A World Leading SFI Research Centre

Science Foundation Ireland sfi For what's next

CONNECT
Centre for Future Networks

Password security: recommendations versus reality.

Hazel Murray
Lecturer, Munster Technological University, Ireland

MTU
Ollscoil Teicneolaíochta na Mumhan
Munster Technological University

Trinity College Dublin
The University of Dublin

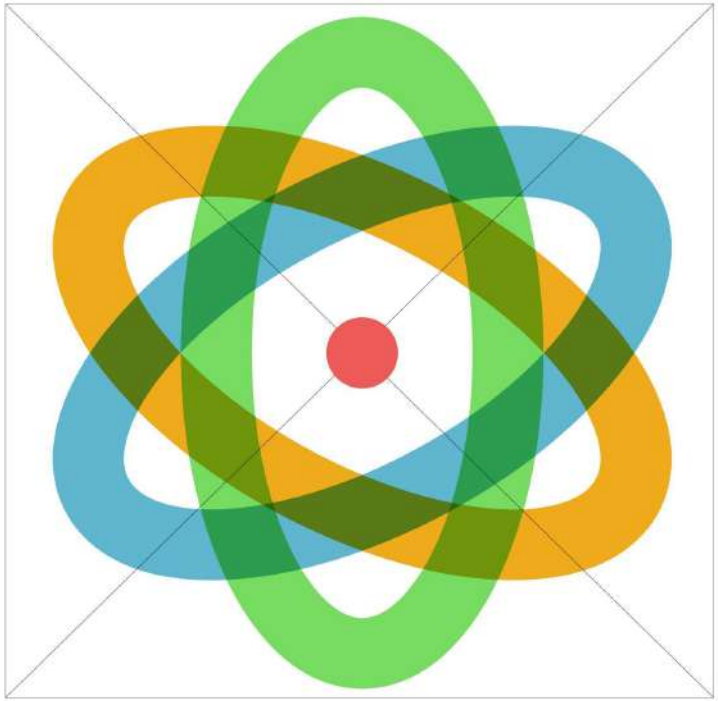
Ireland's European Structural and Investment Funds Programmes 2014-2020
Co-funded by the Irish Government and the European Union

European Union
European Regional Development Fund

Science Foundation Ireland sfi For what's next

Contents

- Password Advice
- The costs and the benefits
- The reality!
- Automation in attack vectors

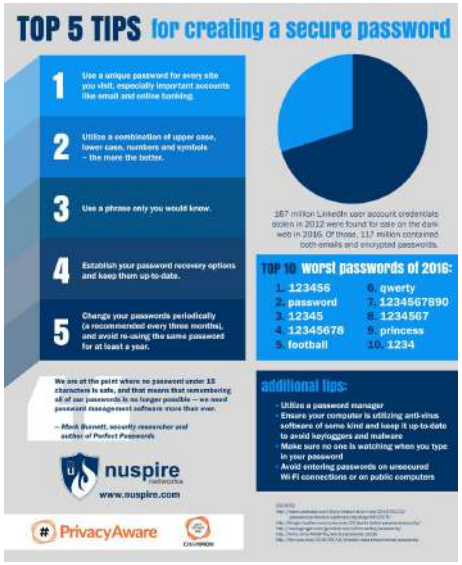



How safe is your password?
Website databases will often 'encrypt' your password to make it more secure. They do this by putting them through a system that will effectively turn it into a code known as 'hash'


Password security
Attackers use a variety of techniques to discover passwords, including using p
freely available on the internet. The following advice makes password security
users – improving your system security as a result.
are cracked...
...and how to improve your system
e Force
Stealing Passwords
4
Average number of websites users access using the same password
22
Average number of UK citizen's online passwords
Help users cope with 'password overload'
Only use passwords where they are re
Use technical solutions to reduce the b
Allow users to securely record and stor
Only ask users to change their passwo
of suspicion of compromise
Allow users to reset password easily
Help users generate appropriate passwords
Put technical defences in place so that


10 PASSWORD SECURITY TIPS
01
02
03
04
05
06
07
08
09
10


Norton Identity Safe Tips
Password Generator
Use the Norton Identity Safe Password Generator to create highly secure passwords that are difficult to crack or guess. Just select the criteria for the passwords you need, and click "Generate Password(s)". Remember, the more options you choose, the more secure the passwords will be.
Rather than a list of password advice Norton has a password generator where you can test your passwords strength.
Password Protection - to support GAFE Password Creation
2 July 2016 - Natasha Walden
To view the original link click here.


TOP 5 TIPS for creating a secure password
1 Use a unique password for every site you visit, especially important accounts like email and online banking.
2 Utilize a combination of upper case, lower case, numbers and symbols – the more the better.
3 Use a phrase only you would know.
4 Establish your password recovery options and keep them up-to-date.
5 Change your passwords periodically (a recommended every three months), and avoid re-using the same password for at least a year.
167 million LinkedIn user account credentials stolen in 2012 were found for sale on the dark web in 2016. Of those, 117 million contained both emails and encrypted passwords.
TOP 10 Worst passwords of 2016:
1. 123456
2. password
3. 12345
4. 12345678
5. football
6. qwerty
7. 1234567890
8. 1234567
9. princess
10. 1234
We are at the point where no password under 15 characters is safe, and that means that remembering all of our passwords is no longer possible – we need password management software more than ever.
– Mark Burnett, security researcher and author of Perfect Passwords
additional tips:
Utilize a password manager
Ensure your computer is utilizing anti-virus software of some kind and keep it up-to-date to avoid keyloggers and malware
Make sure no one is watching when you type in your password
Avoid entering passwords on unsecured Wi-Fi connections or on public computers
nuspire networks
www.nuspire.com
#PrivacyAware


HOW TO CREATE A SECURE PASSWORD
datastore365


Tips for Teens: Password Safety
Keeping Your Identity and Information Safe and Secure
Sameer Hinduja, Ph.D. and Justin W. Patchin, Ph.D.
April 201
1. Protect them
Never, ever give your password (on Facebook, Instagram, Skype, email, or any similar service) or cell phone unlock code to anyone—even a friend. Friendships sometimes don't last, and that password can be used against you.
2. Remember your secret answer
When you create an online account, and it asks you to provide an answer to a question you should know - don't treat it lightly or as a joke. Make sure it's something you will remember months and years from now in case you have a problem at that time.
3. Don't disclose information about you
Do not use passwords based on personal information (your login name, birthdate, address, phone number, mid-
6. Change it up
Change your password often. It takes time and is a bit of chore, but do it anyway. It takes more time and is more a chore to try to recover from a hacked account or fro identity theft.
7. Don't send it to others
Never provide your password via a text message or ov email or in response to a request. You could accidental send it to the wrong person or that person might show to someone else. Or it could be a scam.
8. Don't post it
Do not place a written copy of your password on the sid of your monitor, under your keyboard, in your lapto case, etc. Figure out a secure place where you can sto


Password Guidan
Tip 7: Don't store passwords
Passwords should never be stored as plain text, even if protected system is relatively unimportant. This sectio developers and engineers, and will help security practi provide more secure methods of password storage and
We've read how users re-use passwords and employ predictable password creation strategies. This means an attacker who gains access to a database containing plain text passwords already knows a user's credentials for one system. They can use this information to attempt to access more important accounts, where further damage can be done.
Periodically search systems for password information that is stored in plain text. Consider establishing automated processes that (for example) regularly search for clear text emails and
However, a attacks and for reversin retrieve pa reason, a 's before hash
In summ

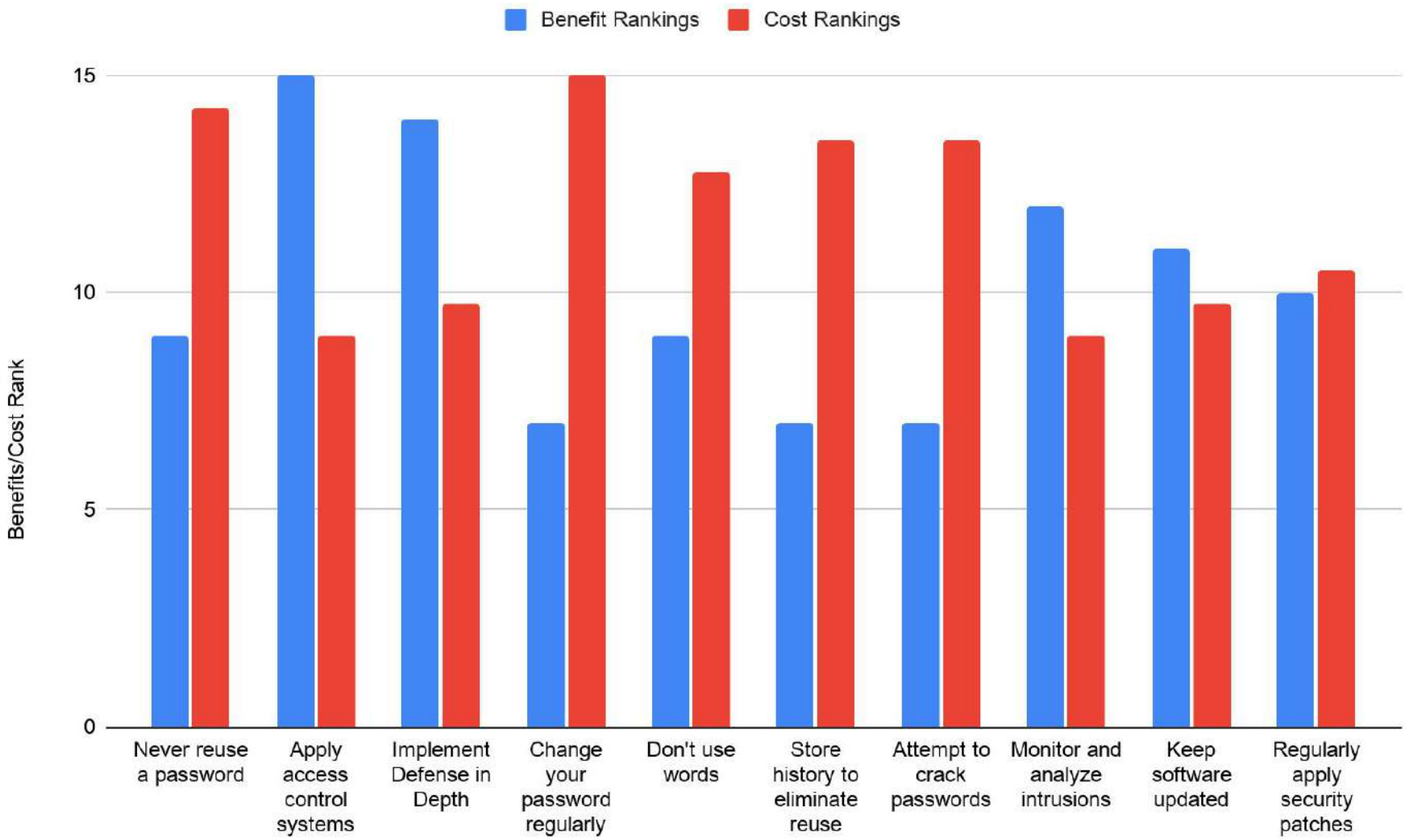
Contradictions

Statements for 4 advice categories

- Reuse
- Phrases
- Composition
- Expiry

Reuse	✘	✓	
Never reuse a password.	5	6	←
Alter and reuse passwords	3	3	←
Don't reuse certain passwords.	0	5	
Phrases	**✘**	**✓**	
Don't use patterns.	0	6	
Take initials of a phrase.	0	4	
Don't use published phrases.	1	2	←
Substitute symbols for letters.	1	2	←
Don't use words.	0	16	
Composition	**✘**	**✓**	
Must include special characters	5	7	←
Don't repeat characters.	0	3	
Enforce restrictions on characters.	1	12	←
Expiry	**✘**	**✓**	
Store history to eliminate reuse.	0	5	
Have a minimum Password Age.	0	1	
Change your password regularly.	4	7	←
Change if suspect compromise.	0	10	

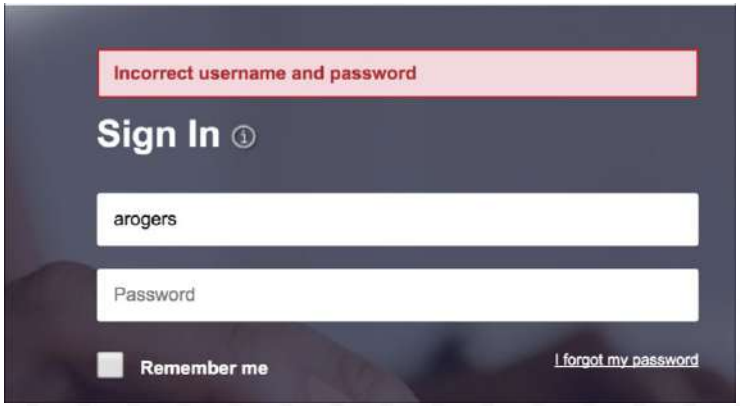
Costs and Benefits



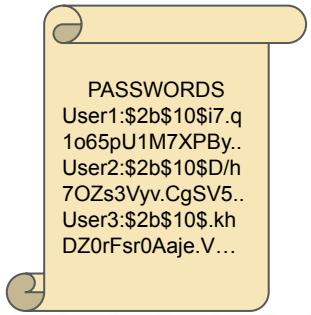
The reality!

Your PASSWORD will expire in 90 days

Online guessing



Offline guessing



P@sswordMay

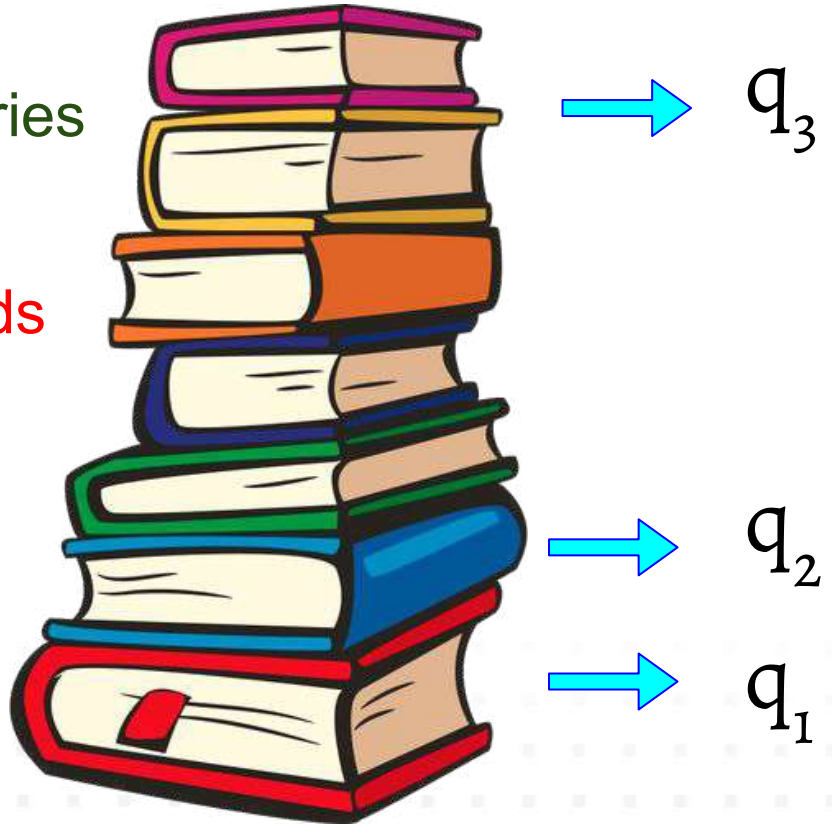
P@sswordJune

Automated attack

Multiple language dictionaries

Lists of common passwords

Website of user specific information



Automated attacks

Facebook 13
Facebooku
computerispowerfacebook

linkedin
LinkedIn
jobsearch

Summary

- Password advice is contradictory
- Does not represent best practice and security research
- High user and organisation costs and low security benefits
- Consider the attack landscape when giving advice.
- For a general user automated attacks are what we need to be most concerned about.
- Tailored blocklisting

Thank you

Contact:
hazel.murray@cit.ie

Trinity College Dublin The University of Dublin
Ireland's European Structural and Investment Funds Programmes 2014-2020
Co-funded by the Irish Government and the European Union
European Union European Regional Development Fund
Science Foundation Ireland sfi For what's next