From Dave's Laptop

Well, although the color and the message are more friendly now than in "the old days," seeing "the blue screen of death" still means that your computer is "toast." I'm finally up and running again after seeing such a screen last night and restoring the whole drive from a backup.

I have no idea what caused the failure. This was the first blue screen I've seen in several years.

I'm fairly paranoid about such failures, since having no laptop means that most of my work (like sermons) can't get done. In order to prevent and/or recover from such disasters, I have real-time cloud backup that backs up changes to my files just as soon as I make them. I back up the entire computer to an external drive every night (incrementally, for the geeks out there). I create restore points every week. I even have a backup laptop that can be pressed into service at a moment's notice. And with the news about Janet's email being hacked this morning as well, I thought it timely to opine about a few technical things this week.

One member helpfully suggested this morning that if I'd get an Apple computer, I wouldn't experience crashes, and I know that's true. I began my computing life with a Macintosh 512e nearly thirty years ago, and I was a passionate Macintosh person for many years. Then I became a church administrator and inherited the management of a Windows network, so I got a Windows laptop in order to learn that system. One thing led to another, and now I've got so much money tied up in Windows software that I doubt that I'll ever return to a Mac (sigh).

As bad as having your operating system crash is, it's not nearly as much trouble as having your email hacked or your bank accounts compromised. I'm no expert on cyber-security (though we do have many such folk in the congregation!), but I do take such things very seriously, and here are a few suggestions.

If your computer ever leaves your home (such as a laptop), it needs to require a strong password in order to boot or to wake up, and if you have a smart phone, it needs to have the strongest password you can manage in order to access it at all. Yes, I know such things are aggravating, but they're not as aggravating as having your information and accounts stolen.

Many banks and email providers now provide what's called "dual authentication" in order to access your account(s). What this means is that once you've entered your first password in their website, their site then generates a code that is texted to your phone, which you then enter on the screen in order to access your account.

There are actually quite a few methods of dual authentication, but most of the common ones require your particular cell phone in order to log on. And yes, this is inconvenient, but it also means that even if a hacker steals your email address and figures out your password, your accounts still cannot be accessed unless they physically have your phone. (And you'll probably want the ability to "remote wipe" your phone in case it is lost or stolen.)

Speaking of passwords, there are many websites that give good advice about creating "strong passwords," which usually means passwords that are not easy to remember. The strongest ones tend to look like long strings of random characters, which most of us could never remember.
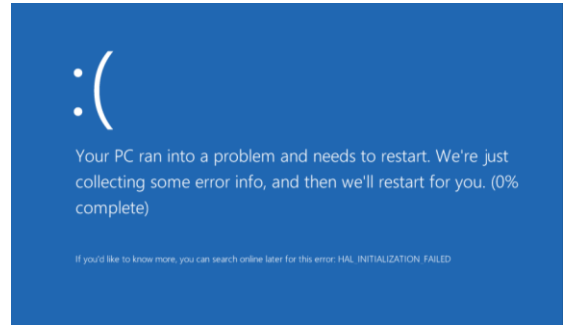
I probably have at least 100 passwords, most of which are both unique and strong. I could never, ever remember them, so I manage them with one of the many password managers available these days. I've used several, but the one I like best is *LastPass*. With a strong master password (which I do have to remember), dual authentication, and automatic logout, I think that keeps my passwords about as secure as ordinary people can accomplish.

And the way I remember to back up my laptop every night and to create a restore point every week (plus the way I remember almost everything else) is to use a "to do" program that reminds me to do it. I actually use four "to do" programs. I keep my calendar and my contacts in *Microsoft Outlook*. I keep my long-range to do lists in *Microsoft OneNote*. I keep my daily "to dos" in *Todoist*. And I keep my reminders to pay bills in *Quicken*.

It does take some effort on the front end to get everything into a "to do" application the first time (and they're no help at all if you don't look at them) but once you're up and running, it's a lot harder to forget to do things. I've told you before that Jill and I make our tithe contributions electronically through our bank; but the way I remember to do that is that Quicken lists those contributions as "Not Paid" until I actually transmit the funds. That way I can easily tell if I've gotten busy and missed a tithe opportunity, and I can catch up at once.

Along this line, I was interested to see an article in the current *Baptists Today* with the title, "Divine Devices or Digital Distractions," and the author suggested that e-contributors could even use their phones or tablets to make their offerings online during the worship service as the offering is being received, so that all are participating in that aspect of worship together. The article reported that 91 percent of American adults have a cell phone, and more than half of us have smartphones, so such a thing really is possible.

While there's much to be said for having a Bible that you can mark up and in which you can make notes, many of us already use our phones and tablets to access the Bible or to follow up on ideas presented in sermons. And many of us—especially young people— really *are* able to listen to the message and look up a website related to the message at the same time.

One pastor encourages his congregation to regularly post *Tweets* and *Facebook* updates indicating that they're in church, or even to post quotes or statements in the message that seem especially helpful. If you're good at texting, you can even take notes on the sermon with your phone as the service proceeds.

In the end, while our desktops, laptops, tablets and smartphones certainly can be digital distractions, they also make possible the communication of the Gospel and research on biblical and theological topics in ways and with depth that could not have been imagined by most of us even ten years ago. Just be sure you've got strong passwords, dual authentication, and current backups before you do very much!

Dave
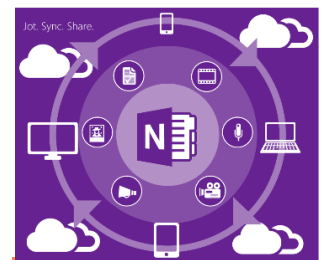
The Joshua Code: Fifty-Two Verses Every Believer Should Know
O.S. Hawkins (Thomas Nelson, 2012)

Week Six: Being Comes Before Doing

"*Blessed are those who hunger and thirst for righteousness,
for they will be filled*" (Matthew 5:6).

"The Lord began His famous Sermon on the Mount with a series of verses that have come to be known as the Beatitudes. Our verse for this week is planted squarely in the middle of this section. All the Beatitudes coming before it point to it, and all of the ones following it issue out of it. It is important to understand what our Lord is driving home here. These are the *Be*-attitudes and not the *Do*-attitudes. Being comes before doing, for what we do is always determined by who we are.

"The Beatitudes are not a set of rules, such as the Ten Commandments, by which we are to live. The Ten Commandments have to do with actions; the Beatitudes have to do with attitudes. The Ten Commandments have to do with conduct; the Beatitudes have to do with character. Why is it so imperative that we believers incarnate these Beatitudes into our very being? It is because our actions flow from our attitudes and our conduct issues out of our character."

The Pathway *toward* the Life of Blessing: Matthew 5:3-5

The Passageway *into* the Life of Blessing: Matthew 5:6

The Proofs issuing *out of* the Life of Blessing: Matthew 5:7-10

(Remember that if you want to know "the rest of the story," you'll need to get the book. ☺)