5 Tips to Educate Users About Good Password Policies

Devolutions

DEVELOPING GOOD PASSWORD POLICIES IS ESSENTIAL FOR BUSINESSES OF ALL SIZES

Data breaches are happening all the time, in both big enterprises and even more so in SMBs – which experts view as "ground zero" for cyber crime.

As a result, developing good password policies is essential for businesses of all sizes. But it's not the whole story, because the policies must also be adopted and enforced. That's why users make the difference between success and failure.

With this in mind, here are 5 tips to educate your users about good password policies:

1 HELP THEM UNDERSTAND HOW SERIOUS THINGS ARE

Cyber security can seem abstract for some users — especially those who don't work in IT. Yes, they know it's an issue, but they can't grasp how a data breach at work would affect their day-to-day life.

Start by helping them understand that hackers don't just steal corporate data — they also **steal confidential employee information to commit identity theft**, which can lead to everything from draining bank accounts to taking out fraudulent loans and mortgages.

What's more, even if a data breach doesn't directly take money out of an employee's pocket, it's certainly going to cost the business a lot of money to investigate and clean up. There could also be major reputational damage that leads to customer loss. All of this affects the strength and stability of the organization, which could lead to job losses or worse. A staggering 60% of small firms go out of business within 6 months of a major cyber attack.

2 SIMPLIFY THE MESSAGE

IT pros know all about concepts like botnets, DDoS attacks, drive-by downloads, spear phishing campaigns, and so on. But **some (and probably most) users aren't familiar with this jargon.**

As such, it's important to **simplify things as much as possible**. Think of the Reddit forum ELI5, which stands for "Explain Like I'm 5". TechAdvisory.com has also put together a glossary of cyber security terms that your users may find helpful.

3 CHECK PASSWORDS

It's not that you don't trust your end users to create strong passwords — but, well, some things in life you should verify, and not just take on faith. After all, what some users think of as strong and complex passwords might in fact be the opposite!

It's a good idea to **ensure that all user passwords are robust instead of vulnerable**. If they aren't, you should re-educate users and provide them with examples to help make it clear. If you use RDM, the built-in password analyzer is ideal for establishing and enforcing strong passwords across the organization.

4 PROVIDE PRACTICAL INFORMATION

Through our blog In the Trenches, we publish content to help you understand and **explain the world of cyber security to your users**. Here are a few examples:

- How to Protect Your Data at Home
- Prevent Insiders from Breaching Your Data
- Are Your End Users Suffering from Security Fatigue?
- 4 Types of Security Tools that Everyone Should Be Using
- Top 10 Password Policies and Best Practices for System Administrators

5 USE THE RIGHT TOOLS

Choose the right tools and train users on how they should use them. For example, with Remote Desktop Manager (RDM) and Devolutions Password Server (DPS), you can easily set password policies and implement Privileged Access Management (PAM). You can also easily manage passwords across your entire organization, from technical users to business users.

The Bottom Line

IT pros know that good password policies are vital, and that everyone must work together to make them work. We hope that the above tips make your task easier, while also helping your users be part of your organization's cyber security solution — and not the problem!