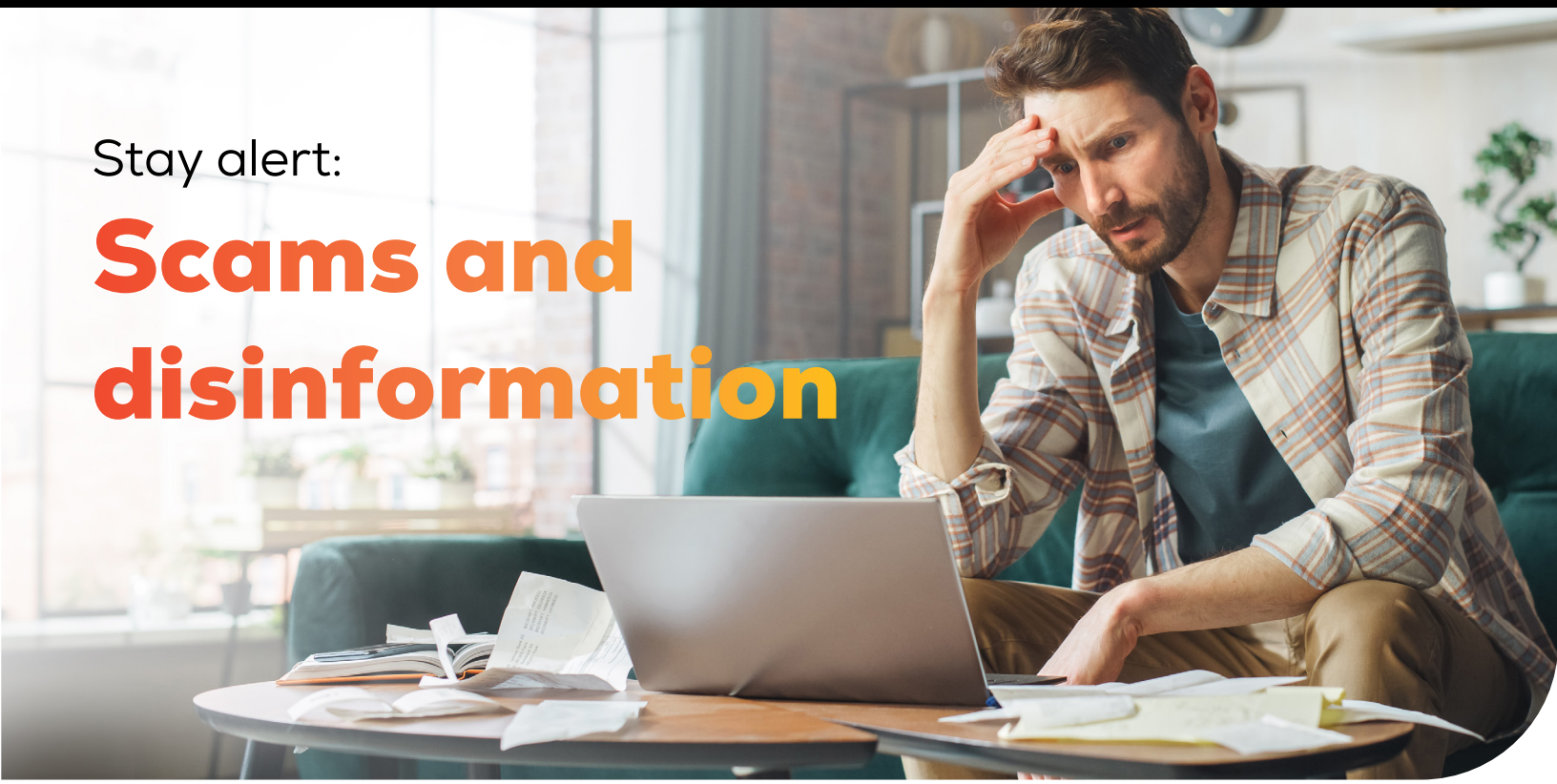


Stay alert:

Scams and disinformation

Learn to spot the signs of online fraud

The internet has made positive contributions to society, but it has also made it much easier for cybercriminals, scam artists and others with malicious intent to find their next victims. The good news is that, once you know what to look for, you'll be able to spot most suspicious activities right away. Scammers are constantly refining their schemes, so even seasoned internet users need to keep up to date and not let their guard down.

This guide will help you identify common scams, offer advice for protecting your personal information, teach you how to spot fake news and explain how you can secure your personal devices and networks. But in the end, the best way to protect yourself from scams is to rely on good, old-fashioned common sense.

Cybercrime cost Americans **$12.5 billion** in 2023, according to the Federal Bureau of Investigation.

Be aware of the most common scams

Scammers use various tactics to trick individuals into giving away money, personal information or access to their devices. Knowing how to recognize these scams is the first step in protecting yourself from online fraud.

Phishing scams

Phishing involves scammers pretending to be legitimate institutions (like banks or government agencies) to steal personal and sensitive information like social security numbers, passwords and account numbers. These scams typically occur via email but can also happen through text messages or social media.

WARNING SIGNS:

- Urgent language requesting immediate action
- Requests for personal information such as passwords or bank details
- Links to websites that look legitimate but have slightly altered URLs

RED FLAG WORDS:

- "Verify your account"
- "Urgent action required"
- "Confirm your password"

Advance-fee scams

These scams try to convince you to pay upfront fees for services or products that never materialize. Common examples include job offers requiring payment for training or equipment or claims that you've won a prize but must pay taxes to claim it.

WARNING SIGNS:

- Requests for money to cover expenses before receiving a product, service or prize
- Promises of high returns for a small upfront investment
- Scenarios that seem too good or strange to be true

RED FLAG WORDS:

- "Transfer fee"
- "Inheritance tax"
- "Processing charge"

Almost **1 in 3 Americans** reported being a victim of a cybercrime.[1]

BE AWARE OF THE MOST COMMON SCAMS:

Lottery or sweepstakes scam

Like an advance-fee scam, scammers notify victims that they've won a large sum of money in a lottery or sweepstakes but must pay a fee to unlock the prize.

WARNING SIGNS:

- Notifications for lotteries or contests you did not enter
- Requirements to pay a fee or provide bank account details to claim a prize
- Official-sounding language paired with poor grammar or spelling

RED FLAG WORDS:

- "You won"
- "Claim your winnings"
- "Congratulations winner"

Tech support scams

Perpetrators claim to offer tech support while actually intending to install malware or steal personal information.

WARNING SIGNS:

- Unsolicited calls or pop-ups claiming your computer has a virus
- Requests for remote access to your computer
- Pressure to act quickly by paying for support or downloading software

RED FLAG WORDS:

- "Virus detected"
- "System alert"
- "Immediate support needed"

Romance scams/catfishing

Scammers create fake profiles on dating websites or social media to form relationships and eventually persuade their targets to send money.

WARNING SIGNS:

- Requests to move conversations off dating platforms to private messaging
- Inconsistent personal details
- Declarations of love or affection very quickly
- Requests for money citing emergencies, travel costs or medical expenses

RED FLAG WORDS:

"Financial assistance", "Don't tell anyone", "Trust me"

REMEMBER THE 4 L's:

To protect yourself from scammers

These four common-sense rules go a long way to keep your info safe online.

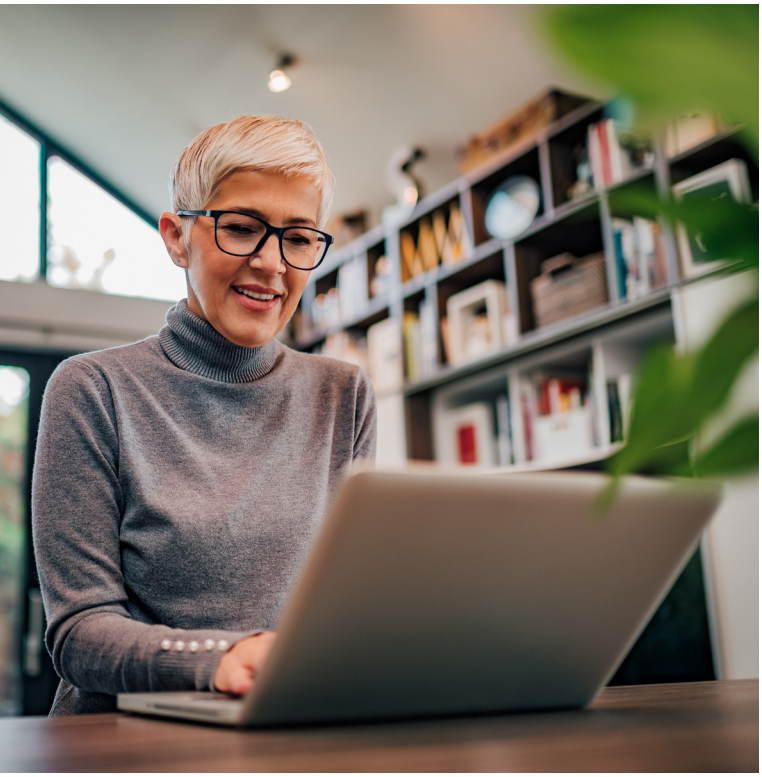
1. **Limit** what you share.
   Never share account numbers passwords or social security numbers.

2. **Look** closely at the URL.
   Is the address spelled correctly? Does the web address start with "https://" which shows messages are encrypted using SSL (Secure Sockets Layer) for your protection?

3. **Layer** your security.
   Using VPNs and two-factor authentication makes it difficult to steal your private info.

4. **Listen** to your gut.
   If a stranger's offer seems too good to be true, it probably is. Proceed with caution.

If you're ever in doubt, stop and assess the situation. Online criminals create a false sense of urgency to catch you off guard and get you to act quickly.



The importance of security software and firewalls

No matter how vigilant you are about fraudulent sites, sometimes you slip up. You click on a scammer's link or mistype a URL, only to fall victim to a phony site. You should install anti-virus and anti-malware software on your computer and online devices. This software acts as a filter. It helps the bad guys from getting in, but it also alerts you when you travel into dangerous territory.

Other best practices to avoid scammers

- Strong passwords and VPN software.
- Enable two-factor authentication.
- Limit access to your home router.

Not all information you find online is reliable

Disinformation. Propaganda. Innuendo. Lies. Hoaxes. Fake news. Whatever it's called, using false information to manipulate and shape public opinion isn't new. The digital age, however, has made it easy and inexpensive to create and spread it — while making it harder to spot. In fact, artificial intelligence (AI) can create "deep fakes" — computer-generated representations of world leaders, celebrities, events and data — in seconds.

It's not an easy problem to solve. But there are three steps you can use to judge information you find online.

> "Don't believe everything you read on the internet."
>
> —Abraham Lincoln*

3 ways to be a smarter information consumer

1. **Check the source:** Assess the credibility of the source providing the information. Look for established news organizations known for their adherence to journalistic standards. Be wary of unknown websites or platforms that may not have editorial oversight or fact-checking processes.

2. **Verify with multiple sources:** Cross-reference the news with multiple trusted sources before accepting it as true. Fake news often exists in a vacuum, while multiple reputable media outlets usually report credible stories.

3. **Analyze the evidence:** Look for evidence that supports the claims made in the story. Good journalism includes quotes from experts, data and other verifiable facts. Beware of articles that lack evidence or rely heavily on unnamed sources or vague attributions like "experts say" or "some people claim."

PRO TIP:

Check before you forward.

Fake news is often sensationalistic, designed to latch onto your curiosity and relies on your impulse reaction to share novel, unexpected or bias-reinforcing information. Do your part to avoid spreading misinformation by doing a quick fact-check before passing it along.

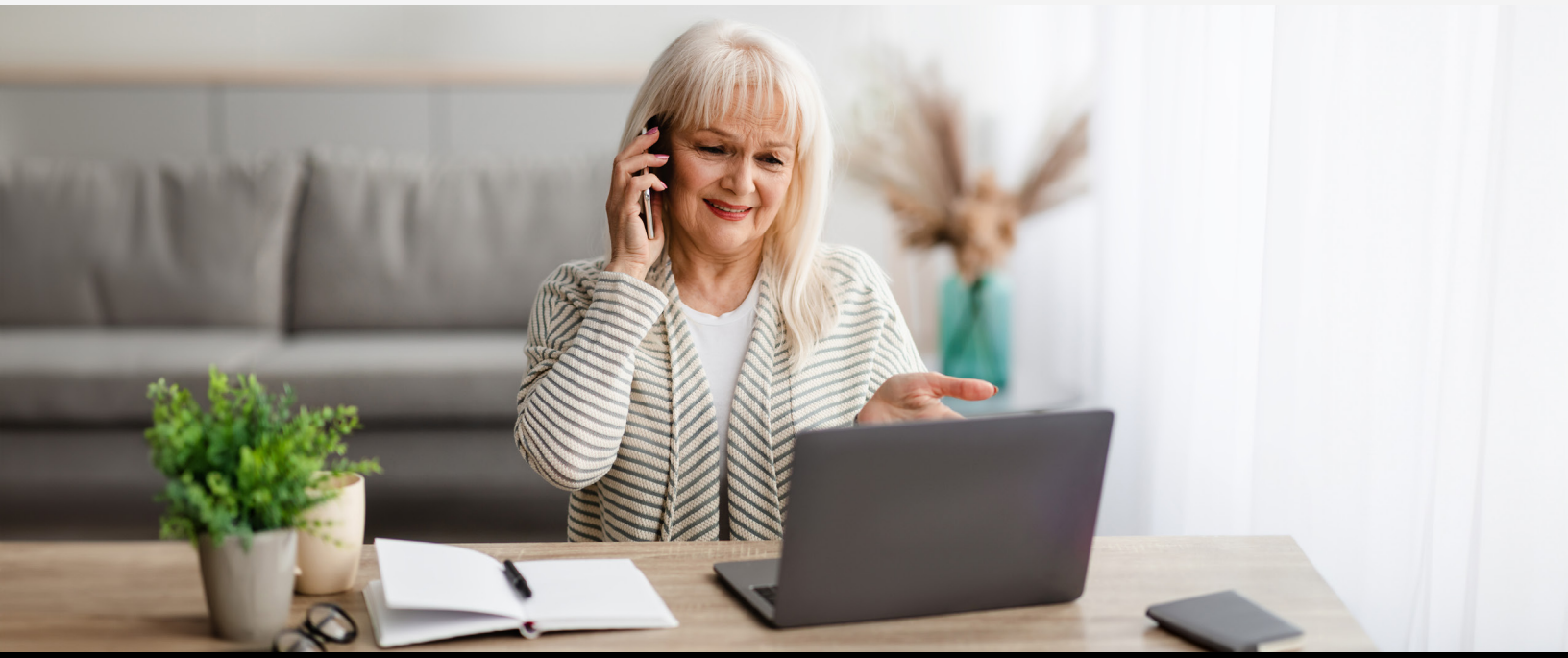
**Of course, Abraham Lincoln never said this. He died more than a century before the internet was invented.*

TRUST YOURSELF:

Avoiding scams and misinformation comes down to critical thinking

- **Listen to your gut:** If something feels wrong or too good to be true, it probably is.
- **Err on the side of caution:** The best response to sketchy messages is often no response.
- **Ask questions:** Never hesitate to ask for more details if something seems unclear.
- **Check facts:** Always double-check information through reliable sources or authoritative websites.
- **Consult trusted people:** Discuss it with friends or family members — two heads (or more) are often better than one.
- **Beware of pressure:** Watch out for anyone rushing you to make a decision or from getting a second opinion. Genuine opportunities don't need an immediate answer.

By staying inquisitive, cautious and connected with your trusted circle, you're better equipped to dodge scams!



About Brightspeed

Launched in 2022, Brightspeed is building a future where more communities can benefit from a more connected life. We believe where you choose to call home shouldn't limit your options — and we're building the infrastructure to provide millions of homes with fast, reliable internet. So wherever you're streaming, gaming or working, you'll enjoy an uninterrupted experience. **Learn more at www.brightspeed.com**.

In collaboration with ciena