DECCA AITKENHEAD

I had been scammed – it felt like an electric shock

Decca Aitkenhead was at work and distracted when her ‘bank’ rang to warn that fraudsters were targeting her cash. Hours later, she was penniless

The Sunday Times, December 29 2019

I have always flattered myself that I’m intelligent. I often listen to Radio 4’s Money Box while making lunch, and can’t believe my ears to hear about all the people who answer their phone to a random stranger and end up transferring all of their money into the stranger’s account. What were they thinking?

One Wednesday afternoon this month, the phone rang while I was busy writing at my desk. Having won the interviewer of the year prize at the British Journalism Awards the night before, I was in high spirits, mildly hung over, short of sleep and behind on my deadline. I was going to ignore the call, until I saw the name on the screen: PhoneBank, Lloyds’ telephone banking service.

A man with a Lancashire accent and a kindly voice told me he was calling from the bank’s fraud department to query a possibly fraudulent transaction from my account that morning of £1,250 to the airline Emirates. “I wish,” I joked. But no, that definitely wasn’t me. Surely no one would buy plane tickets fraudulently, though? They’d be so easy to identify. The man said it didn’t look like the real Emirates but a fake company account typically used by fraudsters. He was concerned that my online banking had been compromised and gave me

three precise times that day when someone had logged in to my account. Had that been me? Absolutely not. Could anyone have access to my login details? Of course not.

He told me my account was being accessed from an IP address in Kent. I had been at London Bridge all day. He paused to check. “It’s in, er . . .” and he named a village. “Do you have any association with that place?” I used to live near there, I told him. Did I still have any association with it? I said I now rented out my house there. He gave me the four digits of my old postcode — it was bank policy not to divulge the full postcode, he said, to prevent defrauded customers taking the law into their hands. He asked if my tenants could have my login details. Whoever was accessing my account had tried to change my home address, he told me, and gave the full address of a house in Cambridgeshire. Did I have any association with that address? Emphatically not.

By now we had been on the phone for half an hour. I kept glancing at the clock, keen to get on with my work. The man was apologetic for taking so long, and kept deploying the corporate phrases bank staff are trained to use: “I realise this is a very distressing call to receive and I don’t want to add any unnecessary distress”; “Thank you for your patience and co-operation”; and so on.

He kept putting me on hold while he “spoke to his line manager” — at one point he said that she was listening in to ensure he observed all procedures correctly. While on hold I put him on speaker phone so I could write while I waited; every time he came back on the line his first question was: “Am I on speaker phone? You need to take me off so no one can overhear and compromise your security.”

He told me the account was being accessed via a tablet. I don’t own one. Did I have the Lloyds app on my phone? No. He asked if I had up-to-date antivirus protection on my laptop. I wasn’t sure. Had my laptop been behaving oddly when it powered down? Not that I’d noticed.

He asked me to log in on my laptop and go through my current account statements for the past three months, looking for any payments going out for less than £1 to Netflix, PayPal or Apple Pay. These would indicate and help to identify fraudulent activity. I couldn’t see any, but the man was concerned to establish that I was looking at the authentic Lloyds site and not a fake site created by fraudsters using malware. To verify it was genuine, he asked me to read out each account number and balance to ensure the numbers matched those on his screen.

He told me he was running a diagnostics test but that it had paused at 72%. While waiting for it to resume, he asked if I was in an open-plan office. Yes. He told me to take my laptop somewhere I couldn’t be overheard, to protect sensitive information. I motioned to my colleague opposite: “It’s the bank, my account’s been hacked” — and took my laptop to a private meeting room.

He then listed a series of attempted transactions in Europe using a cloned copy of my bank card. I was desperate by then just to get this resolved and get back to my now very overdue article. We had been on the phone for nearly two hours when, having spoken to his “manager” again, he said the security breach was too serious to risk leaving my accounts open — they must be frozen immediately.

I had already lost half the afternoon on the phone and apparently would now have to go into a branch the next day to open new accounts, which the man said would take an hour. My heart sank. Increasingly panicky about lost time, I asked for an appointment at 9.30am, when my local branch opened. He put me on hold before telling me the earliest available appointment was 10am.

Before my accounts could be frozen, he said that all my funds had to be transferred to a secure new account, where they would be safe until I came into the branch in the morning. He explained that when TSB and Lloyds divided into separate banks, they had retained a joint security facility whereby Lloyds customers in my circumstances could open a TSB Premier account, and vice versa. I used to have a Lloyds TSB Premier account, so knew the monthly fee was £15 a month, which he correctly cited. It would, of course, be waived, because I was a victim of fraud.

He told me to go to the transactions and payments page on the Lloyds site and create a new recipient in my name. He stressed that it was critical that my name began with capital letters. He then told me to enter a sort code and account number, and waited on hold while I verified the new recipient through the standard automated call from Lloyds.

He then told me he was adding two security questions, to make absolutely certain I was on the authentic Lloyds site, and told me to tell him as soon as they appeared. When they did, he instructed me how to answer them. Following his instructions, I transferred all but a few pounds and pence from each of my accounts into the new one. It was the policy of Lloyds to leave some funds in compromised accounts, he explained, so they could monitor continuing activity to apprehend the fraudsters. The accounts would remain open for 30 days and the remaining balances then be transferred to my new accounts. I would receive an email in the next 10 minutes containing the login details for my new TSB account. These would be computer-generated; he could not give them to me over the phone because that would compromise my security.

He put me on hold again while I waited for the email. Five minutes later the line went dead. When no email arrived, I called PhoneBank. “We haven’t called you today,” the woman said. I told her she was wrong: I had been on the line to PhoneBank for three hours. “I’m very sorry, Ms Aitkenhead,” she said, “but you haven’t been speaking to us.”

Nothing in life can prepare you for the sensation of realising you have transferred practically every penny you own into a stranger’s bank account. It was quite surreal, like an of out-of-body experience — hot and cold shock flooded through me like an electrical current. Colleagues say I turned white, like a cartoon character.

Disorientation and disbelief turned into humiliation and shame. Replaying the conversation in my head, I was horrified by how obvious so many of the man’s deceptions were in hindsight. I had given him my bank account numbers and balances; he had made me get out of earshot of colleagues who might have cautioned me against following his instructions; he had prepared me for the security questions, so that instead of heeding them I had merely ticked the boxes as instructed; he had left some funds in my accounts to avoid alerting Lloyds to the fact they were all being cleaned out; he kept me on the line long enough for him to empty the new TSB account.

How on earth had I not seen that at the time? I thought I knew how banking scams worked. Why had I fallen for it? The combination of urgency and reassurance had been hypnotically compelling: he built up an impression of alarming security breaches, using personal details harvested from God knows where, then presented himself as my saviour — and I fell for it. I wasn't angry with him as much as in awe of the operation's psychological ingenuity. It is, I now know, what's called "social engineering".

Ultimately, though, none of that explains why I gave away all my money to a stranger. Had the word PhoneBank not appeared on the screen when my phone rang, I would have hung up within the first minute. The trust I had invested in that nine-letter word took my breath away. I hadn't known that fraudsters have devised software that can do that. And as a result of that ignorance, I was penniless.

Lloyds was eventually able to reimburse Decca Aitkenhead