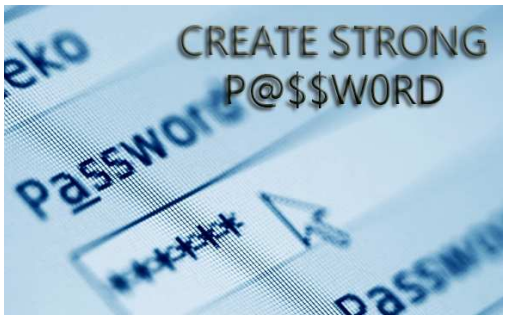
Logon Security



Security is a HUGE issue.
Every responsible business has to ensure that the business's security is top notch. Each user is responsible to use those resources correctly. When we say "resources" we mean logon security, procedures and protecting information. Business owner/Managers must trust that everyone entrusted with the use of your systems are protecting it the best they can.

What should you be doing & what are the best practices?
It all starts with Logon. Two factor authentication (2FA) is currently the most secure way to protect information from logon hacking. In the not too distant future there will be other, more advanced methods to access systems, but for now the best is 2FA.

After logon, understanding how data is protected and when is important. Data needs to be protected in three forms: In transit, in use and at rest. Those are pretty self-explanatory, but the technology to protect data in each of those forms is not. In Transit requires one or more types encryption. In use requires desktop security and at rest requires different encryption.

If any of this strikes interest, give us a call to chat.