Intrada TECHNOLOGIES

Safeguarding Your Digital Identity:

The Vital Role of Strong Passwords in Protecting Against Cyber Attacks

It is essential to use strong passwords that are unique and hard to guess to maximize the security and privacy of user accounts. Organizations should ensure that their staff is aware of best practices when it comes to password management and provide resources such as tutorials, articles, and tools that will help them create secure yet memorable passwords.

Here are some basic rules to follow:

- Passwords should be at least 8 characters in length or longer, with 10 characters being the recommended minimum.
- Utilizing multiple words or phrases that have some personal significance can also help make a password much more secure.
- Consider using special characters whenever possible.
- It is essential to never reuse any of these passwords across multiple accounts. Each password should be unique and memorable for each account.
- Never use passwords that can be found in a dictionary.
- Never use common passwords like 'password', '123456', 'iloveyou', 'abc123', '111111', and 'letmein' and 'qwerty'.
- Don't share personal passwords with business accounts.
- Don't use shared passwords or share your password with other staff members.
- Consider changing your business passwords every 6 months and personal passwords yearly.
- Consider using a password manager to help manage and secure passwords.
- Setup MFA whenever possible.

By taking these measures, and ideas and following best practices when it comes to strong password management, organizations and individuals can greatly reduce the risk of unauthorized access to their systems, accounts, and data. For more information on security services from Intrada, give us a call.

31 Ashler Manor Drive
Muncy, PA 17756

intradatech.com
800-858-5745

Exceeding Expectations.