Password Security

City of Albuquerque

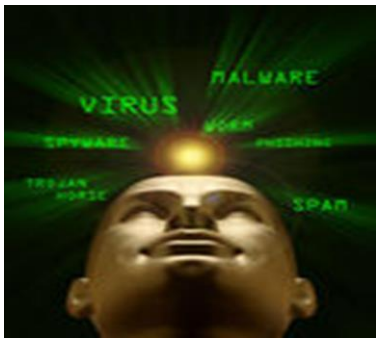
Cyber Security Newsletter
October 2013

Overview

Why do I need a strong password?

How passwords are cracked.

Keeping your personal passwords private, secure, and unbreakable is one of the most important steps you can take for safer computing. If your passwords slip into the wrong hands, your identity, finances, and personal information could be in jeopardy.



Find out more about how to choose strong passwords, how often to change them, why you should have more than just one, and other important password tips and tricks on this web page.

"Because many people use the same or similar passwords for different computers and multiple accounts, gaining access to one password often provides access to other systems and accounts.

Strong Passwords

Using passwords are important steps in ensuring privacy and security on the computers you use every day, at home and at work. Unfortunately, many of the passwords people use are simple or have been in use for a long period of time and for a lot of accounts. Simple passwords can be easily guessed by people who know you, or can readily be cracked by people with experience.

Consider these findings...

Research has shown that more than 40 percent of all individually-chosen passwords are readily guessed by someone who knows you.

In a recent survey of password use, more than 3,000 account passwords were cracked out of a test sample of more than 13,000 with multiple, and easily accessible tools.

Because many people use the same or similar passwords for different computers and multiple accounts, gaining access to one password often provides access to other systems and accounts. Best practices are to have unique passwords for social media accounts and financial accounts. This will reduce the risk of all your accounts being at risk in the event one of your passwords is compromised.

How passwords are cracked

Dictionary programs are one of many tools frequently used to crack passwords. A hacker will launch a dictionary attack by passing every word through a dictionary, which can contain foreign languages in addition to the entire English language, to a login program hoping that a word will eventually match the correct password. Even worms and viruses will attempt to guess passwords.

"In tests on live systems, dictionary attacks are so routinely successful that software implementing this kind of attack is readily available."

Ways in which passwords are vulnerable:

Many people do not change the default password that comes with some computer security systems. Lists of default passwords are available on the Internet.

A password may be guessable if someone chooses a piece of personal information as their password. Such items include an address, son or daughters name, birth date, telephone number or using your log-in identification as your password. Personal data is now available from various sources, many online such as Facebook, and can often be obtained by someone using social engineering techniques such as posing as a friend.

A password is vulnerable if it can be found in a list of commonly-chosen passwords. Dictionaries, often in computer-readable form, are available for many languages, and lists of passwords are easy to get a hold of. In tests on live systems, dictionary attacks are so routinely successful that software implementing this kind of attack is readily available.

A password that is too short, perhaps chosen for ease of typing, is vulnerable if an attacker can obtain the cryptographic hash (mathematical function which maps values from a large domain into a smaller range) of the password. For example, computers are now fast enough to try all alphabetic passwords shorter than seven characters.

For Additional Security Awareness information go to the City of Albuquerque Cyber Security eweb site at CABQ Cyber Security.