

How an Internet Outage and a Misdialed Number Lead to Fraud – Part 1

August 9, 2024 - It has been about a week now since my wife and I were watching TV and the screen froze. Like millions of American families, we've cut the cord and moved exclusively to streaming our favorite shows, so my first suspicion was that we were having an internet issue. One look at my router confirmed that suspicion. So my wife looked up Spectrum's phone number on her phone and placed a call. And that's when the trouble started.

Somehow or another she misdialed the number. The person who answered the call simply asked, can I help you? He had a heavy Indian accent, but there is nothing unusual about that when you're calling customer service these days. And since she had placed the call, she assumed that she knew who he worked for. So she described the problem, and the person answering the phone was ready to play along.

He asked her for her ZIP Code, which she provided. He then told her that there were no outages in our area so he would have to dispatch a technician. And since they had a cancellation on another appointment, he could have someone at our house within about four hours. So far, so good.

Then he told her that Spectrum had instituted a new policy. The company would only dispatch if she would agree to provide a credit card number. The card would be charged \$30 if they dispatched but nobody was home at the time the tech showed up. But there would be no charge as long as someone answered the door. They had put the policy in place because the company was experiencing a lot of technicians being stood-up on appointments that hadn't been cancelled by customers. Sounds perfectly logical. After all, companies do incur significant costs when dispatching technicians. And if nobody is there to let them in at appointment-time, those costs are nothing but a waste of money and time. So she gave him her debit card number.

The call was on speaker phone so I heard all of this going on, and I was actually buying into it. The person on the other end of the call had us wait while he ran the debit card. And after a couple of minutes, he came back on the line to say that the charge wouldn't go through. Chase Bank was experiencing an outage, he explained, so she would need to provide a card from another bank. So she gave him a B of A credit card number.

By this time the agent on the other end of the call had gotten a little pushy with my wife, and I didn't like that. So I piped up and asked to be transferred to a representative in the United States. They agreed and asked us to hold for a minute. Then a new person picked up the phone and introduced himself as Mr. O'Leary... trying to mask an Indian accent. Something wasn't right here.

At just about the same time, I received a text from Chase Bank saying that a charge of nearly \$150 had just been denied due to suspected fraud. I was asked if we had authorized the charge, and I said no. That immediately cancelled my wife's debit card. Mr. O'Leary then asked if he could help us. I said, I don't think so, hung up on him and initiated to cancel that credit card.

While I'll publish a Part 2 to this story in a day or two, because dealing with the banks was Oh, so much fun, I need to point some things out about the scenario above.

First, as an advocate for privacy and data security, I tell people all of the time that they shouldn't give out their personal information on calls unless they are the ones to initiate the call and they know exactly who they are talking to. As a part of that advice, I tell them to look up the phone numbers themselves. My wife has been hearing that from me for over 20 years now, and it is exactly the procedure she followed. In this case, all of those precautions didn't make a bit of difference simply because of a misdialed number. So if you are making a call, and you get asked to provide personal information by the person receiving the call, I'm going to amend my advice. Before you give out that information, you might want to make sure that you dialed the correct phone number.

Secondly, if your bank allows it, make sure you setup charging thresholds for two factor authentication on you credit and debit cards. We had done that with our debit card, but not with all of our charge cards. The only reason we were able to jump on cancelling the B of A card so quickly was because of the warning we received from Chase Bank about the debit card.

And as always, it is up to you as a consumer to be vigilant. Even if you make a mistake... and we clearly did here... you can correct it without much damage if you act quickly. If you're in a situation where you have to provide personally identifiable or financial information, and something doesn't seem quite right, end the contact immediately and then move to rectify the issue as quickly as you can.

by Jim Malmberg

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, [click here](#). Registration is easy and free.

Follow ACCESS