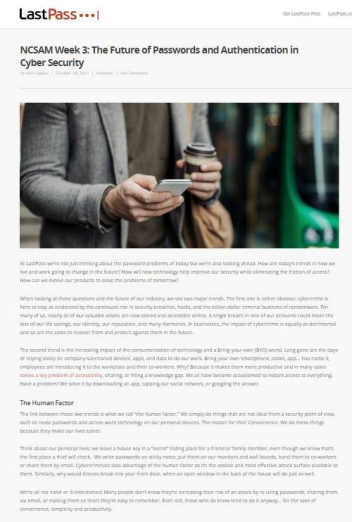
CLIENT LastPass

PROJECT Blog post: The Future of Passwords and Authentication

OBJECTIVE Attract search traffic and readership and nurture leads.

COPY EXCERPT

The Future of Passwords and Authentication in Cyber Security


LastPass

NCSAM Week 3: The Future of Passwords and Authentication in Cyber Security

Call or write CopyEngineer to receive a PDF of the complete blog post.
Or view it online at:
https://blog.lastpass.com/2017/10/ncsam-week-3-future-passwords-authentication-cyber-security.html/

At LastPass we're not just thinking about the password problems of today but we're also looking ahead. How are today's trends in how we live and work going to change in the future? How will new technology help improve our security while eliminating the friction of access? How can we evolve our products to solve the problems of tomorrow?

When looking at these questions and the future of our industry, we see two major trends. The first one is rather obvious: cybercrime is here to stay as evidenced by the continued rise in security breaches, hacks, and the billion-dollar criminal business of ransomware. For many of us, nearly all of our valuable assets are now stored and accessible online. A single breach in one of our accounts could mean the loss of our life savings, our identity, our reputation, and many memories. In businesses, the impact of cybercrime is equally as detrimental and so are the costs to recover from and protect against them in the future.

The second trend is the increasing impact of the consumerization of technology and a Bring-your-own (BYO) world. Long gone are the days of relying solely on company sanctioned devices, apps, and data to do our work. Bring your own smartphone, tablet, app… You name it, employees are introducing it to the workplace and their co-workers. Why? Because it makes them more productive and in many cases solves a key problem of accessibility, sharing, or filling a knowledge gap. We all have become accustomed to instant access to everything. Have a problem? We solve it by downloading an app, tapping our social network, or googling the answer.

The Human Factor

The link between these two trends is what we call "the human factor." We simply do things that are not ideal from a security point of view, such as reuse passwords and access work technology on our personal devices. The reason for this? Convenience. We do these things because they make our lives easier.

Think about our personal lives: we leave a house key in a "secret" hiding place for a friend or family member, even though we know that's the first place a thief will check. We write passwords on sticky notes, put them on our monitors and wall boards, hand them to co-workers or share them by email. Cybercriminals take advantage of the human factor as it's the easiest and most effective attack surface available to them. Similarly, why would thieves break into your front door, when an open window in the back of the house will do just as well.