By Linda Windler, Thoroughbred Systems

Computer Corner

New-Techno-Intoxication

Those who attended the Kansas Rural Water Association's 2015 Conference and Exhibition were part of some of the fun we had with the theme "The Many Hats We Wear". The theme was portrayed with imagery and even some quirky poetry in the style of good ole Doctor Seuss.

When Doctor Seuss set pen to paper he was never slowed down trying to come up with just the right word to express himself. If the English language didn't supply the word Seuss wanted, he just made one up. Words like schlopp – an ice cream-like confection usually served with a cherry on top, or floob-boober-bab-boober-bubs – naming the creatures that are recognized by their bulbous bodies as they float through the water. By-the-way floob-boober-bab-boober-bubs is similar to the sound made by a KRWA employee when loosing their footing in the water while helping a city or water district deal with a bad leak. But I digress.

These days it seems like every time you turn around someone is coining a new word or phrase, especially in these high tech times. Well, I have decided to add a phrase of my own to that mound of techno-terms: New Technology Intoxication. Seuss might have said something more like New-techno-intoxification, but I will go with my first version.
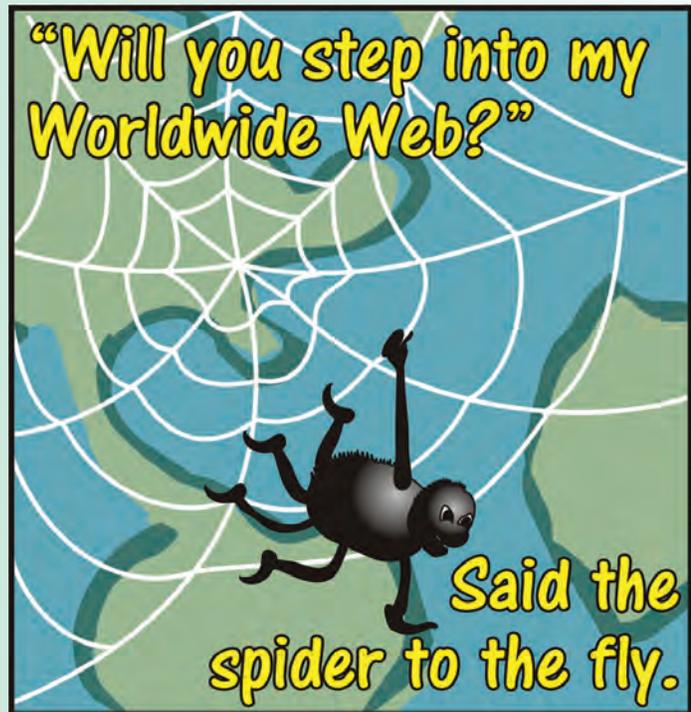
Yes, New Technology Intoxication! That's defined by people who think just because one CAN do something, one should, i.e., just because a new way of doing something or a new thing is invented, it is a good thing and should be immediately embraced in every conceivable way. That way of thinking would have us blowing up this world we live in with nuclear bombs just because we can.

The new technology I speak of, that has me particularly concerned about it's applications and it's possible consequences, is obviously not as serious as a nuclear explosion, but companies and individuals who have been negatively affected while using this ability sometimes feel they have had a bomb dropped on them.

I am speaking of the same subject we talked about in our column in an earlier issue of *The Kansas Lifeline* magazine entitled "The Perils of Cloud Computing". The reason I am revisiting this subject is because I personally had one of those bombs dropped on me since that article was published.

Do you trust your data to a stranger?

"The Cloud" is of course one of these newly invented terms for the world of technology. A decade ago if one spoke of "The Cloud" folks would think a reference was being made to the weather or, sometimes the way one's thought process functions after not getting enough sleep. Of course these days "The Cloud" refers to that mystical virtual world of Internet storage and access of data. "The Cloud" can't be reached by a car or a phone or the postman. It's an invisible virtual world that sometimes seems limitless in its possibilities and its reach. Something that should be remembered though is that there is actually a physical place where one's data is stored and actual human beings who are in charge of YOUR data. You just don't know them or know where they actually are or have any way of accessing them or your data except what they supply you with.

Anyone who read that earlier piece "The Perils of Cloud Computing" will know that it did not deny the usefulness of the Internet. The article simply warned against businesses and individuals who put themselves and their businesses at risk by storing their important data on "The Cloud".

It has long been warned not to let children and teenagers have unmonitored access to the Internet due to those that would do them harm, yet folks often leave their sensitive data where Internet bad guys may get at it. Maybe it is no accident that we sometimes refer to this virtual world as the "Web" given that it sometimes behaves as the spider in a web just waiting for the unsuspecting insect going about its daily business to happen by.

Of course, when we are referring to storing data on "The Cloud" we are not just referring to visiting the Internet, but actually keeping our information, our data – not on our own hard drives within our own homes and offices, but on "The Cloud", i.e., on a giant hard drive

> **We put our complete trust in the hands of people we don't know. The term to describe these people would be "strangers".**

owned by a business in a building somewhere. In doing so, we relinquish ALL physical control of our own data. We put our complete trust in the hands of people we don't know. The term to describe these people would be "strangers". If things don't go well it is not as though there is a place to drive to, to confront these folks when they have let us down. And, it is likely we will not get any satisfaction trying to reach them by phone either. Email contact often only results in an impersonal, pat answer, that gets us nowhere.

I speak as one with experience. As I stated earlier, I got a taste this last year of what can happen when you trust your personal data to "The Cloud". No, I didn't have my bank account emptied, as many have, or lose all my business records because I trusted them to storage and backup on "The Cloud" – that will never happen to me as I would never do that to begin with. What happened to me happened to thousands of others when Yahoo was attacked by hackers. One fine winter day I went to check my email, something that I use to track the things I need to do for and know about customers, and guess what, all of November and December was missing. GONE!

I quickly discovered that I could type the word December or the word November in the Search, and I could see all of the files listed, but I could not open any. This was outrageous! The Yahoo site provided no help on this problem. Now, understand, I was not attacked; we are not talking about a virus that sought out my computer. No, it was Yahoo that was attacked, and thousands of Yahoo's clients suffered because of it. It is their security that failed, something that I had no possible way of controlling.

After finding no help from the Yahoo site my next step was to call the technical support number Yahoo offers. It took some time before I was actually speaking with a person, or trying to, as it was a bad connection, I'm pretty sure outside the U.S.A., and we didn't always understand each other. The strangest thing was that this person kept asking questions about what I did for a living and how business was. He was making me very uncomfortable, as he seemed to be sizing me up financially. He connected with me over Team Viewer, a program used to view a computer from a remote location, supposedly to help me. But he did not do one single thing that was of any help. He acted all the while like he had never heard of the problem I was having – but then suddenly he said that for $99 (I would have to give my credit card information) he could connect me with someone who could get all my data back. Suddenly he knew all about this attack and had a solution that would cost me. He also told me that this offer was only available for the next few minutes. I had had it. I disconnected from Team Viewer with him immediately and told him I would like to speak to his supervisor to which he said "NO!"

I hung up and went to the FBI's site where I filed a report of what I believed to be an attempt at extortion. Next I called Yahoo's corporate office and was put through to, what else – a voicemail of course! I left a message explaining that it looked to me as though they may have rouge employees running an extortion scam and if they would care to speak to me about it they could call me, but, either way, I had filed with the FBI. I never heard back from Yahoo, typical, but a few days later my emails were restored.

> **He acted all the while like he had never heard of the problem I was having – but then suddenly he said that for $99 (I would have to give my credit card information) he could connect me with someone who could get all my data back.**

From now on, I am going to duplicate the most important of the information onto my own hard drive which I will continue to backup regularly. At present that will just be copy and paste of important text involving customers to my customer database.

In addition to picking a few things to copy to individual customer files on a database on my local hard drive, I will be forwarding emails to my private Web site email address, a practice detailed in an Internet article I recommend everyone read, "Take Control of Your Email Address". See it at this link: https://konklone.com/post/take-control-of-your-email-address. I ran across that wonderful, specific and instructive piece of work when I was researching ways of putting control of my own data back into my own hands.

That thought-provoking article reviews about how we enjoy the government protected right of mandated portability where our cell phones are concerned, but our email address situation is just the opposite. In other words, if we are unhappy with AT&T we can pick up our marbles and our phone number and go elsewhere. If we couldn't do that, we would feel tied to one phone company due to the difficulty changing our number would cause us. Well, isn't that the situation we are in with email? Imagine if one could pick an email address for a lifetime. It can be done and this article covers the nuts and bolts of it. And, that is just the first step to control. How and where data is stored is the second.

If folks reading this editorial get nothing more out of it then to go check out the Internet article "Take Control of Your Email Address" https://konklone.com/post/take-control-of-your-email-address, then I would be happy, or, channeling Dr. Seuss, Wappity Boppity Happa-dilly-ish-is.

Linda Windler and her husband Merle are owners of Thoroughbred Systems, Inc., Topeka. The company specializes in utility billing for cities and rural districts, computer networking and associated training. Contact: lindawindler@yahoo.com