# Messaging Do’s and Don’ts

## Overview

Messaging serves as a primary mode of communication in both our personal and professional lives. However, quite often we can be our own worst enemy when it comes to text messaging safely and securely. Learn the most common mistakes people make and how you can avoid them in your day-to-day lives.

## Auto-Complete

Auto-complete is a common feature in many messaging apps. As you type the name of the person you want to message, your app may automatically select the person for you. This feature can lead to mistakes, especially when multiple contacts share similar names. For example, you may intend to send a sensitive text to a co-worker but instead accidentally message your daughter’s coach who happens to share a very similar name. Always double-check the full name of the person you intend to message before you hit send.

## Replying to Group Messages

Group chats are another common feature, but make sure you are aware of all group members who are on the thread before responding. When you are replying to an entire group, you want to be sure your reply is appropriate for everyone in that group. Another common mistake is accidentally replying to the entire group instead of a specific person. Take your time in responding: Double-check before hitting the send button.

## Emotion

Avoid sending messages when angry, upset, or emotionally charged. That message could cause you far more harm in the future, perhaps even costing you a friendship or a job. Instead, take a moment to calmly organize your thoughts. If you *must* vent your frustration, open a new message with no recipient selected, type out exactly what you are feeling, then walk away from your device. Perhaps make yourself a cup of tea or go for a walk. When you return, delete the message, and start over again. You will most likely be in a far calmer and clearer state of mind. Consider direct communication via phone or in-person for a more effective conversation. It can be difficult for people to determine your tone and intent with just a text message.

## Privacy

Traditional SMS messaging lacks robust privacy protections; once sent, you lose control over the message. Messages can be forwarded, posted publicly, shared as a screenshot, or disclosed due to court orders. For private communication, pick up the phone and call the individual. Finally, if you utilize your work device for messaging, remember that your employer may have the authority to monitor and potentially read messages on work devices.

## Malicious Messages

Like with email, cyber attackers are going to try to trick, fool, or scam you with messages. These messages can include malicious links they want you to click, requests for you to share personal information, or pressure for you to call a phone number. Have you ever received an odd text message with just the word "Hi" in the message and wondered what that is about? That is a cyber attacker trying to start conversations with you, often the beginning of something called a romance scam. If you receive odd or suspicious messages on your device, simply delete them.

In addition, as also is the case with email, it's possible to spoof the source of a text message. Be certain that you know the identity of the person with whom you're texting before divulging any personal information, particularly if you did not initiate the conversation. You can also block any unwanted or suspicious phone numbers or accounts attempting to message you.

## Secure Messaging

Make sure that whatever messaging app you are using is current and up to date, ensuring it has the latest security features. Consider dedicated secure messaging apps like Signal for enhanced security and privacy.

## Guest Editor

Michele Tomasic, Women in Cybersecurity (WiCyS), Deputy Director, is a dynamic leader committed to advancing women in the cybersecurity field. With a robust background in people and operational management, she leverages her expertise to promote inclusivity, diversity, and empower women in the cybersecurity workforce.

## Resources

**Securing Your Mobile Devices:** https://www.sans.org/newsletters/ouch/securing-mobile-devices/
**Disposing of Your Mobile Devices:** https://www.sans.org/newsletters/ouch/disposing-mobile-devices/
**Avoid The Most Common Email Mistakes:** https://www.sans.org/newsletters/ouch/avoid-the-most-common-email-mistakes/
**Signal:** https://signal.org