2026-2-24
GTK

WSJ Print Edition

Surfside Is Not Alone

Surfside Beach has joined a growing list of municipalities hit by similar email phishing scams.

Peterborough, N.H., lost $2.3 million in 2021 and recovered just $650,000, prompting officials to dip into reserves and cut spending. Insurance didn't pay. Lexington, Ky., was conned out of $3.9 million a year later, but authorities seized all of it from a private bank account. The crime has led to five federal convictions.

Artificial intelligence is empowering scammers, said Timothy Lynch, chief of the FBI's Cyber Enabled Fraud and Money Laundering Unit. In years past, he said, they overused "kindly," a word seen in at least one Surfside Beach email. AI smooths syntax and diction, polish that helps overseas crooks with poor English.

Of all the anti-scam safeguards, none beats human verification. "Call a known number to ensure a request is authentic," Lynch said.

image

SCOTT CALVERT/ WSJ (TOP 2)

Surfside Beach Mayor Robert Krouse, above left at center, has defended the town's actions amid the cyber scam. Wildcat Contractors CEO Alyssa Bowker, above, with her husband and company president, Kyle Bowker, and their daughter, says 'I didn't get scammed, they got scammed. Why should I not be paid?'

A $545,598 Trap Ensnares a Small Town

Scammer's email bilks 'Family Beach,' leaving a contractor unpaid for services

BY SCOTT CALVERT

SURFSIDE BEACH, S.C.— The trap began with a routine bureaucratic ritual: the head of a family-run contracting company and a small town public-works director trading emails about when the municipality would cut a six-figure check for utility work.

Lurking online, a cybercriminal pounced. Someone posing as a company employee emailed the director to request an electronic transfer. Days later, the town sent $545,598.30 to a Utah bank account.

Surfside Beach had fallen victim to a "business email compromise" scam, a swindle that cost $3 billion nationally last year, the Federal Bureau of Investigation says.

In such ruses, fraudsters fool people with malicious software, phishing emails or tweaked digital addresses. Once in, they can spot legitimate email threads about invoices and business matters.

In Surfside Beach, a probe is under way to determine how the breach occurred. The money is still missing, and the fallout is rippling through the enclave of about 4,300 year-rounders, a place known as the "Family Beach" for its laid-back contrast to nearby Myrtle Beach.

Locals are speaking out at Town Council meetings, and residents such as Cecilia Horne, 67 years old, are questioning the competence of their leaders. "Where's the professionals?" she said from the seat of her golf cart.

The company, Wildcat Contractors, has yet to be paid and has had to tap reserves to help cover the errant $545,000. "I didn't get scammed, they got scammed," Chief Executive Alyssa Bowker said of the town. "Why should I not be paid?"

Surfside Beach Mayor Robert Krouse said the emailed payment request appeared genuine. "We don't see where the town erred," he said.

The South Carolina Law Enforcement Division is investi--gating, and the summary of a forensic analysis released Wednesday by the town said its email accounts weren't improperly accessed, without pinpointing the scam's origin. But one thing is clear: The ploy was designed to trick.

The fraudster set up dummy websites and email addresses. One domain reads " wiidcatcontractors.com"— with the third letter in the email address a capital I, visually identical to a lowercase L in some fonts. Another tacked an "s" on

Surfside to create surfsidesbeach.org. Such "typosquatting" led town and Wildcat employees to communicate unwittingly with the scammer, emails viewed by The Wall Street Journal show.

The trick is so subtle it can "pass the human eyeball test," said Ben Bernstein, a cybersecurity expert at Huntress Labs.

While the details of the breach in Surfside Beach are still being scrutinized, cyber intruders have a typical toolbox for such crimes. To time their strikes, they set up flags on infiltrated email systems so they see when payment-related messages land. They also route legitimate emails to trash so only the fraudster's voice gets through.

At the time of the debacle, Wildcat was well into a project to bury overhead lines on two-lane Ocean Boulevard.

On March 9, Bowker received an email from Surfside Beach's public-works director about the job's fourth payment. She owns the 130-employee company, based in Gastonia, N.C. Her husband, Kyle Bowker, is president. "I will keep an eye out for the check," she replied at 10:51 a.m., though the town says the director doesn't recall that message.

About 90 minutes later, someone posing as Wildcat's project manager emailed the director, asking that the money be sent electronically instead.

That day, the scammer filled out Surfside Beach's ACH form, short for Automated Clearing House, an electronic bank network used to pay vendors. It had what Alyssa Bowker calls multiple red flags. The contact name isn't her employee, and it lists a Los Angeles phone number, though the email address is her project manager's. The bank is in Utah, and her signature, she says, appears blurry and lifted from elsewhere.

Town Finance Director Melanie Gruber said the ACH form didn't raise suspicions. "It looked legit to us," Gruber said.

It isn't unusual for a vendor to switch from check to ACH, Town Administrator Gerry Vincent noted.

The fraud was unmasked April 27 after Bowker heard from town officials following her payment inquiries. Their message: We paid you. When the town sent Bowker the ACH form and emails, she spotted "wiidcat" in some emails.

Krouse, the mayor, said the town's IT department found no breach of its network—the same conclusion Bowker said Wildcat's IT consultants initially made about its network—and that the ACH request came from a valid Wildcat email. Krouse added that he awaits the investigative findings.

The town has bolstered its controls and now requires passwords for large contracts and closer scrutiny of ACH transfers. Historically, authorities have clawed back funds about 75% of the time when scams were reported within 72 hours, said Timothy Lynch, chief of the FBI's Cyber Enabled Fraud and Money Laundering Unit. Because it took 45 days for this heist to come to light, recovery is "highly unlikely," he said.

"The most important thing, other than trying to get as much money back as we possibly can," said Councilor Rick Lawhorn, "is that we never have this happen again."