

Passwords: The Necessary Evil

October 24, 2019



Presenters

LuAnn Keyton & Joe Beckman

Senior Information Security Analysts

Purdue University Technical Assistance Program

cyberTAP

Agenda

- 1) Why do we use passwords?
- 2) Oh, the problems we've seen!
- 3) How to create a secure password
- 4) Password managers
- 5) The future: Multi-factor authentication
- 6) Discussion & Questions



“The three golden rules to ensure computer security are: do not own a computer; do not power it on, and do not use it.” Robert Morris



The first computer password was developed in 1961 by Fernando Corbató's team for MIT's Compatible Time-Sharing System (CTSS). *CTSS was a computer designed for multiple users (like computers in a modern day computer lab).*

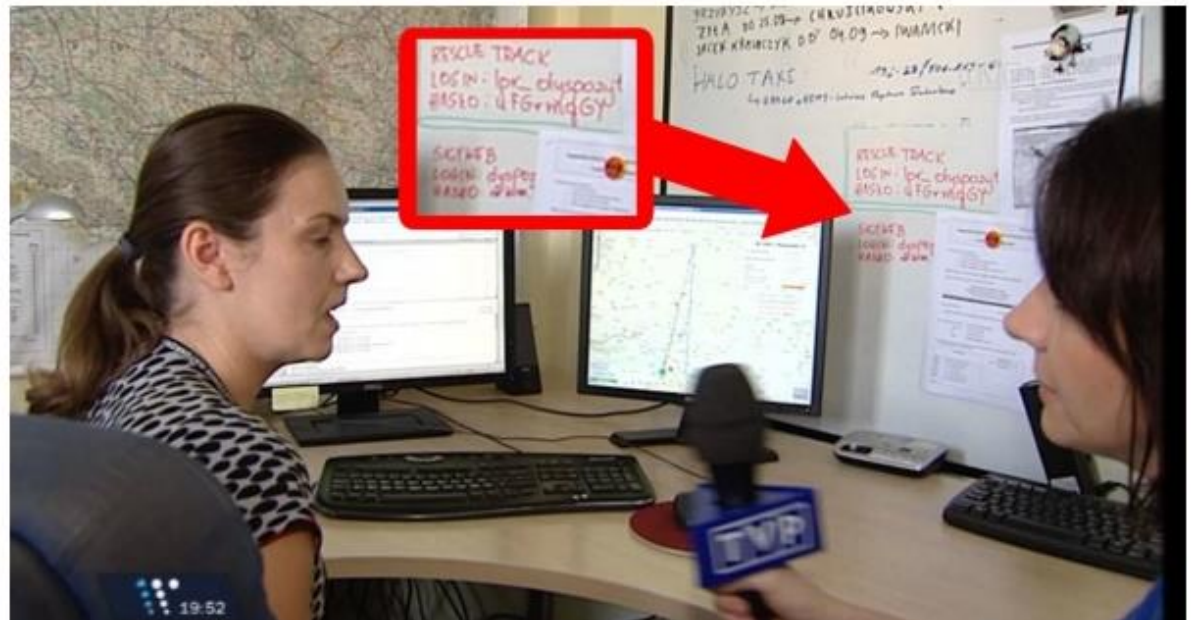
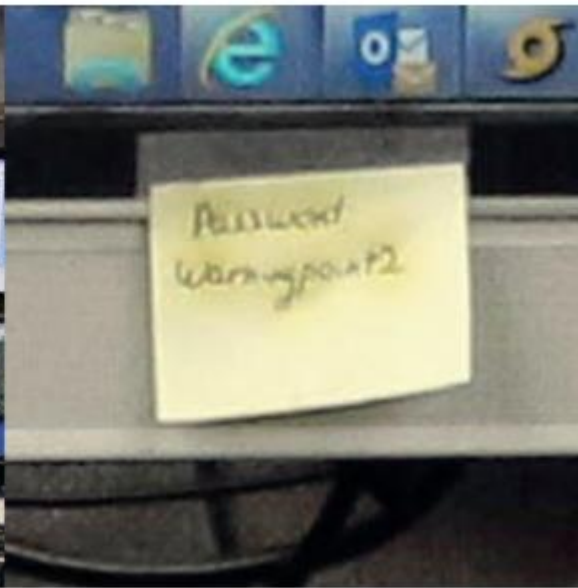
Photo: MIT Museum, <http://www.wired.com/2012/01/computer-password/>





In 1962, a software bug infected the system's master password profile and a list of all CTSS user passwords became available to anyone who logged in. Or so we thought...

In reality, a Ph.D. researcher Allan Scherr printed out all of the CTSS passwords in an attempt to increase his daily usage of the computer. To spread the blame around, Scherr gave the passwords to a bunch of other users. This was the first computer password-related security breach.



Your identity is a steal on the Dark Web.

Here are what the most common pieces of information sell for:



Social security
number



\$1

Online payment
services login info
(e.g. Paypal)



\$20-\$200

Credit or debit card
(credit cards are more popular)



\$5-\$110

With CVV number
\$5

With bank info
\$15

Fullz info*
\$30

Drivers license



\$20

Loyalty accounts



\$20

General non-financial
institution logins



\$1

Diplomas



\$100-\$400

Passports (US)



\$1000-\$2000

Subscription
services

\$1-\$10

Medical records

\$1-\$1000**

*Fullz info is a bundle of information that includes a "full" package for fraudsters: name, SSN, birth date, account numbers and other data that make them desirable since they can often do a lot of immediate damage.

**Depends on how complete they are as well as if it is a single record or an entire database.

Note: Prices can vary over time and prices listed below are an estimation and aggregation based on reference articles and hands on experience of Experian cyber analyst the last two years.

Ge.tt	Ixigo	Roll20	Houzz
Account Number: 1.83 million	Account Number: 18 million	Account Number: 4 million	Account Number: 57 million
Size: 1.56GB	Size: 7.23GB	Size: 759 MB	Size: 7.9GB
Compromised data: name, password hash, Facebook ID, and referrer	Compromised data: passwords md5, full name, IP address, username, email addresses, and some passport numbers	Compromised data: names, encrypted passwords, email addresses, and more	Compromised data: email addresses, passwords, name, and registration date.
Breach date: December 2017	Breach date: January 2019	Breach date: January 2019	Breach date: July 2018
Price: \$192(0.02345494 BTC)	Price: \$262(0.03200622 BTC)	Price: \$135 (0.01649175 BTC)	Price: \$1040 (0.12704757 BTC)
BUY	BUY	BUY	BUY

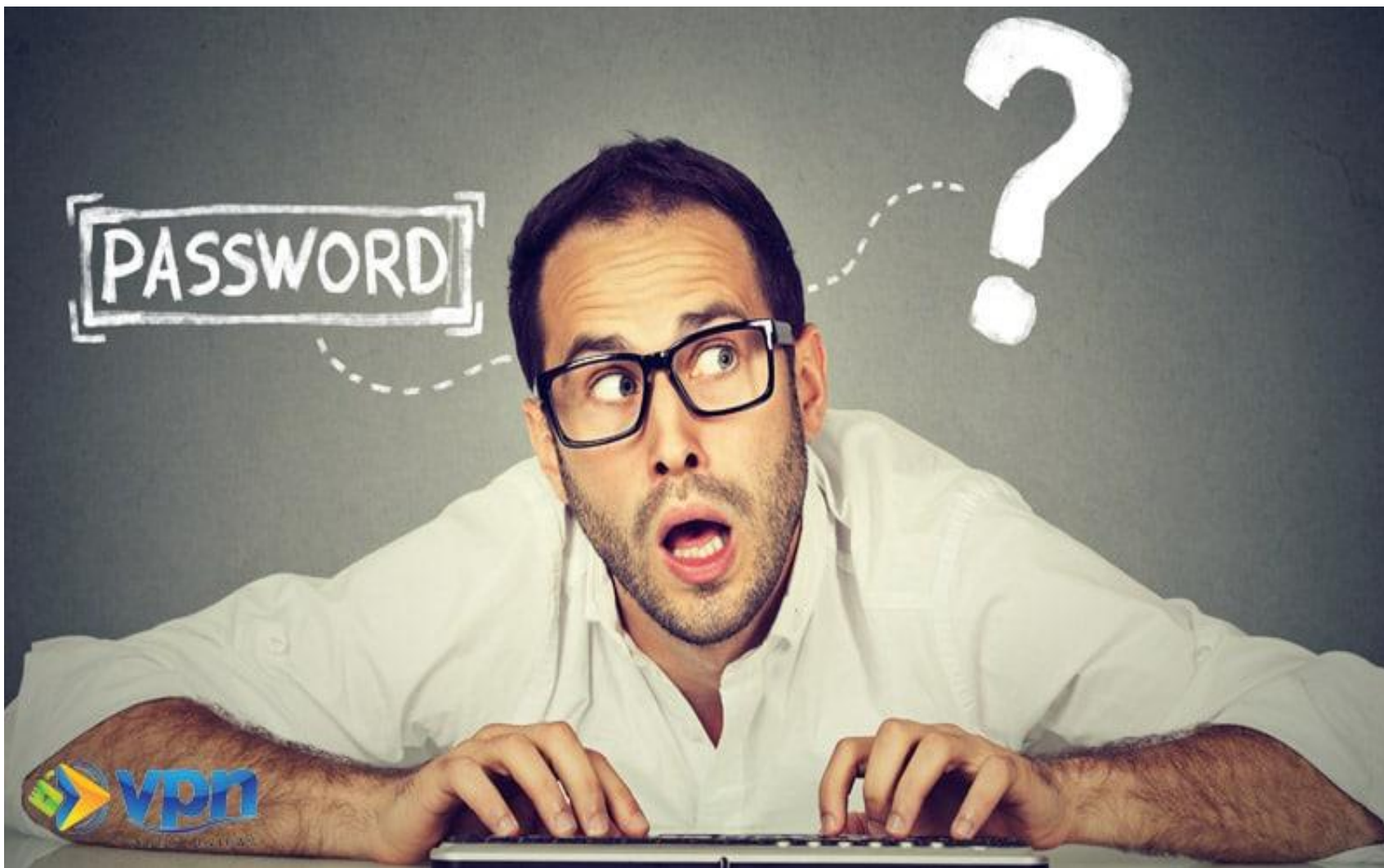
The following prices are estimates, if i think a specific job takes more time and money i will either refund you or you will send the remaining once we talked.



If you are unsure about which category to choose, choose the lower priced one in question.

You will only pay for successful jobs, if i can not do anything for you i will refund you. But keep in mind depending on your target specific things might take longer and require an addition payment, but only after i can show some success.

Product	Price	Quantity
Small job, for example: Email and Facebook hacking, installing trojans, small DDOS	250 EUR = 0.03363 ₿	<input type="text" value="1"/> X Buy now
Medium-large job, ruining people, espionage, website hacking, DDOS for big websites	500 EUR = 0.06726 ₿	<input type="text" value="1"/> X Buy now
Large job which takes a few days or multiple smaller jobs, DDOS for protected sites	900 EUR = 0.12107 ₿	<input type="text" value="1"/> X Buy now
UPGRADE: INSTANT reply within 30-60 minutes instead of 24-36 hours for urgent cases. If i need longer this will get refunded. Only buy this together with one of the other options.	200 EUR = 0.02690 ₿	<input type="text" value="1"/> X Buy now

- Cybersecurity maturity is still at an early state in healthcare
- Healthcare data tends to be richer in both volume and value than financial services or retail data
- Medical identity fraud usually takes longer to detect than other types of fraud
- Cybercriminals are becoming increasingly sophisticated in their attack approaches and use of malware



[Home](#)[Notify me](#)[Domain search](#)[Who's been pwned](#)[Passwords](#)[API](#)[About](#)[Donate](#)  

';--have i been pwned?

Check if you have an account that has been compromised in a data breach



Generate secure, unique passwords for every account

[Learn more at 1Password.com](#)

[Why 1Password?](#)

Is My Password Unique?

Is My Password Full of Character?

Is My Password Long Enough?

Is My Password Memorable?

Song or Nursery Rhyme Strategy

hail, hail to old purdue!
all hail to our old gold and black!
hail, hail to old purdue!
our friendship may she never lack.


<https://www.youtube.com/watch?v=NNnBirex89U>

hhttp!ahto

hHtop!ahTo

hHto9!ahTo

hHto9!ahT@



If you use this as your base password, you can keep it and add a prefix and suffix for each website where you need a password.

Base: hHto9!ahT@

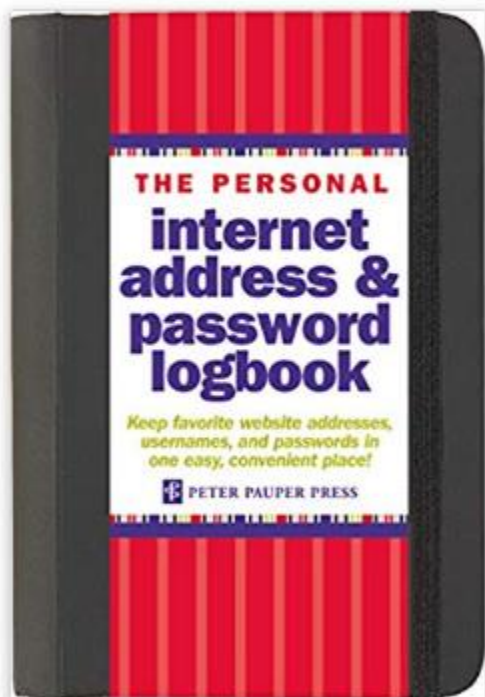
Facebook: bhHto9!ahT@F

ChaseBank: bhHto9!ahT@Ch

Or, you could use a password generator like <https://passwordsgenerator.net/> to accomplish the same outcome.

You can either use the same generated password and change the beginning and end as we did with the song. Or, you can create a totally different password for each app or website.

If you create a different word for each site or app, you'll need to look at a password manager to manage them.



The Personal Internet Address & Password Log Book Hardcover-spiral – July 4, 2010

by [Peter Pauper Press](#) (Author, Editor)

★★★★☆ 2,345 customer reviews

#1 Best Seller in Internet & Telecommunications

 **Best Price**

[See all formats and editions](#)

Hardcover-spiral

\$6.44

14 Used from \$7.93

30 New from \$5.80

2 Collectible from \$25.00

Password Managers

Store Passwords using encryption.

Create secure passwords for you.

Some will also enter the password for you into the website login automatically.

For a small additional fee of \$2 or \$3 per month, they will store your passwords in the cloud and allow all passwords to sync across your devices.

Some warn you when you are reusing a password.

#1



Our Partner



[Read Full Review](#)

22 Reviews

- Only password manager with US Patent for its security architecture
- Generate unique passwords
- Instant security alerts
- Change dozens of passwords with one click
- Quick, secure signing across multiple platforms
- Auto-fill forms, auto-login to your favorite websites
- 2017 Webby Award People's Voice award in the Mobile Sites/Apps>Services & Utilities category

[SEE DASHLANE DEAL >](#)

#2



Our Partner



[Read Full Review](#)

3 Reviews

- **Get 30% off RoboForm!**
- Free version available
- Two-factor authentication
- Supports all major browsers
- Automatic bookmark-style logins
- Provides secure access to your passwords wherever you are
- Supports Windows Biometric Framework, Apple Touch ID and Face ID
- One subscription that works across all devices
- All data encrypted with AES-256 and PBKDF2 SHA256
- Unlimited logins

[SEE ROBOFORM DEAL >](#)



Our Partner



[Read Full Review](#)

- **Special offer 50% off**
- Award-winning password manager and form-filler
- Unlimited storage automatically fills out forms and logs you in
- Generates superstrong passwords
- Keeps your credit cards safe and ready for checkout
- Works on all your devices and supports 16 browsers, with cloud sync and backup
- Local WiFi sync available for extra security
- Military grade AES-256 encryption, 2FA, biometrics
- Priority support. Lifetime license available (no renewals)

[SEE STICKY PASSWORD DEAL >](#)

#4



Our Partner



[Read Full Review](#)

5 Reviews

- Free 30-day trial
- Plan starts at \$2.99 per month
- 1 GB storage offered
- Unlimited installations
- Zero knowledge protocol
- Unique 128-bit identifier
- Travel mode feature

[SEE 1PASSWORD DEAL >](#)

#5



Our Partner



[Read Full Review](#)

165 Reviews

- **Save 15% on Keeper Unlimited!**
- Free signup
- Zero-knowledge security & Cloud Security Vault
- Rapid time-to-security
- Recognized by GTB Telecoms Consumer Service Innovation
- Supports every platform and the top browsers (IE, Chrome, Safari, Edge, Firefox)
- Two-factor authentication and biometric login
- Seamless syncing across devices

[SEE KEEPER DEAL >](#)

Sticky Password PREMIUM

Search

+ Add Account + Add Group

Web Accounts

- Quick Access
- Web Accounts
- App Accounts
- Identities
- Bookmarks
- Secure Memos
- Sharing Center


Web site

- Amazon Sign In**
https://www.amazon.com/
- Caremark - Sign In**
https://www.caremark.com/wps/portal
- Endeavor Communication SmarHub - Login**
https://weendeavor.smarhub.coop/Login.html#
- insight.rapid7.com**
https://insight.rapid7.com/login
- KPA CTP Member Login - Karen Pryor Acad...**
https://karenpryoracademy.com/ctp/login/#myac...
- Log Into Your DISH Account | MyDISH**
https://my.dish.com/welcome-center
- Login**
https://myaccounts.hsabank.com/Login.aspx?Ret...
- purdue.edu**
https://www.purdue.edu/
- Sign In | Chewy.com**
https://www.chewy.com/app/login?targetUrl=%...
- South Central Indiana REMC - Login**
https://billing.sciremc.com/sciremc/login.jsp

Login

Launch

Sync - cloud Last synchronization: 2:16:34 PM [My StickyAccount](#)

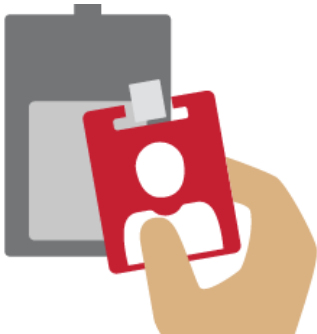


Multi-factor authentication (using more than one thing to log in)

Multi-factor authentication

What is multi-factor authentication?

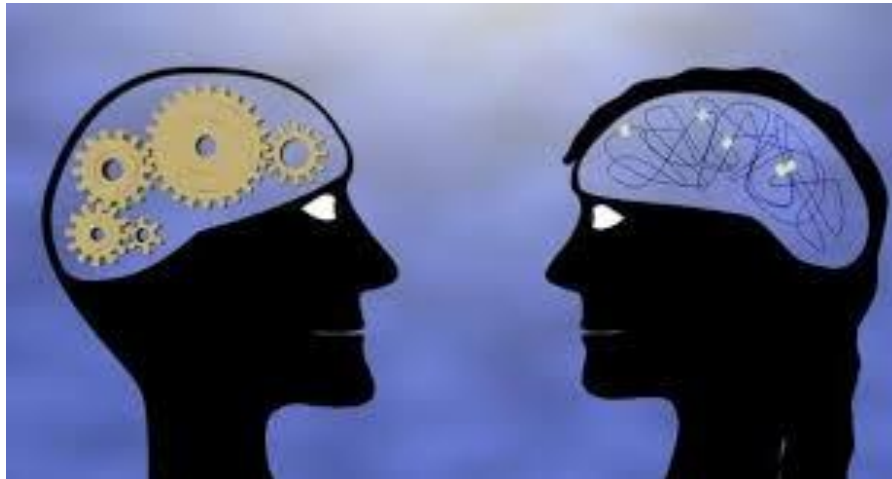
- ...an authentication scheme that requires users to present more than one type of proof of identity in order to authenticate.
- Right now, you probably log in with a username and password. Your username is often public, your password is the secret you know.
- Multi-factor authentication may use something you know, something you have, something you are.



Multi-factor authentication

Multifactor authentication: Something you know

- Your p@s\$w0RD!
- Your mother's maiden name
- Pet's name, elementary school, etc...



Multi-factor authentication

Multifactor authentication: Something you have

- Badges are often used for physical access.
- Physical tokens, mobile phone applications, or software tokens are frequently used for access to computers.
- Integrated physical and logical (computer) authentication systems, badges may be required for every authentication.



Multi-factor authentication

Multifactor authentication: Something you are

- Fingerprint & password or pin are common implementations.
- Problems:
 - Identity theft
 - Reliability
 - Legal
 - Cultural & Religious



Iris Recognition



Retina Recognition



Face Recognition



Fingerprint Recognition



Voice Recognition



DNA Matching



Finger Geometry Recognition



Hand Geometry Recognition



Signature Recognition



Privacy Protection



Getting Access



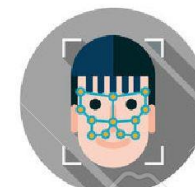
Authentication



Biometric Data Security



Vein Patterns Recognition



Biometric Recognition



Ear Shape Recognition

Multi-factor authentication

What makes MFA stronger than username/password?

- ❖ It is increasingly less likely that an attacker can impersonate you the more authentication a system requires.
- ❖ You're going to notice if someone steals your phone/hardware token, or tries to lift your fingerprint (probably).
- ❖ Theft of a physical token requires geographic proximity. It's pretty tough to do this from Russia or China.


Multi-factor authentication

Common implementations and best practices?

- Implementations in health care:
 - Imprivata/Sonitrol Badge + password or PIN
 - Biometric (thumb-print) + password or PIN
- Best practices:
 - Think hard about what you are trying to accomplish.
 - Give additional consideration to “insider threats” when moving to multi-factor. Consider modifications to policies and procedures.
 - Keep ease of use in the front of your minds. Balance security and usability.



Questions?



This material should not be printed by anyone other than the participant. Reproduction and distribution (including by e-mail) of this material is not permitted without the consent of Purdue University. Although every precaution has been taken to verify the accuracy of the information contained in this document, Purdue University assumes no responsibility for any errors or omissions. No liability is assumed for damages that may result from the use of information contained within.

WE ARE PURDUE. WHAT WE MAKE MOVES THE WORLD FORWARD.