Science Translations
Established 1990
PC410.COM™
PC Updater News

Multi-Factor Authentication
Or “Why all these codes to my phone?”

The current security news is all about ransomware, but from what I see and fix regularly, half of the phish emails I'm asked to look at are about credential theft, where there's automation behind getting you to click an authentic-looking page and enter your email login, or bank login, and then wondering why there was an error message, and seeing issues in the account soon after. What's happening is that a fake login page has captured the login, and then put up a ‘login failed’ message to hide what it just did.

The next step is, and it's increasingly being automated, is to take the captured email address and password, and try to use it at the top 50 banks, or anywhere

else that might include a stored credit card, and then use that account to send money or gift cards elsewhere. What stops that, besides not losing control of a password, is multi-factor authentication. It's available as an option on many online accounts, including Office 365,

So what is multi-factor authentication? NIST, the National Institute of Standards and Technology, defines it well: “An authentication system that requires more than one distinct authentication factor for successful authentication. Multifactor authentication can be performed using a multifactor authenticator or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are.” (from https://csrc.nist.gov/glossary/term/MFA)

There’s some redundant text in there; a 'multifactor authenticator is a device, or 'something you have.' More on that later on.

Examples of something you know:

- Password (must always be unique)
- User name (if not public)
- Answer to a secret question (when it's NOT public info)

Examples of something you have:

- Cell phone (the actual hardware device, not the phone number)
- A hardware key (mechanical, or an electronic device like a YubiKey.)
- A smart card, usually chip-enabled (for physical access)
- A dedicated app for a single use login, usually a bank.

Examples of something you are:

- Fingerprint (readable on many cell phones)
- Retina scan
- Voice identification (already at some banks)
- Facial recognition (already on some phones)

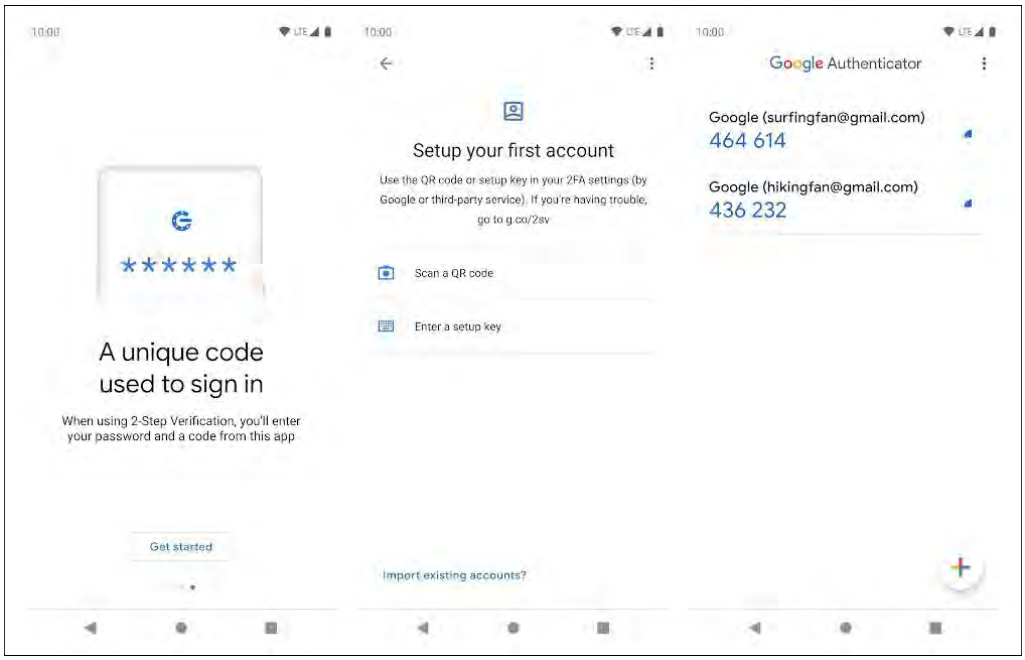
So multi-factor authentication combines one item from any two categories. The usual example is a password and some form of physical key.

Where Banks, Mostly, Get it Wrong

Banking web sites see a constant flow of attacks, and even a small bank with one branch is expected to have world-class security. They don’t, the small banks contract a service to run their online systems, from the lowest bidder. And it shows. The typical error is a message like this when you log in: “We

don't recognize your computer, so we sent a code to your email" or "... to your phone". Emails and text messages are external services you use, not something you know, have, or are. They are not remotely unhackable, not necessarily directed to just one destination, and you don't immediately know when you've lost control of them. They're what some techs refer to as a 'weak signal.'

Google Authenticator screens:



What's Secure?

Correct multi-factor authentication requires two unique items from the lists above, usually something that ONLY you know, like a password that is not used anywhere else, and something you have, like a cell phone. Again, a text isn't part of a cell phone; that's part of your phone number account, or something you rent.

So one solution is something called a time-based key. That means that at some point, you add an app to your cell phone that scans a QR code with a very long random number from each login that you need to use it with. Then when you log into a site, it asks for a user name, a password, and for a temporary code that is calculated in the app based on that saved random number, and adjusted for today's date and time. That creates a six-digit number in the app, and you type that into the web site to complete the login. The code expires every 30 seconds, so you have time to type the password, but someone watching you log in won't have enough information to log in again later.

There are a few of these apps. I like Google Authenticator, and it's available for free in the Android Play Store and the Apple App Store. Authenticator can be

used for multiple web sites, so when you run it, it will show a list of all the accounts you've added to it.

Bonus: it still works if your cell phone service is down, or your email is down, because it's strictly a time-based calculation.

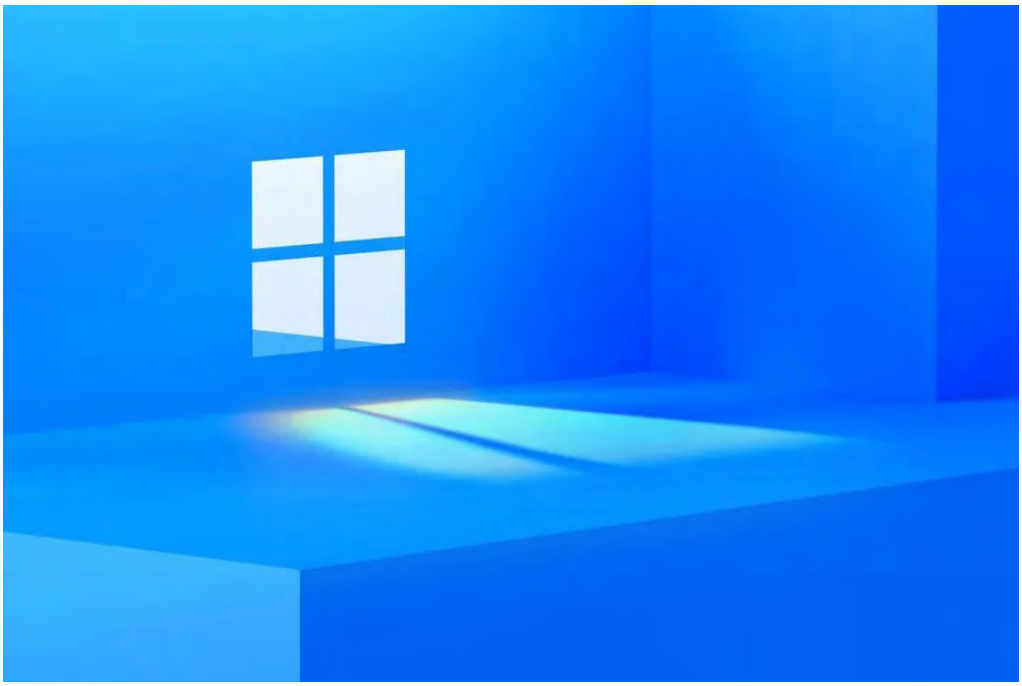
And Caution: If you lose or break your cell phone, you lose your keys. There is a solution to that, of just setting up a second device, usually a tablet, from the same QR code when you setup using the code for each account. (Just scan both devices on the same code at the same time.) Because the codes are time-based, both devices will have the same login codes. When you change phones, you'll need either the old phone or your backup device to turn off the authentication setting for each web site, and then turn it back for the new phone.

Finally, if you use Google Authenticator, you should also run a good malware scanner on your devices to protect the keys, and lock your phone with your fingerprint (something you are), or a passcode (something you know).

Graphcat 6.7 is Ready

I have published the new Graphcat version 6.7 for the new WordPerfect 2021. There are no new graphics catalog options; this is a minor update for compatibility with between Graphcat and WordPerfect 2021. As always, since 1991, Graphcat takes a directory of images and turns it into an editable catalog page, with lots of options and thousands of combinations of sizes, columns, borders, and paper settings.

Upgrades are half-price, from any prior version, ever; email for a discount code. Graphcat is available at https://www.graphcat.com



New Windows

The Spring 2021 semi-annual feature update for Windows 10 has started to arrive. Expect a 10-minute reboot after the 'Windows must reboot to install updates' message if you're running the 20H2 (second half of 2020) version, or 40 minutes from earlier versions. There aren't a lot of new features this time; it's more of a roll-up of 6 months of security patches.

Microsoft has scheduled a press event for June 24th, 11am Eastern time, and the marketing image and a few online comments are hinting at an announcement about Windows 11. And there is that image, above, showing an '11' below the Windows logo. Windows 10 was released in mid-2015, so it's about due for the next big change. Online guesses are that there will be changes in how you download software (the Microsoft Store), and improvements for touch screen users. (More next month...)

For computer help, call 410-871-2877