North Dakota Digital Security Guide

Protecting Our Citizens Online

NORTH Dakota | Information Technology
Be Legendary.

As a citizen of North Dakota, your personal information and online activity can be vulnerable to cyber-threats, identity fraud, and digital privacy risks. This guide outlines best practices to help you proactively protect your digital presence, secure sensitive information, and preserve your personal and financial well-being in an increasingly connected world.

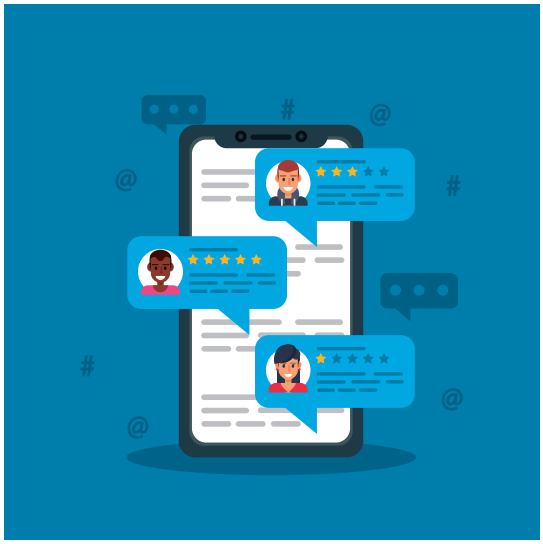
Be Aware of Emerging Threats

Phishing & Social Engineering

- **Always verify a sender's identity** before clicking links or downloading attachments.
- **Be cautious with urgent requests**—scammers often create pressure to act quickly.
- **Never share sensitive info** (passwords and financial details) via email or messaging.
- **Use email filters and report suspicious messages** accordingly.
- **Educate yourself** with simulated phishing exercises and awareness materials.

Online Reputation Manipulation

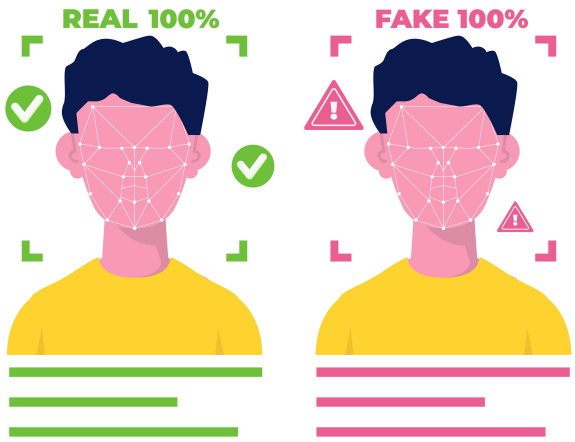
- **Claim and monitor online profiles** across major platforms to prevent impersonation.
- **Use reputation monitoring tools** to track mentions, reviews, and false narratives.
- **Respond calmly and factually** to misinformation—avoid emotional reactions.
- **Report suspicious or false content** accordingly to counteract misinformation.
- **Report fake accounts or harmful content** to platform administrators.



Deepfake Impersonation

What Is a Deepfake? A video, image, or audio created with AI to realistically mimic someone's appearance or voice, often making it seem like they said or did something they didn't.

- **Educate yourself** on the existence and risks of deepfake technology.
- **Verify through multiple channels** if someone contacts you via video or audio with unusual requests.
- **Establish code words or verification questions** for sensitive communications.
- **Be cautious of viral or sensational content**, especially involving public figures or colleagues.
- **Monitor for unauthorized use** of your likeness or voice.



Doxxing

What Is Doxxing? The act of publicly revealing someone's private or identifying information online without their consent, often with malicious intent.

- **Minimize public sharing** of personal and family information (addresses and phone numbers).
- **Use P.O. boxes** or business addresses for registrations and contact info.
- **Enable privacy settings** on social media and opt out of data broker sites.
- **Use a VPN and secure your devices** to reduce data exposure and protect anonymity.
- **Inform local law enforcement** if you believe you're at risk.

Take Protective Measures

Separate Personal & Professional Use

- **Use different email addresses, devices, and accounts** for personal and work activities.
- **Avoid mixing professional and private conversations** on the same platforms or apps.
- **Log into professional platforms (like LinkedIn) using work credentials,** and keep them distinct from personal accounts.
- **Be mindful of sharing personal opinions or photos** on professional profiles that may impact credibility or privacy.
- **Keep data, documents, and access points separate** to reduce risks from breaches or targeting.

Be Cautious With AI

- **Understand what data AI tools collect** and how it may be stored or shared.
- **Avoid inputting sensitive information** (like passwords, personal details, or confidential work content) into public AI platforms.
- **Verify outputs from AI tools—**especially when used for decision-making, research, or writing.
- **Stay updated on AI-generated scams,** like fake customer service bots or phishing emails.
- **Use secure and approved AI solutions** in professional environments.

Practice Caution on Social Media

General Best Practices

- **Turn off location sharing** on all apps and devices unless necessary.
- **Restrict tagging**—enable approval before others can tag you in posts or photos.
- **Don't engage in viral quizzes or games**—they often collect sensitive data.
- **Avoid referencing** vacation plans in public posts.
- **Assume** everything you post can be copied, screenshotted, or misinterpreted.

Special Considerations

- **Use different profile photos** for personal and public-facing accounts.
- **Don't use your full legal name** on personal accounts unless necessary.
- **Avoid posting photos** from your home, neighborhood, or private events.
- **Consider creating a monitored "professional" account** for outreach and limiting personal activity online.

Account Management Tips

- **Delete old or inactive accounts** (e.g., Pinterest, Tumblr or Myspace).
- **Regularly review and update privacy settings**—especially after software or platform updates.
- **Use privacy check-up tools** provided by Facebook, LinkedIn, Instagram, and others.

Post Content With Caution

- **Refrain from commenting** on sensitive work matters from personal accounts.
- **Remember that private accounts can still become public** through screenshots or breaches.

Remove Your Information From Data Brokers

Free Option

Do It Yourself in Four Easy Steps:

1. **Google** your name and state.
2. **Identify people search sites** like Spokeo, Whitepages, MyLife, BeenVerified, etc.
3. **Visit each site's "opt-out"** or "privacy removal" page.
4. **Submit a removal request** (may require verification).

Paid Option

Use a Removal Service:

- **DeleteMe**
- **OneRep**
- **Incogni**
- **Optery**
- **EasyOptOuts**
- **IDX**

Pro Tip: Set a quarterly reminder on your calendar to recheck and resubmit removal requests.

Secure Communication for Work Use

Use Encrypted & Approved Channels

- **Use work-issued systems** (e.g., Outlook, Microsoft Teams, etc.) for official communication.
- **Avoid transmitting confidential information** over SMS or non-encrypted platforms.

Avoid Personal Platforms

- **Never use personal accounts** (e.g., Gmail, iCloud, or Yahoo) for work business.
- **Text messages discussing government matters** may be subject to public records laws.

Messaging Tools

- **Use encrypted apps** such as Signal or WhatsApp.
- **For official communications, avoid using** personal Messenger, Instagram DMs, or TikTok messaging.

Incident Response & Reporting

Immediate Threats or Harassment

Call 911

- If there is imminent physical danger or a threat of violence.

Preserve Evidence

- Such as screenshots, voicemails, messages, etc.

Notify Proper Authorities

- If you suspect you've been compromised.