(Approx. 1586)

Two-Factor Authorization Fiasco

Greg Skalka, President

[Under the Computer Hood Users Group Home (uchug.org)](https://www.uchug.org/)

1editor101 (a) uchug.org

If you are accessing a personal account or app on the web, you should be concerned about that account's security. Bad actors (and I don't mean those who can't get a job in Hollywood) constantly search for our login credentials, hoping to access our accounts and steal money or personal information. The best ways to protect online accounts include using strong passwords and protecting them, resisting attempts by others to gain access to those accounts through scams and phishing communications, and using two-factor authentication on those accounts.

Two-factor authentication, or 2FA, requires at least two identification items of different types to log into an account. It is a subset of multi-factor authentication (MFA). This can be enabled for most online accounts; some account providers now require it. It typically requires providing two or more identifying items from three categories for account access. These categories are something you know (like a password, birthdate, or the answer to a security question), something you have (could be a specific phone, computer, or email account, or a security key, fob, or dongle), and something you are (a biometric like a fingerprint).

To get money from an ATM (assuming you are not trying the big truck with a chain approach), you must provide something you have (an ATM card) and something you know (a PIN). With a 2FA-enabled online account, to gain access, you would typically need something you know (a password) and something you have (either a smartphone or computer that can receive a security code through text message or email). Entering the correct code sent to the device that presumably only you have validates your identity in a second way (in addition to the password).

Your account provider may be using 2FA, and you don't even realize it. Even if you only enter a password for access, the provider may look at the IP address or other identifying information from your device's connection to validate that it is really you (something you have). If you usually log in from one device and then suddenly use another, the account provider may ask for additional verifying information, like the answer to a security question.

It should be evident that trying to make it more difficult for others to access your accounts could also make it more difficult for you. Going through additional steps, like entering a six-digit code you were sent through a text message, takes time and opens up the possibility of being denied access. If you lose your phone, have phone communication problems, have a malfunction in your fingerprint scanner, or lose control of your email account, you may not be able to get timely access to your accounts.

I was a little apprehensive about 2FA at first due to concerns about my being denied access due to some problem outside of my control. I don't remember if I started using 2FA because I enabled it or if some account I already had started requiring it. I have used 2FA for several years on most of my critical accounts. Whenever I am asked to enable it, I look to enable it on some accounts (I have found some that did not support it then; I'm starting to think less of those companies). I typically use my phone as the second form (something I have); I need to ensure I have my phone handy when I want account access on my computer. Receiving a code as a text on a phone is supposed to be more secure than receiving it in an email. It may be a little more work, but I have had a few problems with it denying me access when I needed it.

Recently, however, I have had a few instances of being denied access to accounts through 2FA. My first instance was about a week ago when I was trying to access my Scripps online medical account on my computer to perform an electronic check-in for a medical appointment. Of course, I was in a hurry, trying to do this late at night, just before bed for an appointment the next day, and I would not have time to do it later.

After successfully entering my username and password on the MyScripps web login page, a page was provided to select the method for sending a code: email or text. I have found that my phone usually receives the text in just a few seconds. This time, however, the text did not come right away as expected. I waited maybe 60 seconds (remember, I wanted to finish this and go to bed) and then clicked "Send code again." Again, I waited, this time a little longer. I checked my phone to see that it was on and not in airplane mode or something else that would turn off reception.

After waiting longer than I wanted, I finally selected email to deliver the code. Then, I had to start Thunderbird (my email program) to access my Juno email on my computer. Fortunately, the email with the code was there, and I successfully logged into Scripps and completed my task. At the time, I thought it was strange, but I didn't consider the problems I had any further. The following day, I found that the texts had come in at night.

A few days later, I tried to log into my US Bank online banking account from my computer; I again needed to check my account balance with some urgency. The US Bank 2FA code enter screen comes up right after entering a valid username and password; I may enable only texts to my phone for this. Again, I was used to having the text with the code pop up on my phone immediately, but I waited several minutes without receiving the text message. I now remembered my Scripps incident. There was no email delivery selection on the 2FA code entry screen on the US Bank website, but there was a link to "verify another way." I had hoped it would lead to verification through an email, but instead, it asked me to enter my debit card PIN.

I don't use a debit card for any of my accounts; I may have been sent one by the bank years ago, but I never activated it and had no way to get its PIN. This lack of access to my account was beginning to make me angry.

I canceled out of that screen (the only option) and tried going into the login page to get another code sent, but no code text message came to my phone. Finally, the bank locked me out of online access for too many unsuccessful attempts. I would need to change my password to get access again, and the first step for that was to send me a code that I'd need to enter. Good grief! I searched their website and finally found a number to call for online access support (they don't make things like this very obvious on their site).

While still on their site, I called the number and started my way down their automated phone menu system. Suddenly, while listening to the next set of options, I heard the sound of text messages being received on my phone. I found a bunch of texts from US Bank with 2FA codes that had just come through on my phone. I hung up the call and returned to the web page, but after entering the code from the last text, it said the code had expired, and a new one would be sent. Again, no code text was received. I called the US Bank support number again and found that action again appeared to trigger the receiving of text messages on my phone. Again, I was too late to enter these codes, but I now saw a pattern.

I returned to the bank website and asked for a code to change my password. I then immediately called the US Bank support number, and after a few entries in their audio menu, a text arrived on my phone. I could enter this code in time, change my password, and regain access to my online accounts.

I finally got the information I needed off the website, but I was concerned about what I had to go through to get it. Why were my texts not coming through right away? It seemed like making the phone call (or pressing phone keys) triggered the reception of texts that appeared stuck somewhere.

This seemed like a problem, so I cycled power on my phone and then tried logging into my US Bank online account. This time, the text message with the 2FA code was received right after my password was accepted, just as it had been.

Something in my phone went awry, and cycling the power fixed it. I try to

remember to do that periodically; I need to be better at making that a part of my tech management routine.

I still understand that online security is essential, but I also know how it feels to be locked out due to some malfunction in the system. The lesson in resiliency to take away is not to decrease security to prevent being affected by such a failure. Still, instead, I plan so I'm not doing things at the last minute and making myself vulnerable to problems when something inevitably breaks down.