s

Staying Safe on Social Media

- Adjust privacy settings
- Only accept friend requests you know
- Be careful sharing personal details
- Report suspicious accounts

What To Do If Something Feels Wrong

- Stop and don’t respond
- Talk to a trusted person
- Contact your bank if needed
- Report scams to authorities

Final Tips

- Take your time online
- When in doubt, don’t click
- Ask for help anytime
- Stay safe and confident