BLACK LABEL IT

Password Management Guide

Learn How to Protect Yourself and Your Company from Sensitive Data Loss

INTRODUCTION

DEFINING A STRONG PASSWORD

Nefarious individuals and cyber attackers are on the hunt to break-through your security walls and defeat your passwords.

Keep in mind that passwords are simply the walls around your IT network. Just like a castle, it doesn't matter how strong your walls are if the lock can easily be picked. If every possible password is attempted, sooner or later yours will be found.

The question you must ask is, "Will your passwords be unlocked too soon, or will you have security measures in place that will protect you from intrusion?"

Many people believe that a strong password must be nearly impossible to remember. The fact of the matter is, it doesn't. As long as you follow a couple of naming conventions, you can easily develop and remember a strong password.

The best theory to adhere to is called "Password Haystack" and is defined by Steve Gibson of GRC. "Every password you use, can be thought of as a needle hiding in a haystack." His theory addresses how passwords can stack up against possible cyber-attacks. With just a couple of tricks you can create passwords that are nearly impossible to break.[1]

[1] https://www.grc.com/haystack.htm

PASSWORD HAYSTACK EXAMPLES

GRC's Interactive Brute Force Password "Search Space" Calculator

3 Uppercase | 5 Lowercase | 2 Digits | 1 Symbol | 11 Characters

swBDJune14!

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	**26+26+10+33=95**
Search Space Length(Characters):	**11 characters**
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	**5,748 511,570,879,116,626,495**
Search Space Size(as power of 10):	**5.75×10^{21}**

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	**1.83 billion centuries**
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	**18.23 centuries**
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	**1.83 years**

GRC's Interactive Brute Force Password "Search Space" Calculator

2 Uppercase | 9 Lowercase | 1 Digits | 4 Symbol | 16 Characters

1 Like Waffles !

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	**26+26+10+33=95**
Search Space Length(Characters):	**16 characters**
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	**44,480,886,725,444,405, 624,219,204,517,120**
Search Space Size(as power of 10):	**4.45×10^{31}**

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	**14.14 million trillion centuries**
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	**1.41 hundred billion centuries**
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	**1.41 hundred million centuries**

PASSWORD HAYSTACK EXAMPLES

GRC's Interactive Brute Force Password "Search Space" Calculator

1 Uppercase | 4 Lowercase | 1 Digits | No Symbols | 6 Characters

Admin1

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	**26+26+10=62**
Search Space Length(Characters):	**6 characters**
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	**57,731,386,986**
Search Space Size(as power of 10):	**5.77×10^{10}**

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	**1.84 years**
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	**0.577 seconds**
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	**0.000577 seconds**

GRC's Interactive Brute Force Password "Search Space" Calculator

1 Uppercase | 5 Lowercase | 2 Digits | 2 Symbols | 10 Characters

Pa$$word12

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	**26+26+10+33=95**
Search Space Length(Characters):	**10 characters**
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	**60,510,648,114,517,017, 120**
Search Space Size(as power of 10):	**6.05×10^{19}**

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	**19.24 million centuries**
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	**19.24 years**
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	**1.00 weeks**

Password Rotation Advisement

Password retention and rotation policies can pose a challenge to any organization. The more devices you have, the more work is needed.

However, this is where a strong RMM (Remote Monitoring and Management) platform can help. The RMM's tools will help you automate procedures.

When choosing how often to rotate your passwords, it is best to define how long it will take to change them. You should consider how many devices you need to manage today and how many devices you will need to manage in a year from now, or two years from now. Identify the labor involved and your interest in protecting your equipment. This will help you determine what is reasonable for your situation.

A "Best of Breed" password policy commonly requires rotating passwords, at least on the most vulnerable equipment, every 30 to 180 days. In the IT business, we always consider end users and the labor involved to change passwords. Once you establish good habits, changing passwords every 45 to 60 days should suffice and is most common.

Access Control to Your Password Stores

STORAGE

Storing passwords is a challenge for most companies. Currently, there is not one best solution. Be assured, the industry is working on it. Unfortunately, there's nothing perfect or standardized in this space as of yet.

PLATFORMS

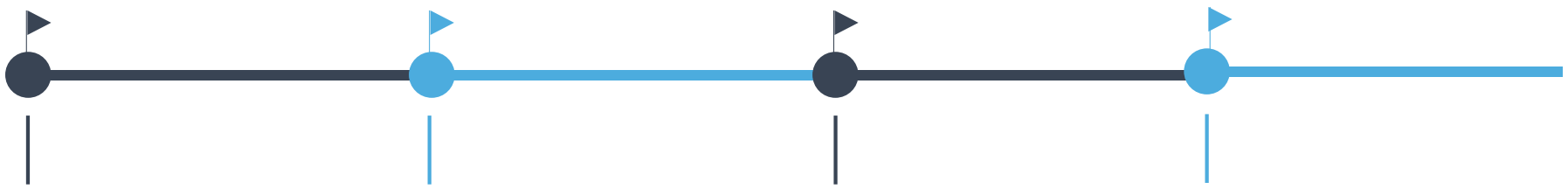
For now, choose a platform that best suits your needs. The available applications need a prudent review. Weigh the convenience of their use. If you choose a cloud option, be sure that there are protections that prevent the cloud operator from accessing your data. If you choose a locally stored option, know who is delegating access. When possible, use technology that tracks access to your passwords or files containing your passwords.

ALERTS

It is also important to set up alerts and general reports. If a desktop or an unknown IP address is accessing your passwords, you'll want to know immediately.

If you do choose to store your passwords locally, ensure that the filing technology supports encryption such as EFS or Bitlocker. Use firewalls and access controls on your network to designate who can access your data and from where.

OPTIONS TO CONSIDER



PASSWORD MANAGEMENT SOFTWARE

Last Pass, Enpass, 1 Pass

- Cloud based, accessible from anywhere, app driven.
- Employees “Trust No One” technology, the vendor themselves can’t reverse access
- If you loose access it might be permanent.
- Supports delegation and multi-factor authentication.

FILE SERVER with NTFS ACCESS CONTROL

- Encryption.
- Group and Individual ACL’s on file.
- Integrates into your business network seamlessly.
- Allows for security groups and your own layered security approach.
- Stores files in the manner and format that works for you.
- Reporting technologies can be implemented.

COMPANY INTRANET

- Access controls and delegation is possible and inherent but will take some effort to setup correctly.
- Store files in the manner and format that works for you within the platform.
- Accessible from anywhere.
- Some versions can employ multi-factor authentication.
- Reporting technologies can be implemented.

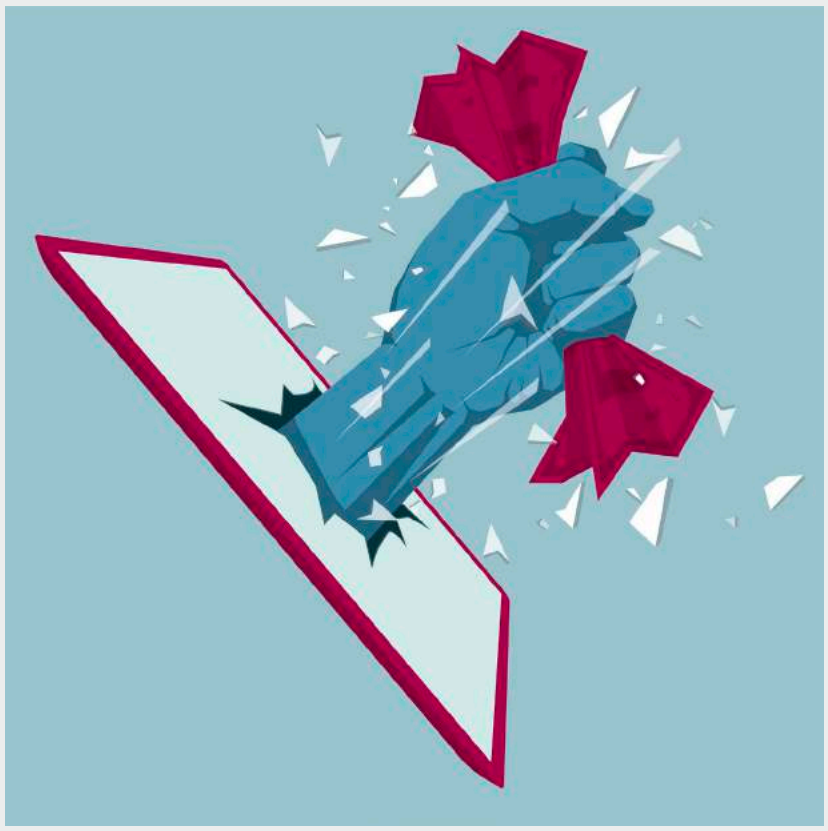
CRM PLATFORMS

- Geared towards integrating with client management software.
- Access Controls are commonly minimal.
- Commonly cloud based.
- The data is accessible quickly.

Cyber Security Password Attacks

There are many forms of Cyber Security Attacks that plague individuals and companies on a daily, even hourly basis.

It’s important to familiarize yourself with each technique. And, better yet, have a plan for protecting yourself and your company from these common attacks.



1 DICTIONARY

A Dictionary Cyber Attack is a technique for defeating a password by trying to determine the passphrase. The person or machine tries hundreds even millions of common words found in a dictionary. Dictionary attacks work because many businesses and computer users rely on using ordinary words as passwords.

2 BRUTE FORCE

A Brute Force Cyber Attack is a trial and error method used by application programs. It tries to decode encrypted data like passwords through exhaustive efforts using brute force. It’s used in place of intellectual strategies.

Cyber Security Password Attacks

3 DENIAL OF SERVICE

A Denial of Service Cyber Attack happens when a perpetrator attempts to make a device or network resource unavailable to its users. They temporarily or indefinitely disrupt the service of a host connected to the Internet. It is typically accomplished by flooding the device with prolific requests in an attempt to overload the system.

4 DISTRIBUTED DENIAL OF SERVICE

A Distributed Denial of Service Cyber Attack is just like a Denial of Service attack only the perpetrator uses multiple IP addresses. The incoming traffic flooding the device is coming from many different sources.

Cyber Security Password Attacks

5 SOCIAL ENGINEERING

Social Engineering Cyber Security Attacks are not only becoming more common, they're also becoming increasingly sophisticated. Cyber attackers use tricky tactics to get humans to break standard security practices. The goal of the attacker is to gain legitimate and authorized access to sensitive data and confidential information. Commonly, Social Engineering Cyber Attacks involve email or other communication methods that evoke urgency.

Conclusion

We hope you learned something about password management and potential security threats. We like to say that protecting sensitive data starts with education. If you have questions about the security of your network environment, give us a call. At Black Label IT, we provide FREE network assessments and IT consultations.

BLACK LABEL IT

Email

support@blacklabel-it.com
www.blacklabel-it.com

Phone

Support : 888-671-3143
Sales : 888-671-3143

Address

130 Nickerson St Suite 210,
Seattle, WA 98109