FS-ISAC | Security Tips Newsletter

5 December 2025 | Issue No. 27

Be cyber smart to stay cyber safe.

When It's Too Good To Be True

Summary

If it sounds too good to be true, it probably is. This phrase serves as a reminder to be vigilant, especially when considering financial offers or information that appears to lack verifiable proof. It's a call to investigate thoroughly before believing or acting on the offer.

Too Good To Be True

One of the tools scammers are increasingly using is Artificial Intelligence (AI). AI is being used to create better phishing emails, deepfake, and other impersonation scams. This means consumers need to be additionally cautious when it comes to a gamut of different ploys.

If you are an online shopper, here is a list of common scams that are too good to be true:

Online Dating Scams. If you are a senior citizen, is it realistic for a young man or woman in their early twenties who looks like a high-end model to want to come to the US to be with you, and all you need to do is wire transfer a large sum of money to them?

Going out of Business Scams. Who doesn't like a good deal on a high-priced item? But those unsolicited emails touting big-discount deals for a limited time may lead to the only thing going out is your money to a scammer.

Investment Scams. Investment opportunities promoted on professional-looking social media and internet websites, promising quick and guaranteed returns, are a fast way to be taken advantage of. Regardless of a "limited time" crypto project, private fund, or pre-IPO stock offering, set emotions aside and perform your due diligence.

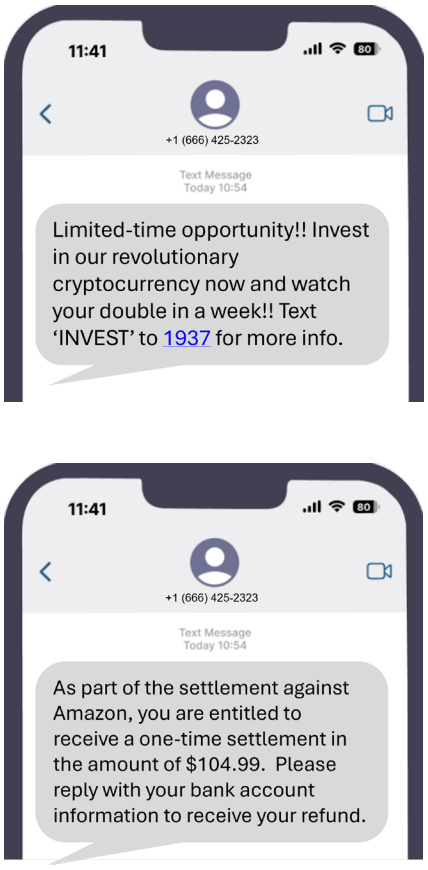

Figure 1. Examples of SMS text scams

Text Message Deals. The hair on the back of your neck should rise when unsolicited text messages reach your phone, offering super deals on high-end electronics, and so on.

Travel Scams. Looking forward to a getaway during the holiday season? That too-good-to-be-true airfare or cruise trip could wind up giving you the worst holiday experience of all time.

Health Scams. As healthcare costs rise, so do the odds of a scammer's success, especially for those with limited financial resources.

Red Flags

New and recycled red flags can change rapidly. We have listed some that stand out frequently:

- The offer cannot be traced back to a legitimate source or does not provide contact information other than an email address.
- The firm's domain has misspelled words or an unfamiliar domain, such as .ru, .tk, or .buzz.
- Guaranteed return on your investment with little to no risk.
- Contacted by an unlicensed investment professional
- Sensational or over-the-top pitches that may have fake testimonials
- Pressure to ‘act now’ or you will miss out on the opportunity.
- Request to pay through cryptocurrency or wire transfers to an unverifiable source.
- The requester requests bank account information that a legitimate source would already possess.
- Payment is required up front, and there are no refunds or returns.
- Untraceable or irreversible payment options only are accepted.
- Received an unexpected email or text message offering great deals from a merchant you have no affiliation with.
- The web domain is not that of the store or firm.
- All feedback about the organization is recent and provides five-star positive feedback.
- The offer is listed as free for popular items.

Prevention Tips

- Stop. Think. Verify before you click - Use reliable resources to research offers to minimize your risk
- Never click on links from people or firms you do not know, or open files attached to emails.
- Always use a secure connection (https:// and padlock icon) when sharing personal or banking information.
- Never provide your confidential information to businesses that already have that information.
- Always use multi-factor authentication combined with hard-to-guess passphrases.
- Stay up to date with all mobile device and tablet patches, as well as personal computer patches.
- Invest in security solutions to block and protect your mobile devices from phishing and SMS text scams.

Resources

- Learn more about AI scams
- Get Safe Online website checker
- Conduct a background check on any investment professional at Investor.gov.

If You're a Victim?

Immediately change any passwords you might have revealed. Consider reporting the attack to IC3.gov, law enforcement, and file a report with the Federal Trade Commission.

Getting Help

If you have been the victim of a data breach or loss of your personally identifiable information, or identify suspicious activity involving your financial institution, contact them immediately.

12120 Sunset Hills Rd, Reston
VA 20190