FEBRUARY 24, 2022

Welcome to the Password Junkyard

INNOVATION & TECHNOLOGY
Smart Society
BY: Enrique Dans

Asking employees to consistently change their passwords does not increase security, only

A few weeks ago, it happened again like clockwork. I was asked to change my password. If there's one thing that is consistent among IT departments, it's systematic, dogged tenacity. They set up a reminder and then comes the time to torture the workforce with a taunting message that passwords will stop working on X day. Usually, this is when the countdown begins and workers can either deal with choosing a new password right then and there (but let's be honest it's never a convenient time) or getting pinged with random reminders for days on end.

Choosing a new password is no easy feat when it's necessary to find one that meets a whole host of requirements: it must not resemble any of the previous seven passwords in even the most remote sense, and it must contain uppercase, lowercase, numbers, special characters, and the frenzied yowling of cats in heat.

What's my issue with asking employees to think of a password? Quite simply: whatever they choose, it will be wrong. Advances in the algorithms that thieves use to figure out passwords – the so-called "dictionary attacks" – have come a long way and now include any known word in nearly every language, and they also know all the variations. Think you can outsmart the algorithms by swapping an E a 3? Or perhaps you use the letter O for the number 0, or the letter I for 1, or you are particularly tricky and use an A for a 4. Nope. Sorry to burst your bubble but your sweet password with the name of your first boyfriend or girlfriend in which you replace vowels with numbers stands as little chance against a dictionary attack as you do against a steamroller in a dead-end street. It will take only a matter of seconds.

Not to mention that many of the most common threats to workplace IT systems don't even employ a very sophisticated dictionary attack. Most, in fact, are done through what some pompously call "social engineering" (we all seem to have a penchant for feeling like engineers). This "attack" entails simply looking behind the monitor to see if a worker has stuck a Post-it note and written on it that is so good it's impossible to remember. Or, someone might even pick up the phone with a variation of "Hey, it's Brad, from IT… I need your password." (Who doesn't have a Brad in IT? If not, feel free to try a Robert or Mary).

> *The hard truth is that if you can remember a password, it's probably not a good one.*

Asking employees to come up with a password is a recipe for disaster. Even if they change their passwords more often than they change their underwear, it won't make a difference to workplace security. Plus, the more we are asked to change our passwords, the more difficult it is to remember them, which means the higher the likelihood that they will be jotted down on some other scrap of paper and left somewhere easy to find. It is just wrong to ask employees to change their passwords and fruitless (and annoying) to do it with such high frequency. What it really serves to do is make everyone believe that their personal annoyance is a small but necessary price to pay for keeping the company data (and probably some of their own information) safe and secure. But, do not be fooled: if you have not yet been attacked by criminals, it is not because of how well and how often employees choose their passwords. It is simply because the criminals can't be bothered with you.

The hard truth is that if you can remember a password, it's probably not a good one. These days, a solid password is an unfathomable jumble of twenty or thirty strange characters, with commas, slashes, hyphens, question marks, uppercase, lowercase, numbers, and any other forsaken symbol you can find on the keyboard. These all come together to create something you wouldn't even be able to put to memory if offered an all-expense-paid trip to an island in the Maldives.

But, listen, you don't actually have to type in this mess every time. (What, are you stuck in the '90s?) Passwords, my young Padawan, are stored in a place called a password manager, and the only password you have to know — and this is the one that had better be a good one — is the password manager's own password. From then on, when you want to log into a site, you just launch your password manager, which stores all of them in that cloud that everyone is talking about and fills it in for you. I feel it's necessary to mention that password managers have mobile versions, so if you're on your smartphone instead of your computer, or on a different computer, you can also launch it from there.

So, even if the baddy from the last James Bond movie comes along, ties you to a chair, blows smoke in your face and threatens to torture you, you won't be able to tell him your password. Simply because you can't remember it! But, what if they demand access to the password manager? Don't we read every day that such and such a company has suffered a cyber-attack? Yes, and indeed, password managers are a fantastic target for such thieves: there is nothing more prestigious than getting into one.

But what can someone actually get from access to a password manager? Quite simply, a list of passwords completely encrypted in a robust way and therefore basically useless to them. It seems reasonable to think that if your business depends on specific security, you wouldn't take a gamble on this kind of thing, right?

Today, password managers are the most reasonable option in personal and corporate security. Instead of periodically tormenting employees by making them come up with passwords that are completely absurd and easy to discover, teach them to use a password manager and to change that one password when and only when the application or service they were using has been attacked. It is not too much to ask the IT department, first, to budget for the purchase of password manager licenses for all employees, second, to teach them how to use them correctly, and finally, to watch out for when a corporate or common personal application has been hacked.

Ah, but… we have to *pay*? Money? Yes. Making a good password manager, managing and maintaining it is something that, surprise, surprise, costs money. If it's free, don't trust it. And no, the passwords proposed by your browser (although they are better than when a person makes them up) are not a viable solution in a corporate environment – they are neither completely secure nor do they withstand issues such as computer theft or a hasty reboot.

Ultimately, the right way to keep a company safe and secure is to implement password managers for employees and combine that with two-factor authentication processes for very sensitive issues (which many password managers already incorporate). You don't have to take my advice, but if you think the cost of security is high, wait until you see the cost of a lack of security.

© IE Insights.

FACEBOOK | TWITTER | LINKEDIN | EMAIL

READ NEXT

AT THE SPEED OF HANDS
FINDING THE SWING IN TEAMS

WOULD YOU LIKE TO RECEIVE IE INSIGHTS?

Sign up for our Newsletter

NEWSLETTER SUBSCRIPTION

RELATED CONTENT

26 / 01 / 2022

PLATFORMS ARE TAKING OVER, HOW DO WE GOVERN THEM?

Platforms have become the foundation for the world's largest companies, from the big techs to unicorns. Professor Juan Santaló analyzes if these platform ecosystems promote innovation, and how they can be governed.

BUSINESS & FINANCE | INNOVATION & TECHNOLOGY
Big Tech

WATCH

24 / 01 / 2022

GIVE IT TO ME STRAIGHT

BUSINESS & FINANCE | INNOVATION & TECHNOLOGY
Technology

READ

20 / 01 / 2022

NFT: THE WRONG QUESTIONS

HUMANITIES | INNOVATION & TECHNOLOGY
Blockchain

READ

25 / 11 / 2021

FORGETTING STAR TREK

INNOVATION & TECHNOLOGY
Technology

READ

05 / 10 / 2021

LOVE LOST BETWEEN BIG TECH AND GOVERNMENT

INNOVATION & TECHNOLOGY
Big Tech

READ

27 / 09 / 2021

HOW TECHNOLOGY CAN HELP WITH THE SDGS

INNOVATION & TECHNOLOGY | SUSTAINABILITY
Technology

WATCH

23 / 09 / 2021

WHEN TOURISM BECOMES A NATION

INNOVATION & TECHNOLOGY | SUSTAINABILITY
Tourism

READ

17 / 09 / 2021

INNOVATING IN THE AGE OF DIGITAL TRANSFORMATION

INNOVATION & TECHNOLOGY
Innovation

WATCH

LATEST NEWS

VIEW MORE INSIGHTS

IE – REINVENTING HIGHER EDUCATION

IE.EDU
IE BUSINESS SCHOOL
IE SCHOOL OF ARCHITECTURE AND DESIGN
IE SCHOOL OF GLOBAL AND PUBLIC AFFAIRS
IE FOUNDATION
IE UNIVERSITY
IE LAW SCHOOL
IE SCHOOL OF HUMAN SCIENCE AND TECHNOLOGY
IE EXPONENTIAL LEARNING