PASSWORD SECURITY

Password security is the first line of defense in protecting a company’s confidential and proprietary information. If a cyber-thief gains access to a single password, they may be able to access all of the secure information on the network.

The best protection against password theft and abuse is the creation and enforcement of a strong password policy. There are guidelines and practices that all computer users within an organization should adhere to. Passwords should be protected and kept as secure as social security numbers and financial account information. Password security is the responsibility of every user on the network.

BEST PRACTICES FOR PASSWORD SECURITY INCLUDE:

- Use a combination of upper-and lower-case characters, symbols and numbers when creating your passwords.
- Longer passwords are more difficult to guess or crack.
- Consider using a pass-phrase that you can easily remember but that uses a combination of characters.
- Never use a name, word or date that can be easily guessed.
- Never share your password or reveal it to someone who asks for it.
- If you believe your password has been compromised, change it immediately and notify IT support.
- Never use the same password for multiple accounts or logins.
- Never keep passwords in a file on your computer or written down near your desk.

AVOID THESE PASSWORD STEALING THREATS:

- Websites that ask you to reset or re-enter your password for a specific account or service.
- Entering your password where someone can see you typing it.
- Responding to text or social media messages requesting that you enter your password to view a message.
- Entering your password when on a public or unsecure wireless network.
- Entering your password on a computer that isn’t yours.

Key Points

- Keep passwords secure and safe.
- Use unique passwords for every account.
- Use a combination of characters and letters.
- Change passwords often.
- Never share your password.