FORTRA

The Power of the Password

Contents

It’s amazing to think that something as small as a password can make or break your business.

Stolen or weak passwords contribute to an alarming 61% of company data breaches. Factor in the average cost of a corporate data breach — $4.24 million in 2021 — and you have one powerful, pricey little word. The fact is, each one of your employees is responsible for multiple passwords. This means your staff is the first line of defense when it comes to protecting your business’ sensitive information. Don’t let inadequate password security be your downfall. Learn more about maximizing diligence and minimizing risk in this guide.

Recognize Your Weakest Links

Many businesses spend thousands of dollars on network security enhancements in the hope of improving their security posture. They invest heavily in the latest cybersecurity solutions and continue to pour time and resources into security improvement initiatives.

Unfortunately, these businesses may overlook one primary vulnerability – the people who work there.

Even the most well-meaning staff member can be an organization's weakest link when it comes to network security. Often this is due to a lack of security awareness. Employees across demographic groups face challenges when it comes to security awareness. The growth of the Internet of Things (IOT), Industrial Control Systems (ICS), Bring Your Own Device (BYOD), and remote work, combined with the highly dynamic hacker universe, creates a moving target when it comes to securing your networks.

Costly Mind Games

Data breaches have a variety of costly impacts on a business, including sizable fines and legal fees, negative media coverage, waning customer loyalty, and damaged company reputation. As organizations become increasingly wary of data breaches and adapt their security, cybercriminals continue to evolve as well. Hackers consistently adjust their tactics, choosing to work smarter, not harder, and utilizing the psychology of human nature to get to the information they seek to abuse. Many exploit a person's willingness to be helpful by making seemingly friendly, harmless requests.

Additionally, scams have become more visually sophisticated. They are often cleverly disguised to appear legitimate, so even somewhat vigilant staff members do not perceive a threat and feel confident in disclosing information that can lead to data breach.

To combat against these offensives, employees must be educated well and often. Strong password security is a fundamental first step in an effective security strategy, so staff need to be equipped with password security best practices to help mitigate the risk of an attack.

No Business is Immune

While most of the main-stream news about data breaches focuses on large enterprises, small- and medium-sized businesses are far from unaffected. In fact, 43% of cyberattacks target small businesses, according to Verizon's Data Breach Investigations Report.

One of the most powerful lines of defense for companies of all sizes is employee education and security awareness.

It's vital to ensure your staff understands that any business can be a target at any time. Dispelling a few myths about hackers can help your employees better recognize attempts.

BREAKING NEWS
NEWS
NEWS
BUSINESS
VIDEO
PHOTOS
If You Have a Taste for Adventure
Adventurous travelers have a trick
to finding a cheap fare: Book a ticket to somewhere
International payments problems - 23 Mar
We are creating a system where very talented
their own style and share everything.

Hacking Myths

Myth#1: Hackers are Rude

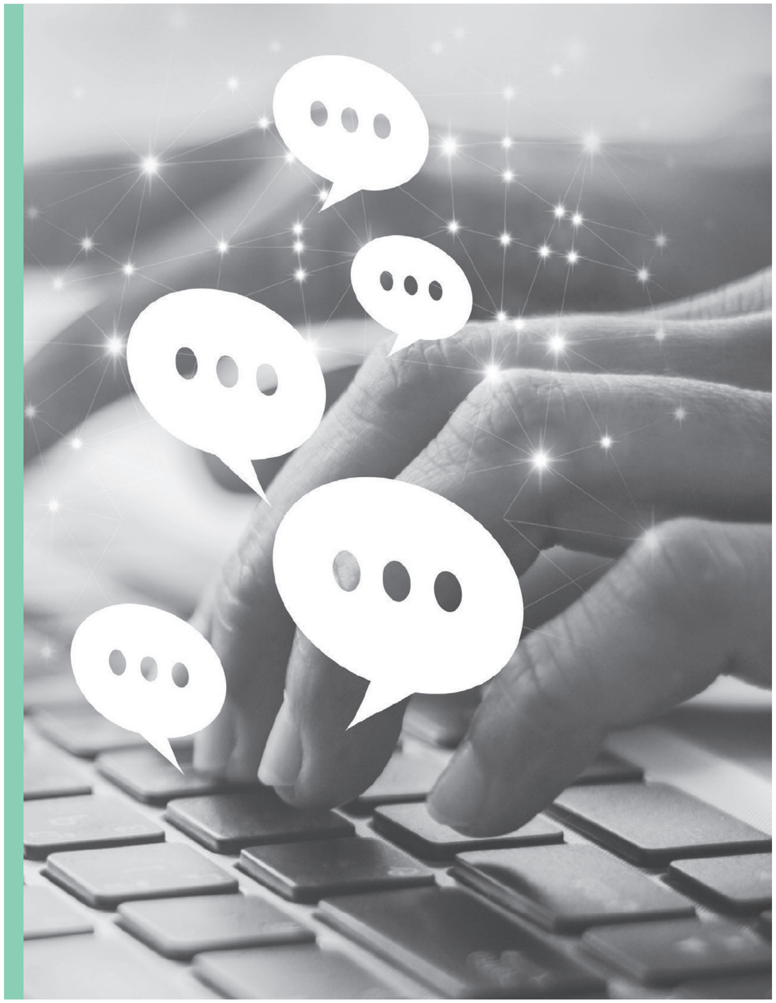
Not all malicious actors are overtly rude. Often, they cleverly disguise themselves, making minimal, polite requests for seemingly harmless data that will actually help them discover credentials or passwords.

Hackers frequently devise scenarios such as:

- Masquerading as a friendly IT team member needing to verify credentials for a software update
- Posing as a representative from HR needing to verify personal details
- Disguised as a coworking innocently requesting lost or misplaced information

Myth#2: Hackers are Always External

A significant portion of cyber threats come from within a company's own walls. A disgruntled employee or a staff member can create back door access, intentionally sabotage equipment or processes, or even receive money for stealing critical corporate information. All employees should closely scrutinize any requests for credentials or other information, even those from a colleague.



Myth #3: Hackers are Dumb

Hackers are intelligent and resourceful. They are notorious for gaining access to proprietary data through the exploitation of weaknesses.

Hackers can design emails to look as though they come from your bank, a trusted vendor, or a social media site. These emails usually request users provide account or personal information or that they click on a link to verify account details. When the link is clicked, the user is taken to a fake website mirrored to look authentic, providing a place for users to enter credentials. The data inputted is sent directly to the hackers.

Additionally, with a $300 processor a hacker can run billions of simple, lowercase, eight-character password combinations a minute to try to access a site.

If a hacker does gain access to a password, they can run that passwords against multiple sites or systems at one time.

If that password has been reused, the hacker will be able to gain multiple points of entry.

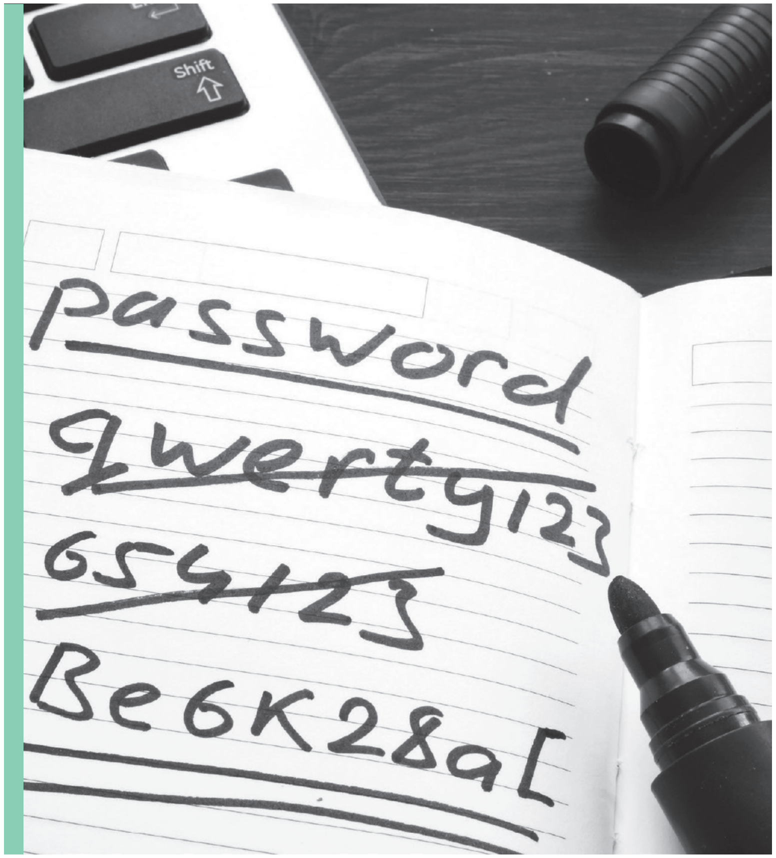
Breaking Bad Habits

Once a staff understands the very real hacker threat, it’s important to arm them with the tools and information to ward off attacks. This can be as simple as correcting basic bad habits or changing mindsets.

Recycling is Wrong

Green living can be great, but not when it comes to passwords. Reusing or recycling passwords across different sites and systems just makes life easier for hackers. All they need to do is capture one password and then they can reuse it over and over to find other systems and applications that can be broken into with those credentials.

About 59% of people use the same password across multiple sites and systems. There are many reasons for this, including apathy or lack of awareness. Additionally, people can just feel a false sense of security, believing “It won’t happen to me.” Unfortunately, statistics don’t lie. A cyber attack happens every 39 seconds, and most often the hacker is trying to steal credentials.



A Personal Mistake

These days, passwords are needed for everything from bank access to Twitter accounts. It's no wonder that staff and individuals continue to create and use passwords which are simple and easy remember. Unfortunately, easy to remember often also means easy to guess. Creating passwords with basic personal data is a bad practice. Social media and other online presences make it easy for hackers to find personal information such as the names of pets, children, or even high schools or colleges attended. Additionally, passwords created from common keyboard patterns can also be easily guessed.

When Sharing is not Caring

Other issues arise when staff share password and access credentials with co-workers. It is essential for employees to understand that tight access controls are a cornerstone of any organization's security strategy. Coworkers and web applications, including instant messengers and email, can be hacked, so it is important no passwords are shared among systems or employees.

Approximately 300 billion passwords are used by humans and machines worldwide. (CybersecurityVentures)

Top 10 Most Common Passwords

(cybernews 2021)

1. 123456
2. 123456789
3. qwerty
4. password
5. 12345
6. qwerty123
7. 1q2w3e
8. 12345678
9. 111111
10. 1234567890

Password Best Practices

Part of creating a culture of security is sharing best practices and encouraging good habits. Below are a few suggestions for fostering healthy cyber hygiene.

Know your NIST

The National Institute of Standards and Technology (NIST) issues guidelines or best practices for corporations regarding securing identities and passwords. While not everyone agrees with NIST guidelines, it's important to know the current recommendations and the reasons behind them. The 2021 NIST password guidelines include a few adjustments in thinking from previous years, including a move away from password complexity and knowledge-based authentication. IT professionals should take NIST recommendations into consideration when rolling out or updating password and authentication policies for staff.

Creative Phrasing

Some experts recommend the use of phrases instead of words when creating passcodes. Substitute favorite team names or pets with a pass-phrase. Simply take the first letters from words in familiar phrases, mix in special characters and numbers and come up with a phrase that is easy to remember.

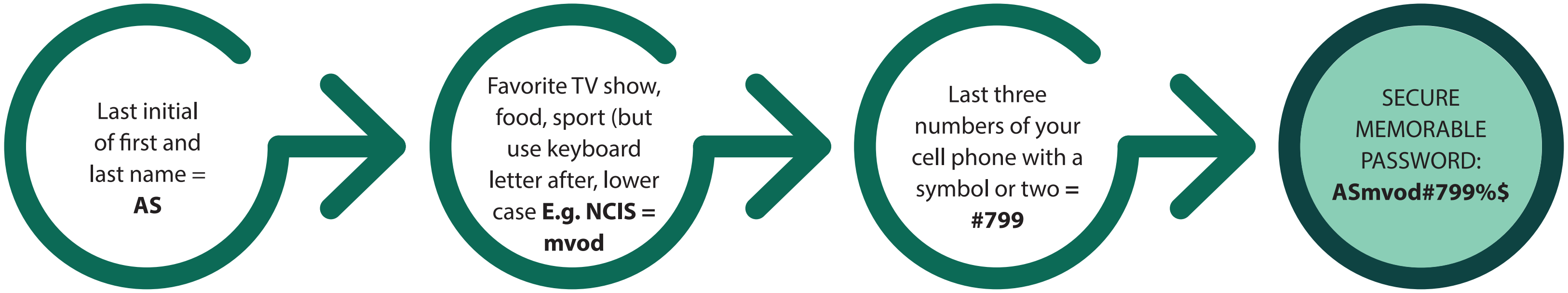
Example phrase:

A long time ago in a galaxy far, far away

Example password:

@L+@1@gf,f@!

Pass-Phrase Security



Last initial of first and last name = **AS**

Favorite TV show, food, sport (but use keyboard letter after, lower case **E.g. NCIS** = **mvod**

Last three numbers of your cell phone with a symbol or two = **#799**

SECURE MEMORABLE PASSWORD: **ASmvod#799%$**

Embrace the Tech

There have been a variety of tools developed over the years to help businesses and users create and maintain secure user access. These tools can be exceedingly helpful in the fight for credentials and access security.

Two-Factor Authentication

Two-factor authentication is a security process in which the user provides two means of identification, one of which is typically a physical token, such as a card, and the other is typically something memorized, such as a security code. These can be easily set up on mobile devices for both personal and business systems.

Biometrics

Biometrics refers to authentication techniques that rely on measurable physical characteristics that can be automatically checked. There are several types of biometric identification schemes such as face, fingerprint, retina, and signature. Biometrics continues to be an area for improvement and is often utilized to aid physic security systems as well as electronic.

Password Management Solutions

A dedicated password manager will store passwords in an encrypted form. This secure method of storage is far preferably to storing written passwords under a keyboard or in desk drawers. Password managers can also flag duplicate or weak passwords and help generate secure random passwords. Most password managers can synch across devices and many offer some type of two-factor authentication.

Effective Security Training and Testing is Key

Regular employee training is imperative when it comes to protecting your organization. Training must be conducted repeatedly at regular intervals to keep staff apprised of the latest cyber threats. Hackers are constantly evolving and adjusting their tactics, so continuing education is needed to maintain security awareness.

Additionally, it's good to put your organization to the test when it comes to security. Just as regular vulnerability scans and pen tests are essential to uncovering weaknesses in you network, social engineering tests can reveal weaknesses in your staff's ability to thwart cyber attacks.

Attack vectors continue to increase, so be sure your security program is comprehensive. By using a vulnerability management solution, combined with penetration testing, social testing, and employee awareness training, you can more effectively mitigate the risks that come at you from different angles.

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.