The Architect's Guide to **Easy Password Management**

It's absolutely critical for professionals like you to protect your clients' sensitive data. Thankfully, one of the most effective ways to bolster your cybersecurity is also one of the easiest: creating strong passwords.

Use this quick reference guide to help you and your firm develop and maintain the best password management habits.

✓ DO

Use a passphrase instead of a password

A passphrase involves writing several words, as well as spaces in between each word, to make it much more difficult for a hacker to crack. It can also be a long string of letters, numbers, and special characters.

Change your default passwords

Cybercriminals already know the default passwords that come with standard computers and software solutions. The last thing you want to do is to keep those passwords unchanged. Be sure to change your passwords as soon as you activate these systems.

Use multi-factor authentication

Multi-factor authentication is a fantastic safeguard, as it requires you to use a separate device or service to verify any login attempts (such as your mobile device). Without presenting the token sent to this separate device, a hacker cannot get into your account.

Install a password manager

Password managers are software solutions that can remember unique and complex passwords for you! By using these tools, you can create complex passwords that you don't need to memorize. These tools can even generate passwords for you.

✕ DON'T

Reuse the same password

By using the same password for everything, a hacker only needs to crack your password once to access all of your accounts. Use a different password for every login to ensure there are stopgaps if a breach occurs.

Store your passwords on a spreadsheet

Don't do cybercriminals any favors by writing all of your passwords in a single document or spreadsheet. This essentially packages all of your sensitive login data in a nice, convenient place for a hacker to easily pull from.

Use personal details as a password

If your birthday, PIN, or Social Security Number is used as a password, then a hacker gains more than just your login if they crack your account. Create passwords that don't give away more information than you want.

Use common dictionary words

You can throw off the hacker's tools by creating words that won't be found in a dictionary. Try taking a common word and replacing certain letters with symbols or numbers. For example, instead of writing "trade," write "tr@d3" instead.

CLIENTPAY®
AN AFFINIPAY SOLUTION

clientpay.com | 855-724-4047
Get a Demo ›