Crossing the Digital Divide Volume 13

"Two-factors"

by Joseph Feigon

for the Observer

I walked into our local bank recently to make a simple deposit. I endorsed the check with the correct account number, and requested the platform agent make a "straight deposit". The bank employee then proceeded to ask me my name and the last four of my social security number. I was taken aback. I was **not** requesting cash back, I didn't bring in a suitcase of twenties, I had a local check for deposit. I've had bank accounts since I was in grade school, I have been asked for credentials when I request a balance statement, or cash back, but not a CHECK deposit? I feel violated and anything but safe. Why?

The Internet enables a degree of anonymity difficult to achieve in real life. We can, with the proper credentials and a good credit card, buy products and services without "exposing" ourselves any more than is required to conclude business. Your online vendors will not ask you (automatically or in person) for anything but item #, quantity, billing/shipping address, and a valid credit card. The credit card has to match the billing address. Fraud happens, but rarely relative to the millions of transactions that take place daily. Most vendors utilize a form of two-factor authentication that protects both buyer and seller. In the case of an online vendor, credit card billing address and credit card details. In the case of our local bank, an account number and a check payable to the account holder should be all that 's necessary to make a deposit. Withdrawals **should** require proof of identity, a Driver's License and Last Four suffice for most banks.

This works discussion is about social media and many email service providers. If you are a Facebook user, or a Google/Gmail/Youtube user, or a blogger on some blog-site, an email address and cellphone number are often used during account setup/creation. If you forget your password, your favorite toy from 3rd grade, or the first time you had chocolate, your cellphone may be the only means by which you can recover your password and regain access to your account.

Two-factor authentication (also known as **2FA** or **2-Step Verification**) is a technology patented in 1984 that provides identification of users by means of the combination of two different components. These components may be something that the user knows, something that the user possesses or something that is inseparable from the user. A good example from everyday life is the withdrawing of money from a cash machine. Only the correct combination of a bank card (something that the user possesses) and a PIN (personal identification number, something that the user knows) allows the transaction to be carried out. 2FA is ineffective against modern threats,[2]like ATM skimming, phishing, and malware etc. (Wikipedia).

Your homework for the week: log onto your social media accounts (Facebook, blogs, MySpace, Instagram, Twitter, etc.), and make sure both your email address and mobile numbers are correctly listed in "settings". If you've not verified your cellphone, click the links to do so. Log onto your Google/Gmail account and confirm the same settings, with attention to "recovery email" address, if you have one. If you have an email address other than gmail, visit gmail.com and create an account with your entire name, e.g. robert.charles.johnson or michael.brian.chadwick, write down the email address and password, and save it where you won't lose it. Having valid two-factor authentication mechanisms will ensure you'll be able to recover a lost password or email address should you ever lose access.