Safe or Scam:
Tackling disinformation in the digital age.

In today's digital era, the internet provides unlimited opportunities for learning, communication, and convenience. But it also presents significant challenges, especially where forms of online scams and disinformation are concerned.

This guide is designed to help you identify these risks and arm you with strategies to protect yourself and your personal information. Because scammers are constantly searching for new and different ways to carry out their schemes, it's important to stay vigilant and watchful for possible "bad actors". And as always, using common sense in all situations will be your first and best defense against those who have bad intentions are concerned.

Stay Alert: Understanding Scams and Disinformation

Recognizing signs of online fraud and misinformation is crucial. As the internet evolves, so do the tactics of those looking to exploit it. Understanding the basics of common scams and the nature of disinformation will prepare you to navigate online interactions safely.

The number of pages with Phishing related scams on the internet **rose nearly 28%** from 2022 to 2023.[1]

Global ecommerce (online shopping) fraud is at an all-time high, with losses reaching **$41 million in 2022**, predicted to increase to **$48 billion in 2023**.[2]

Romance scams resulted in **$3.8 billion** in losses globally in 2023.[3]

Common Online Scams

1 **Phishing:**

This scam involves fraudsters impersonating credible organizations to steal sensitive data like passwords and credit card numbers. Phishing attempts often come via email, featuring links to fake websites that look remarkably real. These scammers may pose as your bank, school or credit card company and play upon fear, uncertainty and doubt as they attempt to get you to share personal information.

2 **Advance-Fee Scams:**

Victims are persuaded to pay upfront fees for services or goods that never materialize. Examples include job application fees or charges for claiming a fake prize. If the offer or situation seems too good to be true, it probably is. Recognize that legitimate awards or products typically do not require up-front money to claim or gain access.

3 **Tech Support Scams:**

Scammers claim your computer has serious issues, a virus or needs an update. In reality, they're attempting to gain remote access or sell you unnecessary software. Never allow remote access or download software from an unknown source.

4 **Romance Scams:**

Perpetrators create fake profiles on dating platforms to form relationships and ultimately con people into sending money. These are often lengthy schemes where the scammers slowly cultivate an online relationship and gain the trust of the victim. Beware of a request to chat via private message (and thus move off the dating platform) or a resistance to meet in person. Requests that involve money for emergencies, travel or purchasing real estate together should be red flags.

5 **Holiday-related Scams:**

In a season where spending and shopping are at an all-time high, it's no surprise that scammers try to target unsuspecting consumers. From fake gift cards to shipping notifications, it's important to stay vigilant during busy and chaotic times.
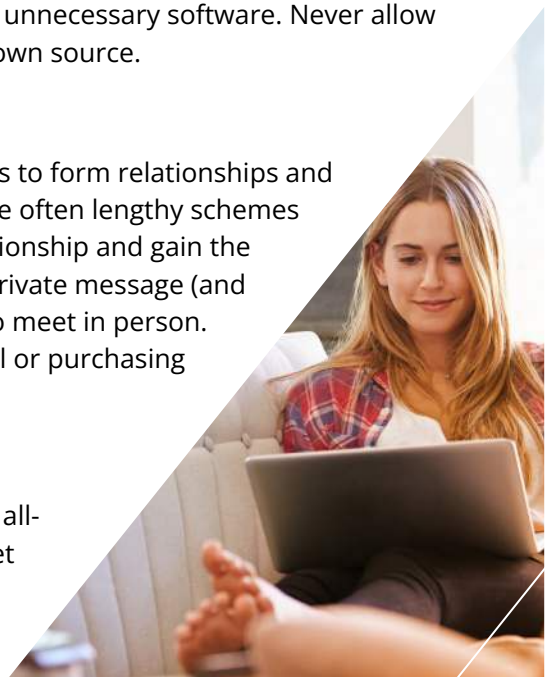
Recognizing Red Flags:

⚠ Immediate requests for money or confidential information.

⚠ Prizes that require payment to claim.

⚠ Offers that guarantee extraordinary returns.

⚠ High-pressure tactics urging quick decisions.

Protecting Yourself

Limit Personal Information

Safeguard your personal details. Avoid sharing sensitive information online unless absolutely necessary. Never share passwords or account numbers via email, and do not provide your social security number to anyone online.
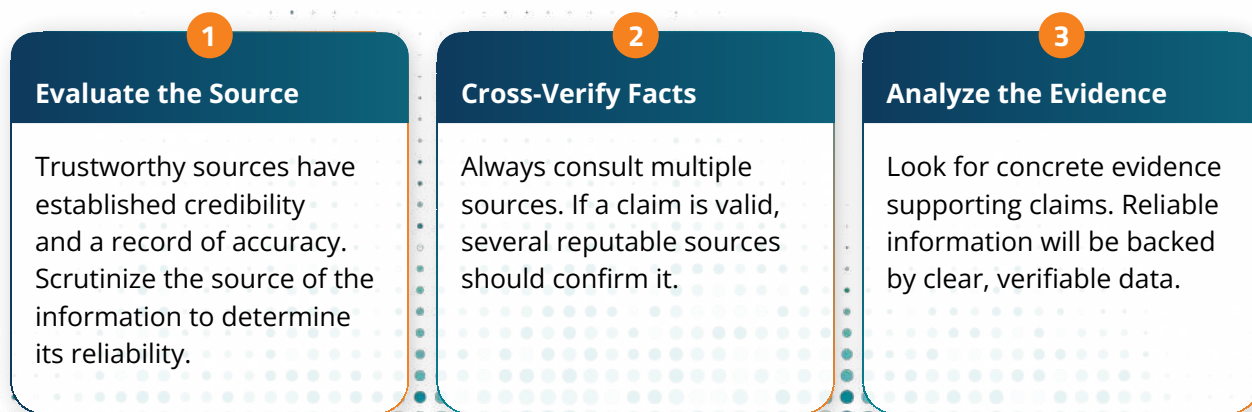
Verify Websites

Ensure websites are legitimate by checking for "https://" in the URL, signifying secure data encryption. When in doubt, research the company's URL, retyping it into a search bar and comparing the two resulting pages. If you see discrepancies, be wary of an imposter website situation.

Implement Security Tools

Use virtual private networks (VPNs) and two-factor authentication for an added layer of security. These tools are available on many sites and can actively protect you and your information.

Dealing with Disinformation

Misinformation thrives in the digital world. Learning to distinguish between reliable and unreliable information is essential.

1

Evaluate the Source

Trustworthy sources have established credibility and a record of accuracy. Scrutinize the source of the information to determine its reliability.

2

Cross-Verify Facts

Always consult multiple sources. If a claim is valid, several reputable sources should confirm it.

3

Analyze the Evidence

Look for concrete evidence supporting claims. Reliable information will be backed by clear, verifiable data.

Security Software and Firewalls

Investing in quality security software is crucial. Antivirus programs and firewalls act as first lines of defense by blocking malware and other threats. Ensure these programs are always up to date to defend against the latest threats. If you're not comfortable installing these yourself, seek out a trusted IT consultant in your area to help. It's a small fee to pay for peace of mind.

Navigating Fake News

In an era where information spreads faster than ever, discerning fact from fiction is crucial. Fake news is not just misleading; it can also be dangerous, influencing opinions and spreading disinformation. Here's how you can more effectively navigate this challenging landscape:

1   Critical Evaluation

- **Source Reputation:** Start by looking at the reputation and purpose of the source. Established news outlets with a longstanding history of credibility are more reliable. Be cautious of new websites or those known for sensationalism.

- **Author Expertise:** Check who wrote the article. Credible information often comes from authors with relevant expertise and a transparent professional background.

2   Verification Process

- **Fact-checking Tools:** Utilize fact-checking websites like Snopes, FactCheck.org, or the BBC's Reality Check to verify claims. These sites investigate stories and claims to ascertain their truthfulness.

- **Cross-reference Sources:** Don't rely on a single source. Look for the same news reported across multiple reputable platforms to confirm its accuracy.

3   Analytical Thinking

- **Question Motives:** Consider why the information was published. Does the article have a political bias? Is it trying to sell something or sway public opinion?

- **Check the Date and Context:** Sometimes, old news stories are shared as current events, which can be misleading. Ensure the story is relevant and current in its context.

4   Visual Literacy

- **Image Verification:** Images can be doctored to mislead. Use tools like Google Reverse Image Search to find the original context of an image.

- **Video Authenticity:** Similarly, videos can be edited to distort reality. Look for unedited footage or multiple angles to ensure you're getting the full story.

Trusting Your Instincts

Trusting your instincts is about recognizing and reacting to something that feels off. It's a vital skill in navigating not only the internet but also daily life decisions:
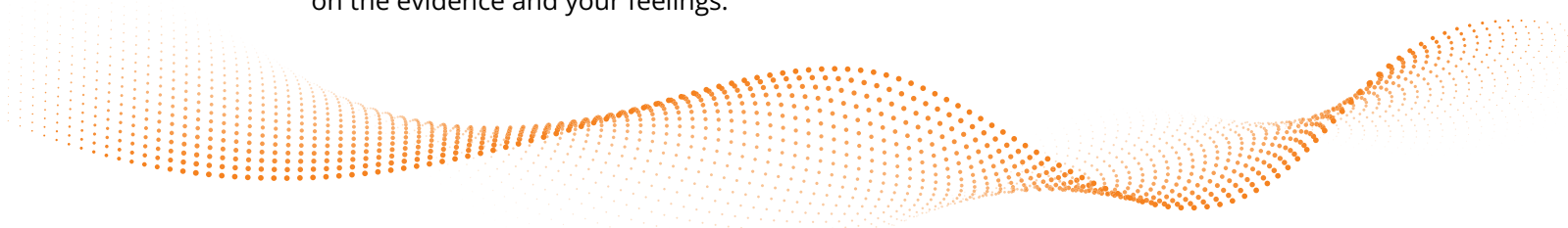
1 Gut Feelings

- **Initial Reactions:** Often, your first reaction is a powerful indicator of whether something is trustworthy. If you feel uneasy about a website, an email, or an online request, take a moment to investigate further before proceeding.

- **Comfort Level:** If you're uncomfortable sharing information or proceeding with a transaction, it might be worth reconsidering. Trusting your comfort level is essential in protecting your personal information and well-being.

2 Learn from Experience

- **Past Mistakes:** Reflect on past experiences where something felt wrong, and you went ahead anyway. What were the outcomes? Learning from these can sharpen your instinctual responses.

- **Familiar Patterns:** Scammers often use similar tactics. Recognize these patterns and trust your experience to guide your actions. Pay attention to scam alerts and anecdotal stories in the media and elsewhere to learn what scammers are trying today.

3 Balancing Skepticism and Trust

- **Healthy Skepticism:** It's beneficial to question things and seek validation. However, balance skepticism with trust by using the verification steps outlined above.

- **Confidence in Decision-Making:** As you gather more information and experience, you'll develop a more refined instinct. Trust in your ability to make informed decisions based on the evidence and your feelings.

About Zayo:

Since 2007, Zayo has focused on creating connections. By building an expansive network, Zayo has become the leading independent provider of light-speed data transmission infrastructure, with dense, high-quality networks connecting every major market in North America. Zayo was built to serve the largest and most innovative companies in the world, providing both major enterprises and individual internet users access to all the benefits the world wide web has to offer.

Together with

ciena