# Advisory

## What Is Spoofing?

**Spoofing is when someone disguises an email address, sender name, phone number, text, or website URL—often just by changing one letter, symbol, or number—to convince you that you are interacting with a trusted source.**

***"Criminals count on being able to manipulate you into believing that these spoofed communications are real, which can lead you to download malicious software, send money,or disclose personal, financial, or other sensitive information."*** **- FBI.gov**

**Take time to carefully view a website before engaging in any search or transaction to make sure it is legitimate. A lot of sites, including retailer sites, look real but are actually fake. A fake site's domain name may have an extraneous letter or number, and the site may have grammatical errors or limited contact information. For example, a fake website can contain the number zero (0) instead of the letter (O), such as www-amaz0n.com. The number one (1) looks very similar to a lower case (L - l).**

**In addition, make sure the web address starts with https :// (not http ://). The letter (s) is important and means the site is a "valid domain site." The web address should also display a green or gray padlock in a closed position. Both indicate, a secure site.**

**Whenever you receive an email, especially an unsolicited email, position and hover over the email address with your cursor. A pop-up will appear and show you the actual address of the sender. If they do not match or the pop-up contains a strange address or a series of symbols/numbers/ letters, do not click on any link, do not respond and delete the email. Never click on the "unsubscribe" link unless you absolutely know the email is legitimate—the link may infect your phone or computer with a virus and the scammer will now know your email address belongs to a real person.**

**Contact Consumer Fraud Protection**
**18th Judicial District**
**Hotline (720) 874-8547 | consumer@da18.state.co.us**