

IT Security - The New World Lock and Key

By: [Joe Miljan](#)

It's another Monday morning at the office, you've just turned on your computer and logged in - all of a sudden you start to notice that your "Home Page" is changed, your computer is very slow and finally the internet connection is extremely slow.... ***Your IT Network has just been Hacked!***



Security in the workplace has been an issue for years yet something commonly thought of as "internal security" such as cameras and locked doors. Today the world has grown and evolved into a computer driven technology, providing innovative e-criminals the opportunity to take advantage of this situation and they are benefiting by your lack of network security knowledge and use of older technology. Now more than ever, there are important types of security needs such as Firewalls, Network Lockdowns, Key Fobs, Passwords and so on, that are needed to secure a companies sensitive records, financial information and their basic lifeline to keep them in business.

Some businesses don't know what they're exposing themselves to, but with an "opened port" on a firewall or router leading to their database or "hole" in the network, the world is able to look at your sensitive material without you even knowing until it's too late. (Take the [Security Test](#) online)

Last month a new company signed on for simple "network support" because they felt their previous IT provider was not giving them the patience they feel they deserved. When our engineer did a network audit we noticed that the tape backup's have not been successful in over 2 months! With that alone a red flag should have gone up. More problems were found... much more! Every port on the firewall was open allowing anyone into the server which nullified the purpose of the firewall entirely.

And to add misery to suffering... Half the staff knew the Administrator Password!!! (*Simple passwords are not enough... did you know that the most common password used today is "password" and the second most common is "admin"? Many users have half a dozen passwords to remember which is why the most common password is 'password.'* The usual solution is to write it down. But how secure is that?) This oversight allowed anyone into the system to change, delete or add anything they wanted... what if one of these people became a "disgruntled employee" later down the line? Finally we stumbled upon another serious issue that could have been disastrous... After the previous IT person was "dismissed" they were trying to hack into the

system using “previous employees passwords” (which worked) and decided to try and delete files as well as “hide” mistakes they made. Luckily we tracked everything they did by backing the system up successfully in case anything like this happened!



Makes you wish we could go back to the old days when we had a safe with paperwork in it or a filing cabinet with a lock on it that held our businesses most prized possessions. Today, this information is resting in your servers, networked to the staff and then to the internet for fast and easy day to day operations bringing business to what we once called “The future of doing business”. With this new system that has treated us well in the past decade or so, we have neglected to see what other possibilities are growing out there such as network hacking, malicious script sent through email in the form of humour from a trusted source, which destroys our data or even worse, a complete breakdown of our network and loss of all information.

Another item I wanted to touch upon was something I stumbled upon last month when a new client came on board and asked simply if we could upgrade their server. The company in this situation changed their IT Firm service to LIBRA IT because they felt like they needed and wanted more experienced engineering in their technical arena.

When this high security *Financial* company signed on we had no idea what we were about to stumble on! If you look at some URL's you will notice most of them start with an *http://*. But then you come across the “secure connections” used by companies like financial or legal institutions which look like this *https://* where the “S” is to signify that it's a secure site and no one can get in unless authorized with log in and password. What this financial company didn't know was that their “secure site” was in no way shape or form secure! Here's how the previous IT firm did it.. To cut corners, their previous IT Firm decided to send all “secure traffic URL” to one web-server housing the main page under the URL *https://* but then translated this to simple *http://* to retrieve the requested “financial data” for the client from another server (being the data storage server). The traffic is then sent back to the first server which once again translated the *http://* to *https://* to again make it look secure! The information was finally sent to the client unbeknownst to them that their personal financial data has no security whatsoever. This was immediately rectified and security was finally restored but with a lesson... when you have security implemented into your network, get certificates of authentication for your records or you may find that you too are exposed to the world of hackers and prying eyes.