a car door ten or twelve times.

It's not that I don't understand network security, or don't want to keep my data secure. It's just that there is no human way to juggle the thousands of unique, 8-character or greater passwords with capital letters, lowercase letters, numbers and at least one "unique" characters that today's security systems demand. I can't remember them, and neither can you.

You want to know the easiest way to hack into a corporate network? Just look at the edge of the monitor or in the center desk drawer of most network users, and you will find their user name and password written on a sticky note for every visitor or janitor to use.

As IT professionals, we have done a crummy job of helping end users manage the security of their data, and those users have responded by simply ignoring us. Sure, their are a few programs like Roboform and Lastpass — or, God forbid, the dreadful Credential Manager built into Windows — that you can try to use to juggle your thousands of passwords, assuming you have unlimited to to enter and update each password you use.

But the problem with these and every other scheme I have tested is that they are, in password lingo, 2ComPl1cat3d! Oh, wait. That's not bad. I may want to use that next month as my network logon password...

Network geeks, in the insane assumption that they are rendering their networks and web sites more secure by all of this password nonsense, have again accomplished the opposite. End users have responded to their irrational demands by using the same user name and password for every site. Or by writing their passwords down in a place they (and everyone else) can easily find them. Or, god forbid, by keeping a text

file of all of their user names and password in an Outlook Note, synchronized to their

passwords need to be stored somewhere, and that means that you have to use a password — probably something that you have to change every month for security reasons — to access where you store your passwords. And you still have to enter and manage them manually.

And then there is the problem of mobility. Unless you plan to give up your Blackberry, your iPad and a slew of other devices, your office computer password manager won't help you a bit on the road. You'll have to create an Outlook Note and sync it to...oh, heck, that's what you do today.

I give Microsoft a B+ for recognizing (downgraded from an A for not doing so 20 years ago!) that this is an untenable situation that makes networks and sites less secure, not more. And a C- for not coming up with a better solution that trying to force users into a Microsoft-only world in order to feel more secure.

My guess is that there is an app here just waiting to be written, and that the first company to come up with a solution will become wealthy beyond their dreams. I also believe that once such a system exists, and we can truly be secure in what we do online, marketers and governments will do their best to keep us from using those technologies in the name of commerce. Or security. Or something.

Which is why it is still 2ComPl1cat3d! to do today.