Real vs Fake Anti-Virus Software

A word about anti-virus software. Everyone has it, whether it's Windows Defender built-into Windows 10, or a paid program like Norton or McAfee. And if you own one of these programs, you probably have an idea that the color scheme of Windows Defender is mainly white and green, and if something needs attention it turns yellow and if there is a virus, it's red. Simple enough, right?
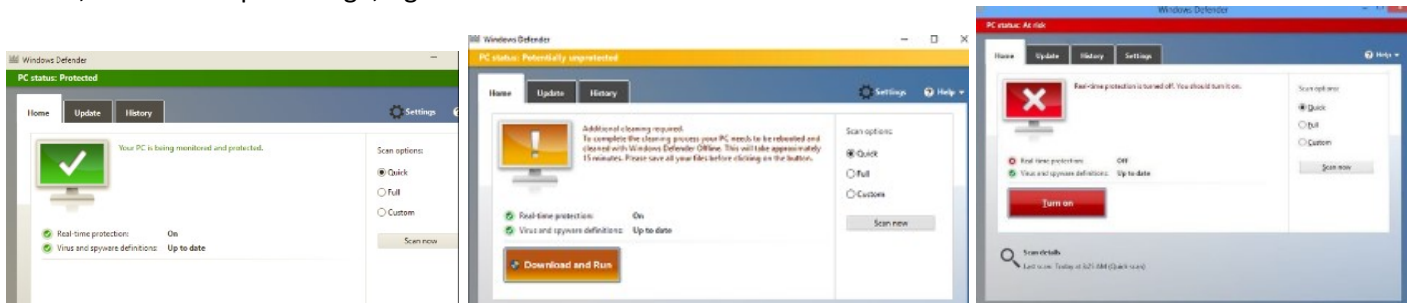
Consequently, if you own Norton software, the scheme is mainly yellow and black, with a green and white info page. Like Defender, if something needs attention, the pop-up window will be yellow and if there is a virus, red.
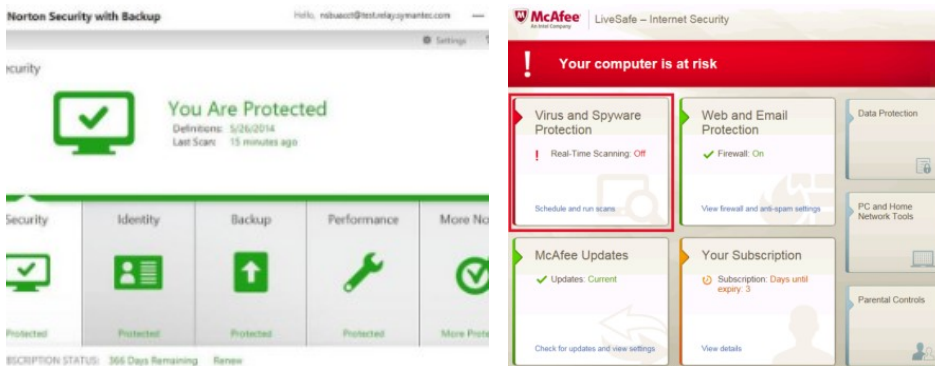
And finally, there's McAfee Security Suite. The theme is red and white with the same green/yellow/red main page.
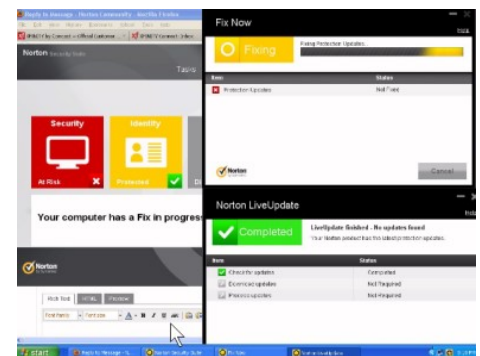
So this brings me to FAKE ANTI-VIRUS ALERTS! Let's say you're browsing the internet and suddenly without warning you get a full-page warning. **Please note one very important glaring omission**. Nowhere on this entire screen does it say Windows Defender, Norton or even McAfee. It says "Resident Shield Alert". And it isn't in a nice neat window like these three programs. It's in your face, it says VIRUS!, THREAT detected!, all kinds of things except the name of your particular anti-virus software. If you see something like this, press and hold the power button on your computer until it shuts down. Turn it back on, run CCleaner first, then run Malwarebytes. Under no circumstances should you click anywhere on the fake virus alert. Do NOT click the "X" in the corner, do NOT click the Ignore button, do NOT click anything. If you get tricked into clicking on it, you'll be greeted with a phone number to call and for $200 your "virus" will be removed and your computer will be loaded with unwanted software, more virii and your checking account compromised. Take away: Know the name of your anti-virus software and if you see anything pop-up on your screen that doesn't indicate a name you know, then shut down and restart your computer.