FrankelZacharia LLC

12 Password Best Practices

With the business world heavily reliant on digitalization, the use of technology in your organization is unavoidable. Although technology can undeniably give your business an advantage, there are many troublesome areas to keep an eye on. This has contributed to the increased interest in cybersecurity.

Password protection is the best place to start if you want to ramp up your cybersecurity. Setting a password to secure an entity's data is called password protection. Only those with passwords can access information or accounts once data is password-protected. However, because of the frequent use of passwords, people tend to overlook their significance and make careless mistakes, which could lead to breaches in security.

This makes it imperative for businesses to devise strategies to educate employees about best practices when using passwords.

6 Password "Don'ts"

Protect the confidentiality of your passwords by following these six password "don'ts":

1. **Don't write passwords on sticky notes:** Although you may feel that writing down passwords improves password protection and makes it more difficult for someone to steal your passwords online, it can make it easier for someone to steal your passwords locally.

2. **Don't save passwords to your browser:** This is because web browsers are terrible at protecting passwords and other sensitive information like your name and credit card number. Web browsers can easily be compromised and a wide range of malware, browser extensions and software can extract sensitive data from them.

3. **Don't iterate your password (for example, PowerWalker1 to PowerWalker2):** Although this is a common practice among digital users, it is unlikely to protect against sophisticated cyberthreats. Hackers have become far too intelligent and can crack iterated passwords in the blink of an eye.

4. **Don't use the same password across multiple accounts:** If you do so, you are handing cybercriminals a golden opportunity to exploit all your accounts.

5. **Don't capitalize the first letter of your password to meet the "one capitalized letter" requirement:** Out of habit, most of us tend to capitalize the first letter of our passwords to conform with the "one capitalized letter" requirement. However, hackers are aware of this, making it easy for them to guess the capitalized letter's position.

6. **Don't use "!" to conform with the symbol requirement:** However, if you must use it, don't place it at the end of your password. Placing it anywhere else in the sequence makes your password more secure.

6 Passwords “Do’s”

Protect the confidentiality of your passwords by following these six password “do’s”:

1. **Create long, phrase-based passwords that exchange letters for numbers and symbols:** For instance, if you choose "Honey, I shrunk the kids," write it as "h0ney1$hrunkth3k!d$." This makes your password harder for hackers to crack.

2. **Change critical passwords every three months:** Passwords protecting sensitive data must be handled with caution because there is a lot at stake if they are compromised. If you use a password for a long time, hackers may have enough time to crack it. Therefore, make sure you change your critical passwords every three months.

3. **Change less critical passwords every six months:** This necessitates determining which password is crucial and which is not. In any case, regardless of their criticality, changing your passwords every few months is a good practice.

4. **Use multifactor authentication:** It’s your responsibility to do everything in your power to keep nefarious cybercriminals at bay. One of the best approaches is to barricade them with multiple layers of authentication.

5. **Always use passwords that are longer than eight characters and include numbers, letters, and symbols:** The more complicated things are for hackers, the better.

6. **Use a password manager**: A password manager can relieve the burden of remembering a long list of passwords, freeing up time for more productive tasks.

Need a password manager? We can help.

Adhering to password best practices requires constant vigilance and effort on your part. For best results, it is strongly recommended to work with a security-focused managed service provider (MSP) like us.

Tim Weidman
402-963-4375
tweidman@fzacpa.com