V2verify™

Passwords Are a Cybersecurity Disaster

The Password Problem

If today’s password problem feels like a losing battle, that’s because it is. Let’s peel back the layers to see why.

1. Despite warnings by security experts, people are still using passwords that are easy to guess. According to Splashdata, the top 5 “bad” passwords of 2018 were 123456, password, 123456789, 12345678, and 12345. Even if a special character, capital letter, or number is required, passwords are still too easy to guess!
2. Users are using the same password for multiple logins. If a hacker can guess your password, chances are they now have access to several of your accounts.
3. 4 Billion user credentials were hacked in the first six months of 2019 and are for sale on the dark web.
4. What is the solution from companies? They add challenge questions (knowledge-based questions). With most people living their life out on social media, this is a very weak second-factor authentication.
5. Now let’s add phishing into the equation. Cybercriminals are successfully mimicking companies every day and spoofing people into giving up their credentials.

Now that we can see the scope of the password problem, let’s take a trip downstream to see how all this affects business today.

Because of the password problem, 81% of all hacked data breaches are a result of compromised credentials. That puts companies at extreme risk for a breach, and the average global cost of a data breach at $3.8 Million or around $148 per record. The numbers are costly, and they don’t even account for the loss of customers or hits to the brand.

In response to this exposure, companies are sinking more time, money, and resources into better security measures. The problem is no amount of money or security is going to help if the attacker is walking through the front door. So, companies look to improve security around user authentication and identity access management by implementing stricter password guidelines and, in many cases, double authentication requirements.

This added security proposes a new problem by adding a tremendous amount of friction to the customer experience. Customers become frustrated when they can’t remember passwords or challenge questions, or when they don’t have access to their email or phone for the double authentication requests. The result is customers are reusing the same password even more, and they are writing them down in notebooks or on sticky notes and leaving them in publicly accessible places. This, as I’m sure you can guess, leads to even more compromised credentials…and the cycle begins again. The increased ability to compromise credentials lead to more data breaches, the need for more security, and even more customer friction which results in…. you see the problem, right?

The Solution

So now that we've framed the problem. What's the solution? Historically businesses struggle with balancing security with great customer experience, one always giving way to the other. It's a complicated problem; fortunately, there's an easy solution – V2verify.

V2verify answers the security problem. V2 provides a solution that cannot be hacked or spoofed by a recording. It can definitively authenticate a user by providing built-in double factor authentication.

V2verify also improves the customer experience. V2 can authenticate a user with 2 seconds of speech. No passwords. No PINs. No challenge questions. Nothing to carry or remember. No customer friction.

V2verify simply requires you to say a couple of words and identify yourself to a contact center or agent, log in to a website, a mobile app, a portal, open a door, access data, or even log in or out of a time clock.

The ROI of Adding V2verify

According to Gartner Group, between 30% and 50% of all IT help desk calls are for password resets, and according to Forrester Research, the average helpdesk labor cost for a single password reset is $70. By using V2verify to authenticate users, the significant cost of resetting passwords can be eliminated.

Eliminating passwords also reduces the attack surfaces for businesses. This greatly reduces data breaches and protects companies from subsequent financial loss.

Eliminating passwords also presents tremendous operational efficiency gains. IT departments no longer have banks of passwords to manage, help desks don't have to reset passwords, and users don't have downtime as a result of being locked out.

In addition, V2verify builds a solid foundation for user authentication and identity access management. This foundation is crucial as businesses begin moving to hybrid environments, and eventually, in supporting and securing the IoT.

Implementing V2verify is a simple process that doesn't require any capital expenditure, and customer onboarding is a simple process that can be completed live, in a self-service environment, or by using previously recorded conversations.

The only way to fix this on-going problem is to eliminate passwords altogether. This sounds like a daunting task, but with V2verify, it's easier than you think!

Contact us today to begin a life without passwords!