



Bexar County IT News

February 2014



Responsive Design Comes to Bexar County

Since its inception, the Internet has been constantly changing and growing, and the ways we interact with it have also changed as new technologies have developed. In the past a computer was the primary method of accessing the internet, but today the ways we can get online are myriad. Smart phones, tablets, stand-alone kiosks, eReaders, gaming consoles, televisions and even refrigerators are now connected to the internet.

For web designers and developers the variety of devices has provided a unique challenge for ensuring users can access a website regardless of the method they choose. Gone are the days of developing a design meant to fit a particular screen size. In an effort to meet this challenge head on, a new technique was developed called responsive design.

Through a variety of methods, a responsive website is a website built to function across all devices in an effort to give the user the best experience possible without having to support multiple sites or versions of content. In its simplest terms, responsive design adapts the layout of a website to the user's viewing device.

As part of the mission to ensure all users can access Bexar County content, BCIT has begun to work with responsive design and strives to ensure that all our websites will be mobile-friendly!





There's a New Peace Officer in Town



For many years Bexar County has included a “Sheriff’s Fee” as a standard part of assessed court costs. Texas Code of Criminal Procedure Article 102.11 provides for a suite of Peace Officer fees, paying law enforcement agencies for services and reimbursing them for certain expenses incurred during transportation of a defendant or witness. As an example, the amount of the Peace Officer fees for a given case might be the total of:

- \$50 per warrant
- \$5 per booking
- \$10 per bond made
- \$5 per release on bond
- \$5 per subpoena served
- \$35 per writ
- \$5 if a jury was summoned
- customary amount for participation in an exam trial, not to exceed \$5
- for transport of a defendant or witness:
 - ◊ \$0.29 per mile
 - ◊ Per diem of \$10 per day or part thereof
 - ◊ Reasonable travel expenses
 - ◊ Overtime

Court Clerks have been burdened for years by having to conduct tedious manual searches through event histories and witness lists for each case, tallying by hand the number of warrants, bookings and subpoenas and adjusting the fee amount before printing each Bill of Cost. Senior management at the District Clerk’s Office has been lobbying for many years to replace the “Sheriff’s fee” with individual Peace Officer fees, and recently BCIT took on the task of making this possible.

As a result of these efforts, Peace Officer fees are a reality as of January 2nd, 2014! With the implementation of this software upgrade, we’ll be able to assess accurate amounts for Court Costs much more quickly and easily than ever before. Assigning reimbursements will remain a manual process since these are not captured in event codes, but clerks have been given a new screen to input those numbers as needed. The system does the work of reading event histories and witness lists to calculate the event-driven fees, and with the touch a button, clerks can now see both the total and a detailed breakdown of fees and reimbursements.





Passwords: The Keys to Security

Passwords are ubiquitous in today's society. If you have a computer and go online, you have at least one password. Between work and home accounts, chances are there are dozens of places where you have to use a password. They help protect sensitive information from falling into the wrong hands. Cybercriminals are constantly trying to steal the valuable data that you possess. So why would you use a password that is easy for them to figure out?

The Bexar County Information Technology Department has password protocols and rules in place for the various systems our employees use; and these rules are designed to help prevent security breaches. The individual employee also bears a serious responsibility to maintain this security by creating strong passwords. Here are some suggestions for producing good ones for work *and* for personal use:

The longer and more complex a password is, the stronger it is. Try to incorporate the following rules when creating passwords.

- Use all the characters on the keyboard including letters, punctuation, symbols, and numbers - not just the letters and characters you use or see most often.
- Whenever possible, use eight characters or more.
- Don't use the same password for everything. (Criminals steal passwords on sites with very little security, and then use that same password and user name in more secure environments, such as banking websites.)
- Change your passwords often. A good rule of thumb is to change your passwords on your email, banking, and credit card websites about every three months.
- The greater the variety of characters in your password, the better. (However, password hacking software automatically checks for common letter-to-symbol conversions, such as changing "and" to "&" or "to" to "2.")
- Avoid creating passwords that use dictionary words in any language, words spelled backwards, common misspellings and abbreviations, sequences or repeated characters, such as: 12345678, 222222, abcdefg, or qwerty.
- Don't include personal information such as your name, birthday, driver's license, passport number, or similar information.

Once you have made up a password you think is robust enough, test your password with a password checker. A password checker evaluates your password's strength automatically. There are numerous password checkers online such as this one from Microsoft <https://www.microsoft.com/en-gb/security/pc-security/password-checker.aspx> . Open one up and test some tentative passwords. But whatever you do, don't use one of the passwords shown below. Cybercriminals with sophisticated hacking software will get these in a split second!

(Continued on page 4)





(Continued from page 3)

In an effort to prevent users adopting what it describes as "weak and easily guessable" choices, the password management company SplashData has just released its list of the 25 worst passwords of 2013.

(1) 123456	(6) 123456789	(11) 123123	(16) 1234	(21) password1
(2) password	(7) 111111	(12) admin	(17) monkey	(22) princess
(3) 12345678	(8) 1234567	(13) 1234567890	(18) shadow	(23) azerty
(4) qwerty	(9) iloveyou	(14) letmein	(19) sunshine	(24) trustno1
(5) abc123	(10) adobe123	(15) photoshop	(20) 12345	(25) 000000

See anything familiar? You would be well advised to get rid of it right away!

Unsung Heroes

David Bradley, inventor of the 'three-fingered salute'. David Bradley says he has accomplished many difficult feats in technology over the years, but becoming best known for inventing the so-called "three-finger salute" - Ctrl-Alt-Delete - to soft boot a computer wasn't part of his original career plan.

But back in those early days, the need to reboot "would happen a lot," Bradley says. "Depending on what you were working on, that could be daily, hourly, even every five minutes if you were working on a particular shortcut."

So Bradley came up with the Ctrl-Alt-Del keystroke combination -- three keys distant enough on the keyboard to make it virtually impossible for someone to hit all three accidentally and simultaneously. "So, if you hit those keys, instead of taking a minute to start up the PC again, it would be much quicker -- the equivalent of turning the machine off and on without running POST."

The combination escaped from IBM labs and hit popular culture when application developers, in the days when programs ran on diskette, decided to publish the combination to help users start their applications faster. After that, end users got used to it, and the rest is, well, history.

Ted Nelson, hypertext creator. The next time you click a link online, raise a metaphorical cup to Ted Nelson. The curmudgeonly Nelson came up with the concepts and terms for "hypertext," "hypermedia," "virtuality" and "micropayment" -- and he did it in 1960.

That was the year, Nelson says, that he first thought up the idea of a "nonsequential" document. In his first year as a Harvard graduate student in sociology, he imagined a global, networked computer system. He envisioned a world where personal computers were ubiquitous and people could navigate their own, individualized paths through the world's art and literature by using "hypertext" links to related documents. They might even legally buy portions of them. Nelson ultimately described his ideas in a paper submitted to the Association for Computing Machinery in 1965. Later on, he elaborated on them in his books Computer Lib/Dream Machines (1974) and Literary Machines (1981).

