520.743.7554
computerdimensions.net
business it solutions

Best Practices For Secure Business Texting

Messaging serves as a primary mode of communication in both our personal and professional lives. In the United States alone, people send around 2 trillion text messages annually. 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.

Share the Bare Minimum

Regardless of the security measures you adopt, it's always a good practice to assume that business communication via text might not be secure. Develop a communication policy that outlines what's permissible for employees to share amongst themselves or disclose to clients via text. The less concrete information you send and ask for, the more secure it will be. Refrain from exchanging personally identifiable information, bank accounts, passwords, and other vulnerable data. Try to limit such exchanges to face-to-face encounters or more secure means of communication - or you can text links telling people to log in to a secure portal where they can view sensitive information.

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.

Improve Connection Security through a Virtual Private Network

A VPN’s main purpose for business communication is to protect your network connection. It creates a layer of encryption that requests have to pass through first, meaning any websites you access or messages you send remain private. That includes your ISP or any hackers hoping to intercept your data. Scammers may send text messages containing harmful links. Some will install malware on your device. Others lead to fake sites that trick you into revealing sensitive login information. Some VPNs that you can find on this VPN comparison table can blacklist such websites. Some of the VPN providers include NordVPN vs ExpressVPN vs Surfshark. They’ll prevent you from accessing blacklisted sites, protecting you from harm even if you carelessly tap on an untrustworthy link.

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.

Ensure Compliance

Texting can be a powerful tool for reaching out to leads and customers. However, there are rules & guidelines you should follow to stay compliant. One important rule to keep in mind involves identification and consent. You have to let the recipient know whom you represent and the purpose of your message. They should also have a means of opting out of the conversation at any time.

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.

Protect Your Messaging Apps with a Password Manager & 2FA
If you use an online texting platform to send business texts, you'll want to make sure your account is secure. As you'll likely be discussing sensitive or proprietary topics, your account must have the best protection.

The first step – assigning a password – is one many already bungle. Any login should be a serious obstacle for hackers, not an afterthought. Yet people treat it like the latter, often carelessly using the same password for several accounts or choosing common ones that are effectively useless. The best way to secure access to your messaging apps and any other services that require an account is via a team password manager. They automate the password creation process and can fill them in during login. Each password is one-of-a-kind and complex enough to be highly resistant to brute forcing. Deploying a manager at the company level can secure hundreds of accounts while eliminating downtime employees spend on entering their passwords or retrieving forgotten ones. Of course, just because the password is tamper-proof doesn't mean someone won't compromise it in other ways. An employee might write theirs down or even share it for one reason or another.

Two-factor authentication can help in this case. Sometimes, it comes bundled with password managers. It prevents compromised passwords from becoming security risks by making them only the first part of account access. The second code arrives via text or is available from authenticator apps. It comes into play during login attempts from unrecognized sources, such as IP addresses you haven't used the account from before. You can just enter the second code and continue, while anyone trying to hack the account may not proceed.

Educate Your Employees
Most security compromises we've touched on happen due to human behavior. Fortunately, you can substantially reduce the risk of such behavior with training. A few sessions discussing the best cybersecurity practices will equip your employees with the skills they need to recognize scam messages and text more professionally. It's also important to emphasize using company devices for business texting purposes. Personal devices pose a security risk and should be avoided. Likewise, you should adopt the same company-wide texting service and discourage business communication outside of it.

Texting remains an effective means of reaching out to clients and coordinating with coworkers. Make sure you bring this late 20th-century tech up to the most recent security standards to continue benefiting from its use without worry.
For questions or a cybersecurity assessment, reach out to Computer Dimensions today @ 520-743-7554.