PASSWORD PROTECTED

NOV 2016

THE PASSWORD'S ROLE IN MODERN DOCUMENT MANAGEMENT SYSTEMS

Record Nations®

777 S WADSWORTH BLVD 3-250
LAKEWOOD, CO 80226

RECORDNATIONS.COM

PASSWORD SECURITY: MORE IMPORTANT THAN EVER FOR BUSINESSES

BY RYAN MCHUGH

Used during childhood to gain entry to treehouses and re-emerging conceptually in the late 20th century in the form of bank pins for ATM machines, the modern password has continued to evolve with rapidly transitioning technology to now have a drastically different appearance today.

Taking on a new form as a figurative key to unlock users' accounts for websites and apps, passwords are becoming increasingly valuable, as greater connectivity online has now enabled passwords to grant access to similarly increasing amounts of sensitive information.

Consequently, with passwords and their security becoming more important in everyday life for businesses and individuals alike, it's essential that anyone using passwords understand the role protecting passwords plays in document management systems and practices, as well as ensure they're staying up to date on best practices for password protection.

From the time accounts are made and passwords are created to the time passwords are used to access information, there are risks to watch out for and to protect against.

While many websites and apps today now requiring additional securities like longer passwords and ranging types of characters should already be a good indicator of shifting ideas on the importance of password security, the fact that countless past data breaches have been traced to poor password protection serves as proof of the damage stolen passwords can cause.

Not just protecting social media accounts from being misused to post inappropriate content, passwords are also used with some of the essential components to secure valuable company electronic document management systems—making it essential to not look at passwords as a tiresome requirement by websites and systems, but instead as a critical defense for information.

From the basic do's and don'ts for creating passwords in a modern and interconnected digital world to the impact that the shifting role of passwords has had on how businesses approach document management systems (DMS), throughout this white paper we provide a breakdown on passwords today and the growing importance of ensuring their security at all costs.

CREATING YOUR PASSWORD: SECURITY DO'S AND DON'TS

When creating an account on a site, app, or any other system today, one of the first steps any will require is creating a unique login and password.

With the growing number of sites like Facebook, Twitter, Google, and LinkedIn as just a few examples of the range of accounts a person can have, it can be easy for individuals to become so accustomed to account creation and needing to remember passwords for these different sites that they begin getting into bad password habits.

To help clarify what exactly are best practices for creating your passwords and keeping them secure, below we outline several of the most common scenarios individuals find themselves in as they manage their passwords, as well as some good and bad password habits to get into and avoid:

MAKING YOUR INITIAL PASSWORD

Initially beginning with a series of small breaches which culminated in the infamous Target breach in 2013, the term "Data breach" is unfortunately becoming a household phrase for consumers and businesses alike today.

The rapid adoption of electronics and digital technologies like document management systems (DMS) has led to a growing number of other major companies using such systems to also fall victim to breaches, with top examples including LinkedIn, Facebook, and Yahoo now topping the list with a record 500 million accounts compromised (greater than the entire US adult population).

With the overall impact and cost of a data breach rising along with the growing number of breaches each year, it's now more essential for businesses to take a serious look at their securities and how they may be potentially putting them at risk for a data breach also.

According to recent data, 63% of data breaches are the result of companies having weak, default, or stolen passwords, leaving many business owners now asking the same question—what *does* make for a secure password?

Everyone remembers their birthday, their anniversary, or the name of their elementary school—and these easy-to-remember phrases and numbers are exactly the easy-to-remember potential passwords attackers guess first. Simply put—passwords shouldn't make sense.

Like a mixed-up bowl of alphabet soup, passwords should be a randomized string of letters, numbers, and special characters—including even upper and lowercase letters for further variety and protection.

Stemming from this, creating a secure password unique to each site is also essential to keeping your accounts secure—particularly for critical passwords like bank accounts, internet and phone providers, and other sites you make electronic transactions on.

In the event that one of your passwords is ever stolen or hacked—whether by a phishing email or other form of attack—someone having access to the account can be damaging enough. If all your passwords are the same as the stolen password however, the impact can snowball, with an attacker skipping from one account to the next in search of sensitive information.

STORING YOUR PASSWORD

So you've ditched your straightforward, "yankees12345" passwords and traded them in for a uniquely randomized number and letter combination on each of your accounts, but now the question becomes how to keep track of them all.

Keeping track of passwords on a piece of paper, in a spreadsheet, or in a browser on a computer leaves them highly vulnerable to theft—cyber or otherwise—which can often leave users struggling to keep their passwords organized.

Rather than resorting to bad habits like using the same easy-to-remember passwords across different accounts or storing

passwords on a computer, a secure and highly-recommended potential alternative is a password manager tool, which allows for encrypted password storage and management for the numerous accounts, platforms, and devices a company regularly uses.

In some cases, a password management tool can further up the password security ante by also including add-ons like biometric recognition and the ability to generate unique and randomized passwords.

SECURING YOUR LOGINS

With a secure password in-hand as users go to log in to their favorite websites and apps, the final area emphasis is ensuring login practices themselves are also as secure as possible.

First and foremost, one of the most straightforward password protections a user can make a habit of is specifically avoiding the convenient opportunity of storing passwords in a browser to auto-fill username and password forms.

When users save accounts to a browser, browsers keep this information in a single location, allowing users to easily go back and manage their accounts and the passwords they save.

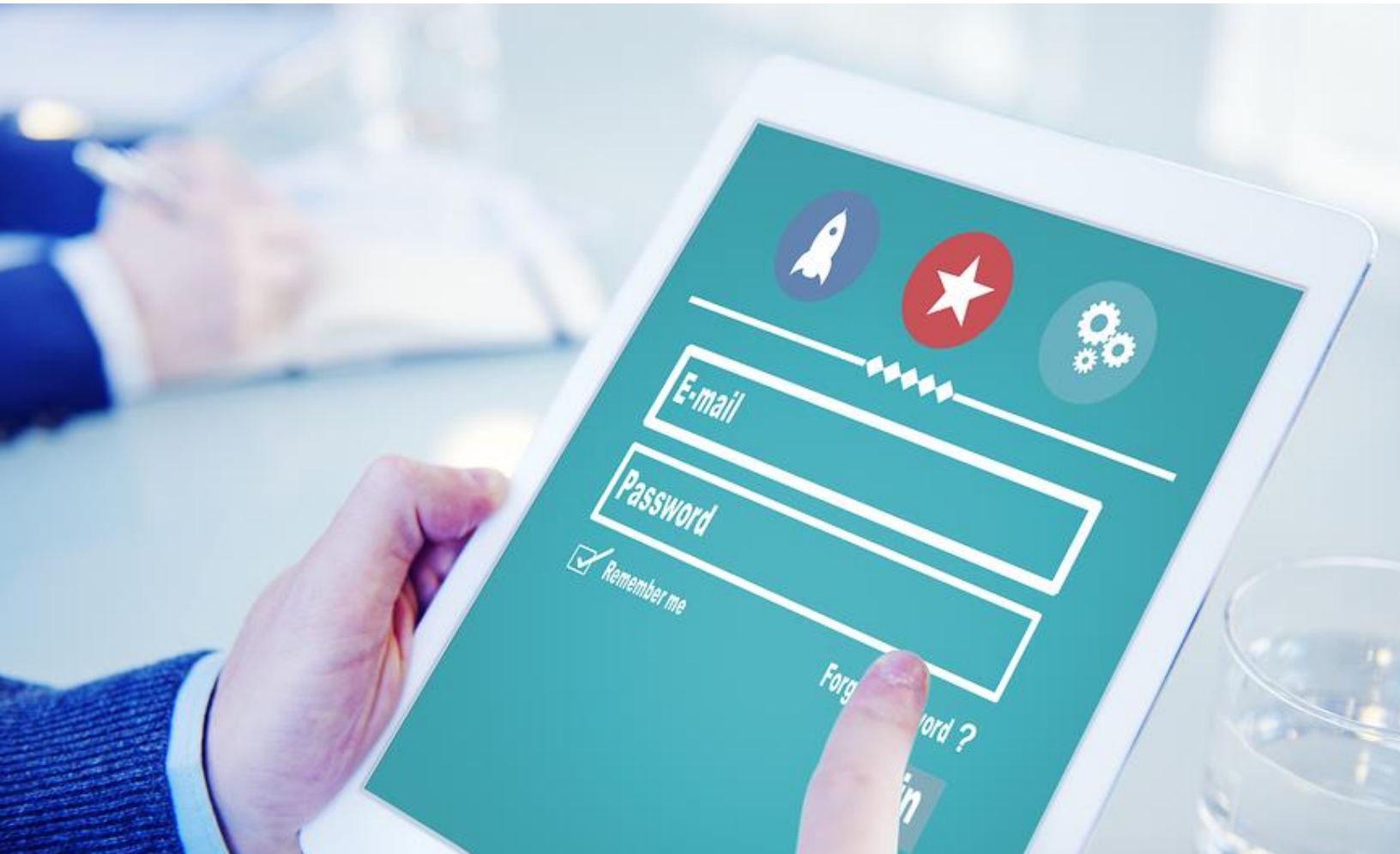
While saving passwords when you login may be nice for getting quick access to accounts, it's also highly risky. With an easy-to-find collection of passwords stored in the browser, all it takes is as a hacked computer or open and unsecured network to provide an attacker a convenient option for "managing" your passwords as well.

To further protect the security of accounts and the passwords used to access them, enabling two-factor authentication is able to offer an additional wall of defense for preventing and protecting from unauthorized logins—even if a password has been cracked already.

Many systems with a two-factor authentication feature implemented will also warn users of an unrecognized and potentially malicious login attempt, providing a good indication it may be time to change your password—as well as other passwords which may be compromised.

Along with avoiding saving passwords and enabling two-factor authentication for logins, also be wary of using public access WiFi.

Like having a conversation as you stand in the checkout line in a store or other public place, other users connected to the network can overhear the information you're sending out over the network. With the use of software and tools like keyloggers, someone spying on you could see your Facebook or email password as you type it to log in.



THE MODERN PASSWORD: NEW WAYS IT'S USED, AND WHAT IT MEANS FOR ELECTRONIC DOCUMENTS

Today, security experts across the globe are able to almost uniformly agree that one of the cornerstones and a basic building block to any well-secured electronic document management system (DMS) is a secure and high-quality encryption system for storing company documents and data.

Although the function of an encryption system is different from social media platforms to post new photos and banking apps for checking in on mortgages, the method one uses for accessing encrypted electronic information is surprisingly similar to the way a user logs into an email account.

Fundamentally, data encryption works likes the cryptic messages ancient Egyptians used in centuries past. These coded message could be understood by only senders and recipients—requiring a secret code to match the random strings of characters and symbols to the corresponding characters needed to decrypt the coded message.

The difference between traditional concepts of an encrypted message and the modern electronic encryption system, however, is that with an encrypted DMS, the "code" one uses to decrypt digital information is specifically called an encryption "key"—a unique password selected and used for accessing the information.

Like the passwords to each and every one of the user's other accounts, the password-protected encryption key works exactly like a key to the front door of one's home or business. Providing access to yourself and the others you trust, a lock on a front door or an electronic encryption system for a DMS at the same time offers security from unauthorized access and misuse.

Considering the protective power and potential of electronic encryption, the metaphoric comparison between an encryption system and the key to a front door can continue to be drawn.

Making hundreds of copies of a door key would be incredibly risky—meaning one only would share copies with those they trust, and similarly, keeping the password-protected encryption key safe and secured must be and always remain a top-priority if businesses plan to protect document management systems from the threat of being breached.

Besides heavy emphasis on protecting encryption keys, however, business owners can also take their password protections to an extra level in an encrypted system by implementing varying levels of access authority for users.

Like a series of doors with different keys needed to unlock each, passwords can be used to further protect confidential information and strictly limit it's access to only those who need it—meaning even if the initial encryption key is stolen, compromised, or cracked, the damage and overall blow dealt to the organization can still be softened.

Despite the power of using password-protected encryption to secure a DMS, however, business owners should be aware of the potential risk in where they store encryption keys. In past instances, companies have unknowingly sabotaged themselves by storing their keys on the same servers as the database itself.

In the event of a data breach caused by a third-party contractor, such as the exploited security gaps in Target's transaction systems, attackers were able to access the remaining majority of company information after a point of entry was already established.

The ultimate point to take away from this is that in a world rapidly transitioning toward digital technologies in both business and everyday life, passwords are more valuable than any other information, and keeping them protected must always remain of the utmost importance.

FINAL PASSWORD CONSIDERTIONS TO KEEP IN MIND

Lost or stolen passwords can range widely in terms of impact—from social media passwords leading to massive internet spamming all the way to DMS encryption keys leading to catastrophic data breaches.

Regardless of what passwords they are or how they may be compromised, one thing remains constant across passwords for all platforms: following the best practices for creating, storing, and using passwords it a critical component to responsibly managing password security and a document management system's security as a whole.

As you now either re-evaluate your current password management practices or begin the process of creating an account and accompanying password for a new system, the following are a few final thoughts to consider:

Are You Using Unique Passwords and Is Two-Factor Authentication Enabled?
Consider the security of your login process—if you're using the same password for social media accounts as the password to your bank account, all it takes is a breach on one site to grant access to much more valuable financial information. Using two-factor authentication will also greatly improve security, as logins from unrecognized sources will be denied even if a stolen password is entered correctly.

How Do You Manage Passwords?
Passwords are granting access to increasing amounts of valuable personal and proprietary information, and it's essential they remain protected at all costs. Passwords should never be written down or stored on one's computer, and similarly encryption keys must always be managed on a server separate from business document management systems.

ADDITIONAL RESOURCES

The Evolution of Password Security

Evolving over time from four-digit PIN codes, passwords and password security has continued to advance and adapt with the changing needs for security in a digital world. Here, we take a closer look not only the password's origins, but also what lies on the horizon for password security.

Expert Opinions on Password Protection

Users continue to run into issues with stolen passwords and hacked accounts, and more often than not, the cause can be traced to passwords. Here, we've collected a variety of tips from security experts on password protection, providing a go-to guide for creating a smart password management strategy.

Will Biometrics Replace Passwords?

Passwords are essential to securing accounts and protecting them from unauthorized access, but if the password is ever stolen, there's nothing to stop someone from getting in. That's where biometrics come in. Using human characteristics like fingerprints and facial recognition for access as opposed to a traditional password, the future of passwords may be evn more personal than you think.