Ed Kipp
Cybersecurity

I first attended college back in the days where your student ID was your social security number. You would take a midterm and the grades would be posted in a list, and you would have to find your social security number to look up your grade. The internet existed, but most people did not know what it was or how to use it. Credit card transactions at the gas station I worked at used carbon paper receipts run through an imprinter. Privacy was almost an afterthought.

With the internet explosion occurring in the years leading up to the millennium, the need for privacy started becoming more necessary. Universities started changing student IDs, credit card transactions were done via an online card reader, and receipts only showed the last four digits. I remember getting phone calls regarding defaulting on the loan for my Toyota 4-Runner – a vehicle I have never owned. The caller would ask for my social security number, but my mom had told me only to give the last four digits. That usually ended the call, either because they were trying to get my entire SSN and could not, or because it was a legitimate call and they realized they had called the wrong person.

With the discovery of the Equifax data breach last year, questions need to be asked – if one of the three agencies responsible for maintaining our most sensitive personally identifiable information cannot keep it safe, who can we trust with it? What security standards need to be in place to keep that information safe, and who should be enforcing those standards? If the majority of people have had their information stolen, should we take the opportunity to create a new standard and type of identifier? And who is trustworthy enough to pull together the standards of protecting whatever data we decide is the new standard?

Security is everyone's responsibility.
SecuringInfo@sdcoe.net - 858-292-3626 - sdcoe.net/cybersecurity
Awareness / Procedures / Training / Vulnerability Assessment