Password Security

SecurIT360
The physics of securing IT

80% of data breaches involve exploitation of stolen, weak, default or easily guessable passwords. Fraudulent password access has led to billions of dollars in financial fraud and damaging public relations for organizations and individuals.

A strong user password is the foundation for personal information security. It is critical that we practice secure password management individually, but also that our organizations have password policies and management systems that require us to use secure passwords.

There are two major components to password security.

- Corporate Password Policy
- Personal Password Practices

Think of it this way. The password policy is like a good lock on a strong door. Your password, and how you protect it, is the key that opens or closes the lock.

Corporate Password Policy

Corporate password policy includes –

- Strong requirements for passwords
- System capabilities and settings which will enforce the password rules
- Consistent training and reinforcement

The following are good basics for corporate password policies.

- Minimum of twelve (12) characters long
- Changed at least every 60 days (30 days is better)
- Requires -
  - At least one upper case character
  - At least one lower case character
  - At least one special character
  - At least one numeric character
- Your twenty-four (24) prior passwords will not be eligible for reuse
- No shared usernames or passwords among users

While these policies are good, they must be supported by system capabilities which require their use. Information system capabilities must keep pace with security standards. In today's cybersecurity environment, it is an absolute requirement to invest in the technology needed to maintain good cybersecurity practices. It would be negligent to ignore this requirement.

Beginning with the onboarding process, password policies (and other cybersecurity policies) should be communicated clearly and reinforced frequently.

Password Security

Personal Password Practices

In addition to strong password policies, we must treat our passwords as critical information to be protected, just as we would with social security numbers and bank account numbers. After all, it doesn't do any good to lock the door and leave the key in the lock.

No Sticky Notes! – Hopefully, we are all aware of this bad habit. You cannot have your password(s) written in plain sight near your computer.

What makes a password secure?

A password should be easy for the user to remember. One of the best ways to make a long password easy to remember is to use a "pass-phrase." You might use the first letters of a song, book, quote or title and mix it with other numbers and characters.

For example –

• We Didn't Start the Fire	W*d*S*t*F*##
• Hello from the other side	H-F-T/O/S/!
• I Love to Play Baseball	Iluv2pl@yb@5eb@11

A password should also be hard for anyone else to guess. It is best not to use an easily identifiable word or phrase that people associate with you, like a nickname or favorite sports team. For example, if your nickname is "Big Red," don't use bigred in your password. Cyber-criminals often use social media sites to research personal information on their targets.

Do not use the same passwords for multiple systems.

How can I remember all of this?

Many of us have fifty or more usernames and passwords to manage including our work and personal life. If you must write them down to remember them, keep them in a secure place that you only you can access. A locked drawer or a password protected document may be a good option, but they still involve some level of risk.

You might also consider a password manager app such as LastPass, Dashlane or Keeper.

Remember, your password is an important key. You do not want to be the person who left the door unlocked…

As always, develop a "cyber-defense" mindset and protect yourself.

If you would like to learn more about Cybersecurity and how to protect your company, contact -

David Burns
Account Manager, SecurIT360
dburns@securit360.com
205.787.1250