CORPORATE SUPPORT SERVICES

Volume 23 | Quarterly Newsletter | January – March 2026

"Smishing": You Can't Always Trust Messages — But You Can Be Prepared

Smishing is rarely discussed, but it is alive and well.

A smishing attack is a general term for a text message that asks you to click a link, respond, or provide personal or corporate information. Unfortunately, the results of a successful smishing attack can include compromised PIN numbers, credit card information, passwords, Social Security numbers, and other private details that could lead to identity theft. In more severe cases, it could provide access to company email, calendars, corporate contacts, and other applications that contain confidential data.

It was recently reported to Summit Technologies (STI) IT that there was an attempt to compromise both an employee and our CEO. Below is what was reported:

Employee Statement:

"I received a text message shortly after being hired at STI from someone claiming to be William Funaro (CEO of STI). The message stated that they were with STI. As a new hire, I did not research the message and assumed it was someone in my chain of command attempting to confirm my phone number or reach out.

Later, I received another text message from someone using the same name. The message stated that they were in a meeting giving a presentation and asked me to purchase Apple gift cards from Staples, CVS, or Target and provide the codes from the back of the cards. I was certain that no one at STI would ask or expect me to do this, so I reported the incident."

Please note the difference between **smishing** and **phishing**. While both are cyberattacks aimed at stealing personal information, they differ in their delivery methods:

Phishing: Typically occurs through email. Attackers send fraudulent emails that appear to be from legitimate sources, tricking recipients into clicking malicious links or providing sensitive information such as passwords or credit card numbers.

Smishing: A form of phishing that occurs via text message. Scammers send deceptive texts that often contain malicious links or prompt the recipient to call a phone number. These messages may appear urgent, claiming issues with bank accounts, package deliveries, or executive requests, pressuring victims to act quickly without verifying the sender's identity.

We are proud that our employee recognized the potential threat and reported the incident. Unfortunately, we must remain cautious with messages from unknown senders and even messages from known contacts if the content seems unusual or out of character. Staying vigilant is critical to protecting both personal and company information.

Year End Reminders with Time and Expense

Enter Daily: Avoid the Daily Floor Check report by logging your time daily.
Submit Timely: Complete expense reports within 5 business days.
Be Thorough: Include required receipts to avoid delays.
Use Clear Descriptions for each expense item.
Review Before Submitting: Double-check for accuracies.
2025 Expenses? Immediately submit any outstanding 2025 expenses. Any questions contact your supervisor. Any questions regarding TERs please reach out to AP at accountspayable@summittech.us

Message from our CEO:

Dear Summit Technologies Team,

As we close out 2025 and welcome 2026, I want to express my deepest gratitude and pride in each of you.

This year has been one of remarkable achievement. Your dedication and innovation strengthened our nation's technology, security, and prosperity. Highlights include our successful transition to MPSC IV, achieving CMMC 2 Certification, and maintaining unwavering commitment to customer satisfaction—milestones that showcase our resilience, collaboration, and excellence.

Through your tireless efforts, we advanced company goals, solved complex challenges, and delivered solutions that truly matter for our clients and country.

You continually inspire me with your talent, passion, and positive impact.

Looking to 2026, I am confident we will achieve even greater growth, innovation, and success—because of you.

Thank you for your extraordinary contributions in 2025. Here's to a brighter year ahead, filled with opportunity and shared success. We do this for our families and those standing beside us—stay in the fight!

Wishing you and your loved ones a joyful, healthy, and prosperous New Year.

With gratitude and best wishes,

William Funaro
Chief Executive Officer
Summit Technologies

If you have any questions, please contact Caty Savage, FSO, at (850) 312-9356 or csavage@summittech.us