Passwords
The Bane of our Existence?

Passwords are sort of the ‘necessary evil’ way to access our modern world. Until something better comes along and unseats passwords, they’re here to stay.
Passwords

- Why do we use passwords?
- What are typical (bad?) password habits?
- What are the risks of bad password habits?
- What makes a good password?
- How to manage my passwords?

- Passwords are really the only practical, widely available way to prove identity currently
- We see lots of password habits, some bad, that we’ll be addressing
- There are a number of risks to employing bad password habits, the worst of which would be identity theft, and hackers compromising your accounts and systems
- Different definitions, but typically: Complex, long(ish), unique, hard-to-guess, easy-to-remember/use
- Lot’s of bad ways (post-its, writing them on a list, etc), best would be to use a password manager
Why do we need passwords?

- Used to confirm identity
- Only practical method... currently
- Easy to implement on variety of devices
- What about biometrics?
  - What happens when you suspect someone has your password?

- Need a way to prove who you are. In person, you might show your ID, drivers license, etc. Online we need another way.
- Must be universal, widely available, easy to implement on various devices and platforms. Many high-tech ideas aren’t supported across all platforms. Many of us in IT hope for a better solution, as passwords have a number of practical flaws.
- Biometrics are useful, but not a good substitute. What happens if someone can duplicate your fingerprint?
What are typical password habits?

What we see regularly around campus....

- Simple, short passwords
- Passwords on a post-it note on the computer or monitor
- Passwords stored in a Word or Excel document... unprotected
- Reused passwords, shared among various services
- Provide password to third-party when asked

- Passwords that are short, simple are easy to crack.
- What is wrong with sharing passwords? How am I supposed to remember them all? Tip: Password Manager! (later)
- Putting your passwords in plain sight is bad (slide 8)
- Putting your passwords in an Excel or Word document isn’t secure. Easy to find using Spotlight or equivalent
- Being tricked/convinced to give password (see social engineering clip, slide 13)
What's wrong with an “easy” password?

https://www.grc.com/haystack.htm
https://www.uic.edu/apps/strong-password/

Caveat: These meters don’t take all cracking techniques into account

Two different password strength meters:
https://www.grc.com/haystack.htm
https://www.uic.edu/apps/strong-password/

These only help with determining complexity, length, etc. Doesn’t take into account passwords that appear on lists, common, easily crackable character substitutions, etc.
What's wrong with an “easy” password? (cont’d)

<table>
<thead>
<tr>
<th>Password</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>abc123</td>
<td>Weak</td>
<td>Weak</td>
<td>Good</td>
<td>Weak</td>
<td>Weak</td>
</tr>
<tr>
<td>trusttool</td>
<td>Norm.</td>
<td>Weak</td>
<td>Good</td>
<td>Norm.</td>
<td>Weak</td>
</tr>
<tr>
<td>mm1701</td>
<td>Med.</td>
<td>Weak</td>
<td>Good</td>
<td>Med.</td>
<td>Weak</td>
</tr>
<tr>
<td>lloveyou!</td>
<td>Med.</td>
<td>Good</td>
<td>Good</td>
<td>Med.</td>
<td>Weak</td>
</tr>
</tbody>
</table>

How long to crack these passwords? 0.0 seconds

Using a password strength checker only gives you part of the picture: complexity and length mainly

Doesn’t take into account that the password may appear on a list, or be easy to derive: common substitutions (0 for o, L for 1, 4 for A, E for 3, etc).

For more information, see John the Ripper (https://www.openwall.com/john/) and open source password cracking tool, and associated downloadable password lists.
What's wrong with using Post-It notes? They're so convenient!
Examples of ways that people write down passwords and make them readily accessible (to the bad guys too!)
...but what if I store my passwords in a Word or Excel file on my computer, and then password protect it?
There are a number of easily available tools out there for cracking passwords for protected files, such as Word, Excel, Acrobat/pdf, etc. They don't always crack every password, but is it a risk you're willing to take?
What's wrong with using the same passwords on different sites?

From the comic at https://www.explainxkcd.com/wiki/index.php/2176:_How_Hacking Works

* Once a hacker has a username and password, it's pretty standard for them to attempt that username and password on many other sites. For example, if your Home Depot account gets compromised, that username and password will probably be tried on banking sites, Facebook, etc.
* Most people don't keep track of where they've used their passwords, so even if you get an alert that a password has been compromised, it won't be possible to change it everywhere it was used, because most folks won't/don't remember where they used their passwords. That leaves accounts vulnerable.
How do I know if my account credentials have been compromised?

- Have I been Pwned?
- Search Security Data Breaches: https://oag.ca.gov/privacy/databreach/list
- Reports in the media

You should probably operate under the assumption that a data breach will happen, so it’s important to protect yourself as much as possible.

Sites for searching whether your usernames (typically your email address) and possibly passwords and other private information were exposed in a known data breach: https://haveibeenpwned.com/

CA Attorney General: https://oag.ca.gov/privacy/databreach/list (search for organizations that experienced data breaches, and were legally obligated to report. Possible/likely that many others have happened, but the organization doesn’t know, or didn’t report)

Data breaches happen on a somewhat regular basis. You should expect that your username at least, and possibly more personal/private information may be exposed as well. Try to protect your self as much as possible.
What is Social Engineering?

LiveSlide Site
http://www.youtube.com/watch?v=fHhNWAKw0bY&t=1m3s

This video clip is from Defcon, a large hacker conference, providing a good demonstration of social engineering. Basically someone conning you out of information you wouldn’t/shouldn’t provide. Can be a bit scary to see what a high-level capable hacker can do.
OK, so given all of this bad news, what can I do?

Ideally, your passwords should be:

- Strong (difficult to crack/guess)
- Unique (not shared)
- Easy to remember and/or use
- Available whenever and wherever you need them

* Not all is lost! You can protect yourself to a large degree. No security is perfect, but we want to work towards improving your security posture.

* Although there are many things you can do, with regard to passwords, choosing and using strong, unique passwords goes a long way. Ideally, they would be easy to use and/or remember, and available on a variety of devices.
First....password no-no’s

- Use any person’s name
- Use a place name, such as the city or state you live in, or the street where you grew up.
- Use any word that’s in any dictionary, in any language (even Klingon)
- Use the name of any character in any movie, video game or work of fiction currently in existence
- Use a common phrase, like “iloveyou” or “letmein”
- Use common number/special character substitutions (“G@nda1f” or “p@S5w0rd”)
- Use repeated characters or well-known patterns (“aaaaaaaaaa” or “1234567890” or “qwertyuiop”)
- Use any of the above, with a single number or character added (“1234567890a” or “qwertyuiop!”)
- Use any of the above, with the letters reversed

These are basic tips for what NOT to do:

- Use any person’s name (your name or the name of your spouse, child, parent, pet, close friend or co-worker)
- Use a place name, such as the city or state you live in, or the street where you grew up.
- Use any word that’s in any dictionary, in any language (even Klingon)
- Use the name of any character in any movie, video game or work of fiction currently in existence
- Use a common phrase, like “iloveyou” or “letmein”
- Use any of the above, with common number/special character substitutions (“G@nda1f” or “p@S5w0rd”)
- Use repeated characters or well-known patterns (“aaaaaaaaaa” or “1234567890” or “qwertyuiop”)
- Use any of the above, with a single number or character added (“1234567890a” or “qwertyuiop!”)
- Use any of the above, with the letters reversed
Demonstrating that although we’ve all been told not to use dictionary words as passwords, stringing unrelated words together actually works well. Adding complexity would be even better (using upper and lower case, numbers, symbols).
How to create a strong password

Should be difficult to crack or guess

Techniques:
• Formula approach
• [https://passwordcard.org](https://passwordcard.org)
• Diceware
• Latin square ([https://www.grc.com/offthegrid.htm](https://www.grc.com/offthegrid.htm))
• more…

Several techniques for creating passwords

Use a formula/recipe to create passwords for each site/service. Only need to remember the formula.
Print a wallet-sized card to carry: [https://passwordcard.org](https://passwordcard.org)
    Interesting explanation of how it works on the site
Use a large list of dictionary words and some dice: [https://theworld.com/~reinhold/diceware.html](https://theworld.com/~reinhold/diceware.html)
    Great strategy for creating long, strong passwords that are relatively easy to remember
Esoteric, unique way to create endless passwords: [https://www.grc.com/offthegrid.htm](https://www.grc.com/offthegrid.htm)
    Uses a simple sheet of paper. Very low-tech, cumbersome to use.
Other strategies exist
How to create a strong password: Formula

Example:

- Pick a base that you won't forget. [BASE]
- Use a random word, broken into pieces. [RAN] and [DOM]
- Use some letters from the name of the website or service. [URLSNIPPET]
- Throw in a random number that you won't forget. [RANDNUM]
- Glue the elements together in a way you'll remember, for example:

  [RAN] + [BASE] + [RANDNUM] + [URLSNIPPET] + [DOM]
  [RAN] + [BASE] + [URLSNIPPET] + [RANDNUM] + [DOM]
  [BASE] + [RAN] + [DOM] + [RANDNUM] + [URLSNIPPET]

* Example of the formula approach. It would take a little effort to create your formula, but once you have it, you can create endless passwords that are different for every site/service.

Important: Don’t let anyone ever get the formula, or else they’re be able to derive all of your passwords.
How to create a strong password: Formula

Example (cont’d):

- **BASE** = satisfactioN
- **RANDOM** = remember, so **[RAN]** = reme, **[DOM]** = mbeR
- **URLSNIPPET** = aaON (all vowels and last consonant of Amazon.com)
- **RANDNUM** = 1964 (year the Beatles performed on Ed Sullivan)

Example = remesatisfactioNaaoN1964mbeR (28 chars for amazon.com)

Don’t let anyone figure out your formula!!!
OK, this seems hard. Isn't there an easier way?
The short answer is: Yes. Use a password manager!

A good password manager can:

• Creates very strong passwords for you
• Create unique passwords for each site
• Remember passwords so you don’t have to
• Protect you from malicious sites
• Keep track of them for you
• Audit passwords
• Sync among your devices, if needed

• With all of these problems and complexity, there is a solution: A password manager. Most computer/IT professionals recommend using a password manager to help reduce, if not eliminate the problems mentioned previously.

• These are the main, but not all of the features and benefits of a good password manager.
Password Manager Recommendations


Link to a good article on why you should get a password manager:

Link to a review of good password managers, with recommendations (same site)
# Pros/Cons of a Password Manager

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>No need to remember ANY of your passwords, other than the master password</td>
<td>All of your eggs are in one ‘basket’</td>
</tr>
<tr>
<td>Create strong, unique passwords for every site</td>
<td></td>
</tr>
<tr>
<td>Keeps track of password usage</td>
<td></td>
</tr>
<tr>
<td>Password generator and auditing</td>
<td></td>
</tr>
<tr>
<td>Protects you from malicious sites</td>
<td></td>
</tr>
<tr>
<td>Automatically fills in your passwords when needed</td>
<td></td>
</tr>
<tr>
<td>Sync passwords among your computers and devices</td>
<td></td>
</tr>
</tbody>
</table>

Reiteration of most of the benefits of a password manager. Main downside is putting all of your passwords in one place. Must be well-protected with a VERY strong master password. Choose a good password manager that is well tested, audited, and has a strong track record (ie never been compromised!)
• Give a brief demo of 1Password, showing how to add credentials, and login easily with credentials.
Questions?