Why Gary Doesn't Need Passwords Anymore

AN IDC INFOBRIEF, SPONSORED BY SECUREAUTH | **JANUARY 2019**

By Jay Bretzmann, Research Director Cybersecurity

IDC ANALYZE THE FUTURE

#US45813520TM

Password Basics

It's elemental: the foundation of any identity-proofing capability starts with something you know. And in many ways, it's an unfair burden to place on an IT user because something you know might be something others can discover, so you're encouraged to cloak this identifier using a combination of letters, numbers, and symbols into a secret password.

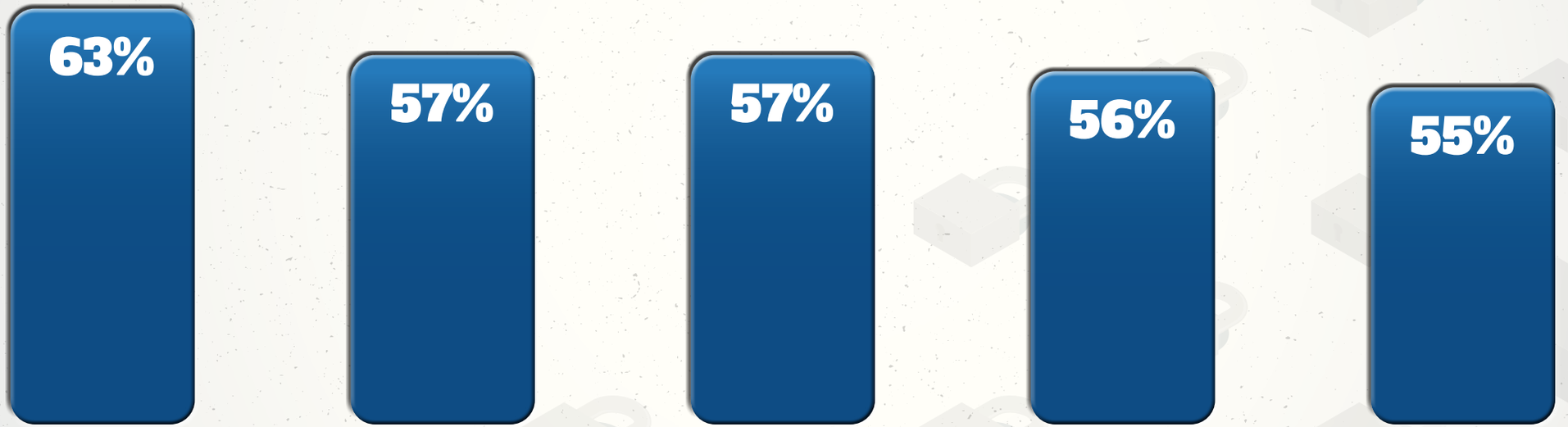
Most of us can do this once, twice, or even three times. But the average adult now uses more than 20 online applications, and many use three times more. That's a lot of passwords to create and remember. Password fatigue is a real condition leading many to use only one password across all systems or create ad-hoc constructions for immediate use and reset them time and time again.

Modern authentication systems help relieve the requirement of something you know by substituting something you have or something you are. The systems seamlessly use intelligence to assess associated levels of risk helping reduce access delays and needless IT expense confirming user identities.

The best of these solutions leverage multiple sensing technologies comparing device IDs, IP addresses, mobile numbers, time of day, geo locations, and past behaviors.

Users Hate Password Responsibilities

Perceptions about personal passwords (Strongly agree and Agree responses combined)



Gary: A Day in the Life of Password Use

From home and on his mobile device, Gary wakes and quickly checks his corporate email and calendar. No password is required as the biometric (facial) recognition authenticates that's its Gary and allows access. Good thing; it's a bad hair day for Gary, but at least he's found his glasses.

In the background, his security service has already done "pre authentication" risk and fraud checks for every employee by trolling through known bad IP address or URL lists, reviewing device configuration info, and flagging recent carrier change or SIM swap situations for mobile users. All done automatically.

During his logon session, Gary is allowed access to his typical employee systems as the identity system recognizes the behavior of Gary connecting through his home Wi-Fi and considers it to be normal. He's up early since it's going to be a big day, but not early enough to raise suspicions—keeping his risk score low.

Today his company is launching a new web-based service. He checks the overnight developments and makes sure everything went out on the business wire on time. Thankfully, it did.