The Monthly Security Awareness Newsletter for You

Top Three Social Media Scams

Overview

While social media is a fantastic way to communicate, share, and have fun with others, it is also a low-cost way for cyber criminals to trick and take advantage of millions of people. Don't fall victim to the three most common scams on social media.

Investment Scams

Have you ever seen a post about an investment opportunity that promises a huge return on investment in an extremely quick amount of time with allegedly little to no risk? The reality is, these guarantees are really investment scams. Fraudsters simply steal your money after you pay them. These scams often include ads or success stories from past customers to promote the investments, but those are just fake testimonials to increase your trust. Often these investment scams are about investing in crypto-currencies or real estate, and payment is often made in crypto-currencies or other non-standard payment methods. If an investment seems too good to be true, it most likely is. Remember, there is no such thing as guaranteed, high-return investments. Only invest your money in trusted, well-known resources, not strangers you meet online pushing a get-rich-quick scheme.

Romance Scams

When criminals develop an online relationship with someone they've identified as lonely or vulnerable to trick them out of money, this is known as a romance scam. The criminal will use whatever tactics they can to build trust, including exchanging fake photos or sending gifts, then share a tragic story about needing money to pay for expenses such as hospital bills or for travel costs to visit the victim in person. To avoid actually meeting in person, these criminals may say they work in an industry that prevents them from doing so, such as construction, international medicine, or the military. They often request money as a wire transfer or gift cards to get cash quickly and remain anonymous. These types of scams are not only common on social media but with online dating apps. Be careful with people you meet online, take things slowly, and never send money to someone you have only communicated with online.

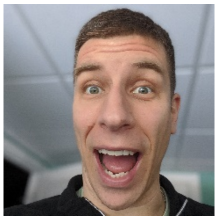
Additionally, if you believe someone you know may be vulnerable to such an attack or is in an online relationship that raises these flags, offer to help them. Sometimes it can be very difficult for someone engrossed in an emotional connection to see just how dangerous the situation has become.

Online Shopping Scams

Online shopping scams happen when you purchase items online at extremely low or unbelievable prices but never receive them. Tempting ads on social media will promote incredible prices and have links that take you to sites that appear to be legitimate and sell well-known brands, but these sites are often fake. Be wary of websites that have no contact information, broken contact forms, or use personal email addresses. Type the name of the online store or its web address into a search engine to see what others have said about it. Look for terms like "fraud," "scam," "never again," and "fake." Be very cautious of online promotions or deals that appear too good to be true. It's far safer to purchase items that may cost slightly more, but from trusted sites that you or your friends have used before.

The good news is: You are your own best defense. You are in control. Just be on alert for scams like these and you will be able to make the most of social media safely and securely.

Guest Editor



Chris Elgee (@chriselgee) is a penetration tester and challenge designer for @CounterHackSec, cyber battalion commander in the Army National Guard, and Certified SANS Instructor. He enjoys learning about the gritty technical details, building it into a larger, organizational understanding, and sharing with students and clients.

Resources

Better Business Bureau Scam Tracker: https://www.bbb.org/ScamTracker
Social Engineering: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Shopping Online Securely: https://www.sans.org/newsletters/ouch/shopping-online-securely-nov-21/
Phone Call Attacks and Scams: https://www.sans.org/newsletters/ouch/vishing/

Translated for the Community by: