HOW TO CREATE A SECURE PASSWORD

INTRODUCTION

Passwords, passwords, love 'em or hate them!

Too many to remember and who doesn't write them down – is that safe?

Ever wonder how to create a safe and secure password that is impossible to crack?

We are here to help!

RESOUCES NEEDED:

o   Your imagination or a random word generator
o   A good memory or a safe to keep them under lock and key

Some fun facts about passwords:

o   Longer the better – 10-20 characters are great – the longer the password, the harder it is for someone to crack
o   Don't use words or phases that link to who you are, where you have lived -- street name, city you were born, date you were married, your business name, your business owner, kids names or birthdays
o   Change your password every three months or when prompted by the service you are using
o   Each password should only be use for one service. Don't reuse your passwords.
o   Each password should only be used on one website. To manage these passwords, a password vault program such as KeePass can be used to store the unique passwords associated with the website. Backup services such as SpiderOak or Dropbox can be used to keep this password vault backed up.

STEP- BY-STEP INSTRUCTIONS

1. Imagination – we know you are busy and don't have time to think up unique and creative passwords, so here's a suggestion:

Use a random word generator. Like the link below:

http://www.textfixer.com/tools/random-words.php

Pick 2-3 words add some numbers, unique characters and a capital letter – and you are ready to go!

Like this: noble3$kitten72True – 19 characters!

2. Safe storage – we know you can't remember all these passwords, and you have a lot more important things to remember to keep your business running. If you have to write them down, don't store them in a file on your computer!! Write them down and lock them up, just like you would for an extra set of your car or warehouse keys, or lock combinations. These should be treated as any other "critical data" that needs to be kept in a secure location.

There are commercial products to store passwords, such as KeePass and backup services such as SpiderOak or Dropbox – all can be used to keep your password backed up and encrypted.

Still have questions, need help? Contact us at our "Ask-an-expert" service or at the link below.

COMMENTS/SUGGESTIONS/FEEDBACK ARE ALWAYS WELCOME AT WEB@THENCSS.ORG