FS2325 (November 2026)



Staying Safe in a Connected World: A Practical Guide to Recognizing Scams and Digital Threats

Philip Estepp, Gerontology Specialist, NDSU Extension

In today's world, digital technologies have become deeply integrated into our daily routines. Banking, shopping, healthcare, communication, entertainment and home security increasingly rely on internet-connected devices and online services. While these innovations can provide convenience, they also create new opportunities for cybercrime, with fraud and scams among the most common threats facing consumers today.

As technology becomes an increasingly integral part of our lives, it is important to know how to recognize potential threats and make informed decisions before sharing personal information, clicking a link, purchasing something or sending money. This guide will help you become familiar with common digital risks and provide you with a practical system for spotting and reacting to threats.

NDSU | EXTENSION

North Dakota State University, Fargo, North Dakota

Cybercrime

Maybe you or someone you know has fallen victim to cybercrime. If so, you're in good company. In the United States, billions of dollars are lost every year to online scams and fraud. In North Dakota, older adults lost nearly $6 million to internet crime in 2025 (Federal Bureau of Investigation, 2026).

Older adults are a prime target for cybercrime. Their perceived access to retirement savings and other accumulated assets can make them especially attractive to scammers. Although older adults are not always more likely than younger adults to report losing money to fraud, they often lose substantially more money when fraud occurs. Adults age 60 and older are also disproportionately affected by certain schemes, including technology-support scams, investment fraud, romance scams, and government or business impersonation. Nationally, adults aged 60 and older reported more than $7.7 billion in internet-crime losses to the FBI (Federal Bureau of Investigation, 2026; Federal Trade Commission, 2025).

For decades, the old adage, "If it sounds too good to be true, it probably is," served as a useful rule of thumb for recognizing scams. In today's digital world, however, *that advice is no longer sufficient.* **Many cybercriminals succeed because they appear ordinary.** They imitate trusted organizations, exploit urgency and emotion, and use increasingly sophisticated technology to make fraudulent communications appear authentic. As a result, recognizing digital threats requires more than intuition; it requires a systematic way of evaluating whether a message, request or opportunity is legitimate. One way to recognize suspicious activity is by spotting red flags.

Red flags are warning signs that something is wrong or deserves closer attention. They are not always obvious. However, with awareness and practice, you can learn to recognize these warning signs and better protect yourself, your personal information and your finances.

Common Red Flags

Unexpected Contact

- You receive an unsolicited phone call, text message, email, pop-up window or social media message claiming immediate action is needed or seeking a response.
- Legitimate organizations rarely initiate contact this way to request sensitive information or payments.

Pressure to Act Immediately

- You're told to act now or face serious consequences, that you'll miss an opportunity or that your help is urgently needed.
- Creating urgency is one of the most common tactics scammers use to prevent people from stopping to verify the request. The intent is "don't think, just act."

Requests for Personal Information or Unusual Payment Methods

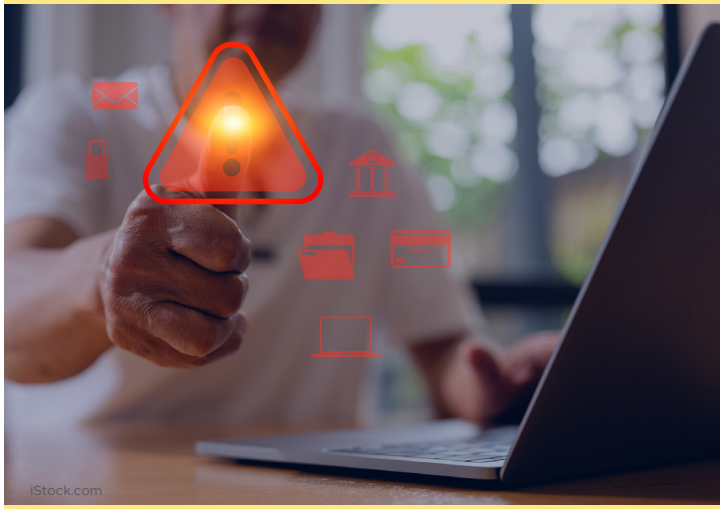
- Someone asks for passwords, verification codes, Social Security numbers, banking information or payment by gift cards, wire transfer, cryptocurrency, cash or payment apps.
- Government agencies, banks and reputable businesses generally will not ask you to provide passwords, verification codes or other sensitive personal information through an unexpected call, text or email, nor will they demand unusual forms of payment to resolve a problem.

Unverified Identity

- Professional-looking emails, websites, caller IDs, text messages and social media accounts can all be faked or imitated.
- Never assume a communication is authentic based on its appearance alone. Independently verify the sender by contacting the organization using a phone number or website you know is legitimate.

Requests for Secrecy

- You are asked to keep the situation confidential or not discuss it with family members, friends, your bank, financial advisor or law enforcement. You may also be encouraged to remain on the phone or continue communicating while carrying out the requested actions, limiting your opportunity to pause, think or seek advice from someone you trust. Sometimes intimidation and threats are used.
- Legitimate organizations will not insist that you keep financial, legal or account-related matters secret from trusted people. If someone insists on secrecy or discourages you from seeking advice, treat it as a significant warning sign and verify the situation independently before taking action.



A single red flag should prompt caution, but multiple red flags strongly suggest that a message, request or communication is not legitimate. When one or several red flags are present, the safest response is to ignore the message, delete it or block the sender. Do not engage by replying, asking the sender to stop contacting you or attempting to verify their claims through the same message, chat or phone call. Instead, if the communication appears to come from a legitimate organization, contact that organization directly using their publicly listed phone number or website.

If you are still unsure whether a communication is legitimate, ask for a second opinion. Asking a knowledgeable friend, family member or professional can be very helpful in spotting red flags and allowing you time to pause and think about the risk. Try asking, "Does this look real?" or "Does this sound like it could be a scam?" In many instances, it is best to ignore unsolicited emails, texts, chats or other communications.

In the past, being "online" generally meant using a personal computer to connect to the internet. Today, the term is much broader. Being online can include using a smartphone, sending or receiving text messages, checking email, using apps or social media and interacting with smart devices such as watches, TVs, speakers, video doorbells and other internet-connected technology. Many households are constantly sending and receiving digital information. Being "online" is now a routine part of everyday life.

Read the following scenario and see if you can identify the red flags. How many warning signs can you recognize?

You receive a text message on your smartphone that appears to be from your bank stating that suspicious activity has been detected on your checking account. Concerned, you call the phone number provided in the message.

The person who answers identifies themselves as a member of the bank's fraud department. They sound professional, know your name and may even verify your address. They explain that someone is attempting to access your account. They tell you that protecting your money requires immediate action because a fraudulent transaction is in progress.

The representative instructs you to not discuss the situation with anyone until the investigation is complete, explaining that doing so could interfere with the case. They remain on the phone while walking you through several steps to "secure" your account, including providing online banking information and transferring your money to a "safe account" until the investigation is finished. You are frequently asked to remain on the line.

The caller seems knowledgeable, the phone number matches your bank's name on caller ID and the situation feels urgent. You recognize several red flags. Before taking any action, you pause and verify the situation by immediately hanging up and calling the customer service number listed on the back of your debit card. The bank confirms that no fraud investigator had contacted you and that the text message and phone call were part of a known scam.



Can You Spot the Red Flags?

1. **Unexpected Contact:** What was the first sign that this communication should have been viewed with caution? (The text message was unsolicited and unexpected.)
2. **Pressure to Act Immediately:** What did the caller say or do to create a sense of urgency? (The caller stated immediate action was needed to prevent a fraudulent transaction.)
3. **Requests for Personal Information or Unusual Payments:** What information or actions did the caller request that should have raised concern? (The caller requested sensitive banking information.)
4. **Unverified Identity:** What made it impossible to know with certainty that the caller was who they claimed to be? (Caller ID, text messages, social media profiles, emails and other forms of contact can appear perfectly legitimate.)
5. **Requests for Secrecy:** How did the caller try to prevent you from pausing, seeking advice or verifying the situation? (The caller requested you to stay on the line and portrayed the situation as time sensitive and urgent.)

Cybercrime is constantly evolving as criminals adopt new technologies and exploit emerging vulnerabilities. By the time communities become aware of an ongoing scam, a new one is already being used. In today's connected world, threats can arrive through a phone call, text message, email, social media, online chat or countless other digital interactions. Recognizing the red flags can help you pause, verify the situation and make informed decisions before sharing personal information, sending money or taking other actions. To learn more and stay informed on current scams, see the recommended resources below.



Recommended Resources

North Dakota Attorney General. The website of the North Dakota attorney general provides up-to-date, reliable information regarding common scams impacting North Dakota residents.
https://attorneygeneral.nd.gov/consumer-resources/common-scams/

Federal Bureau of Investigation, Internet Crime Complaint Center (IC3). The IC3 website allows people to report suspected cybercrime, fraud and scams. It also provides public alerts and annual reports about current cybercrime trends.
www.ic3.gov

Cybersecurity and Infrastructure Security Agency, Secure Our World. This website provides practical guidance for recognizing phishing, using strong passwords, enabling multifactor authentication and keeping software updated.
www.cisa.gov/secure-our-world

AARP, Scams & Fraud. AARP provides numerous articles and information on scams and fraud. Information on various types of scams, how to spot them and support resources for victims are available.
www.aarp.org/money/scams-fraud/

North Dakota Senior Medicare Patrol (ND SMP). The North Dakota Senior Medicare Patrol empowers and assists Medicare beneficiaries and their families and caregivers to prevent, detect and report health care fraud, errors and abuse.
https://ndcpd.org/smp/

References

Cybersecurity and Infrastructure Security Agency. (n.d.). Secure our world. U.S. Department of Homeland Security. https://www.cisa.gov/secure-our-world

Federal Bureau of Investigation. (2026). 2025 IC3 annual report. Internet Crime Complaint Center. https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

Federal Trade Commission. (n.d.). How to avoid a scam. Consumer Advice. https://consumer.ftc.gov/articles/how-avoid-scam

Federal Trade Commission. (2025a). Protecting older consumers 2024–2025: A report of the Federal Trade Commission. https://www.ftc.gov/reports/protecting-older-consumers-2024-2025-report-federal-trade-commission

Federal Trade Commission. (2025b, March 13). What are the signs of a scam? Consumer Advice. https://consumer.ftc.gov/consumer-alerts/2025/03/what-are-signs-scam

North Dakota Office of Attorney General. (n.d.). Common scams. https://attorneygeneral.nd.gov/consumer-resources/common-scams/

NDSU Extension does not endorse commercial products or companies even though reference may be made to tradenames, trademarks or service names.

For more information on this and other topics, see www.ndsu.edu/extension

North Dakota State University is an equal opportunity educator and employer. NDSU Extension and the Agricultural Experiment Station's work is supported by the U.S. Department of Agriculture's National Institute of Food and Agriculture. USDA programs are prohibited from discriminating based on race, color, national origin, religion, sex, disability, age, marital status, family/parental status, income derived from a public assistance program, political beliefs, or reprisal or retaliation for prior civil rights activity. NDSU Extension and the NDAES are committed to providing equal access. Persons with disabilities who require alternative means of communication for program information (e.g., Braille, large print, audiotape, American Sign Language) or other disability-related accommodations may request them at 701-231-1865. Advanced notice of two weeks is preferred to allow for adequate planning.

web-11-26