A Cybersecurity Awareness Month Series

Strong Passwords

What they are and why you should use them

Baker College

10/04/2023

Presenters

- **Stephen Ragsdale,**
  VP of ACM at Baker College
- **Ryleigh Blankenship,**
  Member, Cyber Defense Team at Baker College
- Contributions by Gabriel Collard, ACM Treasurer and Sherri Maciosek, ACM Advisor

Baker College

Overview

- Why You Need a Secure Password
- How to Create a Secure Password
- Keeping Passwords Secure
- Questions at the End

REINER SCT, 2021

Cristianrodri17, 2017

Baker College

Why You Need a Secure Password

Baker College

Did you know?

- It only takes **10** minutes to crack a **7 letter password** with the help of brute force software on today's hardware (Armstrong, 2018)..
- A brute force software attack probes **every possible** combination of letters, digits, and symbols and is **guaranteed** to work, it just takes time, which is why the **longer** the password the **better**!
- Password compromise is the **most common** cause of a data breach (Sobers, 2022; Armstrong, 2018).
- The average cost of a data breach in the United States is **7.91M** (Sobers, 2022).

Bermix Studio, 2023

Baker College

What is at risk?

Some of the things that can be stolen include (Cyber Aware, 2018; NIST, 2022; Spadafora, 2023):

- Money, credit card information, bank accounts, job payments
- Personal data: address, name, phone number, email
- Medical information: change your information
- School information: grades, attendance records, financial aid info.
- Other passwords: access to other sites; do not use the same password on multiple sites!

Anja, 2017

Baker College

How Criminals Obtain Passwords

Dictionary Attack

Automated password guessing using words in the dictionary

Brute Force Attacks

Multiple Password Combinations used at once to guess passwords

Credential Stuffing

Stolen credentials are used to access other accounts and profiles

Password Spray Attack

An attempt to access multiple accounts within the same company that use the same password

Riki32, 2022

Baker College

Hang, 2023

Insecure Passwords

Here are some examples of insecure passwords

- **Single Words:** Baker, College, Finance
- **Numeric or alphabetic order:** 1234, abc
- **Repeating characters:** 0000, aaaa
- **Common words:** Password, Admin
- **Descriptive words about you:** Student, Supervisor, New Employee

None of these are good options to use so it's best to create a secure password (CISA, 2021; EC Council University, 2023; Price, 2023).

Baker College

How to Create a Secure Password

Baker College

Creating Strong Passwords

Here are the attributes of a strong password

- **Long Length:**
  - 12 is okay; 16+ is preferred
- **A Mix of Letters, Numbers, and Symbols**
  - **Example:** 5&Fb^KT9#*)BtK
- **Not sequential:**
  - **Example:** C32eB^m_Q@tW5Lky
  - **Not**: ABCD123!@#$
- **Does not use context specific words**
  - Jsmith10131950 is a weak password for John Smith

Towfiqu, 2021

Baker College

National Institute of Standards and Technology Password Guidelines 2023

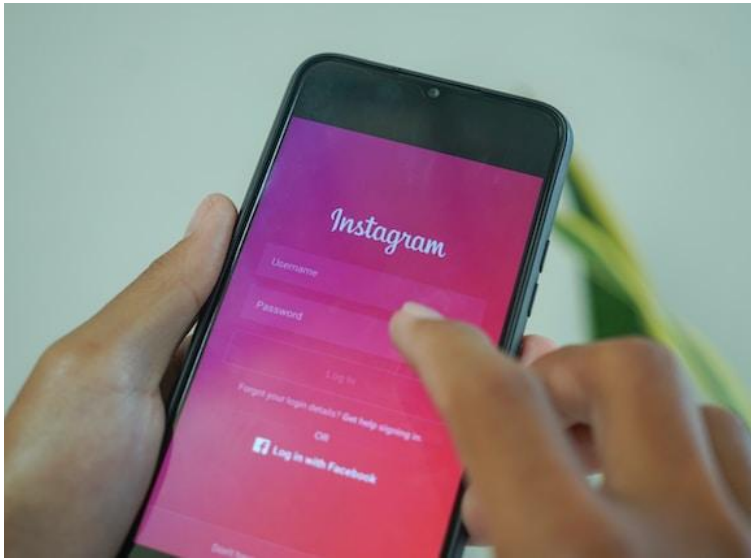
Creating Strong Passwords

More example Strong Passwords

- **Unique:**
  - **Example:** Gt9WmV!38Lt@4
- **Phrases or Famous Quotes that You Know**
  - **Example: mDgtN$2yL@StB1!!**
  - “My dog turned 12 years old on September 11”

However, Do NOT Share your passwords

- Sharing lets others have access and is compounded if the same password is used for multiple accounts!



Zativa, 2022

Baker College

National Institute of Standards and Technology Password Guidelines 2023

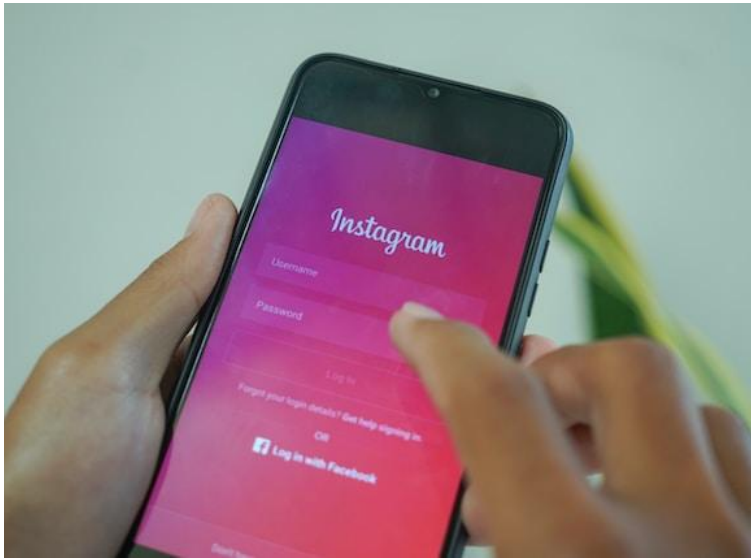
Creating Strong Passwords

- **Having trouble creating strong passwords? Use a password generator!**

https://bitwarden.com/password-generator/

- **Want to know the strength of a password?**

https://bitwarden.com/password-strength/



Zativa, 2022

Baker College

PASSWORD CHALLENGE
Which password in each group is the strongest?

Group #1

A. Password
B. 9@55w073
C. P@55w07d
D. Pa55w0rd

Group #2

A. ()@22yB0s1ne55_13*
B. H@ppy8usin35513*
C. H@22yBus1ne5513_*
D. HappyBussiness13*

Baker College

PASSWORD QUIZ ANSWERS

Group #1

A. Password

B. 9@55w073

C. P@55w07d

D. Pa55w0rd

Group #2

A. ()@22yB0s1ne55_13*

B. H@ppy8usin35513*

C. H@22yBus1ne5513_*

D. HappyBussiness13*

Baker College

PASSWORD CHALLENGE
Which password in each group is the strongest?

Group #1

A. 1234567*abc!!
B. ab!33cd72*efg01+
C. Tabl3topper_1945*
D. Twenty20_24#19

Group #2

A. Hello-World!*773
B. 855662356546486 8 (Bank Account Number)
C. Mon$er_M@$#
D. Th!r733nG&nTh!rd33

Baker College

PASSWORD QUIZ ANSWERS

A. 1234567*abc!!

B. ab!33cd72*efg01+

C. Tabl3topper_1945*

D. Twenty20_24#19

A. Hello-World!*773

B. 855662356546486 8 (Bank Account Number)

C. Mon$er_M@$#

D. Th!r733nG&nTh!rd33

Baker College

Keeping Passwords Secure

Baker College

Keeping Passwords Secure

There are several ways to keep your passwords secure

- **Use a password manager** (LaSalle, 2022, NIST 2023)
- **Change them frequently** (CISA, 2021; EC Council University, 2023).
- **Not reusing passwords** (Cyber Aware, 2019)
- **Use two-factor authentication**

Bicker, 2022

Baker College

Password Manager Pros

Password managers can be a good tool use (National Cybersecurity Alliance, 2022)**.**

- **Pros:**
  - Saves time.
  - Easily creates and stores strong passwords
  - You do not have to make or create more than one password.
  - Uses encryption

Jovanovic, 2017

Baker College

Password Manager Cons

Password managers can be a good tool use BUT

- **Cons:**
  - If someone gets into your password manager, they get all your passwords
  - You need some computer knowledge

Jovanovic, 2017

Baker College

What is Data Encryption?

Data Encryption is a way to protect Passwords

- Once a password is made, its sent to a server to be stored.
- If that server is compromised, the attacker has all the passwords!

!!HOWEVER!!

- Data encryption makes it difficult for an attacker to access plaintext passwords.
- It scrambles and adds characters to make it impossible to read.
- Therefore, if a server is compromised, the password are safe!

Fresh, 2018

Baker College

Data Encryption

- Unencrypted Passwords are easier for attackers to compromise.
- Encryption uses hash functions on passwords to help protect them.
- Salting: extra characters to your passwords before hashing them.
- Encryption types include
  - SHA-2: Gives higher security, better than SHA-1
  - Bcrypt: Sturdy hash protects from brute-force
  - PBKDF2: also protects from brute-force
  - Argon2: most secure against brute-force and hash-table attacks

Schmitz, 2023

Baker College

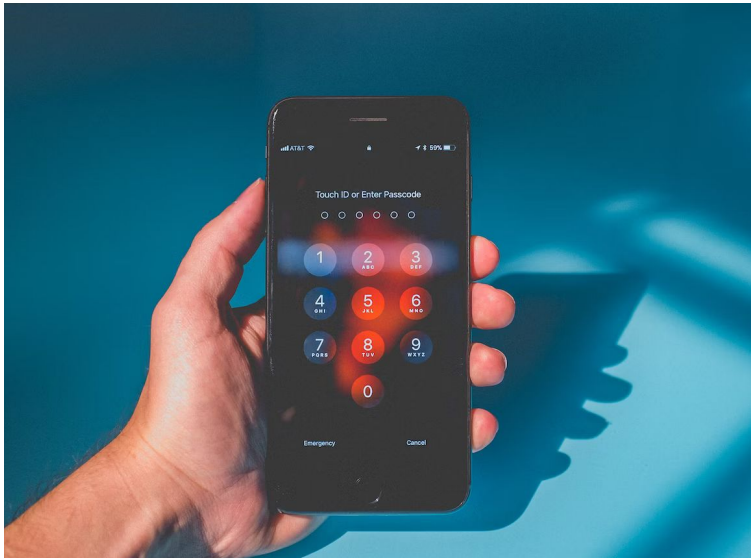
Password Policies

Password policies can help make your passwords more secure

- By enforcing extra requirements, third-party password policy tools can help to prevent common passwords, short lengths, and even compromised passwords

- With poor password policies, your data is not secure even with Two-Factor authentication

- Some tools can find accounts in Active Directory that use passwords that have been breached, etc.



Eliason, 2017

Baker College

Denyer, n.d.

Password Policies

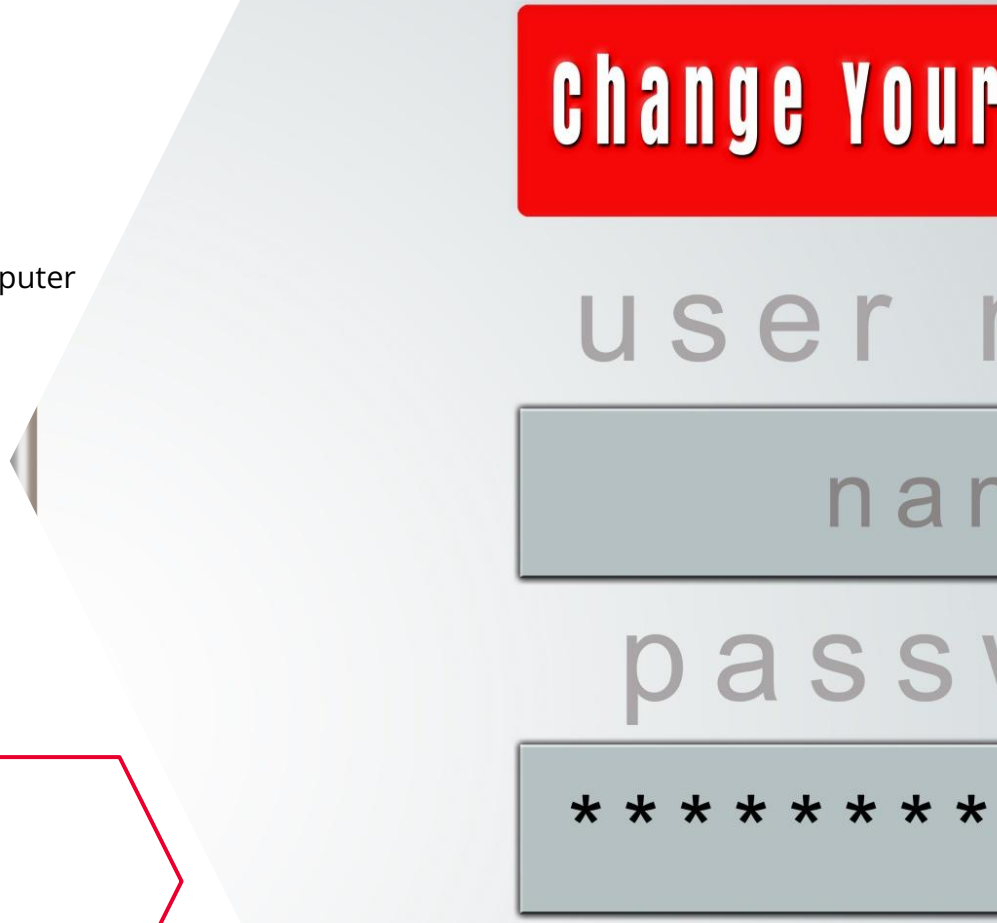
- Passwords should be regularly changed (esp. weak passwords)
- Keeping the same password creates vulnerabilities.
- These items apply more to weak passwords than strong passwords
- A trending philosophy for the use of strong passwords is not to change them

Baker College

Denyer, n.d.

Password Policies

- If you find out you used an insecure network.
- You have malware or a virus infecting your computer or device
- Highly recommended every 3 months or if your account was breached
- You have removed people from your account.
- You are no longer using an account.



Baker College

Two-Factor Authentication

What is Two-Factor Authentication?

- **Pros:**
  - Extra layer of security by preventing unmanaged devices
  - Confirms to the SSO (Single Sign On Systems)
- **Cons:**
  - Phones are easily lost, broken, or stolen
  - Increase in log-in time and can be mildly irritating

To learn more about 2FA, please join us next week on Tuesday, October 10, 2023, from noon to 1:00 pm ET for an excellent discussion on multi-factor authentication!

Fresh, 2018

Baker College

Thank you!

Questions?

Baker College

References

Anja. (2017). *Computer Security Internet* [Photograph] Pixabay. https://pixabay.com/illustrations/computer-computer-security-internet-2038627/

Armstrong, M. (2018). *The Price Tag Attached to Data Breaches.* Statista. https://www.statista.com/chart/9918/the-price-tag-attached-to-data-breaches/#:~:text=Data%20Security&text=As%20well%20as%20the%20negative,price%20tag%20of%20%247.91%20million

Bermix Studio. (2023). *A Person Wearing a Mask Using a Laptop* [Photograph]. Unsplash. https://unsplash.com/photos/56CjIvG10lo

Bicker, D. (2022). *Protect Your Data* [Photograph] Pixabay. https://pixabay.com/photos/data-protection-security-computer-7158385/

CISA. (2021). *Be Cybersmart. Cybersecurity Awareness Month 2021: Do Your Part. #Becybersmart.* https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20Awareness%20Month%202021%20-%20Creating%20Passwords%20Tip%20Sheet.pdf

Cristianrodri17. (2017). *Cybersecurity Image of Text* [Photograph] Pixabay. https://pixabay.com/illustrations/security-computer-science-computers-2337429/

Cyber Aware. (2019, May 29). *6 Steps to Better Password Hygiene.* Business Victoria. https://business.vic.gov.au/learning-and-advice/hub/6-steps-to-better-password-hygiene

References

Denyer, C. (n.d.). *Dialog Box Change Password* [Photograph]. Public Domain Pictures. https://www.publicdomainpictures.net/en/view-image.php?image=143721&picture=dialog-box-change-password

EC Council University. (2023, Mar 23). *The Importance of Strong Passwords and How to Create Them.* https://www.eccu.edu/blog/technology/the-importance-of-strong-secure-passwords/

Eliason, K. (2017). *Person Holding iPhone* [Photograph]. Unsplash. https://unsplash.com/photos/mgYAR7BzBk4

Fresh, Y. (2018). *Switched-on iPhone* [Photograph]. Unsplash. https://unsplash.com/photos/dk4en2rFOIE

Hang, C. (2023). *AI Generated Hacker Computer* [Photograph]. Pixabay. https://pixabay.com/illustrations/ai-generated-hacker-computer-safety-8135912/

Jovanovic, B. (2017). *Cyber security, Smartphone, Cell Phone Image* [Photograph]. Pixabay. https://pixabay.com/photos/cyber-security-smartphone-cell-phone-2765707/

LaSalle, C. (2022). Cybersecurity Awareness Month 2022: *Using Strong Passwords and a Password Manager.* Blog Series 2022.National Institute of Standards and Technology. US Department of Commerce. https://www.nist.gov/blogs/cybersecurity-insights/cybersecurity-awareness-month-2022-using-strong-passwords-and-password

References

McAfee. (2023, September 24). *How Often Should You Change Your Passwords?* https://www.mcafee.com/learn/how-often-should-you-change-your-passwords/

National Cybersecurity Alliance. (2022, May 26). *Passwords.* https://staysafeonline.org/online-safety-privacy-basics/passwords-securing-accounts/

National Cybersecurity Alliance. (2022, September 6). *Password Managers* https://staysafeonline.org/online-safety-privacy-basics/password-managers/

Price, E. (2023, September 30). *Your Long Password Is Still Easy to Crack.* Ziff Davis, LLC. https://www.pcmag.com/news/your-long-password-is-still-easy-to-crack

Riki32. (2022). *Scam Text Image* [Photograph]. Pixabay. https://pixabay.com/illustrations/scam-hacker-anonymous-7478783/

Spadafora, A. (2023, September 30). *Billions of usernames and passwords leaked online — what you should do right now.* Tom's Guide, Future US, Inc. https://www.tomsguide.com/news/billions-of-usernames-and-passwords-leaked-online-how-to-see-if-youre-affected

References

Sobers, R. (2022, May 20). *89 Must-Know Data Breach Statistics [2022].* https://www.varonis.com/blog/data-breach-statistics

Towfiqu, B. (2021). *A Golden Padlock Sitting on Top of a Keyboard* [Photograph]. Unsplash. https://unsplash.com/photos/FnA5pAzqhMM

Zativa, M. (2022). A Person Holding a Cell Phone with the Amazon App on the Screen [Photograph]. https://unsplash.com/photos/_rSRv9T98G4