PASSWORDS:

The real threat to your security

wwpass®

HACKING THE CODE

The tide-turning victory of World War II wasn't on a beach, in the air, or the sea, but in New York City. Military codes for both the Axis and Allied powers were constantly trying to be broken by the enemy, and luckily, the New York Public Library had the phone books that deciphered the Japanese naval codes.

The side that managed to crack the enemy's military code was invariably the side that won. So, inventions like the Enigma Machine were employed to dumbfound opponents with a supposedly un-crackable code. Except for one thing: **There's no such thing as an un-crackable code.** Ultimately, deciphering code is puzzle solving. If a human structures a puzzle, another human can piece it back together.

It explains the motivation of hackers today: From infiltrating company data centers for customer data to disrupting political processes, digital thieves are solving these modern-day puzzles and turning in to a major menace for businesses.

They're fast and stealthy, too: When web servers first go online, spyware makes contact within twenty minutes. Now that the hackers are hiding in the network, it's a waiting game until someone slips up and reveals passwords and usernames.

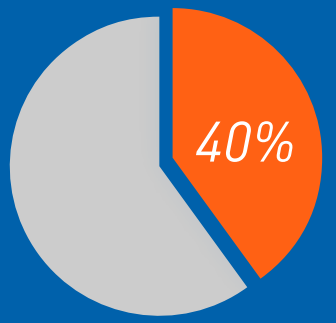
The username and password combinations are known as human readable credentials (HRC). And they're the biggest lapse in Internet security.



The results have been predictable for years:

People just don't pick very secure passwords.

*Based on natural behavior, as well as statistics, HRCs are not effective at locking digital accounts. About **40% of people per year** had accounts hacked, passwords stolen, or received some sort of notice of compromise to their accounts.*



STOP REHASHING THE PASSWORD

Remembering unique and random character strings for every online account is infeasible, so employees tend to implement all sorts of dubious methods.

- Duplicate passwords across accounts are common and hazardous.
- Changing passwords often is also a futile routine, given how ineffective it is.
- Using password managers is a better approach, but it still protects passwords with yet another password.

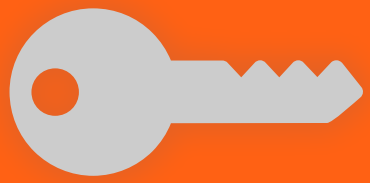
Goofy blunders like these happen daily. The wrong people keep gaining access and these human-readable credentials aren't hacking it anymore.

*SplashData records an annual list of the top twenty-five most popular—**and worst**—passwords. The top five have depressingly held the same ranking for years:*

123456 ***password***

12345

qwerty 12345678



You might as well just leave the key in the door.



HOW TO PREPARE FOR CYBER SECURITY'S STORMY FORECAST

CYBER CRIMINALS KNOCK ON DATA'S DOOR

The frequency of major corporations reporting email hacks is increasing, leaving millions of their users at the mercy of time and random chance. Even if the login credentials are protected by the user, a data breach within the company network can make a complex password moot.

Yahoo has suffered multiple data thefts. Some of them have taken years to uncover, with the latest breach traced back to 2013. Restoring credibility or offering stronger security is irrelevant; it's impossible to be secure with total certainty.

Beyond identity theft are more sinister motives. The real potential of exploiting access control is much worse: Compromised passwords contribute to internet outages and massive distributed denial-of-service (DDoS) attacks.

Cyber-crime takes many forms beyond theft. HRCs are critical security lapses in the age of information warfare.

Hackers have plenty of motivations to DoS a target, which can act as a smokescreen while they steal data, a nasty digital prank, or an ideological or political statement. A network attack is fundamentally no different than knocking out a power grid. It's a crime against society, and the automatic programs that hackers use are at super-villain levels.

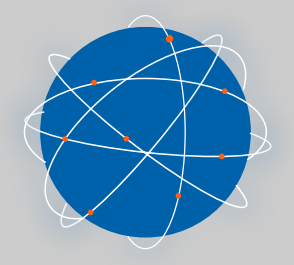
Enter the botnets. Rogue software infiltrates an account or device and stays there; a Trojan virus usually hides on the stricken device, allowing the perpetrators to hijack it whenever they want. This group of commandeered devices forms the hacker's botnet, and it's a formidable weapon.

Data breaches and digital identity theft in e-commerce and the retail industry are routine.



According to IBM, the estimated cost of one commercial data breach averages ***four million dollars****—presuming the breach is even discovered.*

Denial of service *—A cyber attack that hijacks multiple devices to overload a web resource with superfluous traffic.*





HOW BAD IS THE BOTNET PROBLEM?

Stopping hackers from tapping computers and smartphones is hard enough; all devices need this protection. The Internet of Things (IoT)—simple internet-enabled devices such as smart TVs, network routers or Internet-enabled cars—are proving to be one of the most vulnerable lines of attack. These gadgets are just as susceptible to intrusion and are even more likely to go unnoticed. In addition to zombie computers, artificial intelligence (AI) can be employed in various ways to hack humans or devices using multiple attack vectors. At that point, it's not even a hacker that's trying to trick users. They're being manipulated by something significantly more advanced, calculated, and "intelligent."

IoT devices have significant computing power when working together, and a shocking number of them still have factory-default HRCs.

Botnets hide in software, waiting to be activated. Attacks have temporarily disabled anything from a cyber-security journalist's blog to Sony's PlayStation Network. The implication of shutting down a web service is unsettling—especially when they're tipping us off to these malicious attacks.

As long as the standard username/password combo remains, it won't matter if users have a 35-character-long randomly generated code to lock an account. Our locks have too many exploitable loopholes.

If specific websites can be shut down, then a massive internet outage is not just science-fiction, it's likely.

THE PASSWORD TIPPING POINT

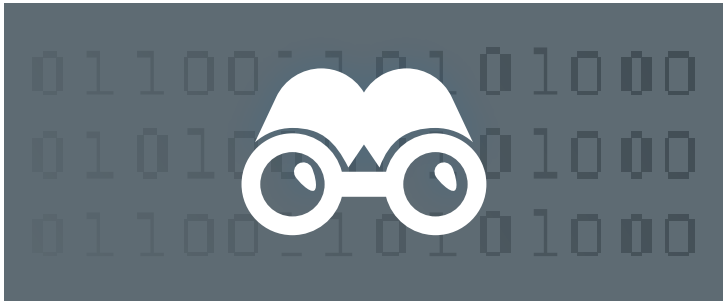


Access Control Needs an Upgrade

In Greek, cryptography means "hidden or secret writing," and computers are better at it than humans. The password works by completing a line of code being sent to where the data is stored. Like the ciphers in WWII, this complete code locates and unscrambles the data. It can't be unscrambled without the missing chunk of the cipher (password).

It is then illogical to secure this computational deciphering process with something simple and memorable, but easily stolen. What was once an organizational necessity is now the internet's biggest lapse in security.

The web has evolved and so have hackers. Shouldn't the whole approach to access control evolve as well?



81%

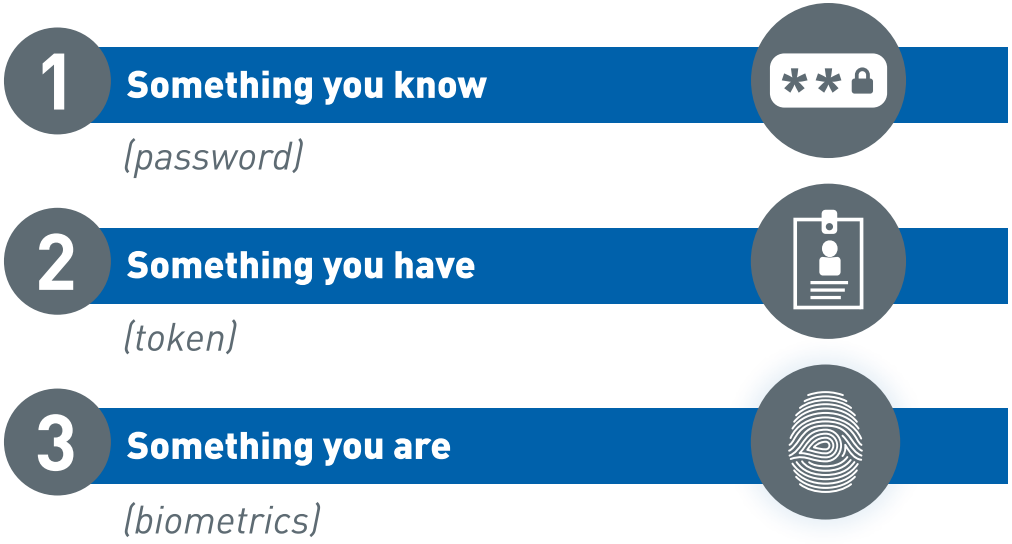
Security breaches due to stolen usernames and passwords, according to Verizon. *This isn't a problem that has an easy solution;* ***it's a structural weakness, which requires rebuilding and changing habits,*** *including IAM systems, the foundation of identity, and more.*

Major network authorities such as the Department of Commerce's National Institute of Standards and Technology (NIST) are already planning to restructure access control.

TAKING IDENTITY FOR GRANTED

> If someone hacks your password, you can change it – as many times as you want. You can't change your fingerprints. You have only ten of them. And you leave them on everything you touch; they are definitely not a secret.
>
> – AL FRANKEN

A password isn't restricted by any proprietary information—anyone can know or guess one. So, as a means of proving identity, it doesn't do much. Effective security makes use of three different form factors for authentication.

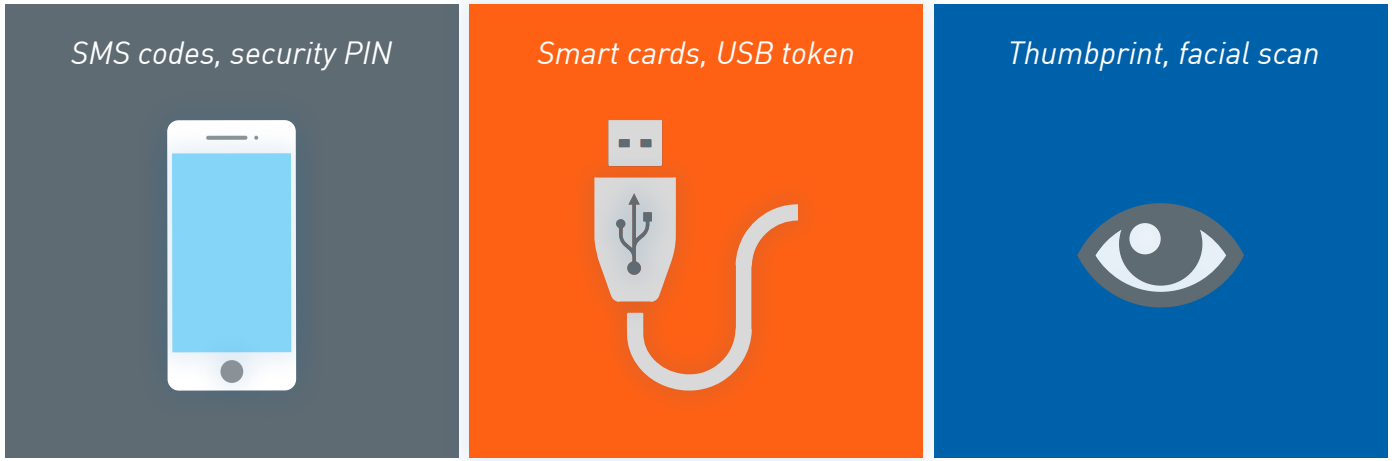


Password Prime Directives

- Make passwords a minimum of x characters (8-10 are the minimum, 12+ is better).
- Use a long, uncommon phrase or set of random numbers, letters, and symbols, including upper and lower case.
- Never reuse a password.
- Don't use names, or any word that can be found in a dictionary.
- Avoid scams with a form of multi-factor authentication.

Multi-factor authentication uses two or more methods of identity confirmation. Since a secret passphrase isn't enough, MFA strengthens security by requiring different types of user knowledge, possession or inherence. Backing up a password with a security token or a thumbprint scan would make it harder for hackers to crack credentials.

These requirements must be met for every user on the network to keep hackers out. The whole point of MFA is to invalidate password exposure. But they're not all created equal: A lot of secondary authentication is a lateral move, unwittingly giving hackers more options, which causes the balance between good cyber security and convenient access to continue to be a challenge.



The good news: MFA methods are common now.

They range from password recovery questions to linking accounts with a phone or email address. Less widespread are USB or smartcard tokens, as well as thumbprint scanners. However, NIST discourages using SMS as a second factor of authentication.

The bad news: Most of them have been hacked.

MFA AND CYBER-DEFENSE

Security Questions	*SMS or Email Confirmation Codes*	*Biometrics*	*Software Authentication Keys*
With verification questions, it's ill-advised to give valuable and unchangeable personal information associated with the user's account. There are too many digital footprints and clues that lead intruders right into people's accounts. The "secret" answers are stolen the same way they steal passwords.	While our phones and emails seem secure, they are the most common cyber attack vectors. Hackers can intercept confirmation codes via SMS with the same illegal password interception strategy. Many businesses are abandoning this method because it's functionally two easily-swindled passwords instead of one.	Getting there, but still not foolproof. There are many ways to recreate biometrics and fool the authentication. Commercial scanners for use with personal devices are just converted into readable and steal-able data, just like the password.	Encrypted security keys like smart cards or USB sticks are effective, if they don't get lost (an unavoidable human error risk). This option might be more difficult for widespread use, but it solves the problem of HRCs by getting rid of them completely.
Cyber-Defense Rating: ★★★★★	*Cyber-Defense Rating:* ★★★★★	*Cyber-Defense Rating:* ★★★★★	*Cyber-Defense Rating:* ★★★★★

Despite multiple authentication methods backing up a password, they still don't address the fundamental problem: All human input is still vulnerable.

Implementing authentication solutions that don't address the core foundation of the problem is like polishing the brass on the Titanic.

THE BEST DEFENSE? REDUCE YOUR VECTORS PRONE TO ATTACK







It's impractical for hackers to directly attack a server or data center, which require too much time and computing power. Criminals are eager to exploit predictable human behavior, and that becomes a war of attrition between the user and the hacker. Humans just aren't designed to store data the same way computers do, so username and password combos remain uncomplicated. How long can users manually reinforce their security before the digital attacks break through?

Hackers' tricks all involve psychological manipulation. In cyber-security terms, this falls under social engineering.



MAN IN THE MIDDLE

ROGUE INTERCEPTION OF HRCS THROUGH SCAM OR IDENTITY THEFT

Whether hackers impersonate a user or a company rep, a well-run scam will work on someone eventually. Social engineering and various schemes can intercept emails and text messages, extracting credentials through the communication.



PHISHING

A HACKER'S ATTEMPT TO DISGUISE THEMSELVES AS A TRUSTWORTHY ENTITY, TRICKING USERS INTO GIVING UP INFORMATION

Common email schemes that broadly target company accounts in attempts to disrupt the network or steal valuable data work, too. Phishing emails have an open rate of 30%, according to the 2016 Verizon Data Breach Investigations Report. Stolen user credentials are just one part of phishing. It remains the most successful delivery method of network-crippling malware.



BRUTE FORCE

UNAUTHORIZED INTRUSION THROUGH SYSTEMATIC TRIAL-AND-ERROR

Guessing will eventually work: Passwords such as "123456" and "password" barely require snooping and programs called password crackers systematically try all possibilities. Both styles of intrusion are why weak passphrases have got to go. A simple password can be cracked in minutes, while a complicated one can take years. Password-guessing software also isn't regulated. Many are open source and free to download.



JOIN THE REVOLUTION, DITCH ALL PASSWORDS

> If you do what you've always done, you'll get what you've always gotten.
>
> – TONY ROBBINS

DO AUTHENTICATION DIFFERENTLY

It's safe to assume that if it's online, it's at risk. One compromised account means all accounts are compromised. Your password will never be foolproof for too long, so changing it regularly is the only defense—until now.

The best authentication approach is one that eliminates the weakest link in most authentication models: the username and password pairs that can be easily hacked and phished. Instead of proving your identity with a user name, you prove it with your personal pass key or token. This defends against hacking when the credentials (certificates) associated with your token (which can be a smart card, USB or mobile app) are anonymous to applications and to participating service providers. In addition, they are not stored on the key itself or on your computer.

Taking a different approach to authentication may be inevitable as well. A devastating cyber attack and revised compliance regulations may cause enough of a stir to expedite a major change to Internet standards. Redefining access control may come sooner than we think.



Ready to ditch your passwords for something better?

Contact us to start today.

Know someone using logins that are dangerously outdated?

Share this to get the word out:

wwpass®

Sources

- Entrepreneur - Password Statistics: The Bad, the Worse and the Ugly (Infographic)
- Splash Data - Announcing Our Worst Passwords of 2015
- Verizon – 2016 Data Breach Investigations Report
- The Hacker News – Password Security – Who's to Blame for Weak Passwords? Users, Really?
- IBM – 2017 Ponemon Cost of Data Breach Study
- IT Security Guru - Changing your password regularly won't fix the problem – you need to change the entire password security system

wwpass®