San Francisco Examiner

That text from your CEO is actually from a criminal. What should you do?

By Jeff Elder | Examiner staff writer |
Aug 23, 2022
https://www.sfexaminer.com/news/that-text-from-your-ceo-is-actually-from-a-criminal-what-should-youdo/article_cbc2d32e-2326-11ed-91d7-534a2f970a50.html

Texting scams involving company executives and employees are on the rise and could potentially paralyze workplaces including hospitals, according to the FBI, the Department of Homeland Security and cybersecurity companies.

You get a text on your phone that claims to be from your company's CEO. "This is urgent," the text says.
The message asks you to do something. Can you buy some gift cards for employees? Can you open an email sent to your work account and click on a link? Can you click on a link in the text and enter your work email and password?

Sound familiar? The Bay Area is getting pelted by a hailstorm of texting scams, according to the FBI, the Department of Homeland Security and cybersecurity companies. And the texts can lead employees to unleash ransomware in their companies' computer systems that could paralyze workplaces, including hospitals just regaining some normalcy after COVID-19.

Do you know what employees should do if they get these texts? Don't click any link. Don't provide any information. Don't reply. Reach out to your information technology team at work — especially if you have already clicked on a link or entered information.

If you're thinking, "I get those texts all the time. Only an idiot would fall for something like that," that attitude is part of the problem. That's because while it's true that only 7% of employees click on scam links, it affects the entire organization. And those employees often click on malicious links several different times. It has to be easier for them to speak up if they don't understand the scam, or what they might have done. Shame hides a problem with serious ramifications.

Addressing that requires a culture change that can make the difference between a hospital getting shut down by criminals demanding ransom — or an IT team repelling the the threat and the hospital staying open.

Federal authorities say Bay Area organizations need to take notice of the problem.

The FBI and the Cybersecurity Infrastructure Security Agency, which is part of the Department of Homeland Security, sent out an advisory earlier this month warning that “Bay Area companies, especially in the healthcare industry, are particularly vulnerable to ransomware attacks” now hitting employees through texts and emails.

“I’ve had almost a dozen companies reach out with the exact same MO [modus operandi] of someone texting them pretending to be their CEO,” Elvis Chan of the FBI’s San Francisco bureau told The Examiner.

“We have seen cybercriminals pretending to be the CEO for the company or a senior executive for the company in order to induce employees to click on a link to detonate ransomware,” Chan said.

Ransomware uses malicious computer viruses that encrypt, or lock up with complicated code, an organization’s computer system. Once the system is incapacitated, the criminals demand a ransom, often paid in cryptocurrency, to release the computer system. Ransomware has typically been hidden in malicious links in emails sent to companies. But cybercriminals are increasingly using text messages to manipulate employees into unleashing destructive computer code on companies.

Chan said when employees click on a ransomware link in a text, their cellphone is infected. When the employee accesses company systems through their phone, the ransomware then spreads to the company network.

But here’s where things get interesting: The type of ransomware hitting the Bay Area right now is often flawed, and cyberattacks can often be stopped by authorities before an organization’s network is shut down — if employees act fast.

“There’s a chance that victims may be able to recover their data without needing to resort to paying the ransom demand,” ransomware expert Brett Callow of the company Emsisoft told The Examiner.In January a Florida hospital thwarted a ransomware attack when the IT team discovered it early.

Telling your IT team right away is important. The FBI and CISA also urge you to promptly report ransomware incidents to a local FBI field office, or CISA at us-cert.cisa.gov/report. For more on ransomware, go to cisa.gov/stopransomware. For more on stopping scam texts, go to fcc.gov.

The employee who clicked on the bad link needs to know they are not in trouble because they can redeem themselves by alerting the IT team and authorities in time to prevent the damage of an attack. What’s required is a culture change, say Bay Area cybersecurity experts. It’s important to understand employees’ perspectives.

Cybercrime delivered by text brings new challenges to employees, says Crane Hassold, director of threat intelligence at San Francisco's Abnormal Security. "We've seen an overarching attempt to pivot to SMS or text messages from email for different types of cyber threats."

Employees who have learned to scrutinize scam emails might not be as prepared to spot a texting scam — especially if it claims to be from a boss. What should employees do? Tell IT and don't feel embarrassed. "Negative consequences are not productive," Hassold says.

"We're all getting these texts," says Masha Sedova, co-founder and president of Berkeley's ElevateSecurity. People who spot the texts as a scam need to take action, she said. "It is my job to raise my hand and say, 'Hey, everybody, this is on the radar. This is what today's text looks like.'"

Sedova said employees should let vulnerable employees know "I'm your security partner. Feel free to let me know if you need to bounce a question off me."
"From a ransomware perspective, that kind of behavior is so critical," Sedova said. "You actually have time — if you can raise your hand, get in touch with the right people."

Sedova's company, which addresses "social engineering," or crime that exploits human behavior,found that 7% of employees ever execute or download malware, but that grows to 31% of departments and ultimately nearly all organizations as a whole. That data came from surveying the behavior of 114,000 end users across 2,000 organizational departments between 2018 and 2020.

"How do we deal with shame around this?" is an important question, Sedova said. "Until we look at the human components, it's not a technology question. It is entirely a human and emotional question."
jelder@sfexaminer.com

Jeff Elder