WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Hacktober 2020:

Password Security

Washington state
Office of CyberSecurity

OFFICE OF
CyberSecurity
STATE OF WASHINGTON

Introduction

Todays Discussion's:

- Users:
  - Do's and Don'ts.
  - Tools to help build and protect passwords.
- Identity Managers:
  - Deciding the rules.
  - Resources and guidance.
- How a hacker can win easy.

Users

- Do’s and Don’ts.
- Multi-factor.
- Testing your password.
- Has your password been compromised.
- Password Managers.

Do's and Don'ts

WaTech
Washington Technology Solutions

DO:

- DO change your password regularly.
- DO pick a password you will remember so you DON'T have to write it down.
- DO use a mix of uppercase and lowercase characters.
- DO use punctuation marks and special characters such as #, $, %.
- DO choose a line or two from a song or poem and use the first letter of each word, preceded or followed by a digit.
- Use a password manager

DON'T:

- DON'T include all or part of your username, first name, or last name.
- DON'T make obvious choices like your nickname, birthdate, spouse name, pet name, make/model of car, or favorite expression.
- DON'T share your password with anyone.
- DON'T use a word contained in English or foreign language dictionaries, spelling lists or commonly digitized texts such as the Bible or an encyclopedia.
- DON'T use an alphabet sequence (lmnopqrst), a number sequence (12345678) or a keyboard sequence (qwertyuop).

OFFICE OF CyberSecurity STATE OF WASHINGTON

Multi-factor Authentication

Multi-factor authentication is a method in which a user is granted access to a website or application after successfully presenting two or more pieces of evidence to an authentication mechanism: knowledge, possession, and inherence.

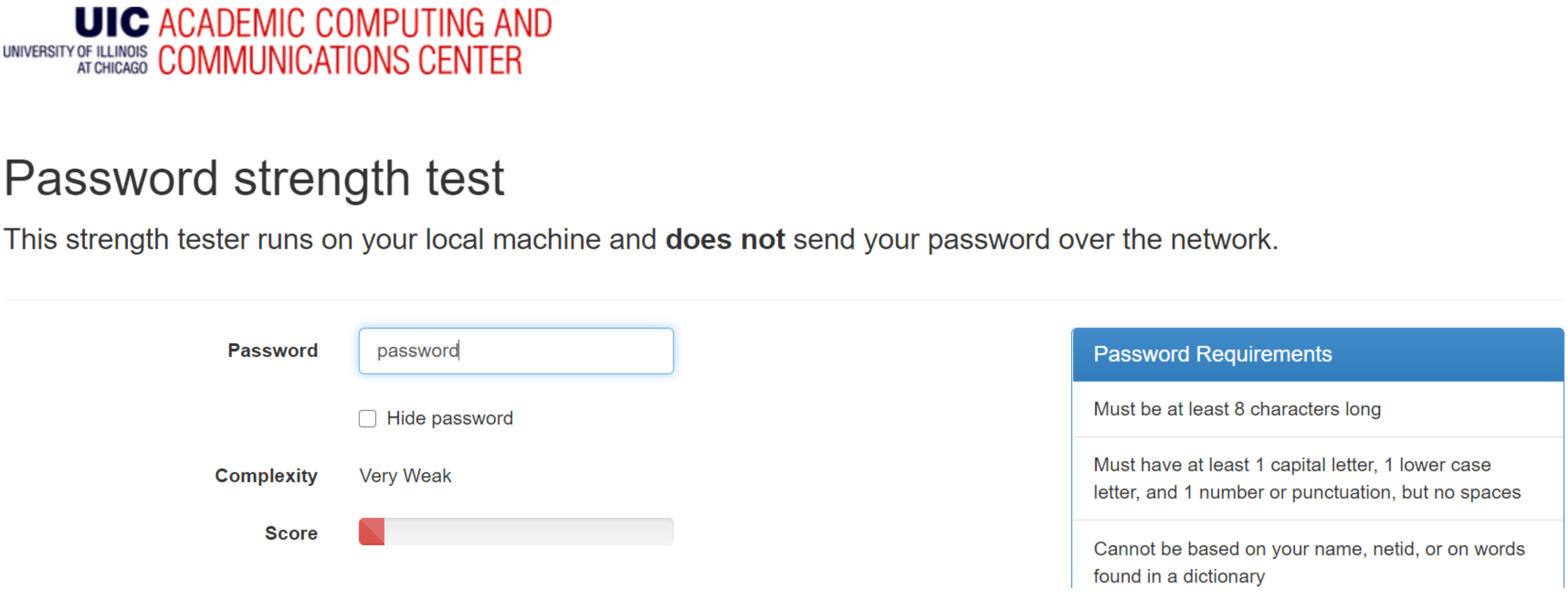
Testing Passwords

- If you are unsure of the strength of your password there are tools that you can use to help you evaluate your choice.

- Let's look at one.

University of Illinois at Chicago

- https://www.uic.edu/apps/strong-password/



UIC UNIVERSITY OF ILLINOIS AT CHICAGO ACADEMIC COMPUTING AND COMMUNICATIONS CENTER

Password strength test

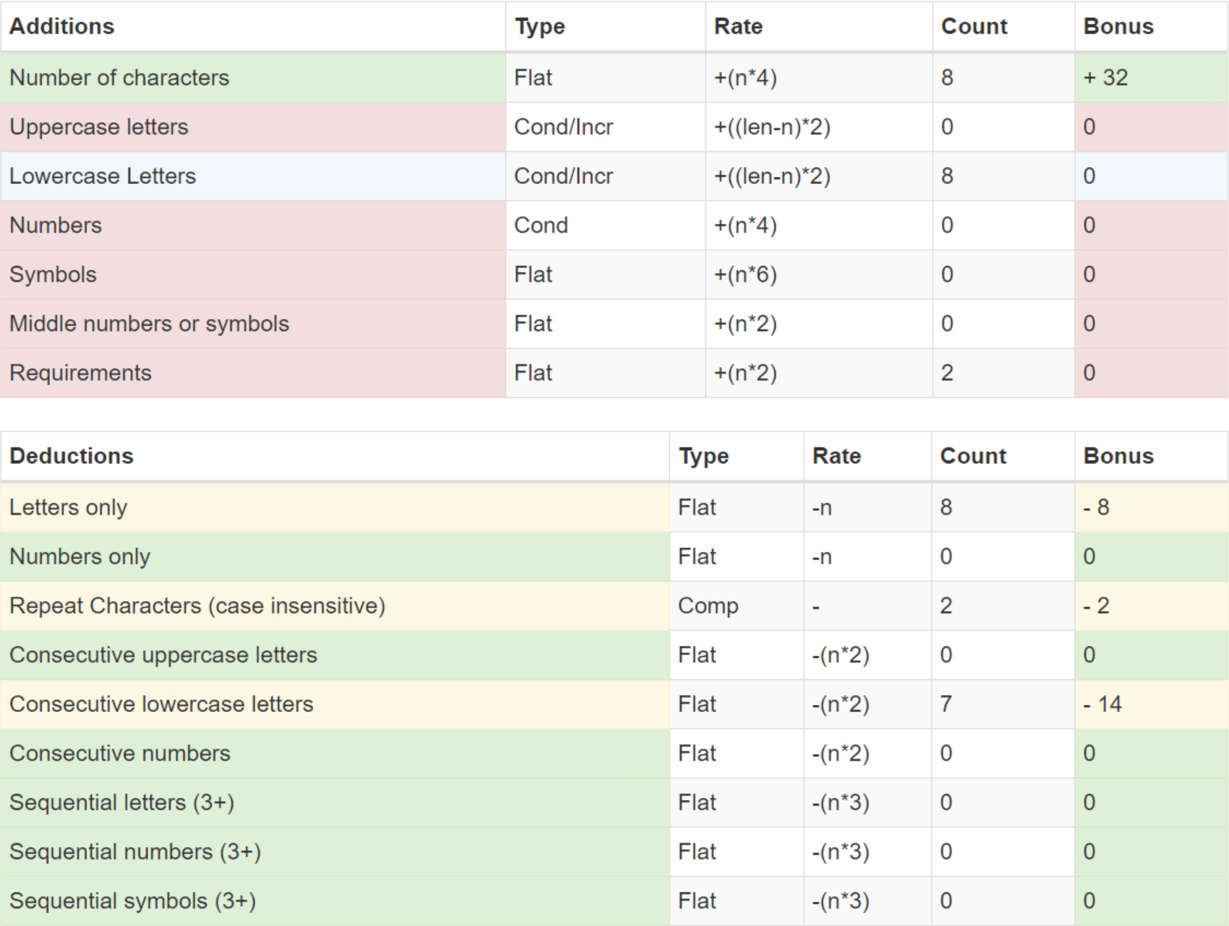
This strength tester runs on your local machine and **does not** send your password over the network.

Password	password
	☐ Hide password
Complexity	Very Weak
Score	

Password Requirements

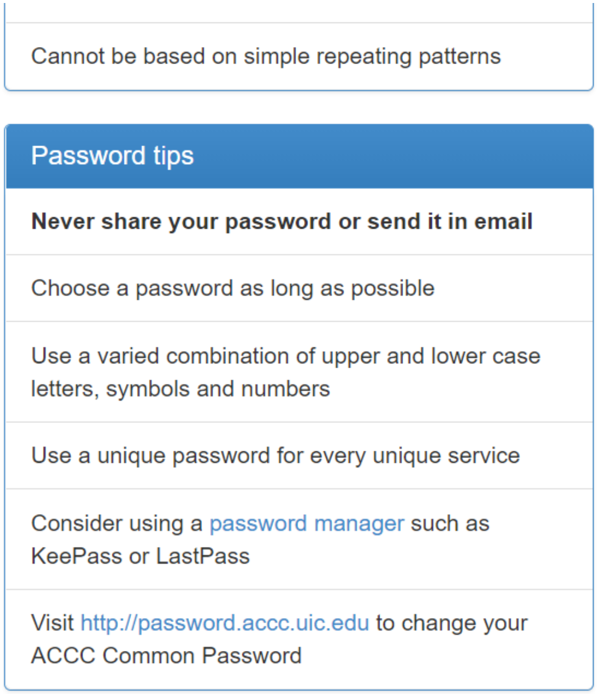
- Must be at least 8 characters long
- Must have at least 1 capital letter, 1 lower case letter, and 1 number or punctuation, but no spaces
- Cannot be based on your name, netid, or on words found in a dictionary

University of Illinois at Chicago continued



Additions	Type	Rate	Count	Bonus
Number of characters	Flat	+(n*4)	8	+ 32
Uppercase letters	Cond/Incr	+((len-n)*2)	0	0
Lowercase Letters	Cond/Incr	+((len-n)*2)	8	0
Numbers	Cond	+(n*4)	0	0
Symbols	Flat	+(n*6)	0	0
Middle numbers or symbols	Flat	+(n*2)	0	0
Requirements	Flat	+(n*2)	2	0

Deductions	Type	Rate	Count	Bonus
Letters only	Flat	-n	8	- 8
Numbers only	Flat	-n	0	0
Repeat Characters (case insensitive)	Comp	-	2	- 2
Consecutive uppercase letters	Flat	-(n*2)	0	0
Consecutive lowercase letters	Flat	-(n*2)	7	- 14
Consecutive numbers	Flat	-(n*2)	0	0
Sequential letters (3+)	Flat	-(n*3)	0	0
Sequential numbers (3+)	Flat	-(n*3)	0	0
Sequential symbols (3+)	Flat	-(n*3)	0	0



Cannot be based on simple repeating patterns

Password tips

Never share your password or send it in email

Choose a password as long as possible

Use a varied combination of upper and lower case letters, symbols and numbers

Use a unique password for every unique service

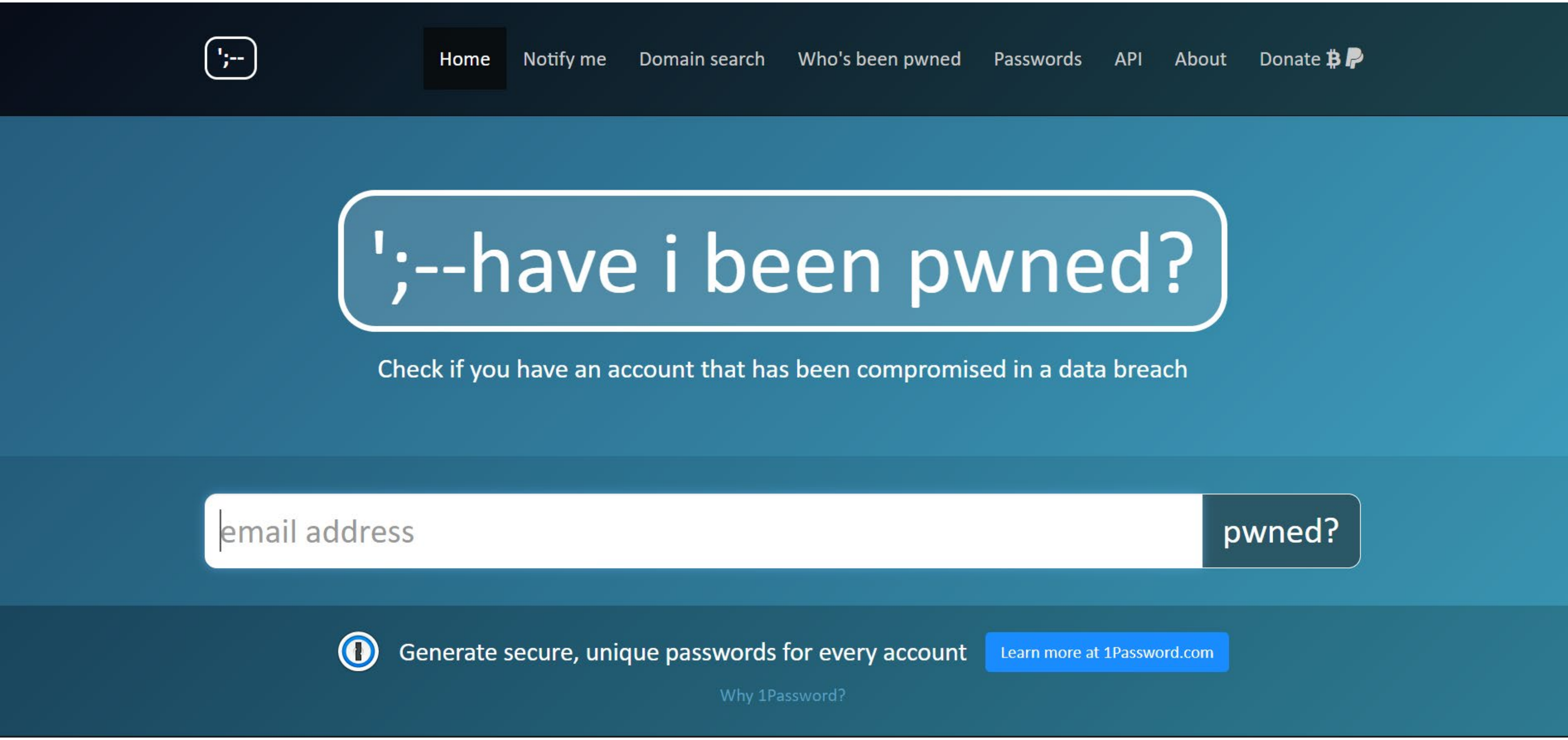
Consider using a password manager such as KeePass or LastPass

Visit http://password.accc.uic.edu to change your ACCC Common Password

Compromised Passwords

If you suspect your account may have been part of a previously reported breach, there is a resource to check.

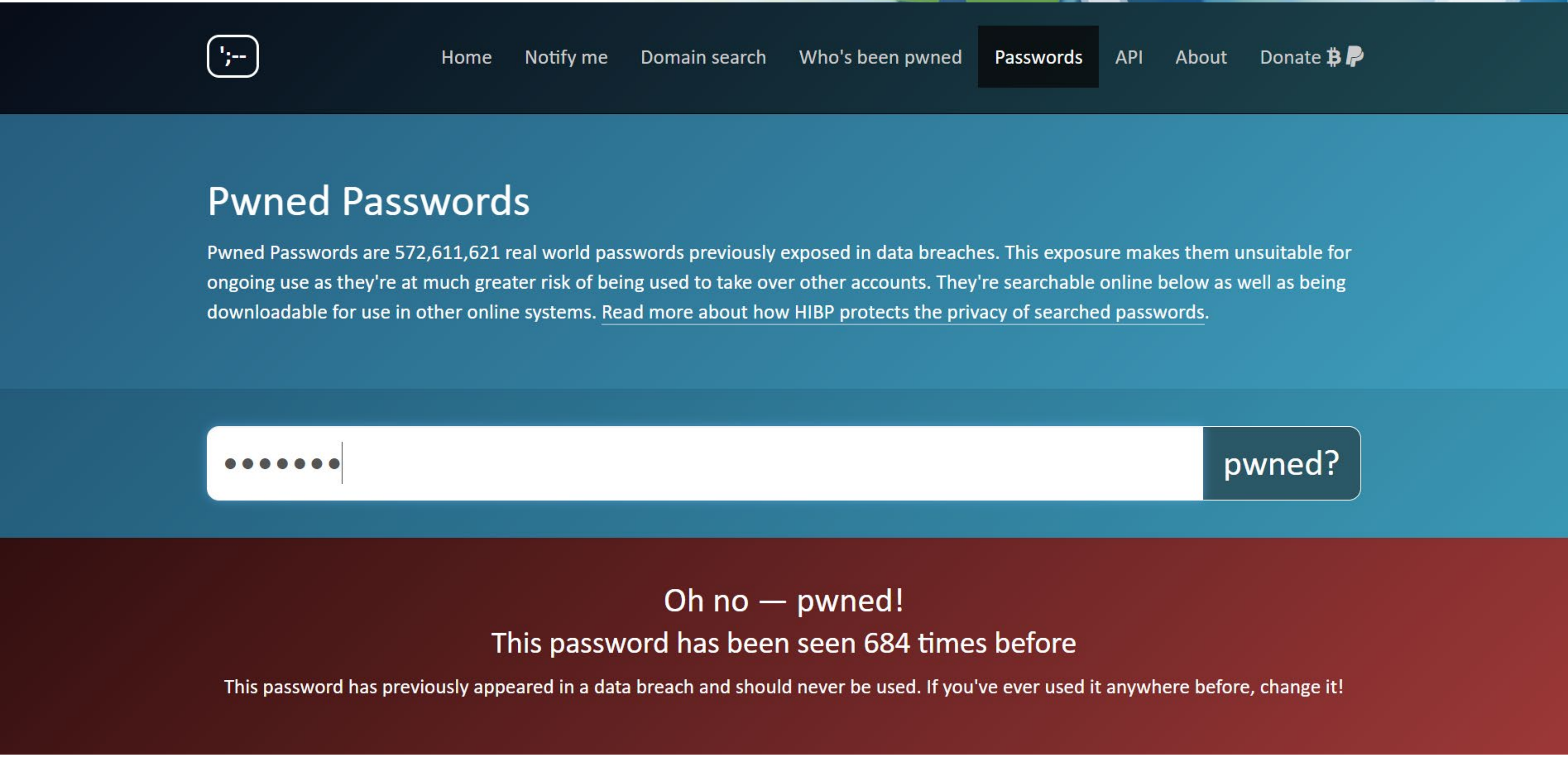
haveibeenpwned.com



';--have i been pwned?

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

haveibeenpwned.com



Pwned Passwords

Pwned Passwords are 572,611,621 real world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online below as well as being downloadable for use in other online systems. Read more about how HIBP protects the privacy of searched passwords.

•••••••

Oh no — pwned!

This password has been seen 684 times before

This password has previously appeared in a data breach and should never be used. If you've ever used it anywhere before, change it!

Password Manager

A password manager is a computer program that allows users to store, generate and manage their personal passwords for online services. A password manager assists in generating and retrieving complex passwords, potentially storing such passwords in an encrypted database or calculating them on demand.

LastPass •••|

Free Password Manangers

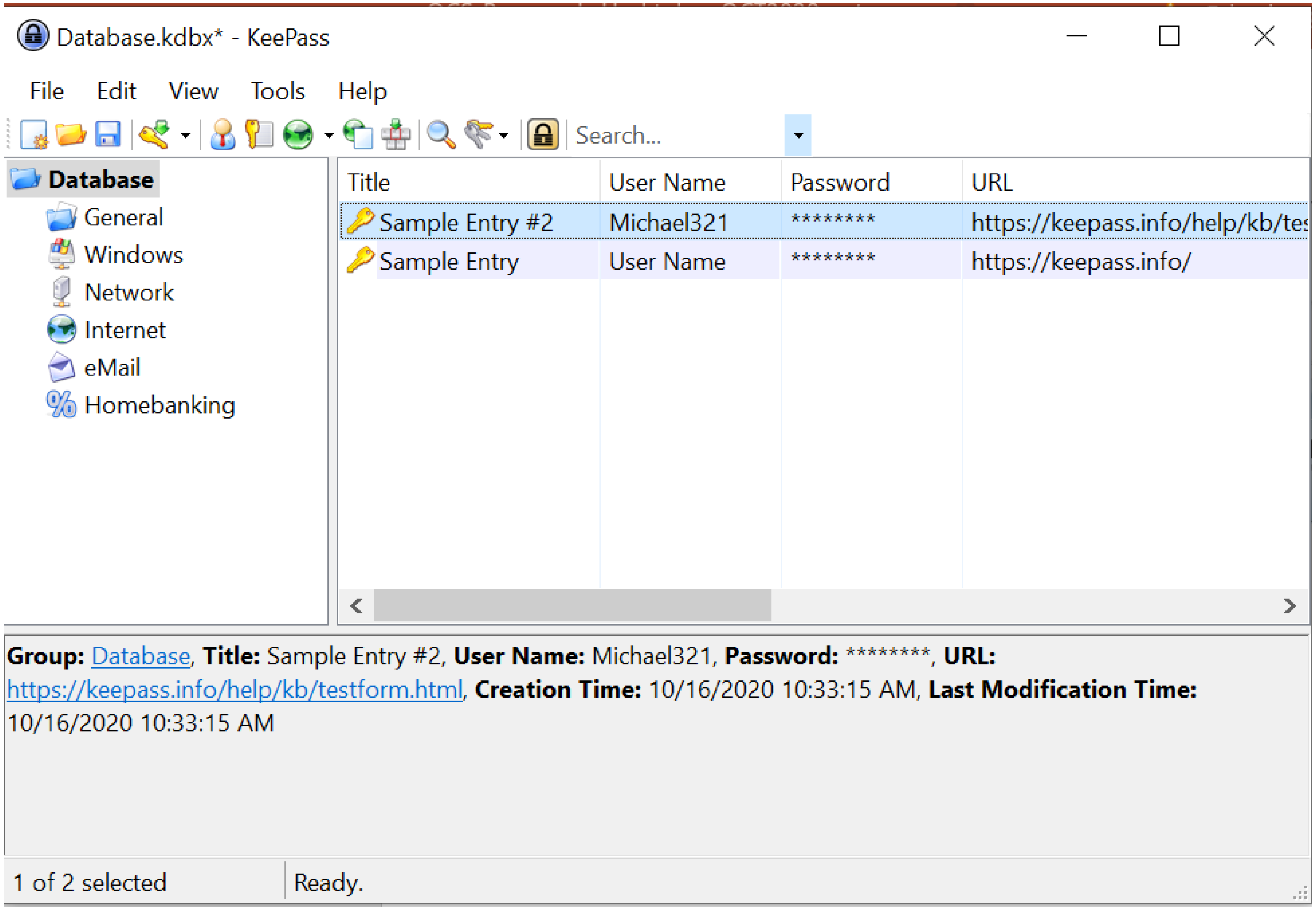
- Lastpass
- Keepass
- Dashline
- Keeper

DASHLANE

KEEPER

LastPass

KeePass



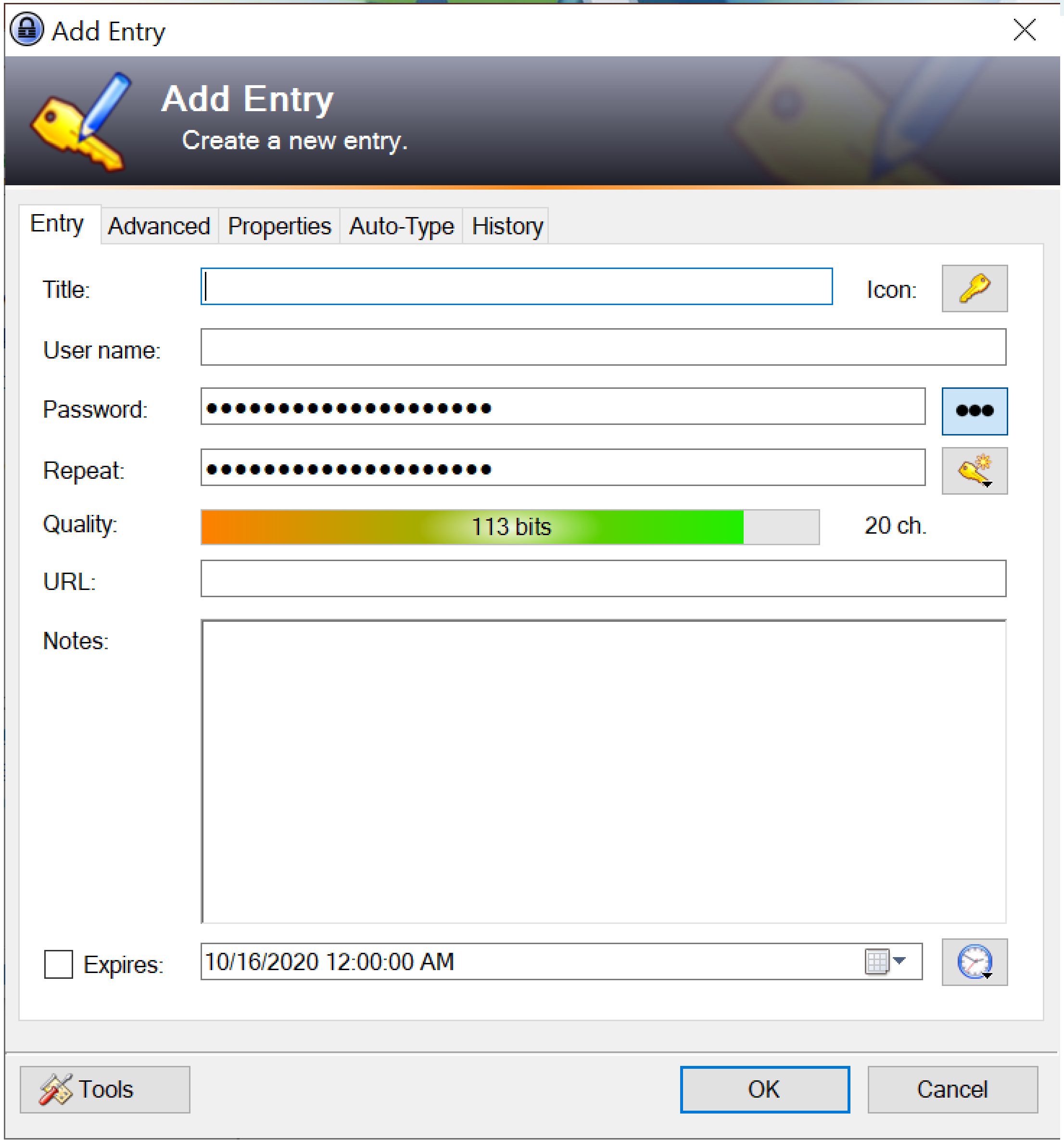
Title	User Name	Password	URL
Sample Entry #2	Michael321	********	https://keepass.info/help/kb/tes
Sample Entry	User Name	********	https://keepass.info/

Group: Database, **Title:** Sample Entry #2, **User Name:** Michael321, **Password:** ********, **URL:** https://keepass.info/help/kb/testform.html, **Creation Time:** 10/16/2020 10:33:15 AM, **Last Modification Time:** 10/16/2020 10:33:15 AM

1 of 2 selected | Ready.

KeePass

WaTech
Washington Technology Solutions



Add Entry

Add Entry

Create a new entry.

Title:

Icon:

User name:

Password: ••••••••••••••••••••

Repeat: ••••••••••••••••••••

Quality: 113 bits 20 ch.

URL:

Notes:

□ Expires: 10/16/2020 12:00:00 AM

OFFICE OF
CyberSecurity
STATE OF WASHINGTON

Identity Managers

- Determine Policy for password
- Resources available:
  - NIST 800-53(Rev. 4)
  - NIST Special Publication 800-63B

NIST 800-53

- NIST has already developed a set of security controls around Identity management that we can review and build from based on our needs.

NIST 800-53

WaTech
Washington Technology Solutions

What is a security control and what are the parameters associated with controls?

Controls are the operational, technical and management safeguards used by information systems to maintain the integrity, confidentiality and security of federal information systems.

Basically: It’s a list of rules with adjustable variables to meet the needs of an information system.

OFFICE OF
CyberSecurity
STATE OF WASHINGTON

NIST Access Controls

WaTech
Washington Technology Solutions

- NIST security controls or broken down into control families.
- We are going to focus on Identification and authentication controls related to passwords for moderate impact systems.

IA-1, IA-2(1), IA-5, ***IA-5(1),*** IA-5(2), IA-5(3), IA-5(11)

OFFICE OF
CyberSecurity
STATE OF WASHINGTON

NIST 800-53 IA -2 Example

WaTech
Washington Technology Solutions

The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

OFFICE OF CyberSecurity STATE OF WASHINGTON

NIST 800-53 IA -5(1) Example

IA-5 (1) AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION
The information system, for password-based authentication:

IA-5 (1)(a) Enforces minimum password complexity of [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type];

IA-5 (1)(b) Enforces at least the following number of changed characters when new passwords are created: [Assignment: organization-defined number];

IA-5 (1)(c) Stores and transmits only cryptographically-protected passwords;

IA-5 (1)(d) Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum];

IA-5 (1)(e) Prohibits password reuse for [Assignment: organization-defined number] generations; and

IA-5 (1)(f) Allows the use of a temporary password for system logons with an immediate change to a permanent password.

NIST Special Pub 800-63B

- This publication is focused on recommendations for password policies.

NIST Special Pub 800-63B Summary

- Length: 8 character minimum and 64 character maximum.

- Password list: Screen new passwords against a list of commonly-used, expected, or compromised passwords.

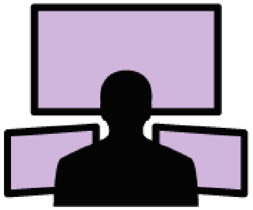
- Composition rules: Skip character composition rules as they are an unnecessary burden for end users.

- Password Expiration: Change passwords only if there is evidence of compromise.

Hackers

Users and security personnel put a lot of effort into implementing strong passwords, policies and other security measure to protect our systems.

All that work can be for nothing if we are not vigilant with who we are share our passwords with.

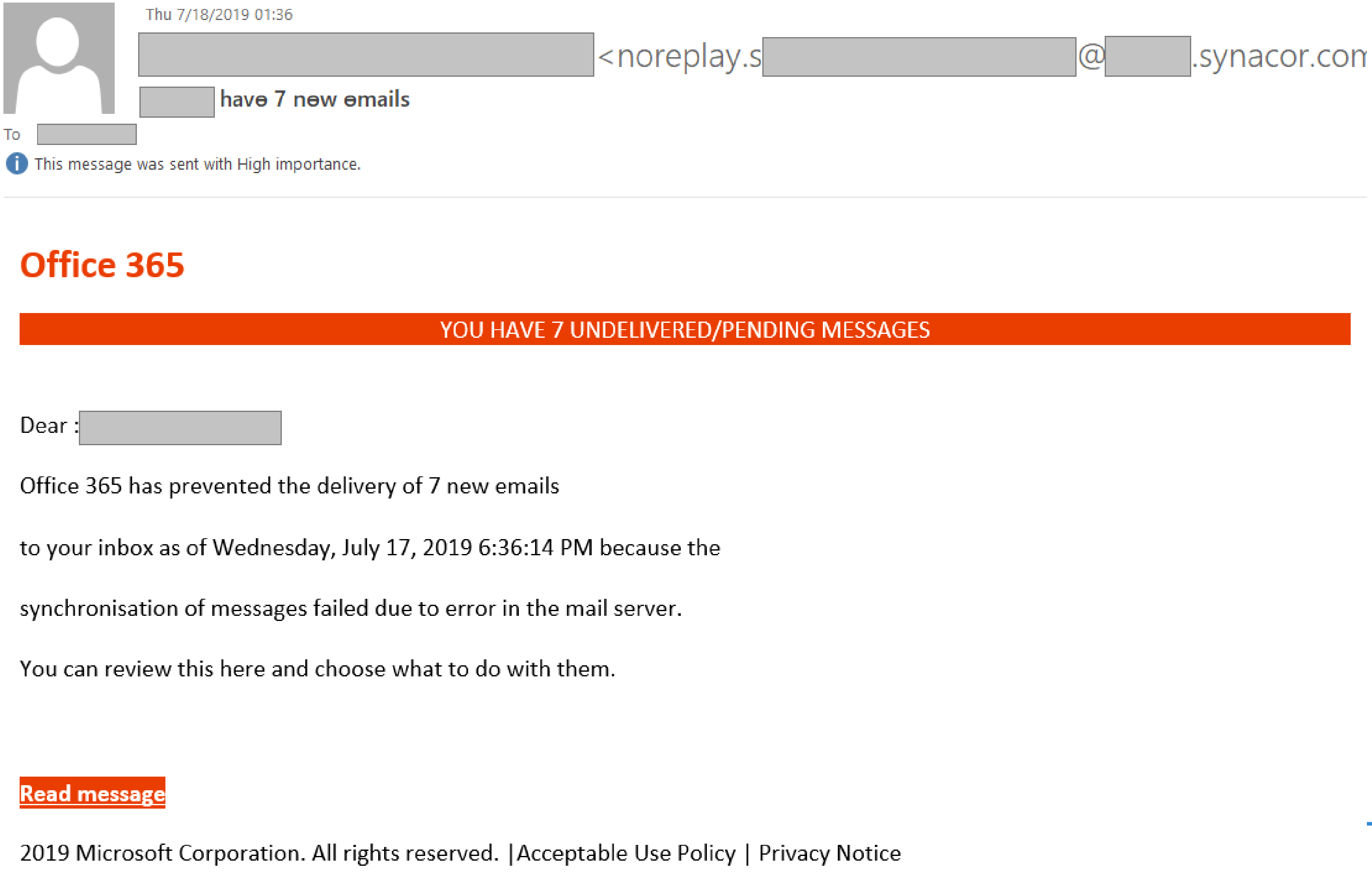


Credential Harvesting

- Credential harvesting emails attempt to trick users into entering their credentials into a fraudulent website to steal their login information

Credential Harvesting Example

WaTech
Washington Technology Solutions



Thu 7/18/2019 01:36

[redacted] <noreplay.s[redacted]@[redacted].synacor.con

[redacted] have 7 new emails

To [redacted]

This message was sent with High importance.

Office 365

YOU HAVE 7 UNDELIVERED/PENDING MESSAGES

Dear : [redacted]

Office 365 has prevented the delivery of 7 new emails

to your inbox as of Wednesday, July 17, 2019 6:36:14 PM because the

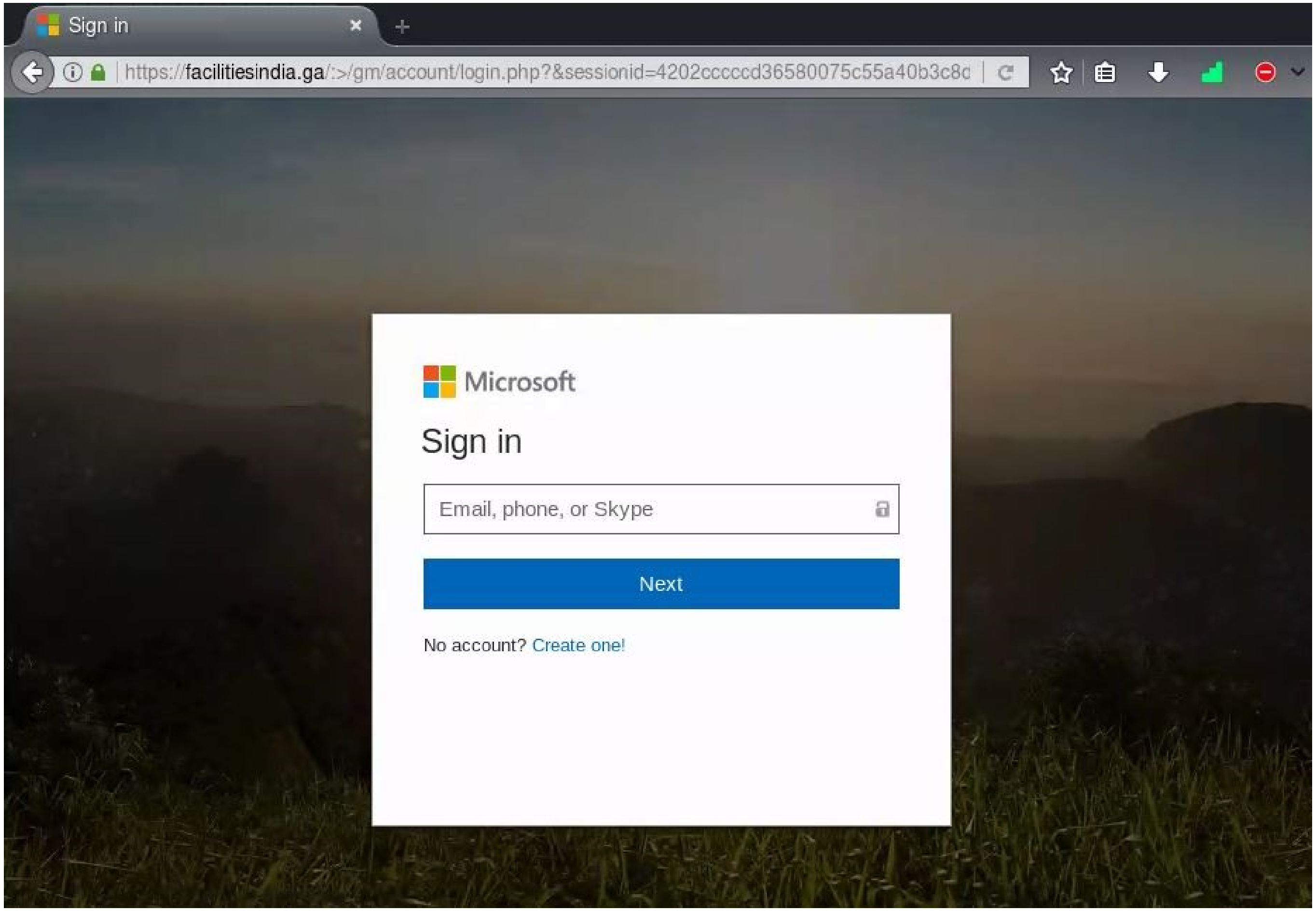
synchronisation of messages failed due to error in the mail server.

You can review this here and choose what to do with them.

Read message

2019 Microsoft Corporation. All rights reserved. |Acceptable Use Policy | Privacy Notice

Credential Harvesting Example



Sign in
https://facilitiesindia.ga/:>/gm/account/login.php?&sessionid=4202cccccd36580075c55a40b3c8c
Microsoft
Sign in
Email, phone, or Skype
Next
No account? Create one!

Resources

- https://www.uic.edu/apps/strong-password/
- haveibeenpwned.com
- https://keepass.info/
- https://nvd.nist.gov/800-53
- https://pages.nist.gov/800-63-3/
- https://cybersecurity.wa.gov/

Thank you!

joshuaeshenbaugh@ocs.wa.gov
or cert@ocs.wa.gov