Best of the Worst Password Practices

Devolutions

I'VE DONE SOME RESEARCH AND IDENTIFIED THE BEST OF THE WORST PASSWORD PRACTICES

Don't you hate it when your boss tells you the reasons cyber security is so important and that the organization must adopt a stronger password policy? Seriously — who is your boss trying to impress?

The big cyber security scare is a giant myth created by governments and technology companies. There's really nothing to be worried about. And so, I've done some research and identified the best of the worst password practices. Feel free to use these to create your policy, and to get your panicking boss to calm down.

1. CREATE EASY PASSWORDS

Complex passwords are hard to remember. Brain cells are precious. So choose the easiest password possible.

2. USE THE SAME PASSWORD EVERYWHERE

Even if you choose easy passwords, having a different one for each account is a pain. Why not keep things simple by using the same password all over the place?

3. SAVE PASSWORDS IN YOUR WEB BROWSER

Who needs tools like Devolutions Web Login and Auto-Login to safeguard your accounts and data? Life is short. Go ahead and save passwords in your web browser. Automation to the rescue!

4. SKIP THE 2FA AND MFA

2FA and MFA – Blah, blah, blah! Who needs these? It's like having to clear customs at the airport whenever you want to log into a different account. I mean, it's not like you have to go through that stuff when using Reddit, right?

5. ALWAYS CHOOSE THE MINIMUM PASSWORD LENGTH WITH THE LEAST COMPLEXITY

Aha — the cyber security police think they can force you to choose long, difficult passwords, right? Well, you can fight back by always choosing the minimum password length with the least complexity. Try this: 12345678+

6. NEVER CHANGE YOUR PASSWORDS

Don't worry if there was a data breach at your bank, on favorite website, or in another account. Obviously, you must be safe, since nobody has taken out a fake mortgage under your name or emptied your bank account. So go ahead and keep your old passwords. Why fix what isn't broken?

7. SHARE YOUR PASSWORDS

Sharing is caring. Everyone knows that. It's one of the first things we learn in school. And now that you're an adult, you should be generous and share your passwords with colleagues and friends. Go ahead and use normal email for this — or even better, Tweet it.

But Seriously, Folks...

OK: if your jaw has dropped open and you're wondering if I've been seduced by the Dark Side of the Force, don't worry. Of course, **all of the above is exactly what you DON'T want to do** — and you just as surely DON'T want your end users doing these things, either!

Instead, you want them to follow smart and safe cyber security best practices, which are rooted in a robust password management policy. **To point you in the right direction, here is some useful advice:**

- Password Best Practices Using Remote Desktop Manager
- Top 10 Password Policies and Best Practices for System Administrators
- 5 Common Password Security Mistakes
- Why Saving Passwords in Browsers is a BAD Idea

What Do You Think?

Tell us what you think of our "best of the worst" password management policies. Do you know of anyone (you don't have to mention their name!) who has committed any or some of the above cyber security sins?

And on the other side of things: **what are your best of the best password policies?** Please share them so that the whole community can benefit from your experience and insight.