
“Been doing this for 30 some years. I don’t think I can remember anything else that has put the stress factor way up that quick.”

That’s what the CIO of an Oklahoma credit union had to say after enduring a phishing attack against his institution in June 2008. Here’s what the *Tulsa World* reported about the attack:

Jun. 12, 2008--Dear Action Line: I received an e-mail message, apparently from Tulsa Teachers Credit Union, that my account had been “compromised” by hackers and shut down by the credit union. It asked me to call a North Carolina (704) number to provide my TTCU routing and account numbers so the credit union could reactivate my account. I’ve been calling the credit union for three days to ask about this but can’t get past the busy signals. I’m sure this is a hoax, but do I need to check on this in person? -- S.J., Broken Arrow.

This monumental “phishing” attack...on Tulsa Teachers Credit Union customers started a week ago and reached the crisis level Wednesday when all 40 of the system’s telephone customer assistance personnel were busy answering panic calls. Also, the lobbies of all credit union facilities were packed with customers on foot asking the same question: “Is my money in trouble?” It’s not.

The attack was unique in that it was three-pronged: it involved not only e-mail phishing attacks but also text-messaging attacks to people’s unpublished cell phone numbers and “vishing” attacks -- live people voice-fishing over the phone asking people for their credit union account numbers.

At 9:47 a.m. Wednesday, the Tulsa Better Business Bureau issued a “scam alert” to all media outlets in which Rick Brinkley, bureau president and CEO, stated, “Within the last 30 minutes, the BBB serving Eastern Oklahoma is being inundated with consumer

calls regarding a text message and/or e-mail stating that the consumer’s account with Tulsa Teacher’s Credit Union has been closed and the consumer is directed to call a 704 area code number (Davidson, N.C.). A recording then directs the consumer to enter a credit card number. The BBB has tracked the telephone number and is continuing to investigate.”

...

“This was a massive attack,” Brinkley said. “We know of five carriers it went out over -- including AT&T, T-Mobile, US Cellular and Sprint -- and I think there were thousands of these text messages that went out. Members and nonmembers alike began calling the credit union about this text message, and it backed up our phone system.”

The attack was eased, Brinkley said, when the credit union’s Internet protection company -- Tacoma, Wash.-based Internet Identity -- (convinced the phone carrier to place) a warning message on the 704 phone number ... telling callers the phone line was originally set up by criminals.

...

Kristi Brooks Cohea, vice president of marketing for Tulsa Teachers Credit Union, said the attacks affected “less than 20” credit union members, and that only a few of them actually provided the requested account numbers. Those accounts were closed and new ones were opened for the customers.

Tulsa World, Okla., Action Line Column: ‘Phishing’ Attackers Hit Teachers Credit Union
http://www.redorbit.com/news/technology/1429000/tulsa_world_okla_action_line_column_phishing_attackers_hit_teachers/
Posted on: Thursday, 12 June 2008, 09:00 CDT

Key Takeaway

Phishing attacks come without warning - and can overwhelm your people and systems.
You need to get prepared NOW, before any attacks hit.

- Train all member touchpoints (branch, phone, website) to inform and reassure members.
- Have public relations action plan ready to go. Reach out to community resources.
- Know how you will get the attacks stopped - FAST.

To get more information about phishing or to learn about Internet Identity’s anti-phishing response services, please contact Internet Identity at (888) 239 6932 or internetidentity.com

