

## A Guide to Better Password Practices

Recently, a few of our customers had their email accounts hijacked. The person or program that commandeered the email accounts caused them to send pornographic links to friends, family, and acquaintances in these customers' contact lists.

While the above situation is more of an embarrassment than a threat to your privacy, think of the implications of an attacker gaining access to your bank account. Or if they got access to your personal information, including your social security number and started opening up credit card or other accounts in your name.

It is very common for trespassers to attempt to break-in to computers & online accounts by trying to guess user-ids and passwords. Most people use passwords that are based on personal information and are easy to remember. But that also make it easier for an attacker to guess or "crack" them.

While there is no perfect password, we recommend to all individuals that they create passwords (including those used for email) that are considered "strong" by industry standards. To be a "strong" password, it must be at least 8 characters long and include 3 out of the 4 following categories: upper case letters, lower case letters, random numbers, and special characters (such as \$, @, or #).

Do not choose passwords based on your personal information like your name or other information about you that could easily found by searching the Internet. Don't use proper names, famous quotations, song lyrics, the name of a TV show, or words that can be found in the dictionary.

You can pick a word phrase that is meaningful to you, and then mix it up a bit by using both upper & lower case letters and replacing some of the letters with numbers and/or special characters. Don't write your password down and leave it next to your computer or taped to the screen. Don't share your password with anyone, and beware of phishing attacks that try to trick you via email into giving out your passwords.

We also advise using care when using computers that aren't your own (such as computers in a kiosk), as such computers could have a Spyware program installed on them to capture keystrokes and send sensitive information over the Internet including your user account and passwords. Also, use caution when connecting to the Internet via an unsecured public wireless connection (i.e. at a local coffee shop or at a hotel).

Finally, be sure to keep your own computer free of Spyware by periodically running an anti-spyware application to insure your keystrokes are not being transmitted over the Internet to someone else.