Passwords are more important than you think

Passwords secure all of the resources in your systems, including email, online accounts, and sensitive business information. Online criminals have advanced and developed state of the art hacking tools that are designed to eventually crack even the most complicated password. The key word being “eventually”. To remain safe you want to use a password that cannot be easily cracked, ensuring the cybercriminals seek easier targets elsewhere.

Password

A password as you know it is typically composed of no more than 10 letters or symbols, or a combination of both. Passwords are random symbols such as “B3746H=?#” or an easy word like “your name”, or can be a combination of both such as “r0Bert?!”

Passwords are relatively easy to guess or crack by both human and robots. The online criminals have developed state of the art hacking tools that are designed to crack even the most complicated passwords.

Passphrase

A passphrase is like a password, but longer and more secure. It can contain spaces in between words such as this: “The road to success is always under construction!” A passphrase can also contain symbols and does not have to be a proper sentence or grammatically correct.

Passphrase Best Practice

Complex passwords such as “B3746H=?#” don’t always mean they are secure. The longer your password the longer it will take a hacker to crack it.

1. Use a passphrase over a password.

2. Never write your password down on a piece of paper.

3. For sensitive information such as bank accounts, use a unique passphrase for each login.

4. Choose phrases that are meaningful to you, that way it is easier to remember. For example:

The cow jumped over the moon

5. Never share a passphrase or your strategy for creating them. If you believe that your passphrase may be compromised or stolen, be sure to change it immediately.

6. Do not use public networks such as free WI-FI in cafes, hotels or libraries to log into work or bank accounts without appropriate precautions. Hackers can use an application to watch all traffic on the public network, once you enter your username and password, the software notifies them and the hacker intercepts the information.

7. Be wary of sites that require you to answer personal questions, such as Facebook quizzes. The answer to these questions are often common passwords or password reminders such as “What is your mothers maiden name?”

8. Use a password manager. A password manager is a secure digital wallet that allows you to safely store your passwords. Create a master password for your password manager and you won’t need to remember all the rest.

Passphrase Security

Attackers use a variety of techniques to crack passwords, including powerful tools freely available on the Internet. The following advice makes password security easier for your end users, aiming to improve the security of your system.

How passwords can be cracked

Manual Guessing

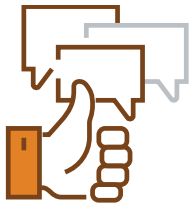
Personal information such as names and date of birth can be used to guess common passwords.

Stealing Passwords

Poorly stored passwords can be stolen such as handwritten passwords hidden close to the device.

Social Engineering

Attackers use social engineering techniques to trick people into revealing passwords.



Searching

Infrastructure can be searched for electronically stored password information.

Phishing Attack

A phishing attack is designed to fool you into revealing information that you wouldn't normally give out.

How to Improve your system security

Help users to generate an appropriate passphrase

- Train your users on how to create passphrases that are hard to guess
- Never re-use a passphrase between home and work
- Discourage dictionary words or names, last names and birthday dates

Encourage users to use passphrases over passwords

- Never share your passphrase with anyone
- For sensitive information such as bank accounts, use a unique passphrases for each login.
- More than 14 characters
- Avoid common or popular quotes and songs

Never give out your details over the phone

Unless you have verified that the person you are talking to is who they say they are. Never give out your login or account details over the phone. To verify a caller, hang up and call them back on their "company advertised" number.

Password Managers

A Password Manager is a secure digital wallet that allows you to safely store your passwords. Create a master password for your password manager and you won't need to remember all the rest.