By Merle Windler, Thoroughbred Systems, Inc.

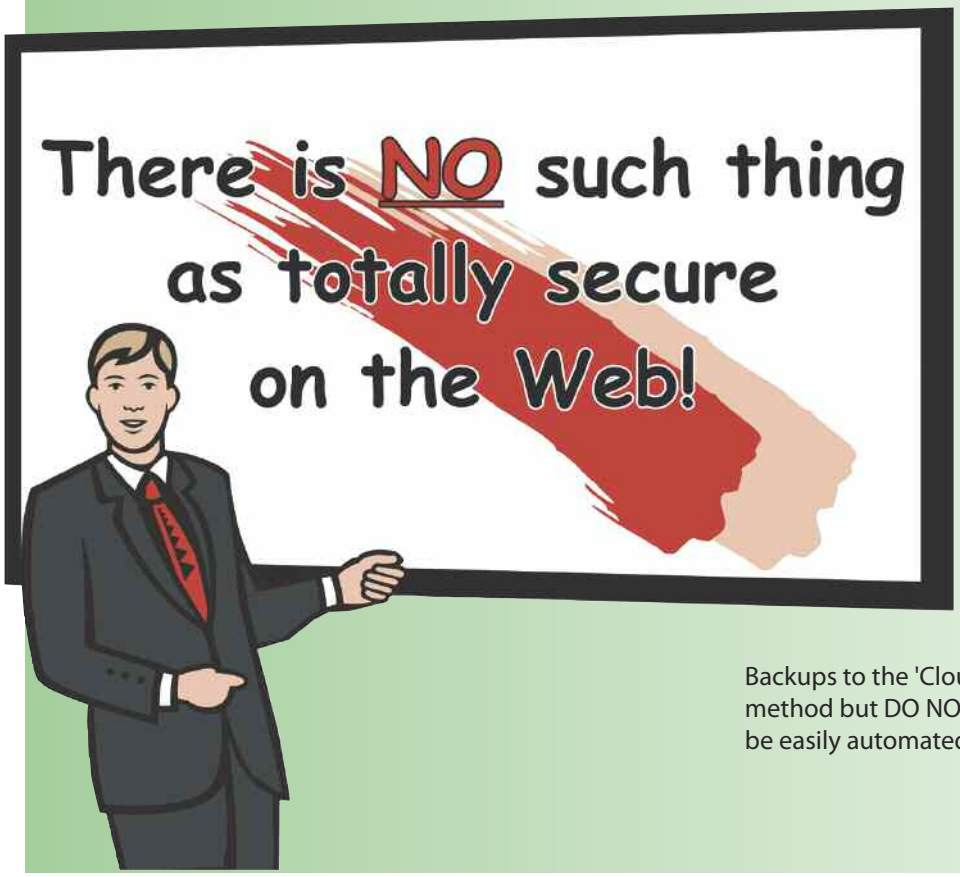
Computer Corner

The Ever-Changing Tech World

For many years we have attended an international conference for software developers every three years. In the last few years it has been offered every two years; they announced at this year's meeting that this would remain a permanent change. Why? Because computer technology now evolves and grows at such a rate that three years just isn't sufficient. More than half of the attendees were from outside the United States. They came from Australia, Croatia, Greece, South Africa, Canada, England, Belgium and so many more places all over the globe. They do programming for companies, agencies, and governments on nearly every continent.

The three biggest topics of the conference were: 1) Web Applications; 2) Mobile Applications; and, 3) Security. Security was the hottest topic at this year's gathering. There were many exciting new technologies, software development tools, integration of software using multiple languages and data formats, and information on modernizing existing applications to integrate in the ever-changing tech world. Our heads are "swimming" in ideas of what we can do to implement these technologies for our customers' benefit.

I will make a few generalizations and statements as take-a-ways of the most important information from the conference that directly applies to rural water districts and small city offices.



1. ALL Microsoft Windows computers should be upgraded to Windows 10 or replaced with new computers using Windows 10 by January 14th, 2020, Time is running low! (Server versions excepted.)

2. Users need to take responsibility for their own data!

Here is a statement I frequently heard during the conference: "...All businesses and government offices should at a minimum have at least TWO 'Onsite' detachable backup devices that store regularly accomplished backups that are rotated to a safe storage location like a fireproof safe, fireproof cabinet, or safe deposit box. Backups to the 'Cloud' are OK as a supplemental backup method but DO NOT meet this need! (These backups can be easily automated with a 'batch file' and Windows

scheduler or software backup program.) An IT person should test the Restoration capability at least once each year..."

We heard this statement repeatedly from world-class programmers, and internationally-respected session speakers during the conference.

During the week of our conference in the Sunshine State, the State of Florida and three cities in Florida were successfully attacked by ransomware. Ransomware is malicious malware software designed to deny the user access to their own data by encrypting the data and making it inaccessible to its owner, for the purpose of extorting money. Already this year, Ransomware attacks have cost U.S. businesses and government entities hundreds of millions of dollars. Are you thinking, "That's only a problem for the big fish?" Think again! Falling victim to a ransomware attack can be as simple as clicking an attachment on a deceptively innocent looking email. The newest ransomware attacks search computers and networks to attack backup devices as well.

Ransomware is malicious malware software designed to deny the user access to their own data by encrypting the data and making it inaccessible to its owner, for the purpose of extorting money.

3. Carefully consider WHAT data is exposed to the Internet.

If your data doesn't need to be exposed to the Internet, then why do so? One of the session speakers gave examples of a medical client exposing Social Security numbers, dates of birth, and other personal information on a Web-based program when there was no real need for such data to even be included in the records that were saved on the Web. They had always done it that way and never gave a thought to potential patient data exposure.

4. Use Safe Practices, tools and applications to give the maximum protection possible.

Poor password practices by employees are one of the largest risks for any organization. Reusing the same password on numerous sites, using common passwords: '1234' and 'Password' are the most used, a person's favorite car and other things posted on social media are also typical mistakes. And, finally, saving a password on the device or inputting the password over an unsecured network is risky.

On an Open WIFI network always ensure Windows settings are selected for privacy.

As an example of safe computer practices, during the conference we were working with one of our customers over the Internet from the hotel room using a Virtual Private Network (VPN) as we have recommended in previous articles. A VPN encrypts our Internet activities and protects both our customer's data and our own. While connected, we noticed other hotel guest's information was readily available to anyone that wanted to view their photos and documents on their computer over the hotel's open WIFI network because they failed to follow simple safety practices when using an open WIFI network.

On an Open WIFI network always ensure Windows settings are selected for privacy. To do that, go to: Network and Sharing Center, then Change 'Advanced Sharing Settings', then Turn OFF 'Network Discovery' and Turn OFF 'File and Printer Sharing'.

Those other hotel guests were unknowingly putting themselves at risk – exposing to anyone within WIFI range the opportunity to view their personal documents and photos.

5. New technologies are in stores today and more are coming every month.

New WIFI 6 compliant hardware now available includes Routers, Mobile Phones, and Laptops. This is the biggest leap in WIFI technology and WIFI security improvements in more than a decade. But, BEFORE purchasing, it is imperative to check that the local provider is ready to support the new technology. Many rural area providers may be slow in adopting this new technology, as it will require quite an investment in infrastructure to support it.

A new generation of 5g mobile network devices like "always connected" laptops are coming but still a ways off. 5g is aimed at dramatically increasing speeds of mobile networks and unleashing options to rival WIFI services. Some exciting changes are in the future but most appear to be several years or more from viability. Mobile Plan data limits, cost of data plans, and data throttling (slowing data throughput when data limits are exceeded) are some of the problems that will need to be overcome.

This year personal privacy rights became a concern to users of voice activated assistants like Alexa, Apple Siri, Google Assistant and Microsoft Cortana. Controversy erupted when it was revealed that in order to improve device function providers reviewed some recordings of the "always listening" devices. Some of the recordings reviewed included sensitive audio, such as doctor-patient conversations and people having sex. Amazon's Ring video doorbell has also been criticized for partnering with hundreds of police departments who in some cases gave the devices away to persons willing to grant police the authority to use video captured by the devices for investigative purposes. Some advocacy groups assert this as the start of a surveillance network.

The Net Neutrality issue continues. Net neutrality is the idea that all traffic on the Internet should be treated equally, i.e., nothing could be throttled, given priority, blocked, or otherwise interfered with. In order to ensure this, proponents say, the government needs to regulate the Internet. Others oppose any interference of the government on Internet Services. The debate continues in the Courts and Congress.

They in no way we are suggesting people do not use the Web but that when using the Internet one must do so with full knowledge of the possible threats.

There was not a single session that did not include the stressing of security. One of the sessions the first slide the presenter put up read… "There is NO such thing as totally secure on the Web!"

In no way we are suggesting people not use the Web but that when using the Internet one must do so with full knowledge of the possible threats.

YOU are responsible to protect yourself and your local water district or municipal office. Quite often, it is YOU and the actions of staff that are the "weakest" security link. Be safe out there.

Merle Windler and his wife Linda are owners of Thoroughbred Systems, Topeka. The company specializes in software solutions for utilities and municipalities, computer networking and associated training. Contact: merlewindler@yahoo.com

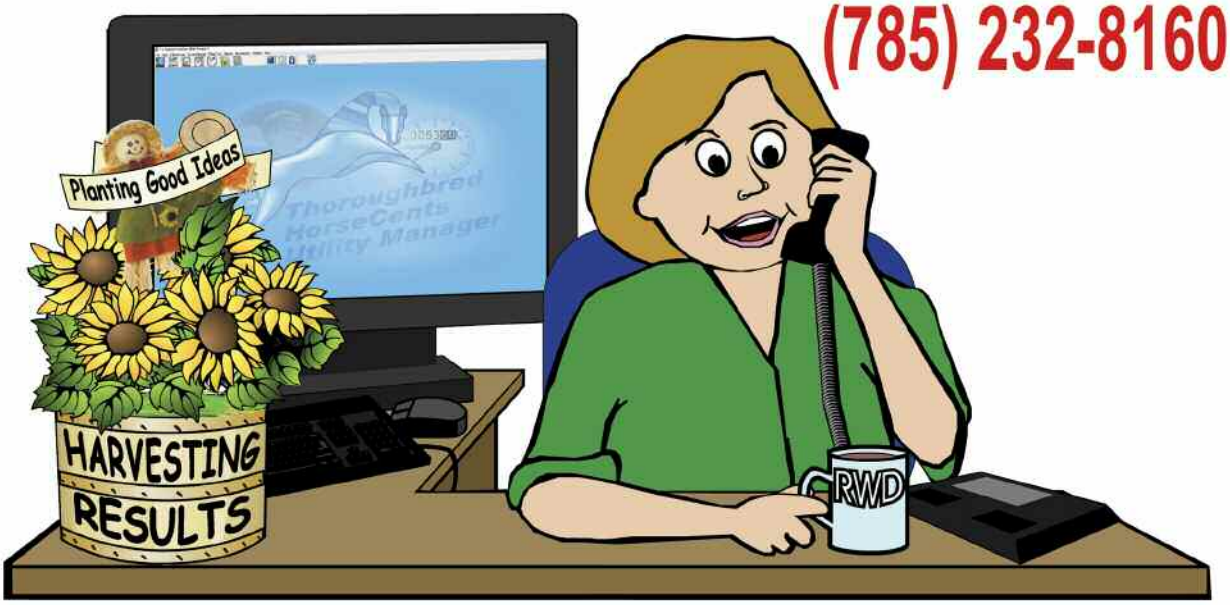
Thoroughbred Systems

Thoroughbred Systems.com

Software Products for Cities and Water Districts

116 S. E. 8th Avenue Topeka, Ks 66603-3905

(785) 232-8160



We've used Thoroughbred for years, even back when the customers read their own meters. We're really hi-tech these days with the latest version of Thoroughbred and Windows 10. I send traditional printed bills through the U.S. Mail to less than half of my customers now, 'cuz now we also have things like email notices & billing, automatic banking & Credit Card Pay. The program's like Burger King, it "Lets us have it our way", with queries and custom reports. There are tons of features that help with everything from water loss to keeping on top of delinquent accounts, rate code studies, work orders, mail merge letters, you name it, all for a low purchase price. Best of all, human beings answer the phone & help me for FREE! You'll love it, startup training can be in person in the water office or via the phone & Internet. And, there are **NO YEARLY FEES**, I get FREE tech support and FREE upgrades for five years. ***Now, if they could just teach my computer to serve up a hot cup of coffee in the morning, IT WOULD BE PERFECT!!!!***