KEEP YOUR DATA SAFE AND SOUND

> How valuable are your point of sale (POS) data, customer information, emails, bank accounts and other financial statements? You back that information up of course. (Right?) But have you taken steps to protect data from being stolen? Data security can seem intimidating, so this month we're going to look at several approaches to securing it.

Strategy No. 1: Hide It

The first way to protect your data is to use "security through obscurity." This approach involves putting the data somewhere it's not likely to be found; it's like hiding a diary under a pillow or at the bottom of a drawer.

For computer files on your local network, you can give them a misleading name or place them in a misleading directory. It's a simple plan, but not always practical — you can't hide data flowing over your wireless network (more on that later) — and it's never truly secure.

Have you ever opened your wireless network settings and seen the names of available wireless networks, also known as Service Set Identification? If you're broadcasting your SSID, your network will appear in that list. Disable broadcasting in your router settings and it won't.

Again, don't mistake this for real security. Your network and data will still be visible to even intermediate scoundrels, but these steps help ensure that you are not the lowest-hanging fruit.

Strategy No. 2: Lock It Up

The second strategy involves restricting access to information. In the case of a diary, this means locking it with a combination or key. In the case of your electronic files, it typically involves passwords and file permissions that determine which users have access to specific data.

The shared weakness is that if the lock/password is broken/bypassed (and user account passwords often are) the information is exposed.

Unfortunately, there is no absolute way to prevent access to the information that travels over your wireless network. It is out there and anyone within range can intercept it.

Strategy No. 3: Encrypt It

Encryption involves using a cipher (something like a formula) and a key (sometimes referred to as a password, although the two are technically different). With this approach, you securely encrypt your data so that if it is exposed, the unauthorized viewer sees unintelligible gibberish.

Here is an example of the word "hello" encrypted using the Advanced Encryption Standard (AES) 256 and the (very weak, used for demonstration purposes only) key "abc":

Ls9GpPbMtoSBgwi7urwJs31jdXKeqjie+XojAkJM6s4=

Here it is again using the same standard and the key "abd":

RcuBkqFhK4gsiRpiZFfftKDW2rwVFPKzlCVi21s8/nA=

Looks pretty secure right? The NSA has even approved it for securing "top secret" information.

Apple offers a built-in whole-disk encryption tool called FileVault. It encrypts all the data on your hard drive and should be considered for most users, especially those with laptops. There are also utilities that allow you to encrypt individual directories and files.

On the PC side, there are many paid programs you can use, just Google "PC encryption software," but consider TrueCrypt (**http://www.truecrypt.org**), a great, free solution. TrueCrypt also runs on Mac and Linux machines.

For your wireless network, encryption is your best defense. The good news is that the kind of NSA-grade security we mentioned above is probably built into your router; you just need to make sure it is configured correctly.

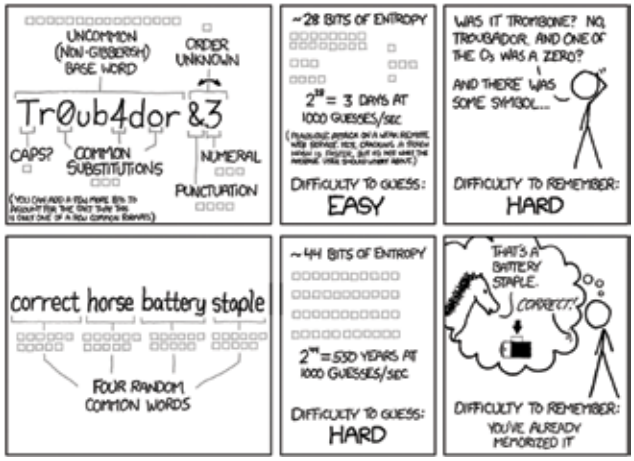
Most wireless routers allow you to select from a number of different encryption standards, including WEP, WPA & WPA2. WEP is the oldest and least secure and should be avoided. Use WPA2, which is the strongest option. Remember, though, that your wireless network is only as strong as the weakest link in your chain. If you have legacy hardware that only supports WEP, consider replacing these devices. A quick fix is to purchase a USB wireless network adapter that supports WPA2 ($20 to $30).

Strategy No. 4: Create Strong Passwords

The old approach of complex and hard to remember passwords (example: "Tr0ub4dor&3") is considered less secure than longer, more human-friendly passwords made up of real words (example: "correcthorsebatterystole").

Why? It involves serious math but knowledgeable hackers would crack "Tr0ub4dor&3" in three days (see graphic). It would require 550 years to crack "correcthorsebatterystaple." And the second one is a lot easier to remember!

Mark Anderson is founder of order-taking and point-of-sale system Floristware. **mark@floristware.com**



MIND BENDER An online comic strip (**http://xkcd.com/936/**) illustrates how we've been trained to create passwords that are hard for humans to remember but easy for computers to guess, such as "Tr0ub4dor&3," versus the other way around, as in the case of the random four-word sequence "correcthorsebatterystaple."