5 Common Password Security Mistakes

Devolutions

WHAT ARE SOME WAYS YOU CAN PROTECT YOURSELF FROM THESE ATTACKS?

We all know that today's hackers are nothing like the "script kiddies" of years past. Back in the old days, hackers were usually interested in wreaking havoc, destroying machines, and getting on the news so they could brag to their friends. These days, things are very different!

That's because today's hackers are motivated by making money — not creating mayhem — and many of them are highly sophisticated and well-funded. As pointed out by IDG's CSOonline.com: "The trend in cybercrime is that it is increasingly more organized, in many cases operating much like legitimate businesses, complete with organizational charts, C-level executives and even human resources departments." And the story gets even worse.

What are some ways you can protect yourself from these attacks? By avoiding making any of these five common password security mistakes:

#1. Weak Passwords

There are many things that make passwords weak and vulnerable. Here are some of the factors:

- Composed **only of letters**
- Composed **only of numbers**
- **Too short**
- **Uses a pattern** (e.g. "QWERTY" or "zaq1zaq1")
- Easy to guess (TIME Magazine reported that **"password" was the second most used password of 2016**, right behind "123456" – can you believe it?)
- Uses **personal information** (e.g. street number of address, dog's name, etc.)
- Generic (passwords such as **"admin" for admins** can lead to big trouble!)
- **Username and password are the same**

The best way to avoid all of the above is to use a good password generator, such as the one that is built into Remote Desktop Manager. And here's some good news for all of your admins out there who go crazy when your users create weak passwords: Remote Desktop Manager also has a special feature that lets you ensure all passwords meet pre-determined complexity requirements. No more QWERTY and 123456!

#2. One Password to Rule Them All

I only have this to say to users who try to save time (or are just lazy) by creating a master password that they use on multiple accounts, machines and devices: NO GOD PLEASE NOOO!

Well, I have more to say: please stop! You're one hack away from an identity theft nightmare that could last for months, or even years. The smartest thing you can do is **create strong and unique passwords for each of your logins.**

#3. Sharing Passwords

The only time it makes sense to share passwords is between colleagues who are using a shared database within a password manager. But of course, those passwords **should only be for work-related** machines, devices and accounts — not for personal stuff.

Plus, the best way to share your work related passwords is to use a password management solution as Remote Desktop Manager that is connected to a shared database. Using RDM offers many security perks such as automatic credentials and passwords brokering so your colleagues can use the passwords without even knowing them.

And if you think it's safe to share passwords with your best friend or even your spouse or family member: think again! No, it's not because they may do something bad. It's because they may unintentionally expose your password to hackers — and you'll end up paying the price.

Think of it this way: **some secrets should just stay between you and you**. This includes your precious passwords.

#4. Improper Password Storage

Even if you have the strongest and most unique passwords in the world, they're unsafe if stored locally in a browser. The same goes for storing passwords in an office drawer, ON STICKY NOTES, or in spreadsheets.

If you're getting a headache trying to remember all of your complex passwords, then **using a good password manager will make your life easier**. To help you make the right choice, check out this comparison grid of the most popular password managers here.

#5. Not Using 2FA or MFA

Several years ago, you had to be a pretty sophisticated IT pro to setup a 2FA or MFA system. But these days, there are **many simple apps out there that anyone can use** — even people totally outside the IT world, who think that a PAM solution is something you spray on cookware.

While MFA may not be accessible for everyone, 2FA certainly is since everyone has a smartphone (and some people have several of them!). If you **need help choosing the right solution**, read our article here.

Your Game Plan

Have you heard the saying "the best defense is a good offense"? Well, this means you should go on the attack and be proactive by locking down your password security ASAP. Here's what your game plan should look like:

- Start by getting a **good password manager**. Trust me, you'll be glad you did. They're easy to use, and well worth the price when you consider what's at stake.

- Next, if necessary **change any/all of your passwords into something stronger and unique**. Yes, this might take a little while — but it's MUCH less time than you'll spend sorting things out after getting hacked.

- **Choose a 2FA or MFA solution**, so that your logins on the public internet will be safer (and as you might have experienced, many banks and online tax filing software vendors have made 2FA logins mandatory).

A Bonus Tip

You can save some time by using a password manager that has a built-in browser extension, such as Devolutions' web login extension. This will **automatically log you into various accounts** (i.e. you won't have to manually input your username/password).

Your Turn

What are your password security tips? Please share them below, so that we can all be a little safer. And if you feel passionately about this topic and want to make your views known, then you're invited to write a guest article that we'll feature here on our blog. Email me at jdupont@devolutions.net and I'll send you more information!