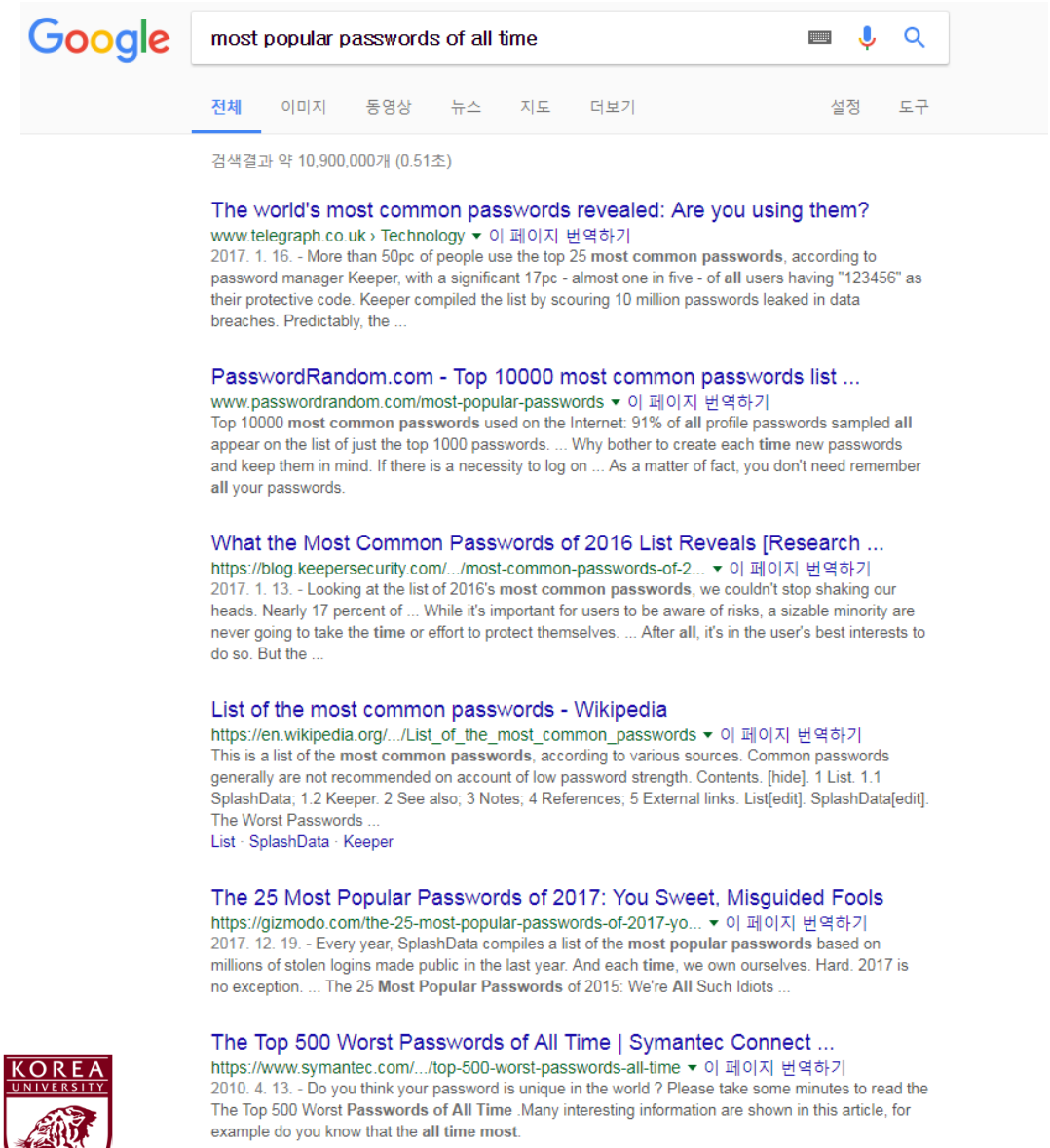
COSC 362

Chapter 3. User Authentication

Means of Authentication

- Something the individual knows
  - Password, PIN (Personal Identification Number), or answers to a prearranged set of questions
- Something the individual possesses (tokens)
  - Electronic keycards, smart cards, physical keys, ...
- Something the individual is (static biometric)
  - fingerprint, retina, face, ...
- Something the individual does (dynamic biometric)
  - voice pattern, handwriting characteristics, and typing rhythm

Password Vulnerabilities



Type of Password	Search Size	Number of Matches	Percentage of Passwords Matched	Cost/Benefit Ratio[a]
User/account name	130	368	2.7%	2.830
Character sequences	866	22	0.2%	0.025
Numbers	427	9	0.1%	0.021
Chinese	392	56	0.4%	0.143
Place names	628	82	0.6%	0.131
Common names	2239	548	4.0%	0.245
Female names	4280	161	1.2%	0.038
Male names	2866	140	1.0%	0.049
Uncommon names	4955	130	0.9%	0.026
Myths and legends	1246	66	0.5%	0.053
Shakespearean	473	11	0.1%	0.023
Sports terms	238	32	0.2%	0.134
Science fiction	691	59	0.4%	0.085
Movies and actors	99	12	0.1%	0.121
Cartoons	92	9	0.1%	0.098
Famous people	290	55	0.4%	0.190
Phrases and patterns	933	253	1.8%	0.271
Surnames	33	9	0.1%	0.273
Biology	58	1	0.0%	0.017
System dictionary	19683	1027	7.4%	0.052
Machine names	9018	132	1.0%	0.015
Mnemonics	14	2	0.0%	0.143
King James bible	7525	83	0.6%	0.011
Miscellaneous words	3212	54	0.4%	0.017
Yiddish words	56	0	0.0%	0.000
Asteroids	2407	19	0.1%	0.007
TOTAL	62727	3340	24.2%	0.053

Passwords Cracked from a Sample Set of 13,797 Accounts

*Computed as the number of matches divided by the search size. The more words that need to be tested for a match, the lower the cost/benefit ratio.

*Stallings and Brown, Table 3.2

Always Happening

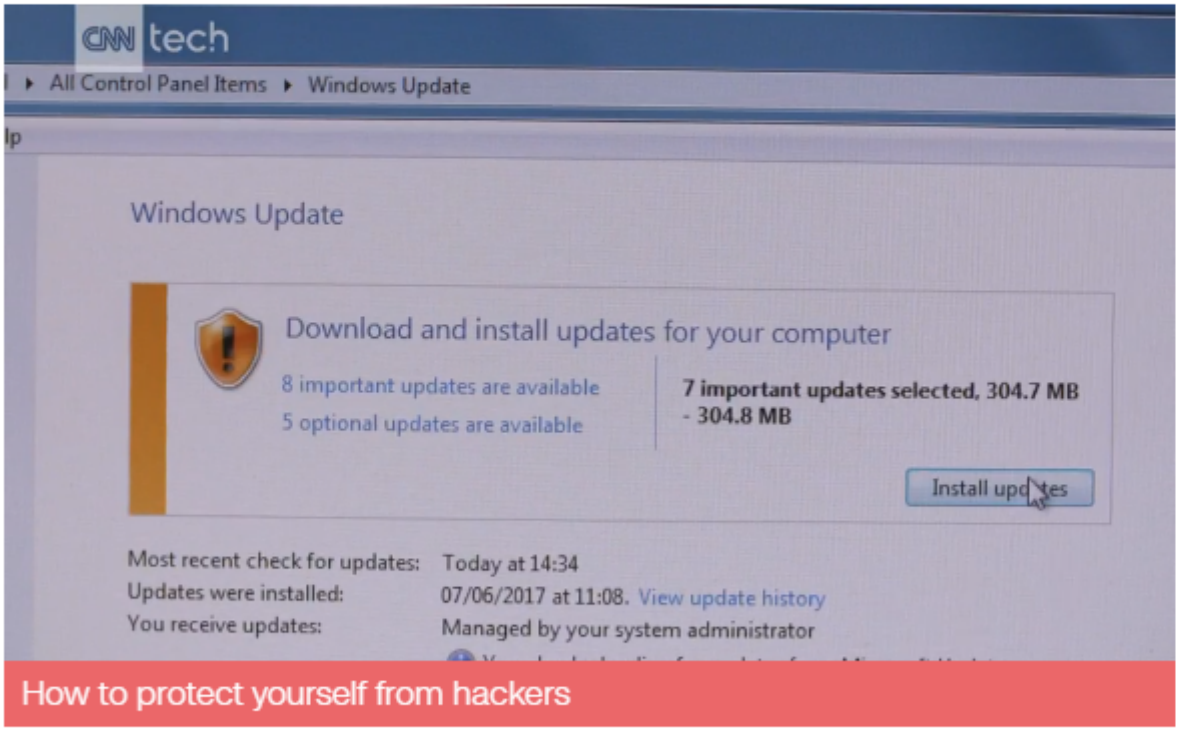
Same old story…

Cyber-Safe

Google says hackers steal almost 250,000 web logins each week

by Selena Larson @selenalarson

November 9, 2017: 4:13 PM ET



Google is digging into the dark corners of the web to better secure people's accounts.

SEC hands down $35 million fine in Yahoo hack

by Heather Kelly @heatherkelly

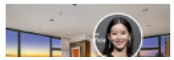
April 24, 2018: 5:28 PM ET

DOJ: Russian agents behind Yahoo cyberattack

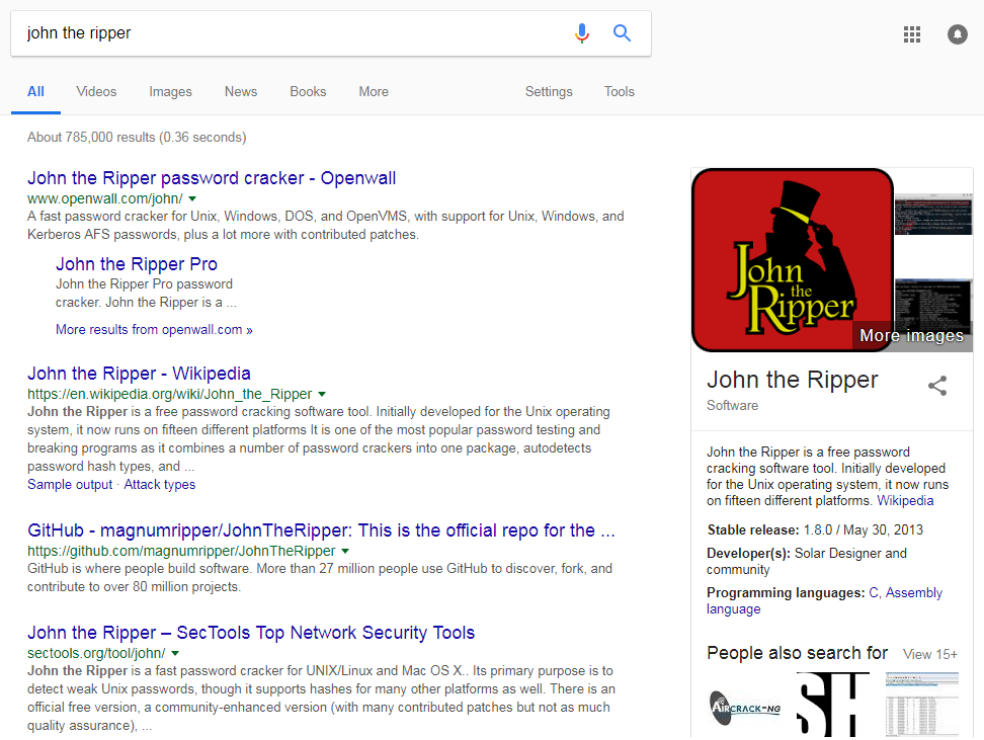
Yahoo may have changed its name, but it's still paying for a massive 2014 data breach.

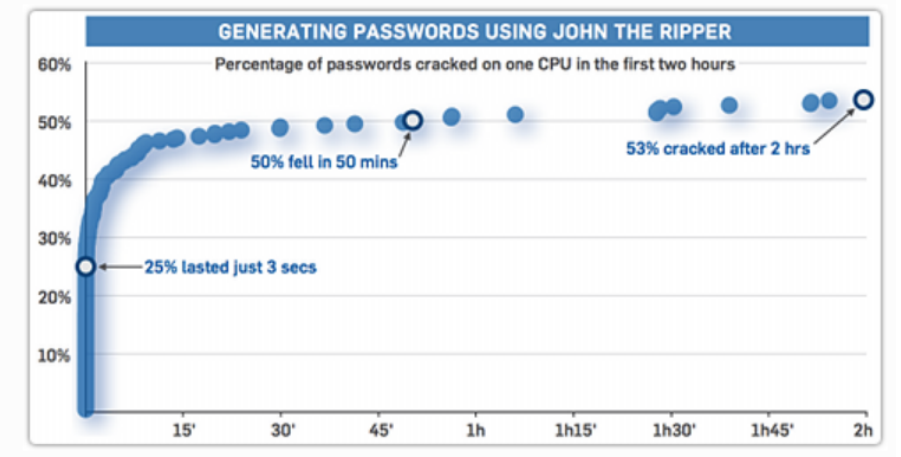
Altaba, what's left of Yahoo after the company sold most of its properties, has agreed to pay $35 million to settle charges that it misled investors about the hack, the US Securities and Exchange Commission said Tuesday.

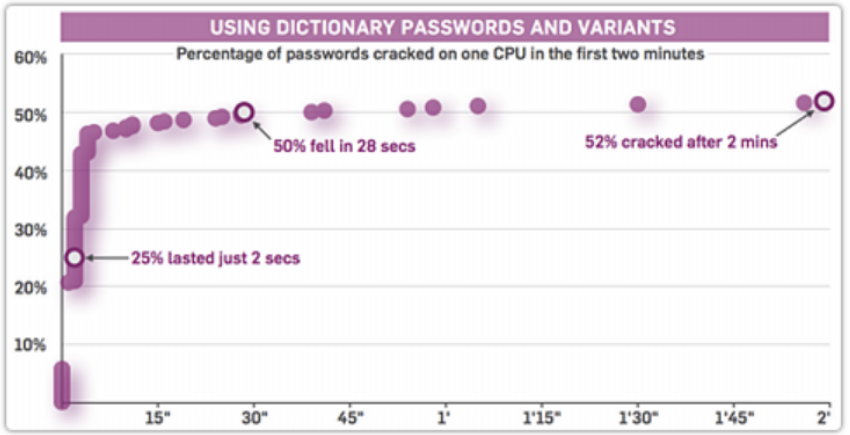
In 2017, Yahoo completed the sale off its core business to Verizon for $4.48 billion. It retained large stakes in e-commerce company Alibaba and Yahoo Japan and changed its name to Altaba.



No surprise at all







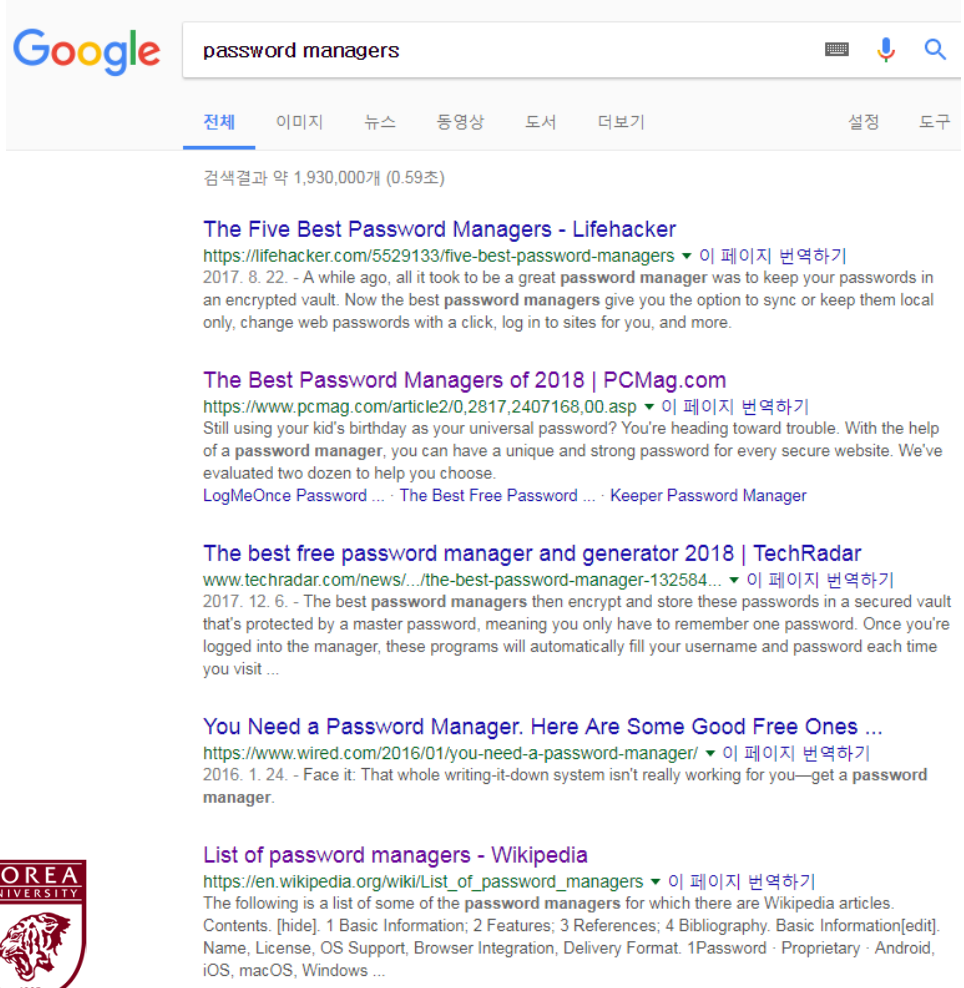
(Text-based) Password Vulnerabilities

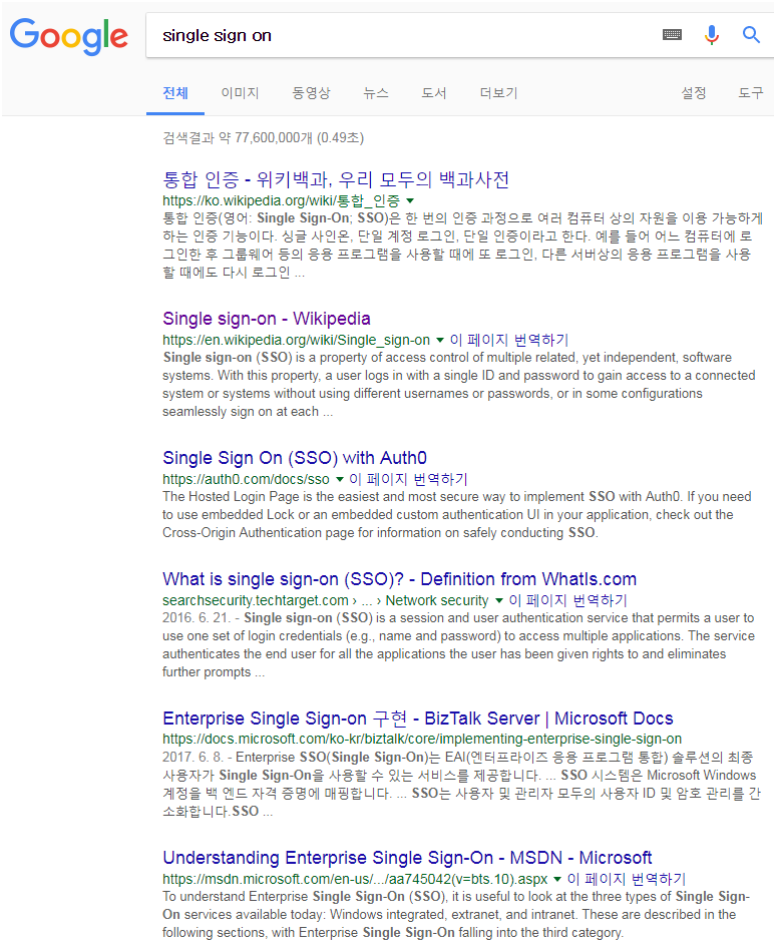
	How it works	Threats	Potential Countermeasures
Offline dictionary attack			
Specific account attack			
Popular password attack			
Password guessing			
Shoulder surfing (or social engineering)			
Workstation hijacking			
Exploiting user mistakes			
Exploiting multiple password use			
Electronic monitoring			

- Especially difficult when managing passwords on multiple sites

Password Managers, Single sign-on, …

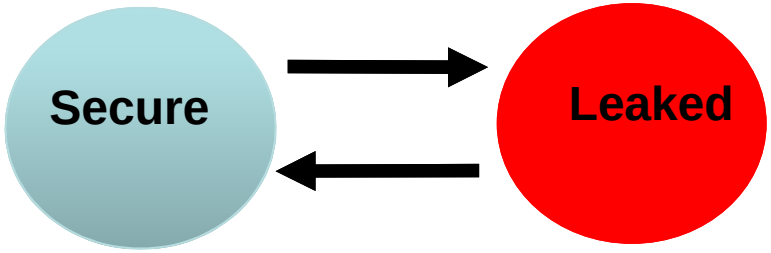
- Is this a good idea?
- Browsers often perform the role of password managers





“Personal” Nightmare

- This list is most likely the tip of the iceberg !
  - Very (extremely?) difficult to remember
  - Heavily reused, small candidate pools, special character rules, …
  - Difficult, if not impossible, to detect attacks in timely manner
  - …

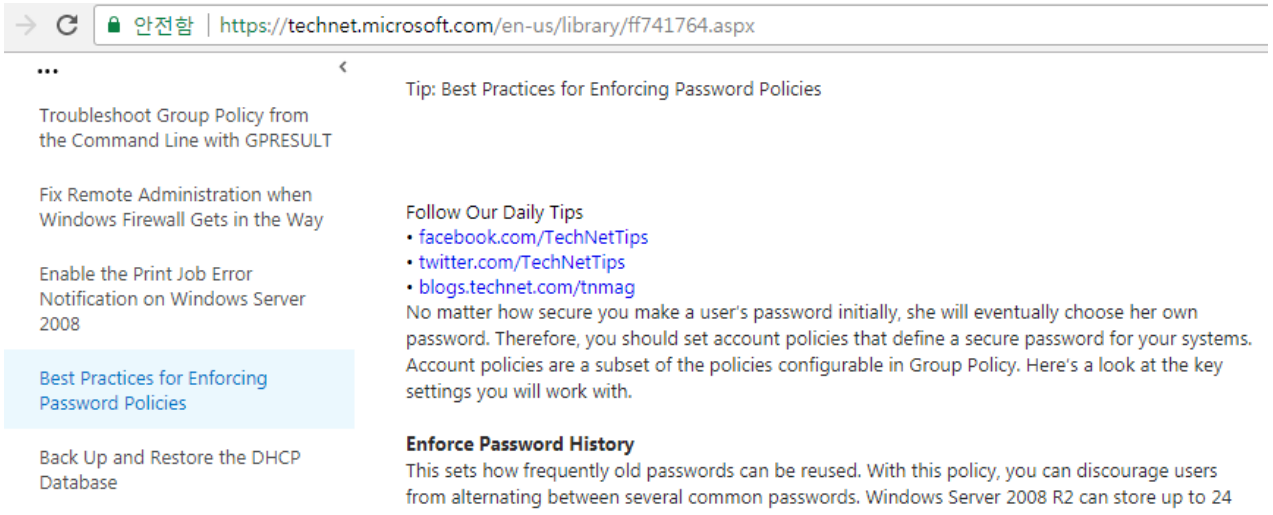


KOREA UNIVERSITY 1905

Personal “trauma”?

Best Practices for Enforcing Password Policies (Microsoft)

- Enforce password history
- Maximum password age
- Minimum password age
- Minimum password length
- Passwords must meet complexity requirements
- Store password using reversible encryption for all users



/etc/passwd

https://en.wikipedia.org/wiki/Passwd

The `/etc/passwd` file is a text-based database of information about users that may log into the system or other operating system user identities that own running processes.

In many operating systems this file is just one of many possible back-ends for the more general passwd name service.

The file's name originates from one of its initial functions as it contained the data used to verify passwords of user accounts. However, on modern Unix systems the security-sensitive password information is instead often stored in a different file using shadow passwords, or other database implementations.

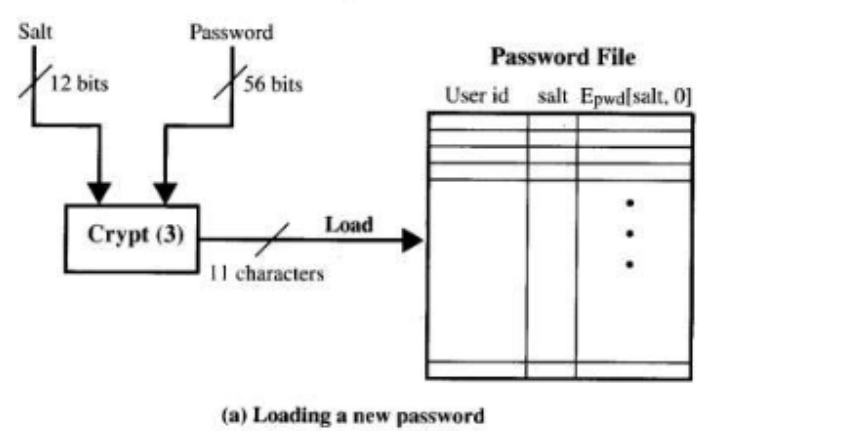
The `/etc/passwd` file typically has file system permissions that allow it to be readable by all users of the system (*world-readable*), although it may only be modified by the superuser or by using a few special purpose privileged commands.

The `/etc/passwd` file is a text file with one record per line, each describing a user account. Each record consists of seven fields separated by colons. The ordering of the records within the file is generally unimportant.

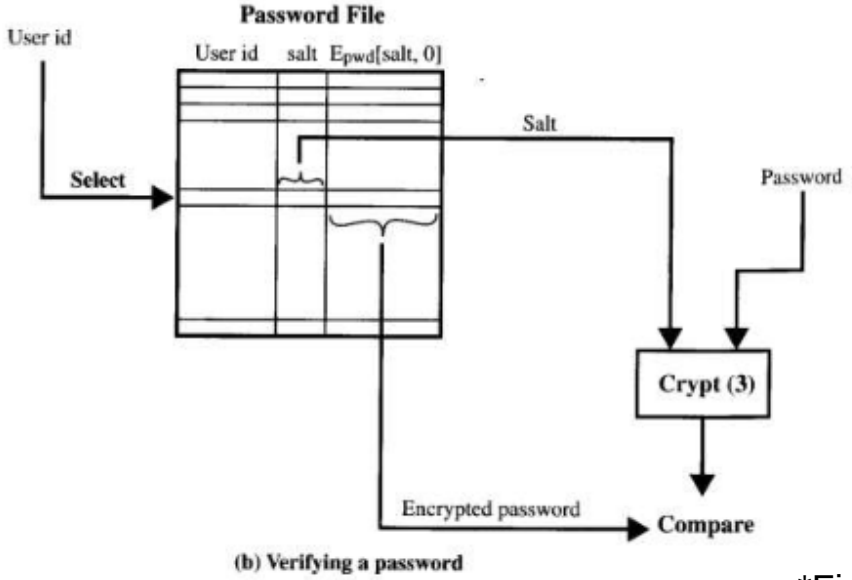
An example record may be:

```
jsmith:x:1001:1000:Joe Smith,Room 1007,(234)555-8910,(234)555-
0044,email:/home/jsmith:/bin/sh
```

UNIX Password Scheme



(a) Loading a new password



(b) Verifying a password

Figure 15.5 UNIX Password Scheme

(From W. Stallings, Operating Systems)

*Figure 3.1 in Stallings and Brown

“Unix salt”

- It prevents duplicate passwords from being visible in the password file
- It greatly increases the difficulty of offline dictionary attacks. For a salt of length b bits, the number of possible passwords is increased by a factor of 2^b
- It becomes nearly impossible to find out whether a person with passwords on two or more systems have used the same password on all of them

/etc/shadow and salt

안전함 | https://superuser.com/questions/822079/etc-shadow-in-old-format-where-is-salt-stored

/etc/shadow in old format, where is salt stored?

3

1

In /etc/shadow I have entries such as `admin:YtChlvAGYzva2:16318:0:99999:7:::`. I know the original password and would like to generate the same hash somehow. However, running `openssl passwd -crypt password` gives me different results every time I run it. I assume salt is involved, so where can I find the salt used to create the original hash?

Edit: I got the original hash using the following command:

```
openssl passwd -crypt -salt Yu password
```

The salt and the encrypted password are both mashed into the string YtChlvAGYzva2.

From the Shadow Password Howto:

> When a user picks or is assigned a password, it is encoded with a randomly generated value called the salt. This means that any particular password could be stored in 4096 different ways. The salt value is then stored with the encoded password.
>
> When a user logs in and supplies a password, the salt is first retrieved from the stored encoded password.

The longer password strings you see with modern systems separate the hash using $. But for the older systems, it was just mashed in (Wikipedia):

> Earlier versions of Unix used a password file (/etc/passwd) to store the hashes of salted passwords (passwords prefixed with two-character random salts). In these older versions of Unix, the salt was also stored in the passwd file (as cleartext) together with the hash of the salted password.

/etc/shadow

안전함 | https://www.cyberciti.biz/faq/understanding-etcshadow-file/

Info on the Linux Kernel Meltdown/Spectre Vulnerabilit

Understanding /etc/shadow file

in BASH Shell, CentOS, Debian / Ubuntu, FreeBSD, HP-UX Unix, Linux, RedHat and Friends, Solaris-Unix, Suse, Ubuntu Linux, UNIX, User Management

last updated August 2, 2017

Can you explain /etc/shadow file format used under Linux or UNIX-like system?

The **/etc/shadow** file stores actual password in encrypted format (more like the hash of the password) for user's account with additional properties related to user password. Basically, it stores secure user account information. All fields are separated by a colon (:) symbol. It contains one entry per line for each user listed in /etc/passwd file Generally, shadow file entry looks as follows (click to enlarge image):

/etc/shadow

shadow(5) - Linux man page

Name

shadow - shadowed password file

Description

shadow is a file which contains the password information for the system's accounts and optional aging information.

This file must not be readable by regular users if password security is to be maintained.

Each line of this file contains 9 fields, separated by colons (":"), in the following order:

login name

It must be a valid account name, which exist on the system.

encrypted password

Refer to **crypt**(3) for details on how this string is interpreted.

If the password field contains some string that is not a valid result of *, the user will not be able to use a unix password to log in (but the u by other means).

This field may be empty, in which case no passwords are required to specified login name. However, some applications which read the /etc not to permit any access at all if the password field is empty.

A password field which starts with a exclamation mark means that th remaining characters on the line represent the password field before

date of last password change

The date of the last password change, expressed as the number of da

e value 0 has a special meaning, which is that the user should chan time she will log in the system.

An empty field means that password aging features are disabled.

/etc/shadow file fields

(Fig.01: /etc/shadow file fields)

1. **Username** : It is your login name.
2. **Password** : It is your encrypted password. The password should be minimum 8-12 characters long including special characters, digits, lower case alphabetic and more. Usually password format is set to `$id$salt$hashed`, The `$id` is the algorithm used On GNU/Linux as follows:
   1. **1** is MD5
   2. **$2a$** is Blowfish
   3. **$2y$** is Blowfish
   4. **5** is SHA-256
   5. **6** is SHA-512
3. **Last password change (lastchanged)** : Days since Jan 1, 1970 that password was last changed
4. **Minimum** : The minimum number of days required between password changes i.e. the number of days left before the user is allowed to change his/her password
5. **Maximum** : The maximum number of days the password is valid (after that user is forced to change his/her password)
6. **Warn** : The number of days before password is to expire that user is warned that his/her password must be changed
7. **Inactive** : The number of days after password expires that account is disabled
8. **Expire** : days since Jan 1, 1970 that account is disabled i.e. an absolute date specifying when the login may no longer be used.

DIY please

```
jsmith:x:1001:1000:Joe Smith,Room 1007,(234)555-8910,(234)555-
0044,email:/home/jsmith:/bin/sh
```

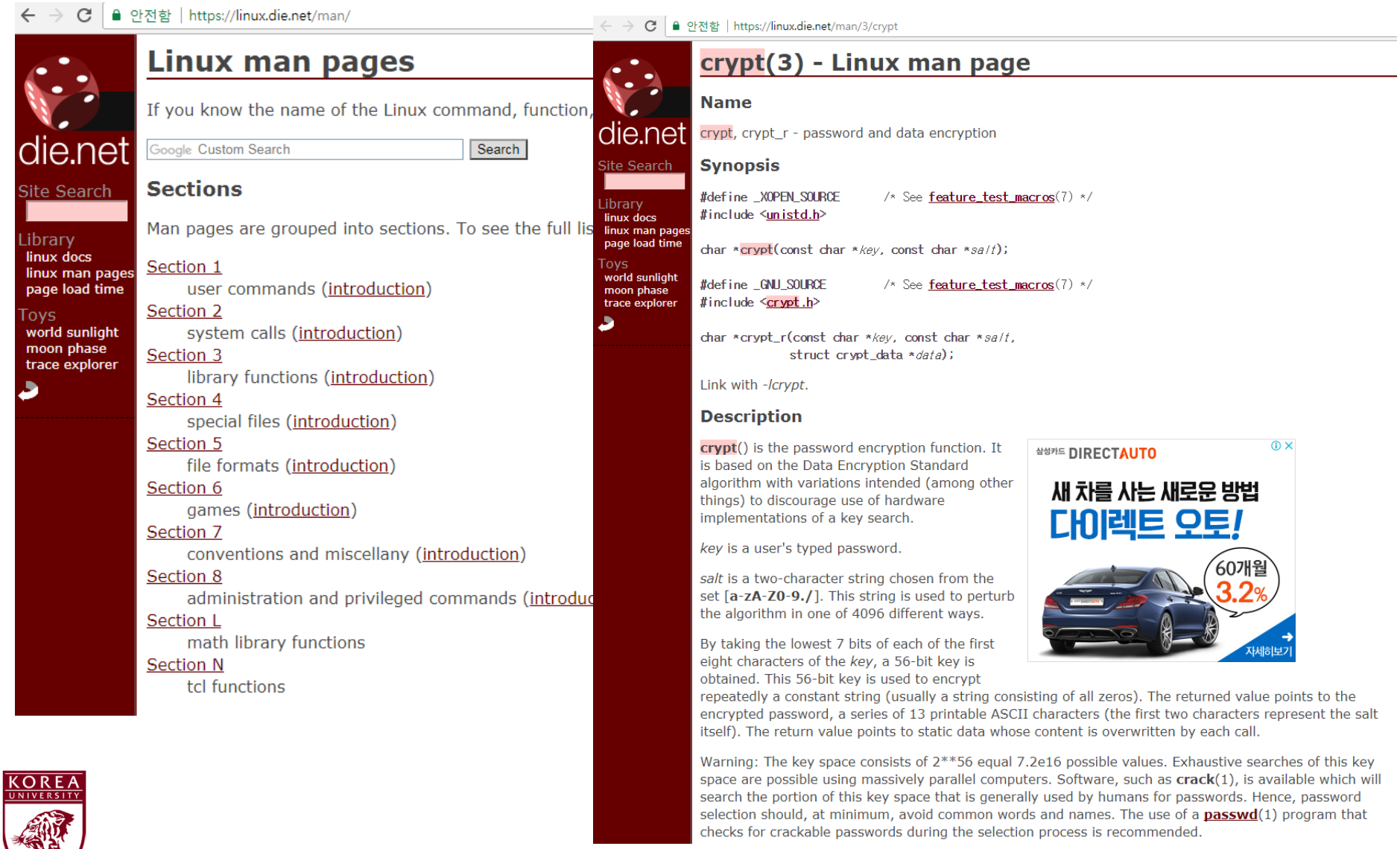
The fields, in order from left to right, are:[1]

1. User name: the string a user would type in when logging into the operating system: the logname. Must be unique across users listed in the file.
2. Information used to validate a user's password; in most modern uses, this field is usually set to "x" (or "*", or some other indicator) with the actual password information being stored in a separate shadow password file. On Linux systems, setting this field to an asterisk ("*") is a common way to disable direct logins to an account while still preserving its name, while another possible value is "*NP*" which indicates to use an NIS server to obtain the password.[2] Without password shadowing in effect, this field would typically contain a cryptographic hash of the user's password (in combination with a salt).
3. user identifier number, used by the operating system for internal purposes. It need not be unique.
4. group identifier number, which identifies the primary group of the user; all files that are created by this user may initially be accessible to this group.
5. Gecos field, commentary that describes the person or account. Typically, this is a set of comma-separated values including the user's full name and contact details.
6. Path to the user's home directory.
7. Program that is started every time the user logs into the system. For an interactive user, this is usually one of the system's command line interpreters (shells).

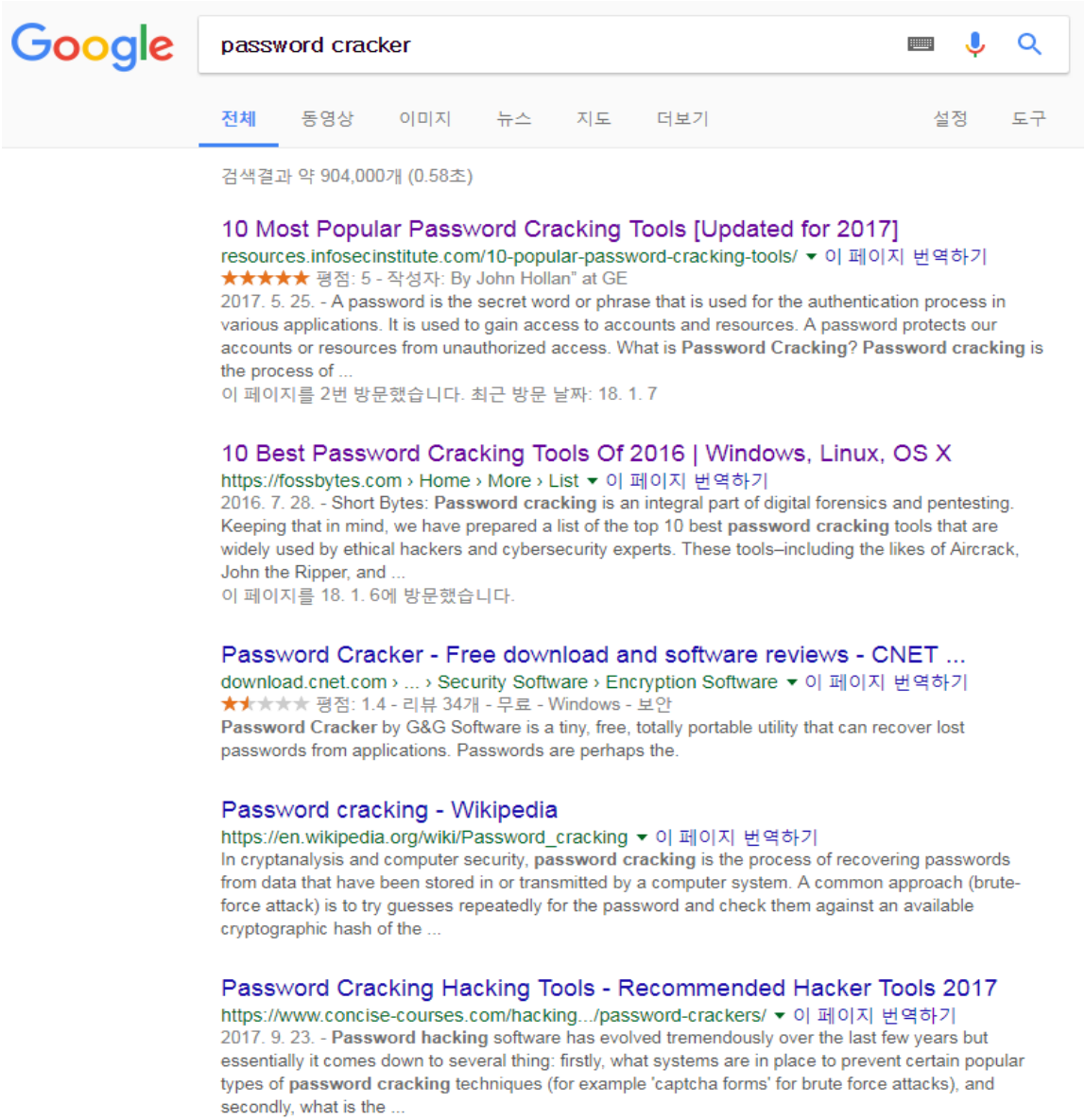
Shadow file [edit]

`/etc/shadow` is used to increase the security level of passwords by restricting all but highly privileged users' access to hashed password data. Typically, that data is kept in files owned by and accessible only by the super user.

crypt and DES



Password Crackers



Password Crackers

- Brutus
- RainbowCrack
- Wfuzz
- Cain and Abel
- John the Ripper
- THC Hydra
- Medusa
- OphCrack
- L0phtCrack
- Aircrack-NG

Typical Password Rules

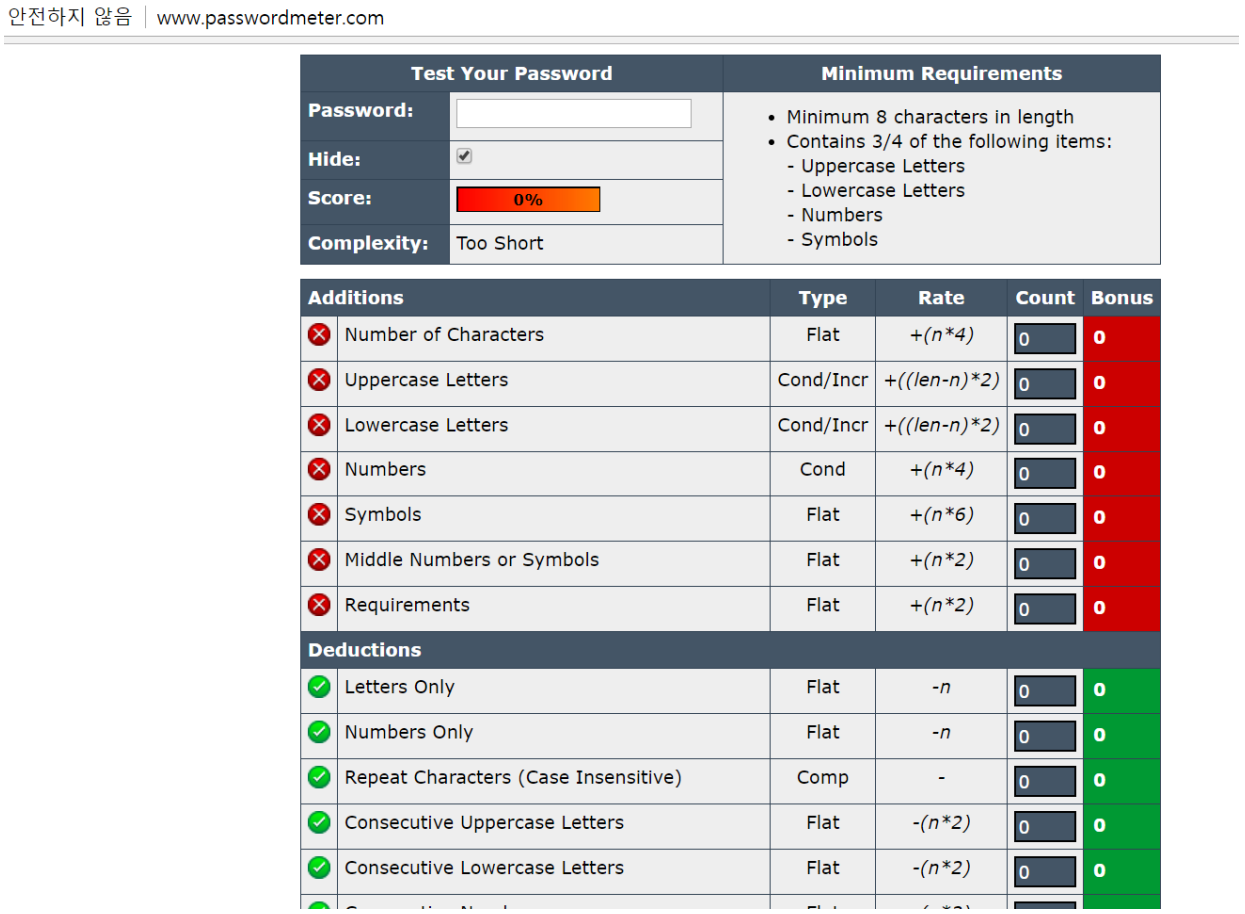
- Trade-offs among enhanced security vs ability to remember
  - Site-specific rules add confusion

Password Rules
Certain rules should be followed to ensure that the password that you choose is secure:

1. Don't use names, surnames, pet names of family members, friends or pets, birthdays, anniversaries, or common phrases.
2. Spaces are not allowed at the beginning and end of passwords.
3. We impose the following password rules:
   - Your password has to be at least 6 characters long.
   - Must contain at least one lower case letter,
   - one upper case letter,
   - one digit
   - and one of these special characters ~!@#$%^&*()_+
   - Your password will expire from time to time.
4. The best place to store your password is in your head, but if you tend to forget these types of things please make sure that you write your password down and store in a very secure place.

Typical Password Rules

- Trade-offs among enhanced security vs ability to remember
- Site-specific rules add confusion

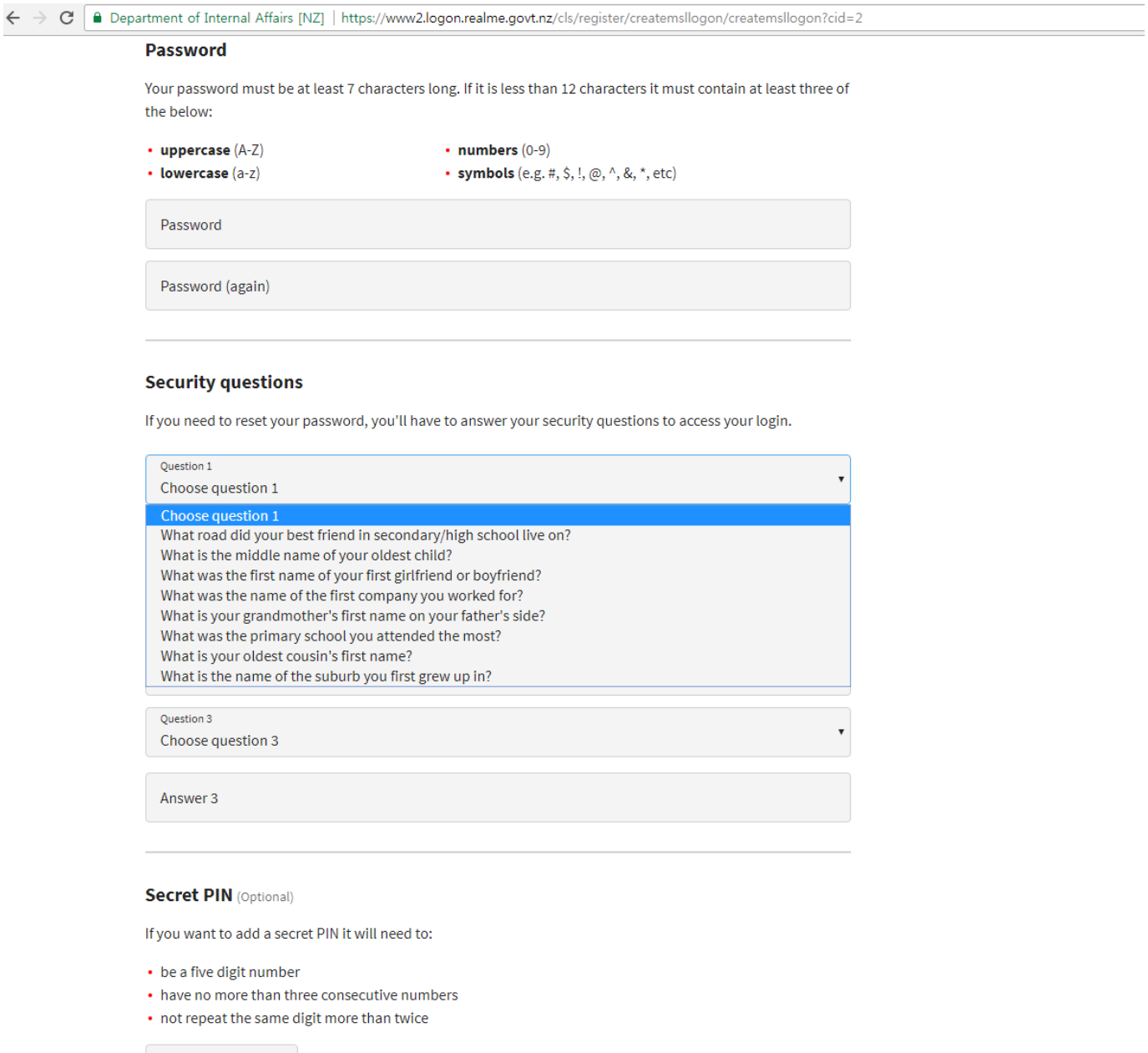


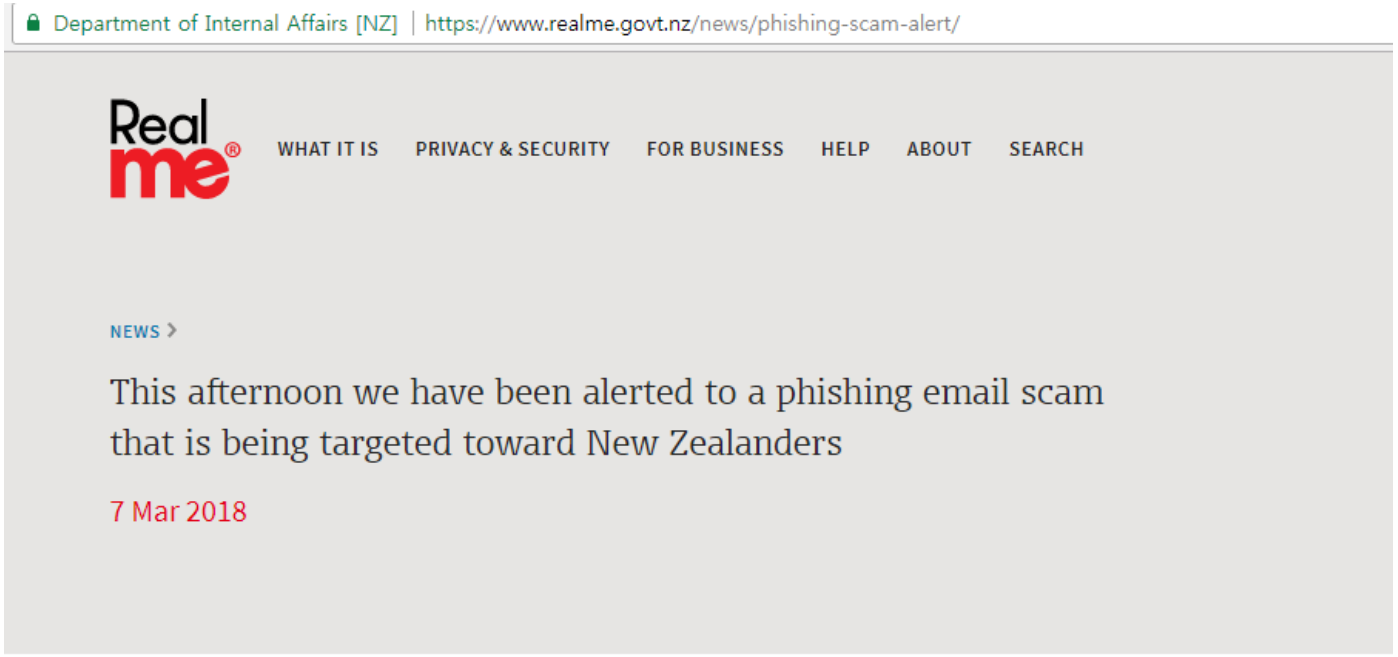
안전하지 않음 | www.passwordmeter.com

Test Your Password		Minimum Requirements
Password:		• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☑	
Score:	0%	
Complexity:	Too Short	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	0	0
Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
Lowercase Letters	Cond/Incr	+((len-n)*2)	0	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)	0	0
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	0	0
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	0	0

RealMe, New Zealand Government





This afternoon we have been alerted to a phishing email scam that is being targeted toward New Zealanders. People have received an email stating that the user has a private message and they need to access their RealMe account. The web link in the email then takes the user to a fake RealMe website that requests the user to validate their identity and upload personal documents (passport and driver's license).

If you receive this RealMe phishing email do not click the web link. Please report the email to: https://www.cert.govt.nz/businesses-and-individuals/report-an-issue/

These emails are coming from non-government email addresses and direct users to non-government web sites.

Neither the RealMe website itself or any customer accounts have been hacked or compromised.

Phishing attacks use 'spoof' emails and fraudulent websites designed to entice recipients into divulging personal financial data such as credit card numbers, identity details, bank and other account usernames and passwords.

안전함 | https://www.google.com/search?newwindow=1&biw=1102&bih=1062&tbm=isch&sa=1&ei=8CYOW7OxHYqx8QWrhbroAQ&q=treat+your+password+like+your+...

Google

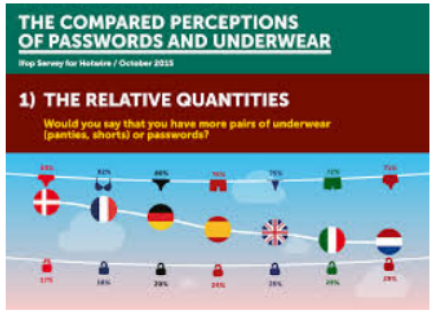
treat your password like your

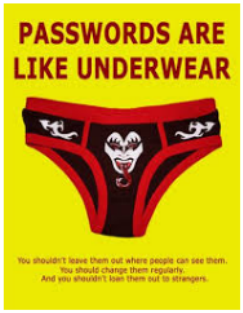
- treat your password like your **underwear** Remove
- treat your password like your **toothbrush**
- treat your password like your **underpants**

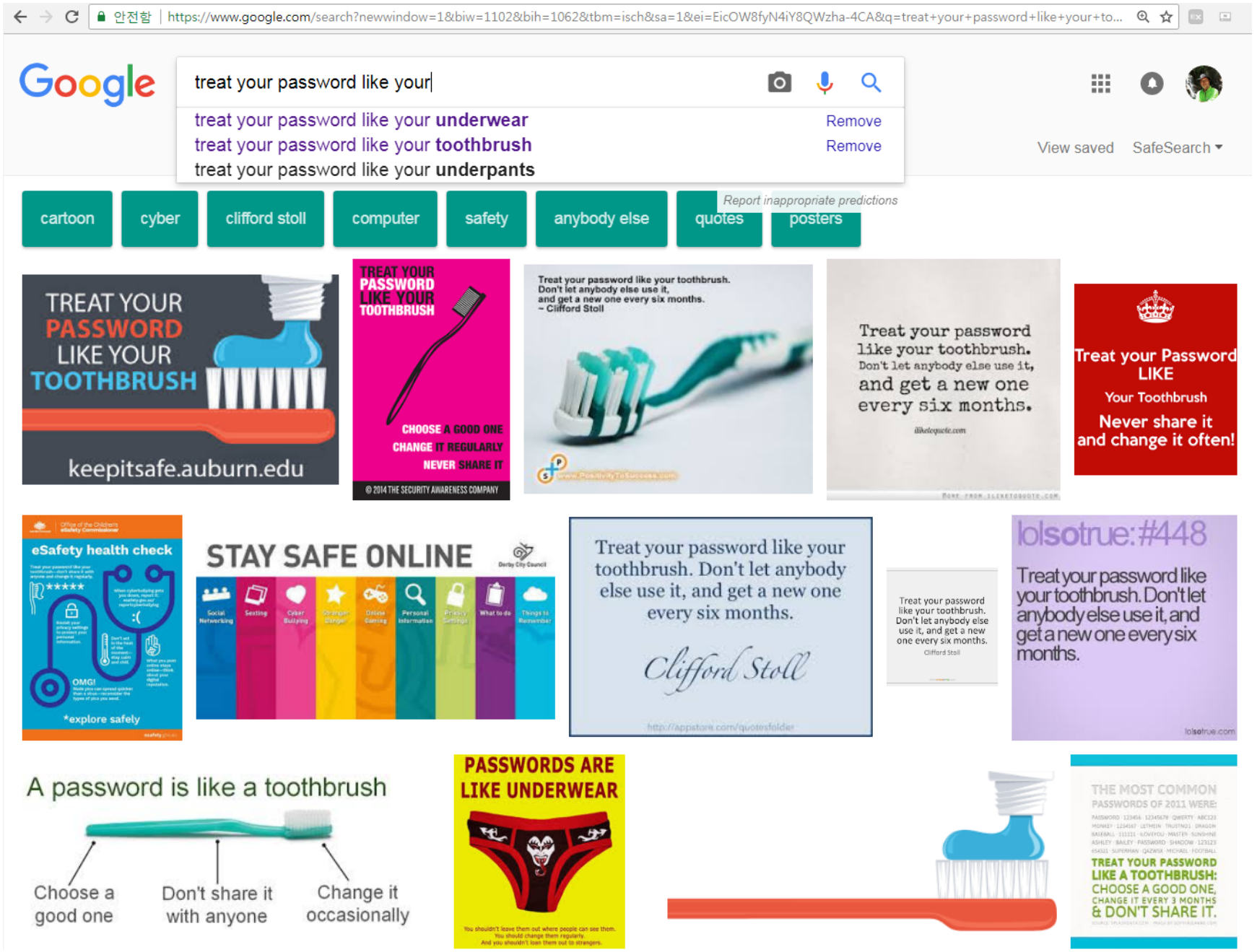
View saved SafeSearch

Report inappropriate predictions

smegma | secure | hacked | instagram account | incorrect | yout underwear | delicately | pulau pangkor | scott heath






https://www.google.com/search?newwindow=1&biw=1102&bih=1062&tbm=isch&sa=1&ei=EicOW8fyN4iY8QWzha-4CA&q=treat+your+password+like+your+to...
Google
treat your password like your
treat your password like your underwear
treat your password like your toothbrush
treat your password like your underpants
Remove
Remove
View saved
SafeSearch
Report inappropriate predictions
cartoon
cyber
clifford stoll
computer
safety
anybody else
quotes
posters
TREAT YOUR PASSWORD LIKE YOUR TOOTHBRUSH
keepitsafe.auburn.edu
TREAT YOUR PASSWORD LIKE YOUR TOOTHBRUSH
CHOOSE A GOOD ONE
CHANGE IT REGULARLY
NEVER SHARE IT
© 2014 THE SECURITY AWARENESS COMPANY
Treat your password like your toothbrush.
Don't let anybody else use it,
and get a new one every six months.
~ Clifford Stoll
Treat your password like your toothbrush.
Don't let anybody else use it,
and get a new one every six months.
Treat your Password LIKE
Your Toothbrush
Never share it and change it often!
eSafety health check
OMG!
*explore safely
STAY SAFE ONLINE
Social Networking
Sexting
Cyber Bullying
Online Gaming
Personal Information
Privacy Settings
What to do
Things to Remember
Treat your password like your toothbrush. Don't let anybody else use it, and get a new one every six months.
Clifford Stoll
Treat your password like your toothbrush. Don't let anybody else use it, and get a new one every six months.
Clifford Stoll
lolsotrue:#448
Treat your password like your toothbrush. Don't let anybody else use it, and get a new one every six months.
lolsotrue.com
A password is like a toothbrush
Choose a good one
Don't share it with anyone
Change it occasionally
PASSWORDS ARE LIKE UNDERWEAR
You shouldn't leave them out where people can see them.
You should change them regularly.
And you shouldn't loan them out to strangers.
THE MOST COMMON PASSWORDS OF 2011 WERE:
TREAT YOUR PASSWORD LIKE A TOOTHBRUSH:
CHOOSE A GOOD ONE,
CHANGE IT EVERY 3 MONTHS
& DON'T SHARE IT.

How Password Crackers Work

- Build a large dictionary of possible passwords and try each of these against the password file
  - Each password must be hashed using each salt value in the password file and then compared to stored hash values
  - Password cracking program may attempt variations (e.g., backward spelling, additional numbers or special characters, etc) on all the words in its dictionary of likely passwords
  - Requires huge computational overhead

Rainbow Table

- Or, potential hash values can be precomputed
- Attacker generates a large dictionary of possible passwords. For each password, the attacker generates the hash values associated with each possible salt value
  - Rainbow Table
    - 1.4GB data, cracking 99.9% of all alphanumeric Windows password hashes in 13.8 secs [Oechslin, Crypto, 2003]
- Larger salt values and a sufficiently large hash values can make such attacks less practical
- Rainbow tables and/or password crackers are readily available (free or for fee)

IMAP, NNTP, NetBus, etc. You can also create your own authentication types. This tool also supports multi-stage authentication engines and is able to connect 60 simultaneous targets. It also has resume and load options. So, you can pause the attack process any time and then resume whenever you want to resume.

This tool has not been updated for many years. Still, it can be useful for you.

2. RainbowCrack

RainbowCrack is a hash cracker tool that uses a large-scale time-memory trade off process for faster password cracking than traditional brute force tools. Time-memory trade off is a computational process in which all plain text and hash pairs are calculated by using a selected hash algorithm. After computation, results are stored in the rainbow table. This process is very time consuming. But, once the table is ready, it can crack a password must faster than brute force tools.

You also do not need to generate rainbow tablets by yourselves. Developers of RainbowCrack have also generated LM rainbow tables, NTLM rainbow tables, MD5 rainbow tables and Sha1 rainbow tables. Like RainbowCrack, these tables are also available for free. You can download these tables and use for your password cracking processes.

Download Rainbow tables here: http://project-rainbowcrack.com/table.htm

A few paid rainbow tables are also available, which you can buy from here: http://project-rainbowcrack.com/buy.php

This tool is available for both Windows and Linux systems.

Download Rainbow crack here: http://project-rainbowcrack.com/

3. Wfuzz

Wfuzz is another web application password cracking tool that tries to crack passwords with brute forcing. It can also be used to find hidden resources like directories, servlets and scripts. This tool can also identify different kind of injections including SQL Injection, XSS Injection, LDAP Injection, etc in Web applications.

project-rainbowcrack.com/table.htm

RainbowCrack | Home | Documentation | Rainbow Tables | Performance | Buy Rainbow Tables | Contact

List of Rainbow Tables

This page lists the rainbow tables we generated.

LM rainbow tables speed up cracking of password hashes from Windows 2000 and Windows XP operating system.
NTLM rainbow tables speed up cracking of password hashes from Windows Vista and Windows 7 operating system.
MD5 and SHA1 rainbow tables speed up cracking of MD5 and SHA1 hashes, respectively.

The largest rainbow tables here are ntlm_mixalpha-numeric#1-9, md5_mixalpha-numeric#1-9 and sha1_mixalpha-numeric#1-9. Each has a key space of 13,759,005,997,841,642 (i.e., $2^{53.6}$).

Benchmark result of each rainbow table is shown in last column of the list below. We generate hashes of random plaintexts and crack them with the rainbow table and rcrack/rcrack_cuda/rcrack_cl program. rcrack program uses CPU for computation and rcrack_cuda/rcrack_cl program uses NVIDIA/AMD GPU.

Video demonstration of some rainbow tables on YouTube:

- Hash Cracking with Rainbow Table ntlm_ascii-32-95#1-8
- Hash Cracking with Rainbow Table md5_ascii-32-95#1-8
- Hash Cracking with Rainbow Table sha1_ascii-32-95#1-8

Perfect rainbow tables are rainbow tables without identical end points, produced by removing merged rainbow chains in normal rainbow tables. To achieve same success rate, perfect rainbow tables are smaller and faster to lookup than non-perfect rainbow tables. In lists below, parameters of non-perfect rainbow tables are in gray.

Rainbow Tables

LM Rainbow Tables

Table ID	Charset	Plaintext Length	Key Space	Success Rate	Table Size	Files	Performance
lm_ascii-32-65-123-4#1-7	ascii-32-65-123-4	1 to 7	7,555,858,447,479	99.9 %	27 GB 32 GB	Perfect Non-perfect	Perfect Non-perfect

NTLM Rainbow Tables

Table ID	Charset	Plaintext Length	Key Space	Success Rate	Table Size	Files	Performance
ntlm_ascii-32-95#1-7	ascii-32-95	1 to 7	70,576,641,626,495	99.9 %	52 GB 64 GB	Perfect Non-perfect	Perfect Non-perfect
ntlm_ascii-32-95#1-8	ascii-32-95	1 to 8	6,704,780,954,517,120	96.8 %	460 GB 576 GB	Perfect Non-perfect	Perfect Non-perfect

KOREA UNIVERSITY 1905

Password Selection Strategies

	How it works	Pros	Cons
User Education			
Computer-generated passwords			
Reactive password checking			
Proactive password checking			

Security Issues for User Authentication

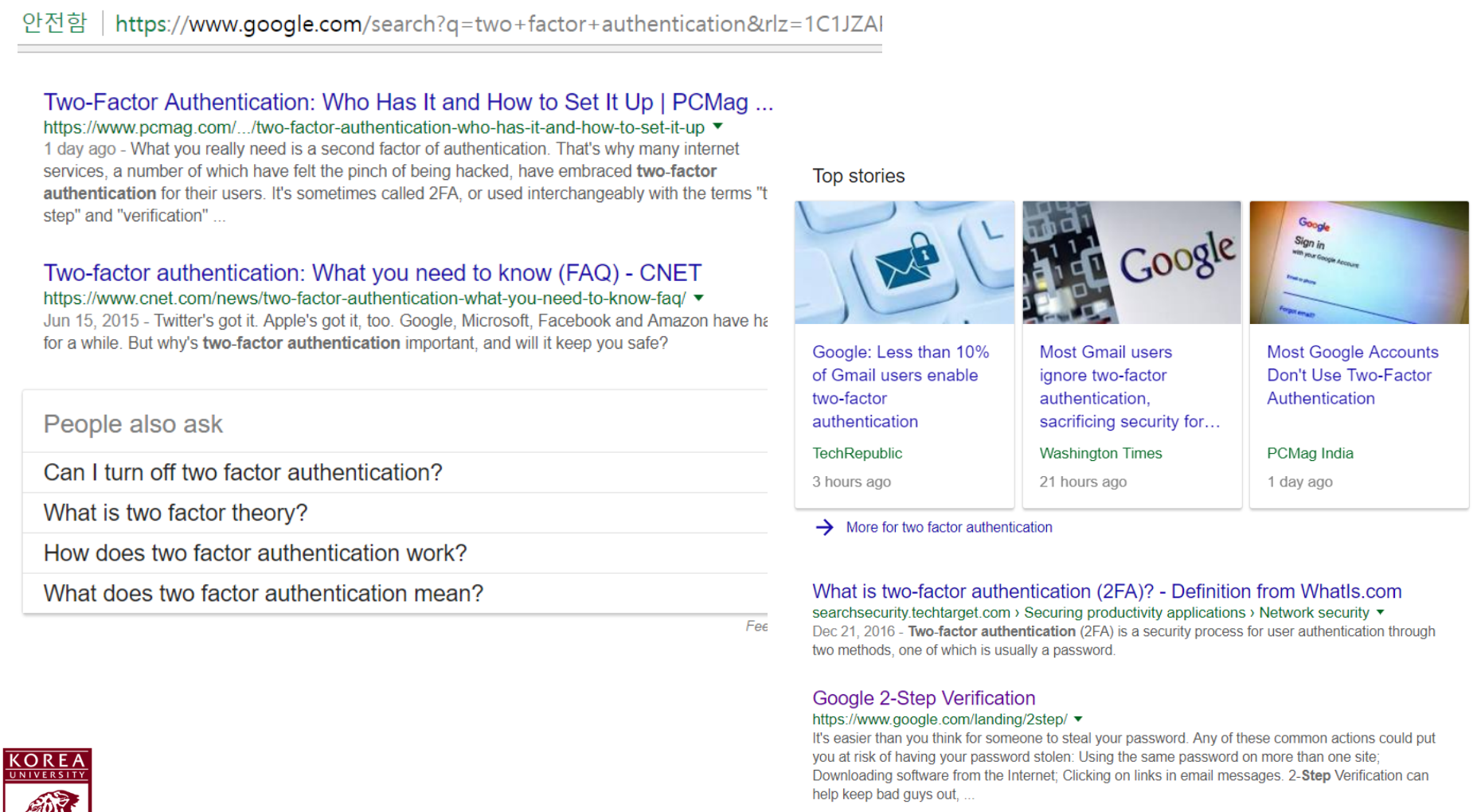
Attacks	Authentication	Examples	Typical Defenses
Client Attack	Password		
	Token		
	Biometric		
Host Attack	Password		
	Token		
	Biometric		
Eavesdropping, theft, and copying	Password		
	Token		
	Biometric		
Replay	Password		
	Token		
	Biometric		
Trojan Horse	Password, token, biometric		
Denial of Service	Password, token, biometric		

Attacks	Authenticators	Examples	Typical defenses
Client attack	Password	Guessing, exhaustive search	Large entropy; limited attempts
	Token	Exhaustive search	Large entropy; limited attempts, theft of object requires presence
	Biometric	False match	Large entropy; limited attempts
Host attack	Password	Plaintext theft, dictionary/exhaustive search	Hashing; large entropy; protection of password database
	Token	Passcode theft	Same as password; 1-time passcode
	Biometric	Template theft	Capture device authentication; challenge response
Eavesdropping, theft, and copying	Password	"Shoulder surfing"	User diligence to keep secret; administrator diligence to quickly revoke compromised passwords; multifactor authentication
	Token	Theft, counterfeiting hardware	Multifactor authentication; tamper resistant/evident token
	Biometric	Copying (spoofing) biometric	Copy detection at capture device and capture device authentication
Replay	Password	Replay stolen password response	Challenge-response protocol
	Token	Replay stolen passcode response	Challenge-response protocol; 1-time passcode
	Biometric	Replay stolen biometric template response	Copy detection at capture device and capture device authentication via challenge-response protocol
Trojan horse	Password, token, biometric	Installation of rogue client or capture device	Authentication of client or capture device within trusted security perimeter
Denial of	Password, token,	Lockout by multiple	Multifactor with token

* Table 3.4, Stallings and Brown

Two factor authentication

§ DYI (Google, Facebook, Microsoft, Apple)



Apple Two Factor Authentication

Apple Inc. [US] | https://support.apple.com/en-us/HT204915

Mac iPad iPhone Watch TV Music Support

Two-factor authentication for Apple ID

Two-factor authentication is an extra layer of security for your Apple ID designed to ensure that you're the only person who can access your account, even if someone knows your password.

How it works

With two-factor authentication, your account can only be accessed on devices you trust, like your iPhone, iPad, or Mac. When you want to sign in to a new device for the first time, you'll need to provide two pieces of information—your password and the six-digit verification code that's automatically displayed on your trusted devices. By entering the code, you're verifying that you trust the new device. For example, if you have an iPhone and are signing into your account for the first time on a newly purchased Mac, you'll be prompted to enter your password and the verification code that's automatically displayed on your iPhone.

Because your password alone is no longer enough to access your account, two-factor authentication dramatically improves the security of your Apple ID and all the personal information you store with Apple.

Once signed in, you won't be asked for a verification code on that device again unless you sign out completely, erase the device, or need to change your password for security reasons. When you sign in on the web, you can choose to trust your browser, so you won't be asked for a verification code the next time you sign in from that computer.

Trusted devices

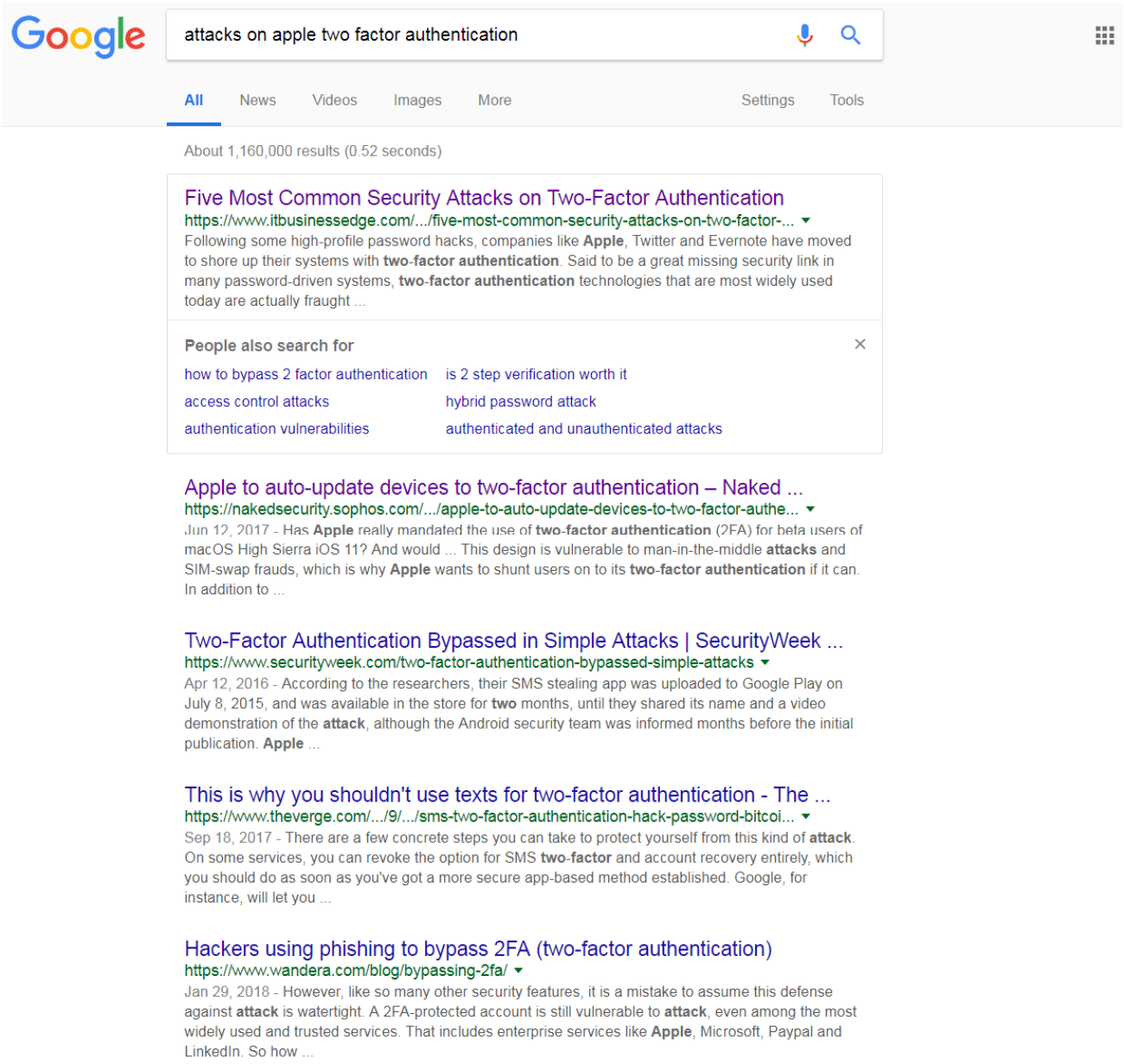
A trusted device is an iPhone, iPad, or iPod touch with iOS 9 and later, or a Mac with OS X El Capitan and later that you've already signed in to using two-factor authentication. It's a device we know is yours and that can be used to verify your identity by displaying a verification code from Apple when you sign in on a different device or browser.

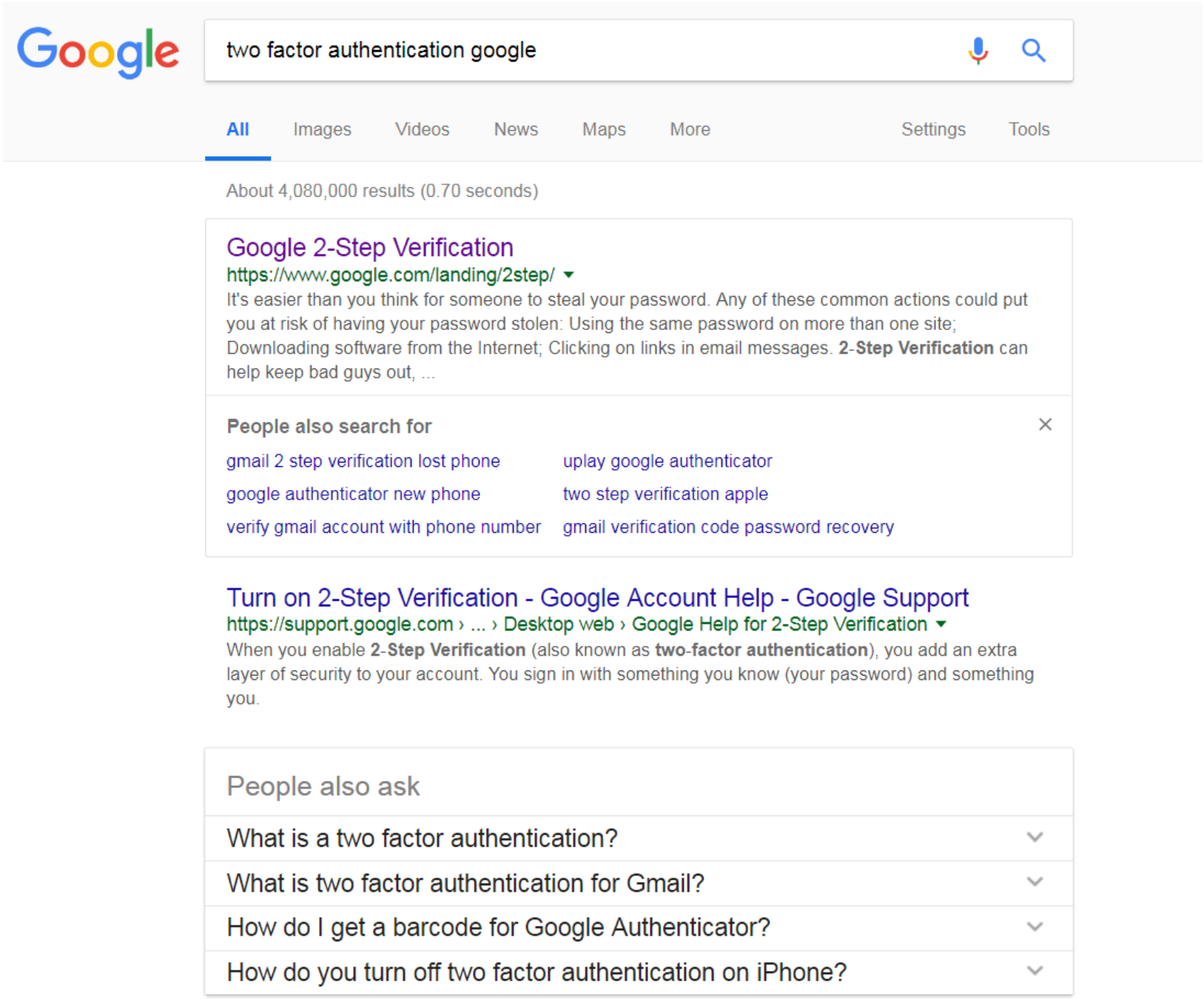
Trusted phone numbers

A trusted phone number is a number that can be used to receive verification codes by text message or automated phone call. You must verify at least one trusted phone number to enroll in two-factor authentication.

You should also consider verifying other phone numbers you can access, such as a home phone, or a number used by a family member or close friend. You can use these numbers if you temporarily can't access your own devices.

As you might have feared ...




Google
two factor authentication google
All
Images
Videos
News
Maps
More
Settings
Tools
About 4,080,000 results (0.70 seconds)
Google 2-Step Verification
https://www.google.com/landing/2step/
It's easier than you think for someone to steal your password. Any of these common actions could put you at risk of having your password stolen: Using the same password on more than one site; Downloading software from the Internet; Clicking on links in email messages. 2-Step Verification can help keep bad guys out, ...
People also search for
gmail 2 step verification lost phone
uplay google authenticator
google authenticator new phone
two step verification apple
verify gmail account with phone number
gmail verification code password recovery
Turn on 2-Step Verification - Google Account Help - Google Support
https://support.google.com › ... › Desktop web › Google Help for 2-Step Verification
When you enable 2-Step Verification (also known as two-factor authentication), you add an extra layer of security to your account. You sign in with something you know (your password) and something you.
People also ask
What is a two factor authentication?
What is two factor authentication for Gmail?
How do I get a barcode for Google Authenticator?
How do you turn off two factor authentication on iPhone?

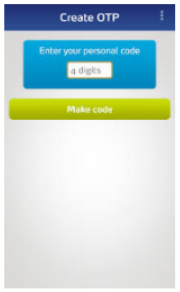
OTP (One Time Password)

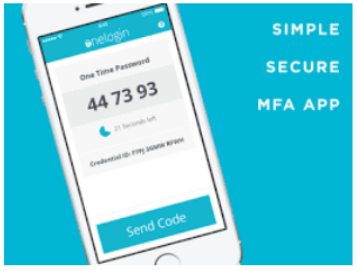
https://en.wikipedia.org/wiki/One-time_password

thus reducing the attack surface further.

OTPs have been discussed as a possible replacement for, as well as enhancer to, traditional passwords. On the downside, OTPs are difficult for human beings to memorize. Therefore, they require additional technology to work.

Contents [hide]

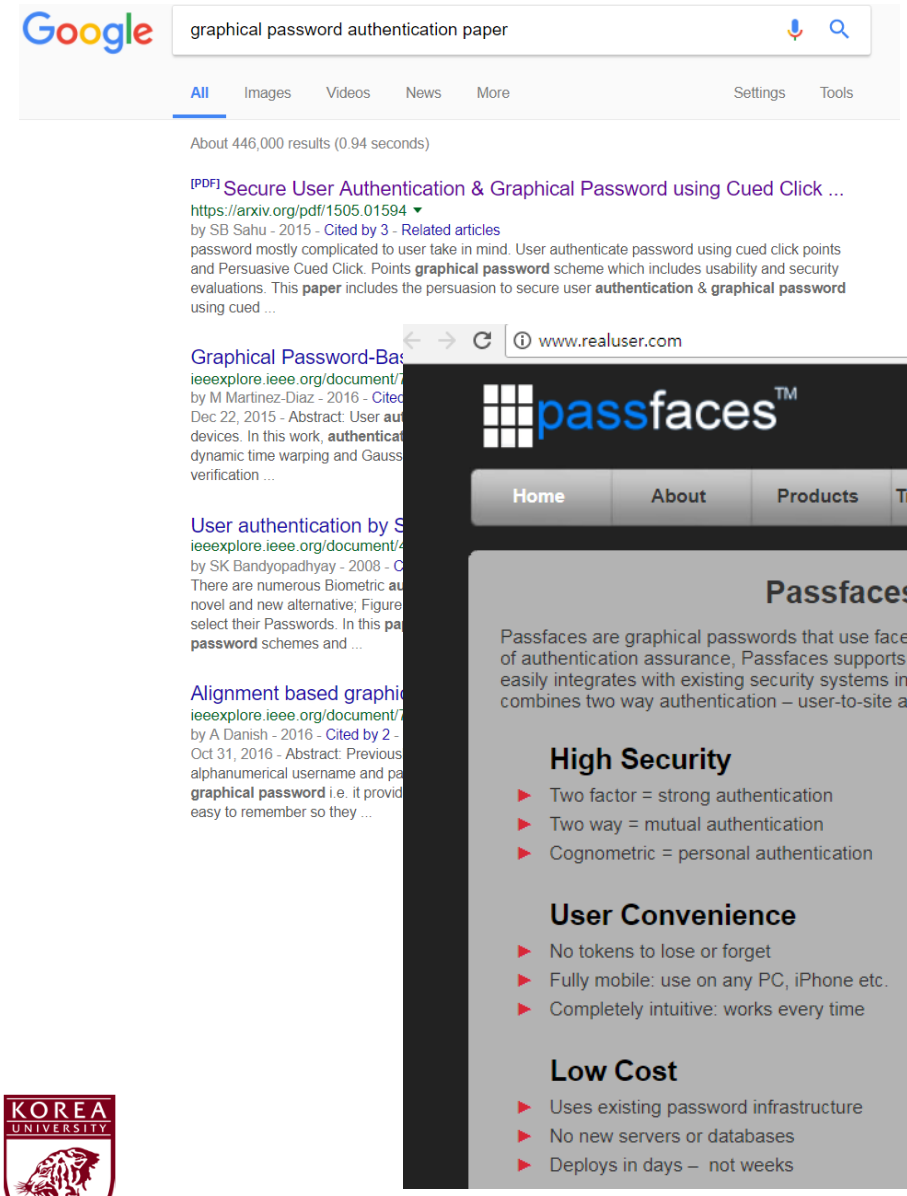


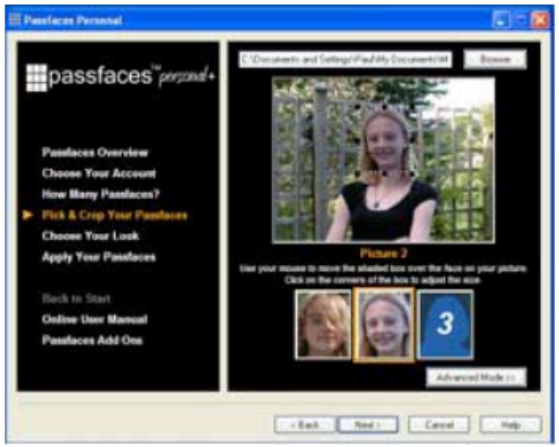


Other Approaches to Authentication

- Graphical Passwords
- CAPTCHA
  - My recent talk at a conference (KOCSEA Technical Symposium, Nov 2017, Univ of Nevada, Las Vegas)
- ...

Graphical passwords





1st To setup, select from 1 to 5 faces from your collection of photos to use as your secret "Passfaces"

2nd To Logon, pick each of your Passfaces from groups containing 8 strangers

Download Passfaces Personal Now

NEW: Personalize Your Logon Experience with Passfaces Personal's Advanced Features

Create Entire Passfaces Logon Grids with Your Own Pictures

Create complete personalized Passfaces logon grids. Use pictures from your own PC, your Facebook* contacts, Web based photo library, or use photos of movie stars, sports heroes etc. from any Web site.

Make Logon Fun!

***Facebook - use your friend's pictures as your passfaces**

We've built a small Facebook application to help you choose your friend's pictures.
Try it now: **http://apps.facebook.com/passfaces**

facebook

Share Your Passfaces Grids with Your Friends

Your personalized Passfaces grids can be shared with friends via email, IM or Facebook etc.

Choose Your Level of Security

Set from one to five secret Passfaces.

Diverse Approaches to Graphical Passwords

word by first entering a picture he or she chooses. The user then chooses several point-of-interest (POI) regions in the picture. Each POI is described by a circle (center and radius). For every POI, the user types a word or phrase that would be associated with that POI. If the user does not type any text after selecting a POI, then that POI is associated with an empty string. The user can choose either to enforce the order of selecting POIs (stronger password), or to make the order insignificant.

In Figure 1, we show an example of a user creating a graphical password. In this example, the user chooses a picture of his or her kids by pressing "Load Image button". Then the user clicks on the kids faces in the order of their ages (order is enforced). For each selected region, the user types the kid's name or nickname.

Figure 1. An example of creating a graphical password using the proposed system.

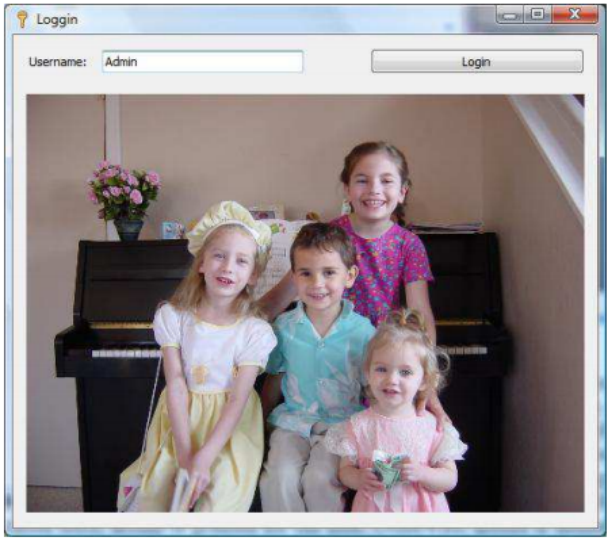


Figure 2. Login Screen

In the proposed system, a user freely chooses a picture, POIs and corresponding words. The order and number of POIs can be enforced for stronger authentication. Together, these parameters allow for a very large password space.

We believe that proposed approach is promising and unique for at least two reasons:

- It combines graphical and text-based passwords trying to achieve the best of both worlds.
- It provides multi-factor authentication (graphical, text, POI-order, POI-number) in a friendly intuitive system.

* Ahmad Almulhem, A graphical password authentication system, World Congress on Internet Security, 2011

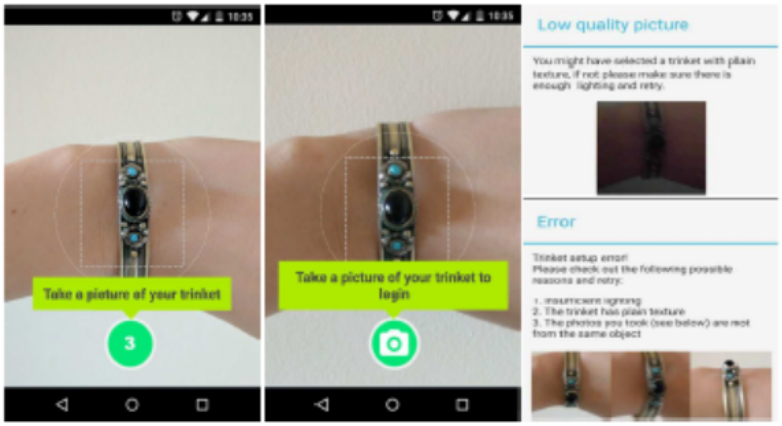
Other Approaches

Camera Based Two Factor Authentication Through Mobile and Wearable Devices

MOZHGAN AZIMPOURKIVI, Florida International University
UMUT TOPKARA, Bloomberg LP
BOGDAN CARBUNAR, Florida International University

Oct 2017

We introduce Pixie, a novel, camera based two factor authentication solution for mobile and wearable devices. A quick and familiar user action of snapping a photo is sufficient for Pixie to simultaneously perform a graphical password authentication and a physical token based aut
based on both the knowledge a
choose their trinkets similar t
that the object is the trinket, i



(a) (b) (c)

Fig. 1. Pixie: (a) Trinket setup. The user takes photos of the trinket placing it in the circle overlay. UI shows the number of photos left to take. (b) Login: the user snaps a photo of the trinket. (c) Trinket setup messages provide actionable guidance, when the image quality is low (top), or the reference images are inconsistent (bottom).

(a) (b) (c) (d) (e) (f)

"Shoulder surfing" attack?

Yet Another Approach...

Sayli Chavan *et al*, International Journal of Computer Science and Mobile Computing, Vol.4 Issue.4, April- 2015, pg. 324-329

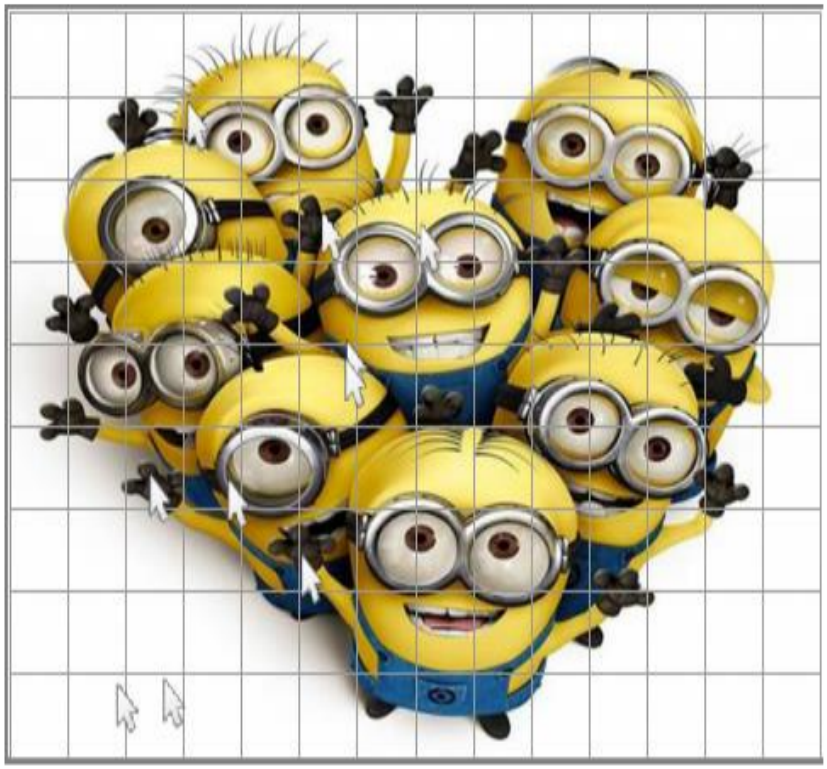


Fig.2: Grid Approach

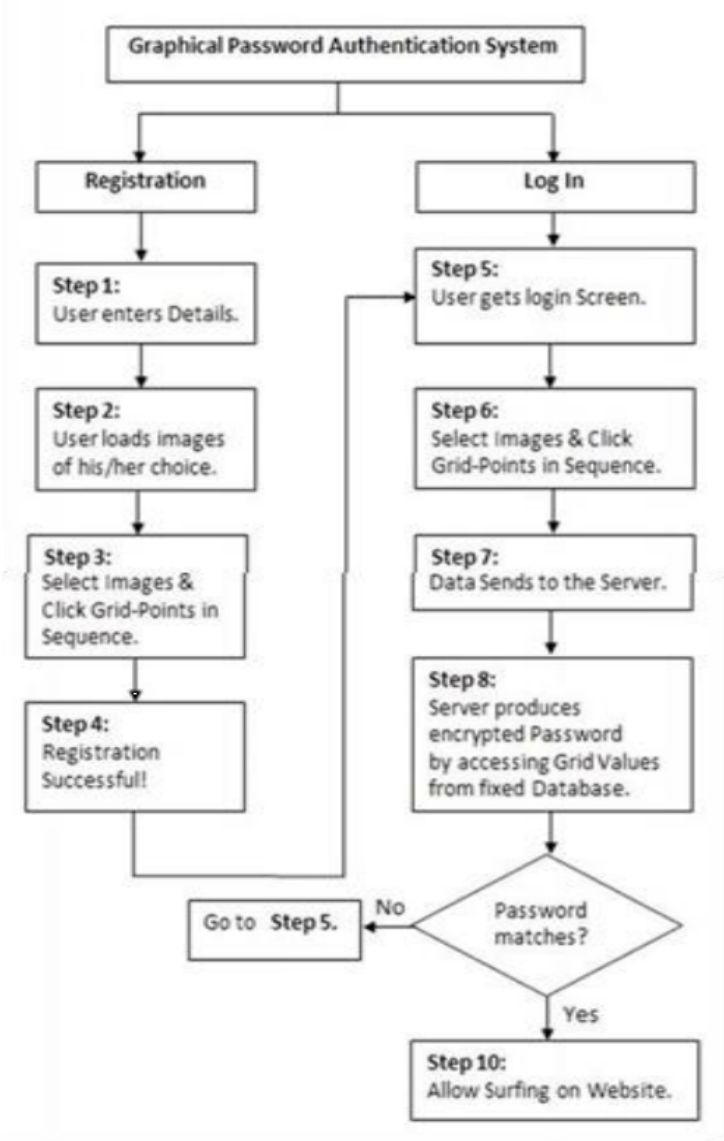


Fig.4: Flow graph.

CAPTCHA

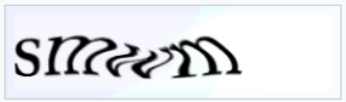
- Completely Automated Public Turing test to tell Computers and Humans Apart)
  - HIP (Human Interaction Proof)
- Often complements text-based password
  - Strengthen security in user authentication
  - Reduce likelihood of service abuse (e.g., bogus account creation)
- Widely used, but security enhancement might not be as substantial as expected

CAPTCHA

CAPTCHA

From Wikipedia, the free encyclopedia

> This article **is written like a personal reflection or opinion essay** that states a Wikipedia editor's personal feelings about a topic. Please help improve it by rewriting it in an encyclopedic style. *(January 2017) (Learn how and when to remove this template message)*



This CAPTCHA of "smwm" obscures its message from computer interpretation by twisting the letters and adding slight background color gradient.

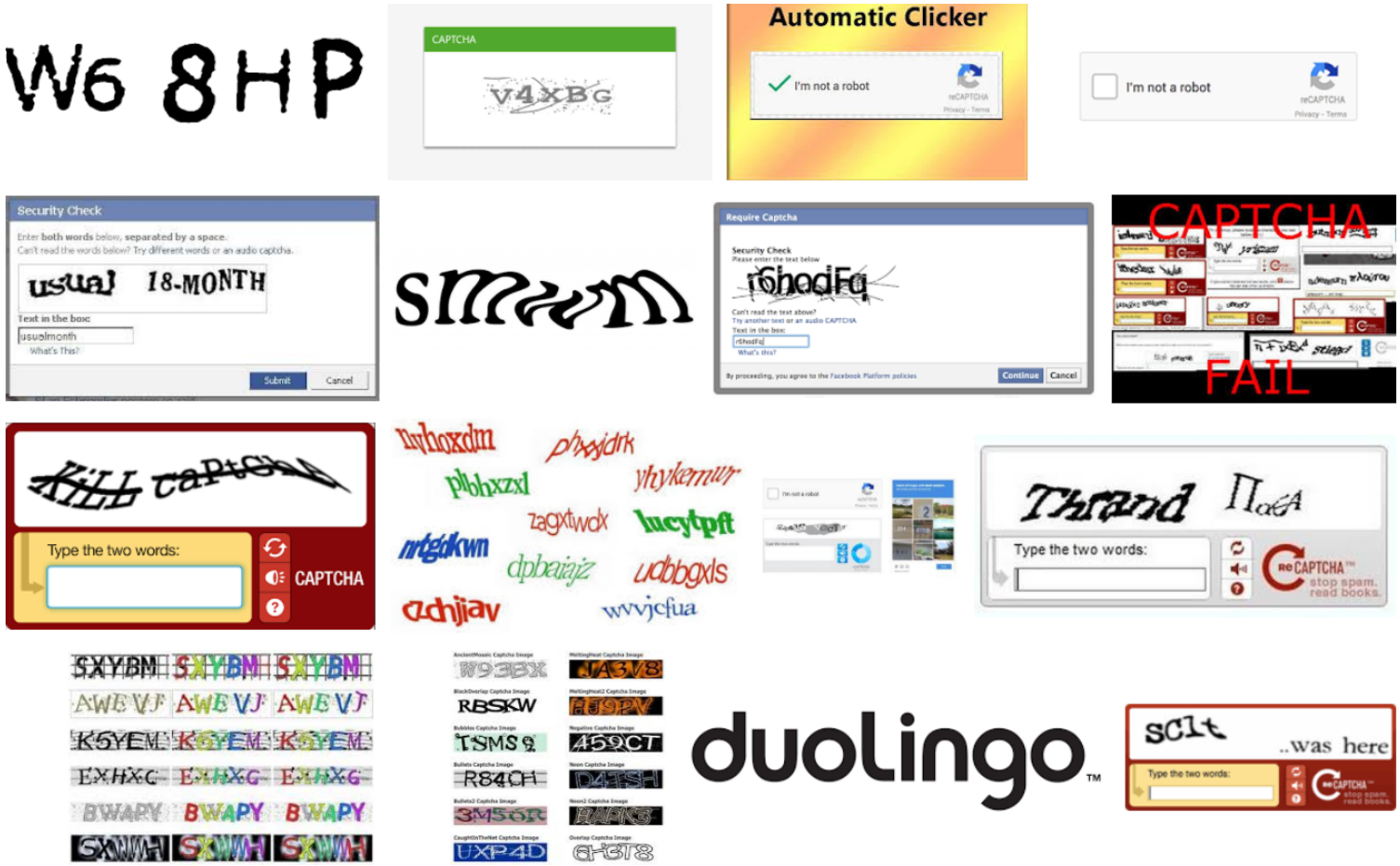
A **CAPTCHA** (an acronym for "**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part") is a type of challenge-response test used in computing to determine whether or not the user is human.[1]

The term was coined in 2003 by Luis von Ahn, Manuel Blum, Nicholas J. Hopper, and John Langford.[2] The most common type of CAPTCHA was first invented in 1997 by two groups working in parallel: (1) Mark D. Lillibridge, Martin Abadi, Krishna Bharat, and Andrei Z. Broder; and (2) Eran Reshef, Gili Raanan and Eilon Solan.[3] This form of CAPTCHA requires that the user type the letters of a distorted image, sometimes with the addition of an obscured sequence of letters or digits that appears on the screen. Because the test is administered by a computer, in contrast to the standard Turing test that is administered by a human, a CAPTCHA is sometimes described as a reverse Turing test.

This user identification procedure has received many criticisms, especially from disabled people, but also from other people who feel that their everyday work is slowed down by distorted words that are difficult to read. It takes the average person approximately 10 seconds to solve a typical CAPTCHA.[*citation needed*]

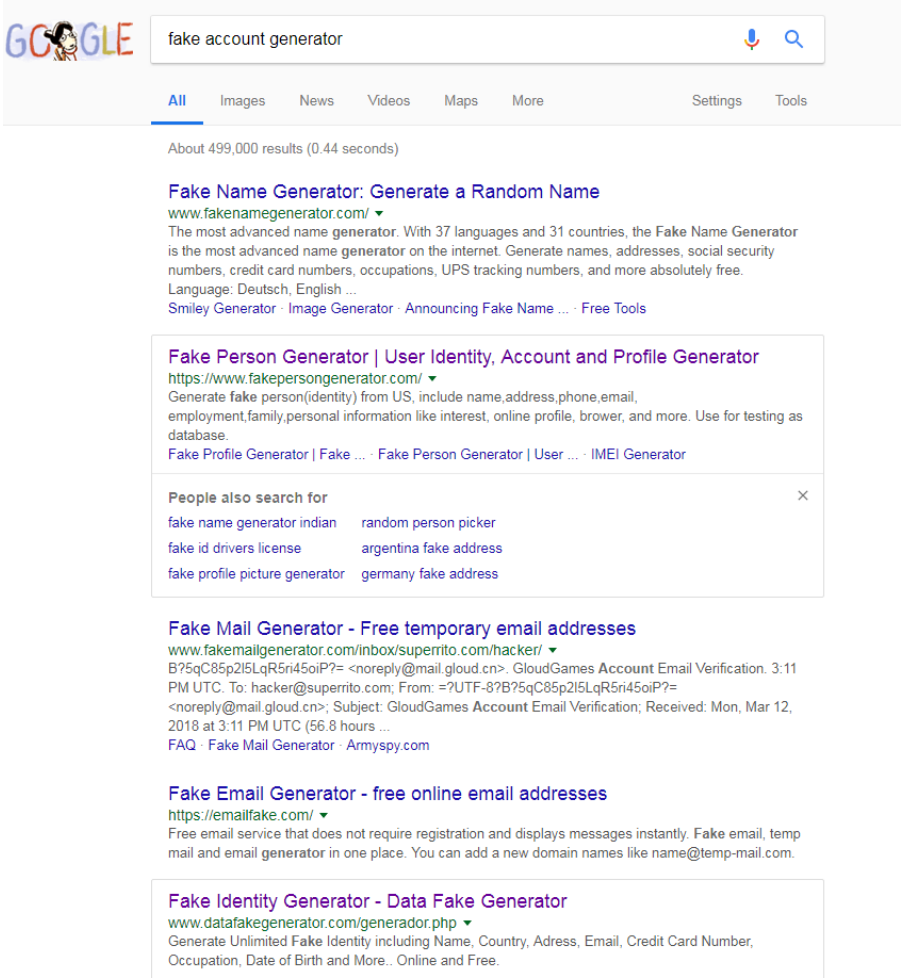
Contents [hide]

- What is your personal experience on CAPTCHA tests
- How can CAPTCHA tests be defeated? Or, Can you?



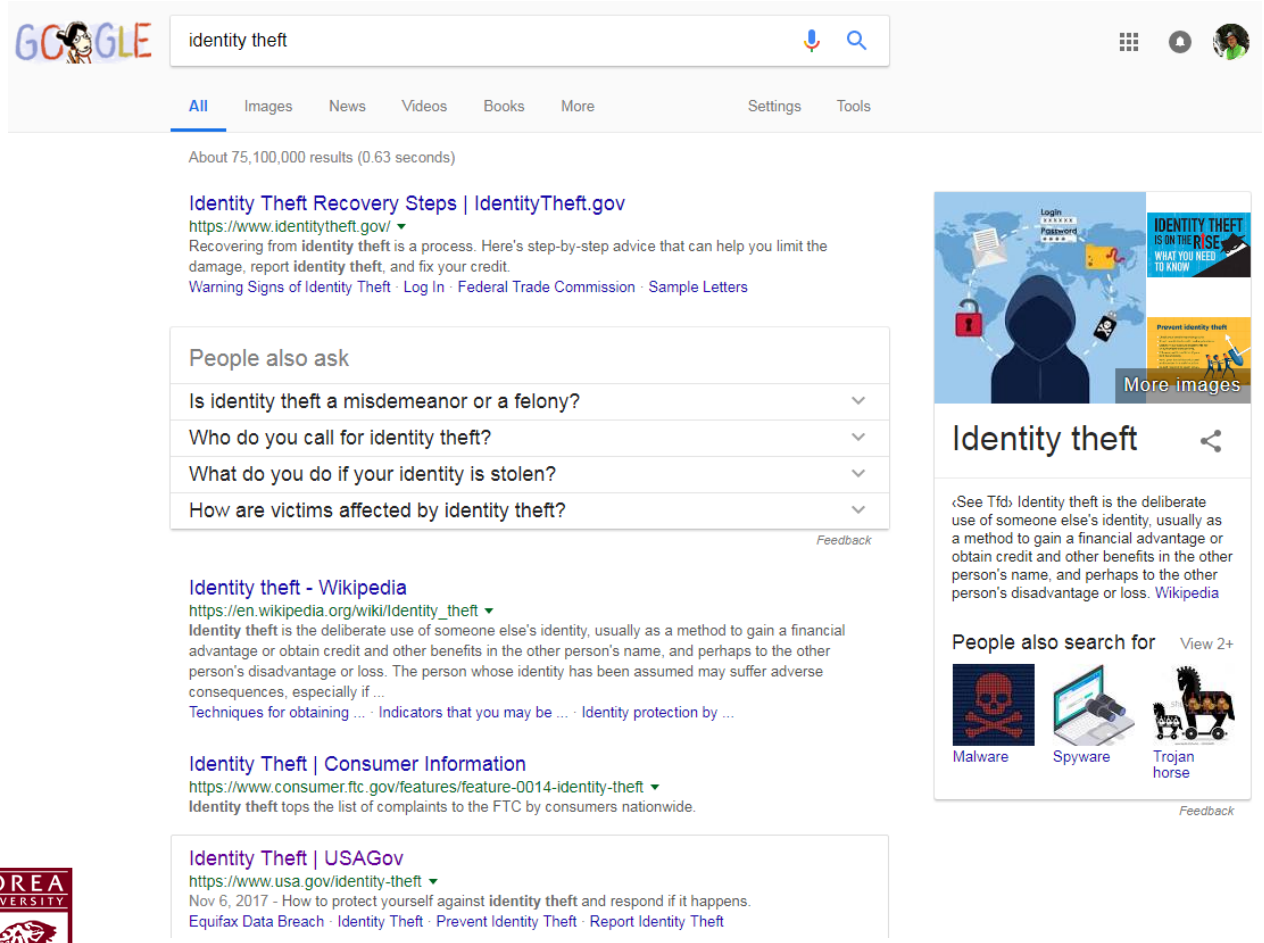
CAPTCHA and “Bogus/Fake” Accounts

- Sources of massive spam mails
- What are possible impacts of having bogus accounts on
  - Facebook
  - Amazon
  - Netflix…
  - Google
  - Microsoft
  - …



Identity Theft

- Will not be discussed, but it is surely a real and serious threat



안전함 | https://www.usa.gov/identity-theft

An official website of the United States government Here's how you know

The .gov means it's official.
Federal government websites often end in .gov or .mil. Before sharing sensitive information, make sure you're on a federal government site.

This site is secure.
The **https://** ensures that you are connecting to the official website and that any information you provide is encrypted and transmitted securely.

USA.gov

Search All Government

Contact Us | 1-844-USA-GOV1

All Topics and Services | Government Agencies and Elected Officials | Benefits, Grants, Loans | Housing | Jobs and Unemployment | Money and Taxes | Travel and Immigration

Español

< Scams and Frauds

- Common Scams and Frauds
- Housing Scams
- Identity Theft
- Online Safety
- Privacy
- Report Scams and Frauds

Identity Theft

How to protect yourself against identity theft and respond if it happens.

What's on This Page

Equifax Data Breach

Equifax, one of the three major credit reporting agencies in the U.S., announced a data breach that affects 143 million consumers. The hackers accessed Social Security numbers, birthdates, addresses, and driver's license numbers.

Other Authentication Tools

- Fingerprint
- Retina
- Face
- …
- Will not be further discussed because we all use smartphones equipped with such authentication systems

Authentication challenges

- NOT necessarily limited to passwords (e.g., mobile payment services, ...)
- Remote user authentication is another challenge
- Potential attacks include
  - client attack
  - host attack
  - eavesdropping, theft, and copying
  - replay
  - trojan horse
  - denial of service

Towards more robust authentication mechanism

("Adding uncertainty to improve user authentication")

Dr. Shinil Kwon, FormalWorks
Prof. Simon Woo, SUNY-Korea
Prof. Sungdeok (Steve) Cha, Korea University*

KOCSEA Technical Symposium
Nov 11th, 2017
UNLV, NV

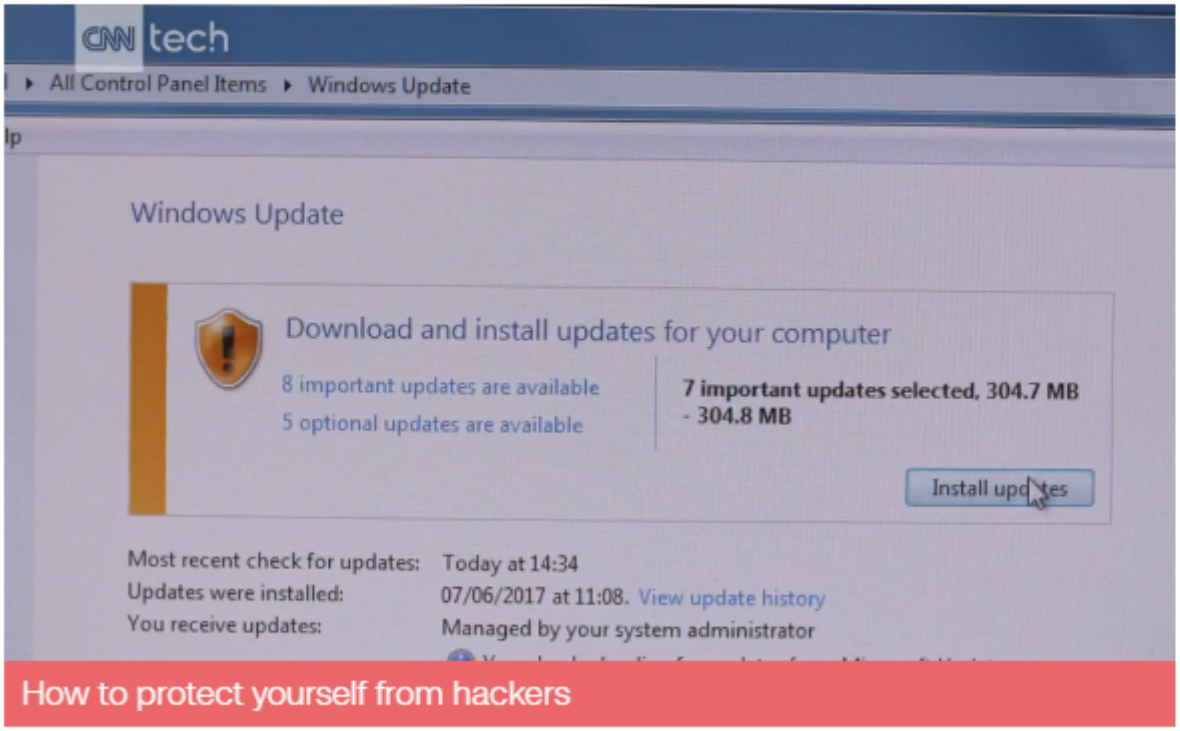
Same old story…

Cyber-Safe

Google says hackers steal almost 250,000 web logins each week

by Selena Larson @selenalarson

November 9, 2017: 4:13 PM ET

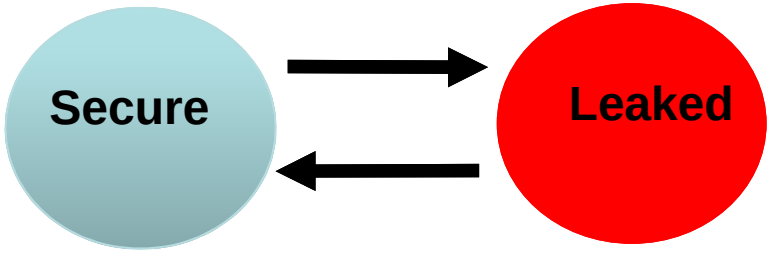


Google is digging into the dark corners of the web to better secure people's accounts.

Always Happening

“Personal” Nightmare

- This list is most likely the tip of the iceberg !
  - Very (extremely?) difficult to remember
  - Heavily reused, small candidate pools, special character rules, …
  - Difficult, if not impossible, to detect attacks in timely manner
  - …



KOREA UNIVERSITY 1905

Personal “trauma”?

New Authentication System using both Images and Texts

- Create highly personalized association between image and text
  - Image: easy to remember and upload
  - Text: highly personalized

yummy
delicious

• • •

2014again!

• • • •

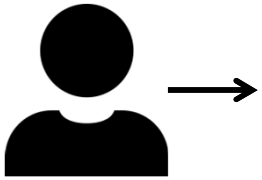
• • ? • • •

2017forever!

oh no 2017! • •

Proposed System:
Account Creation / Login Session

ID: sungdeok

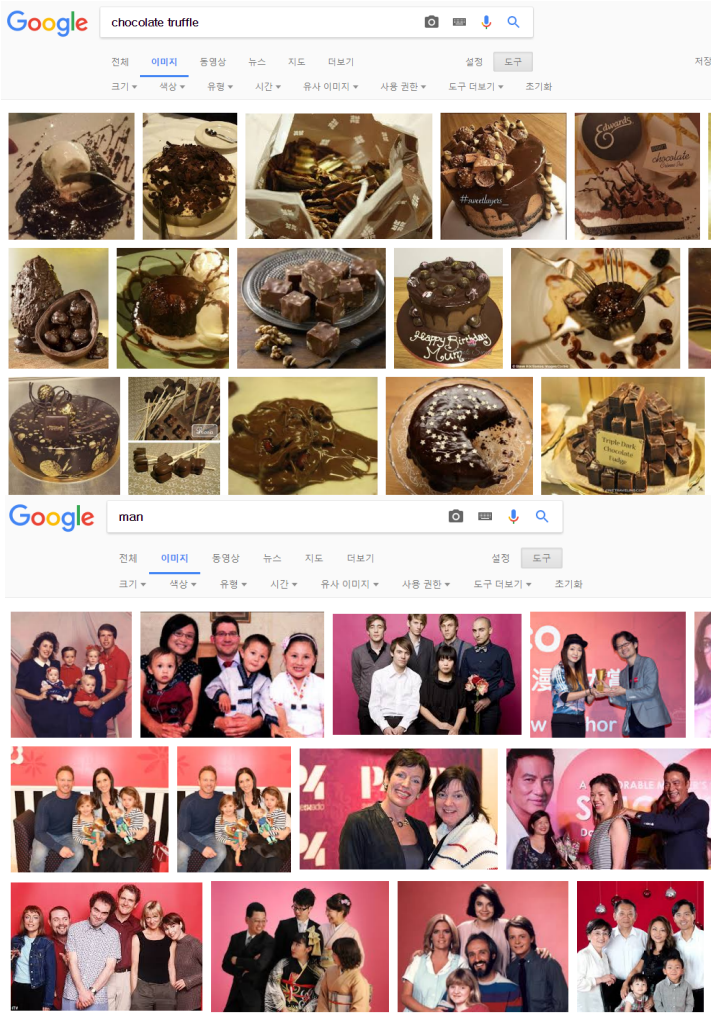


oh no 2017!
• •

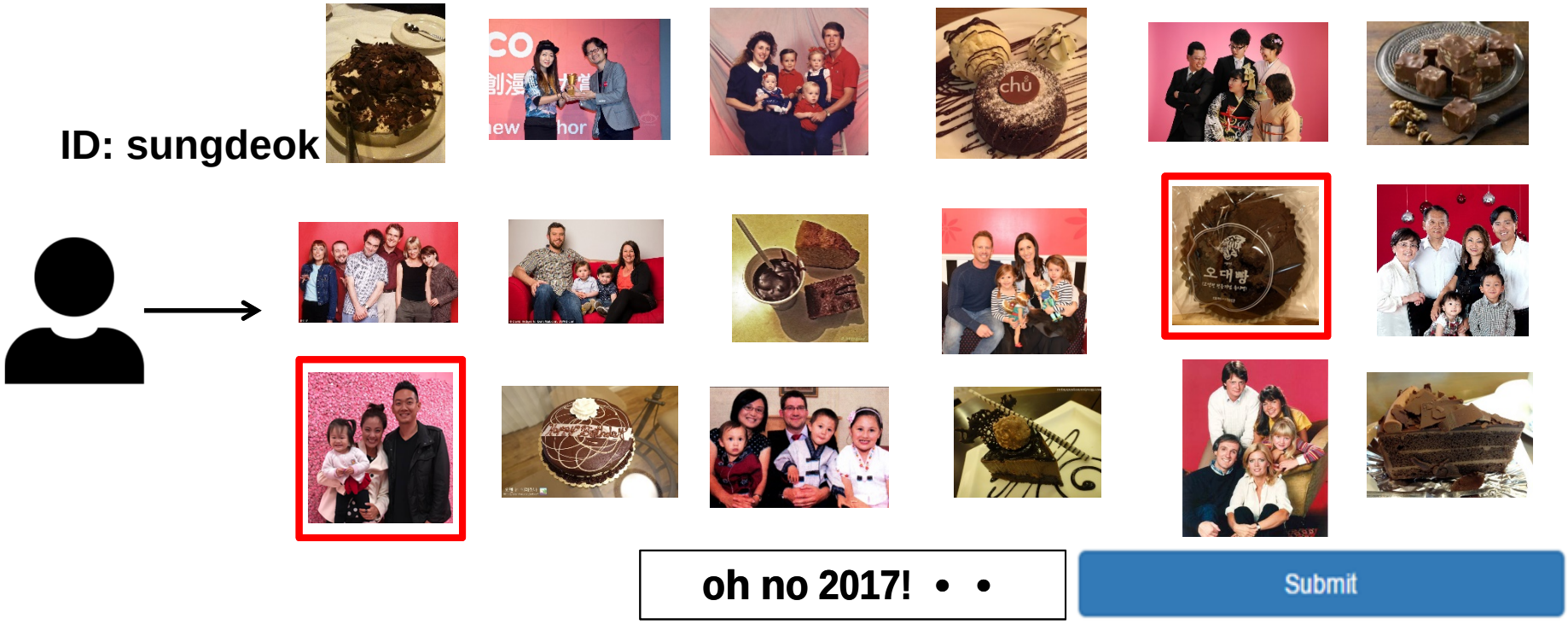
eric • • •

user uploaded images &
short and highly personalized password

System generated “similar but different enough” images to the



Proposed System*: Password Verification



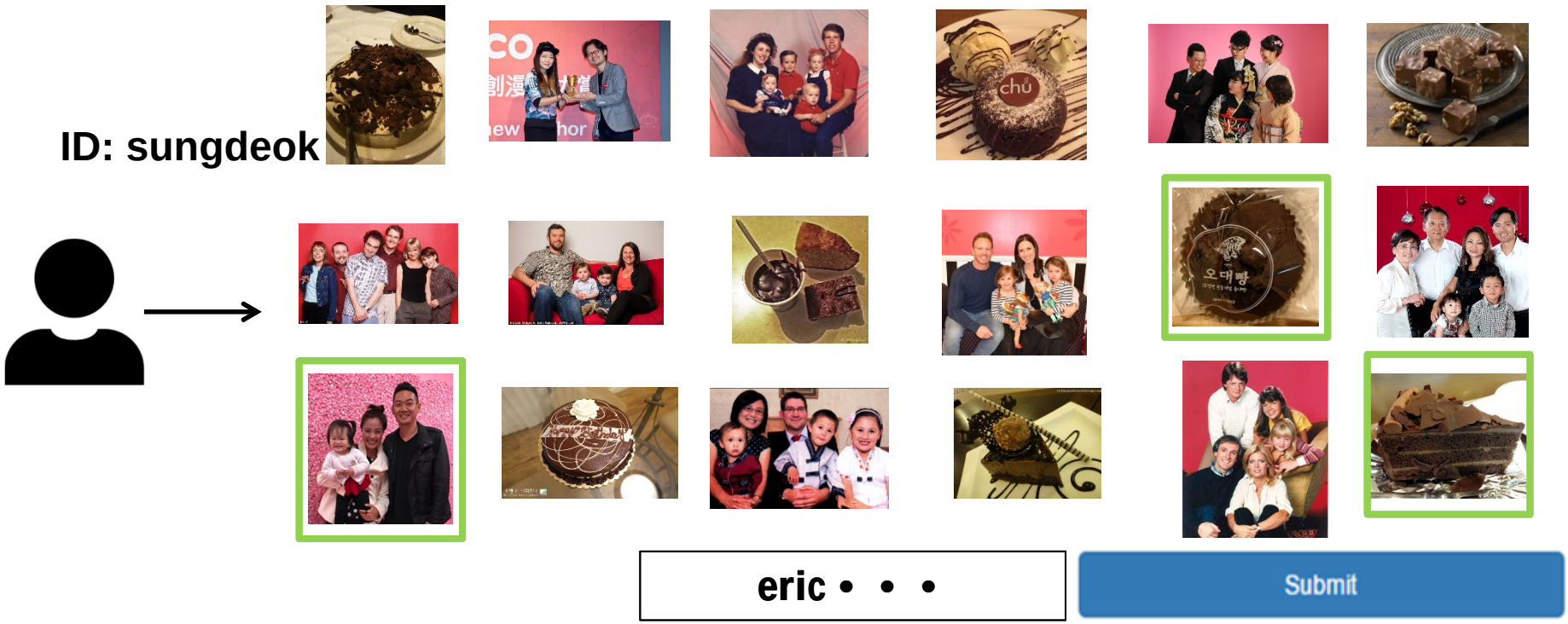
In order to successfully authenticate:

ü Must correctly choose images

ü Must provide the correct text associated with the images

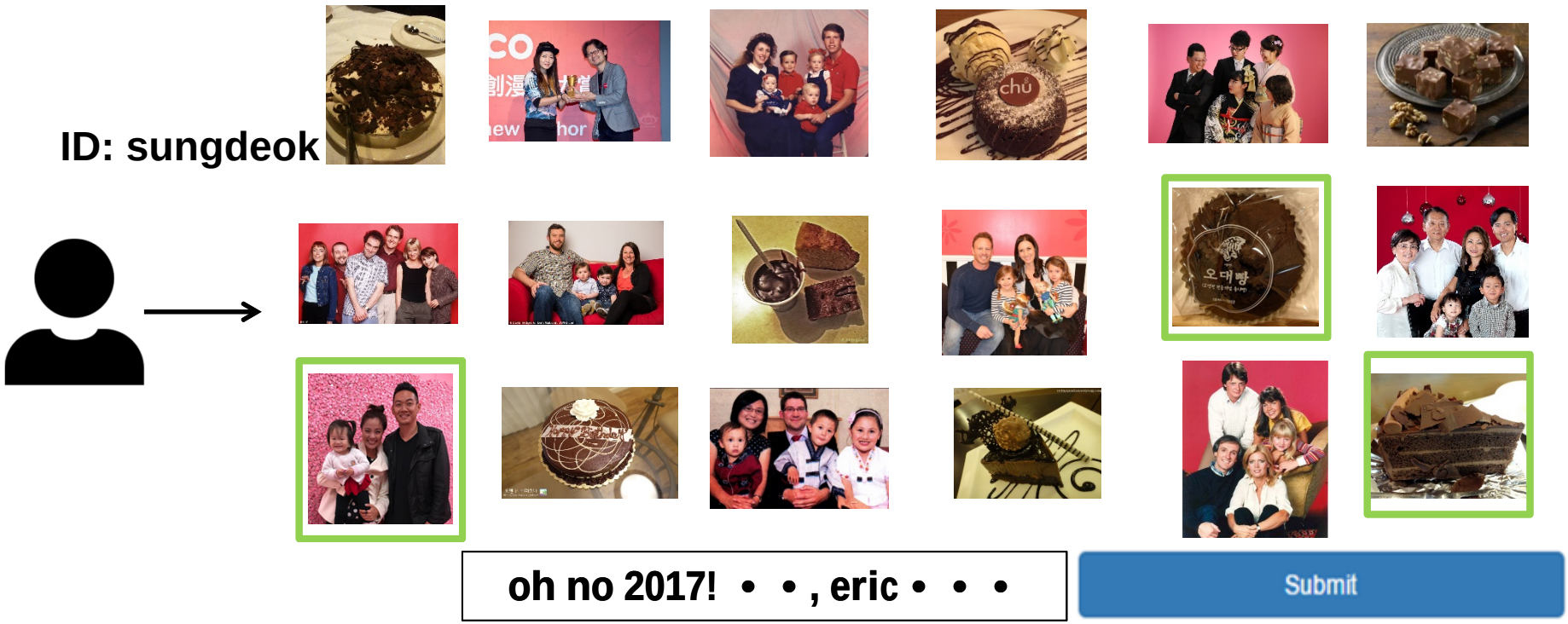
* Not yet built

Another Possibility?



Provided that the image in the lower right corner is NOT a “trap” image

Who Not?



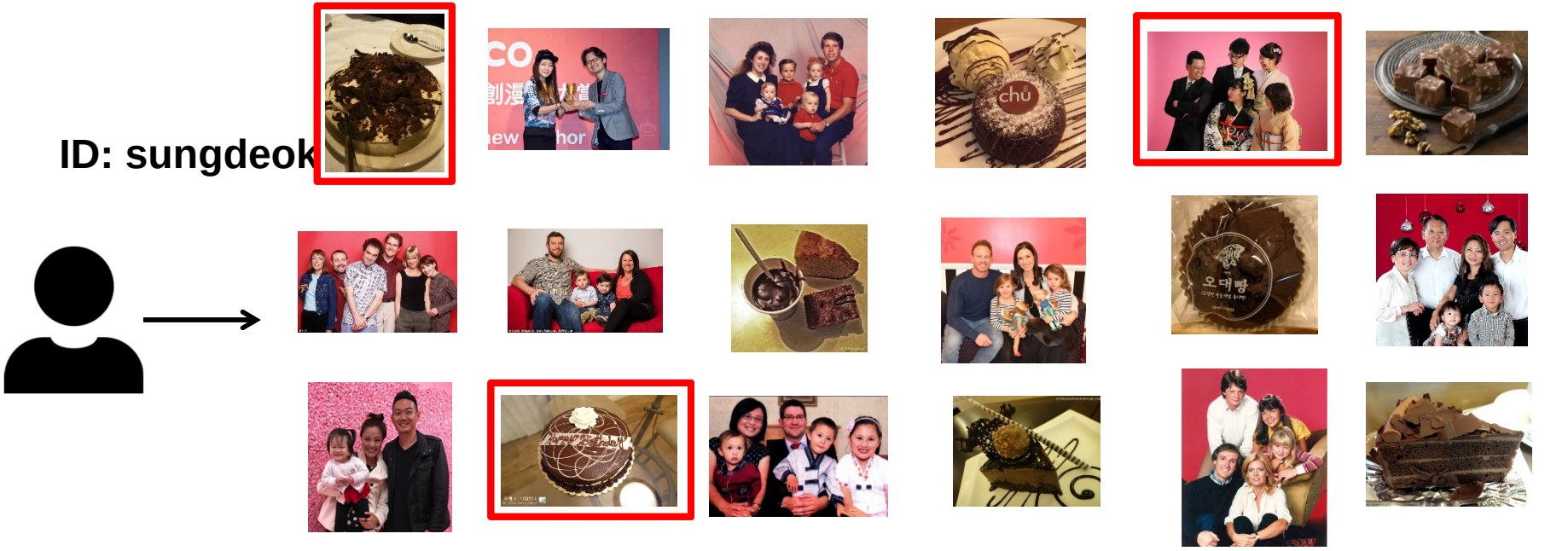
Provided that the image in the lower right corner is NOT a “trap” image

Actual deployment: TBD but should be flexible enough !

- Same images? Different images?
- Random placement of images?
- Number of images presented vs to-be-clicked
  - Mobile vs PC
  - e.g., may allow selection of additional images if they are not “trap” images
- How text password is entered
  - e.g., choose two images, but enter text associated with either image
  - To further introduce uncertainty while not confusing users
- But, absolutely no feedback on failed login attempts !!!

Attack Scenario (1): Random (Human) Attacker

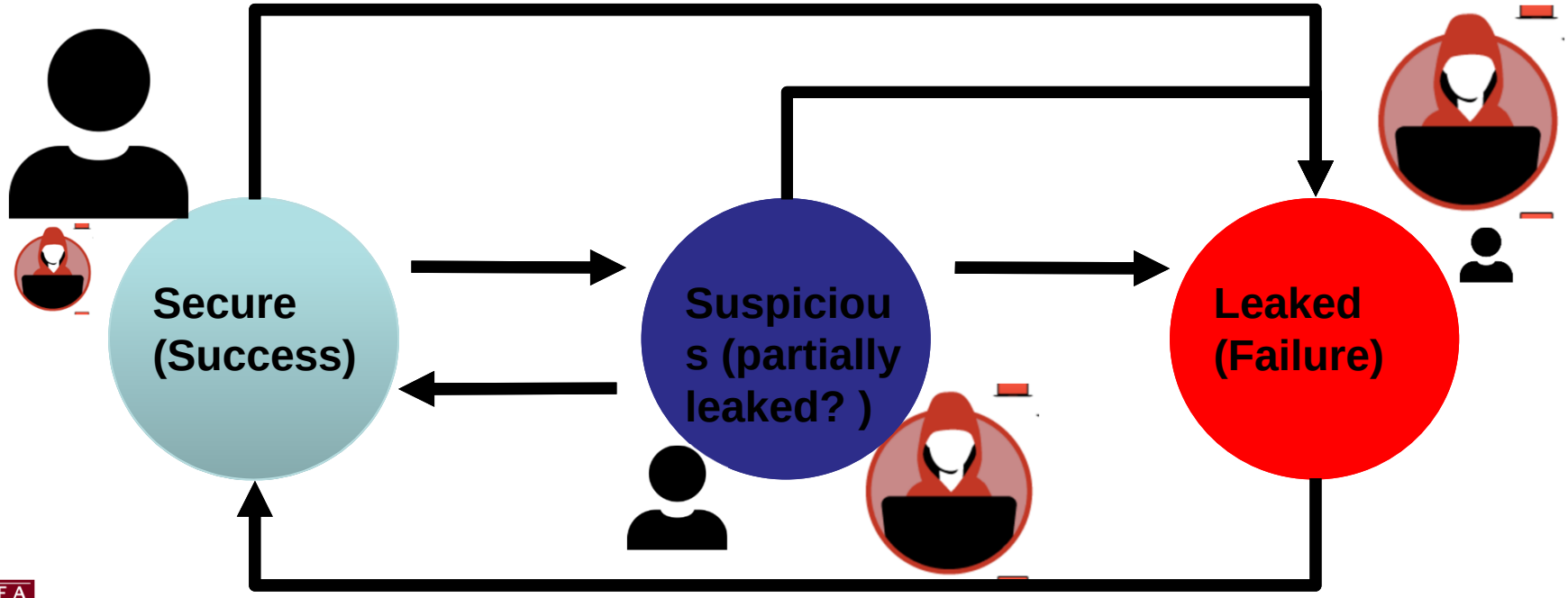
Password Verification



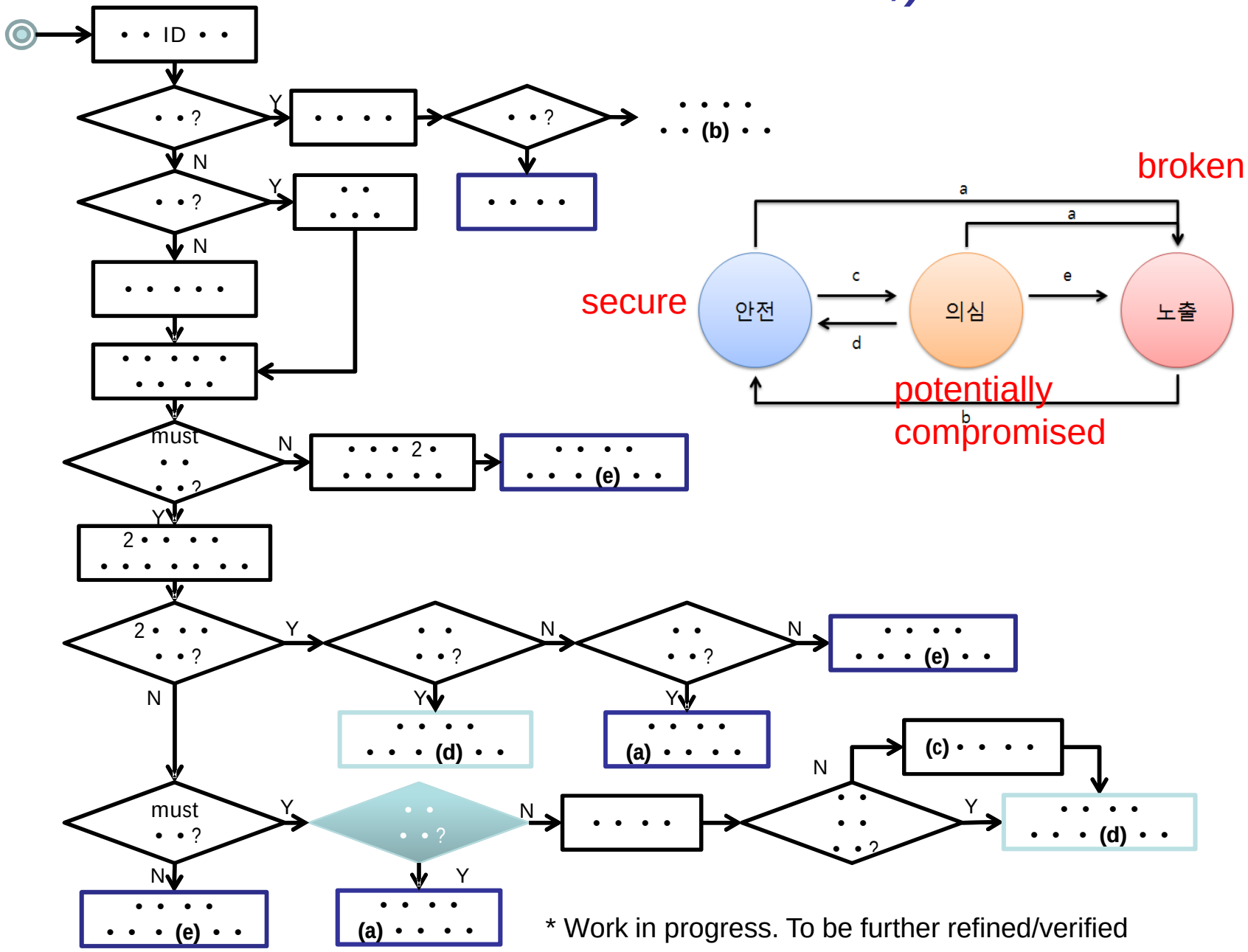
- Intruders are likely to choose wrong or trap images
- Intruders are highly unlikely to enter the correct text pasword
- Can it really survive “social engineering” attacks? To be explored.

Simplified User Authentication State

Based on user's image selection, and text responses, there are several different cases to consider

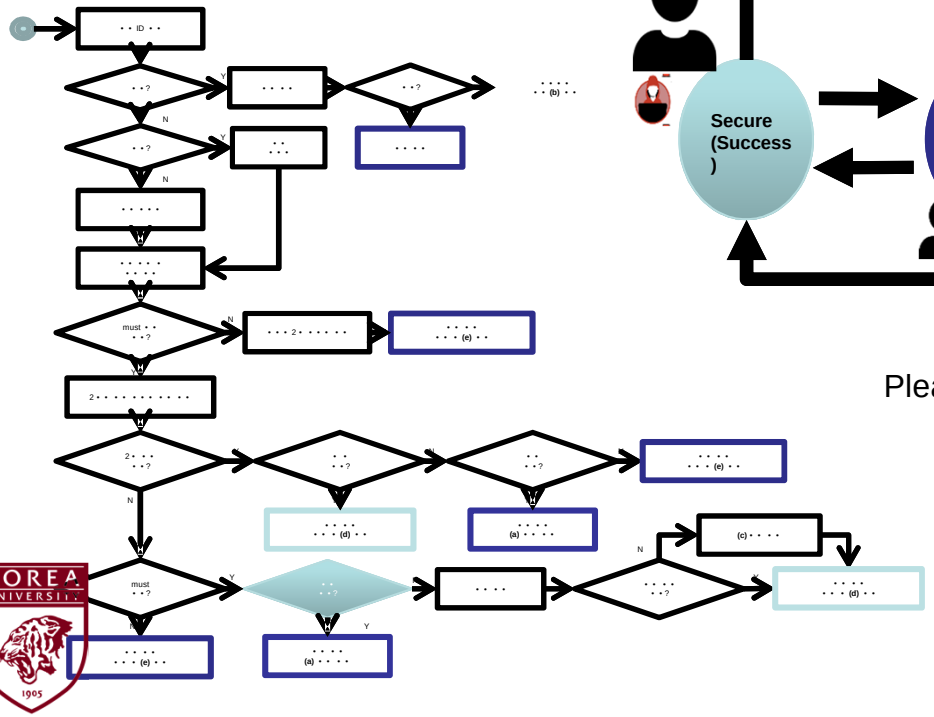


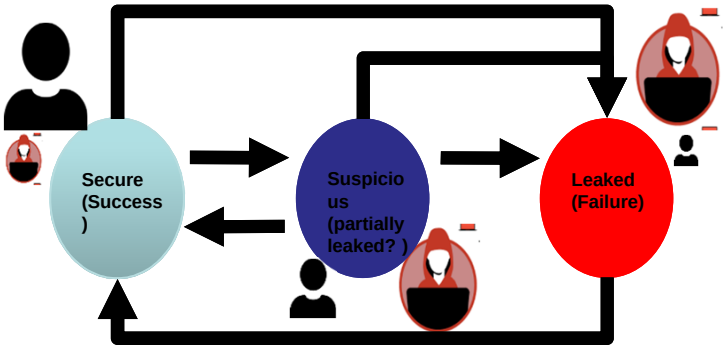
Not a classified slide ;)



Preventive Actions

- It is crucial to effectively estimate, based on patterns of failed login attempts
  - which “element” of the password might have been compromised
  - system might choose to ask text password associated with specific image





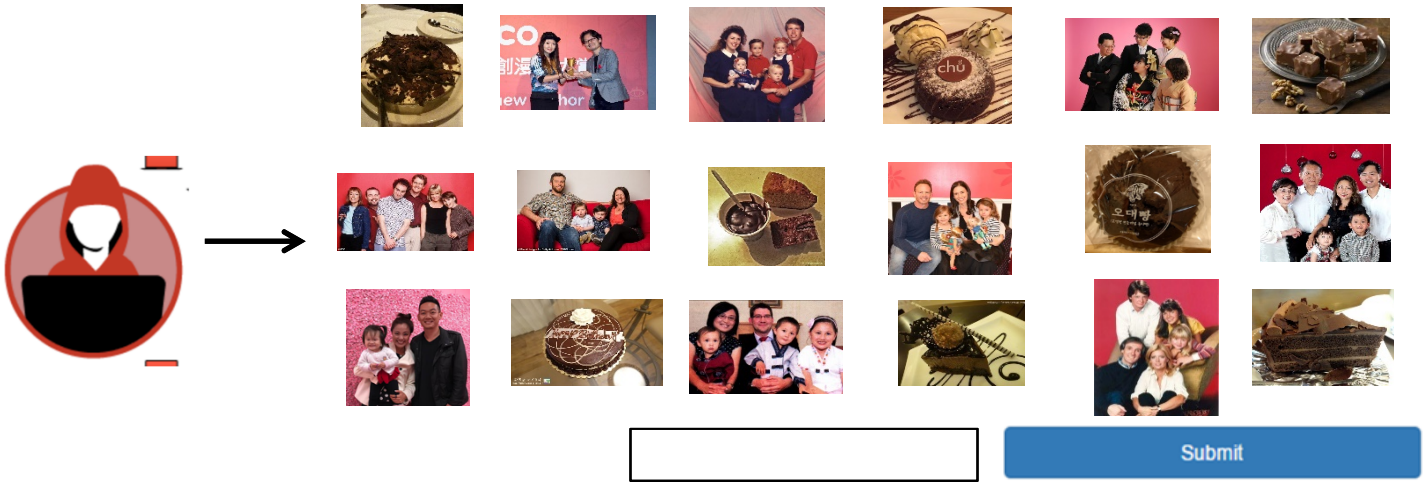
2017 • •

eric

Please update the following password

Dr.* • •

Attack Scenario (2): Automated Attacker



- **Bots are assumed to be equipped with deep learning algorithms, access to powerful search engines, "private" database on actions taken on past failures, etc**
- **Most powerful and nasty attack scenarios imaginable are to be investigated**

Current Status

- Implement a prototype system and perform preliminary user study
  - Ease of use
  - Successful Recall: 1) Image, and 2) Texts
  - Failure Analysis
- Simulate “social engineering” attacks
- Simulate automated/nasty attacks
- …

Conclusions

- Combine the best of both image and text based authentications
  - Built-in password attack and leak detection mechanisms via trap images
  - Highly personalized association between user ‘s own images and text labels
  - Easier to create and remember passwords on multiple sites
- Guidelines to enhance security strength and defeat face recognition algorithms?
  - Self image discouraged, …
- Plan to develop to become secure, scalable (e.g., multi-site), easy-to-use two factor authentication

money.cnn.com/2018/03/18/technology/biometrics-workplace/index.html

CNN tech BUSINESS CULTURE GADGETS FUTURE STARTUPS CNNMONEY

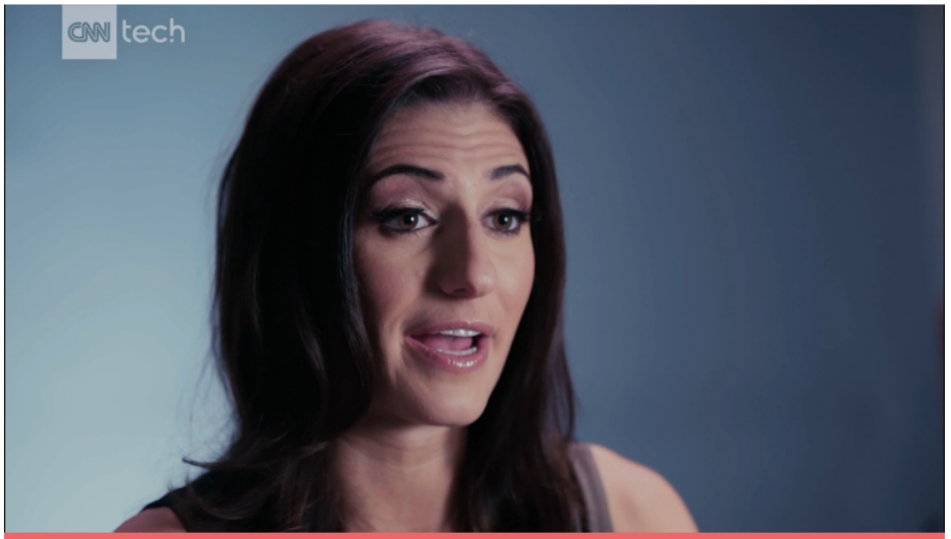
Work Transformed

Beyond passwords: Companies use fingerprints and digital behavior to ID employees

by Selena Larson @selenalarson

March 18, 2018: 3:53 PM ET

Recommend 686



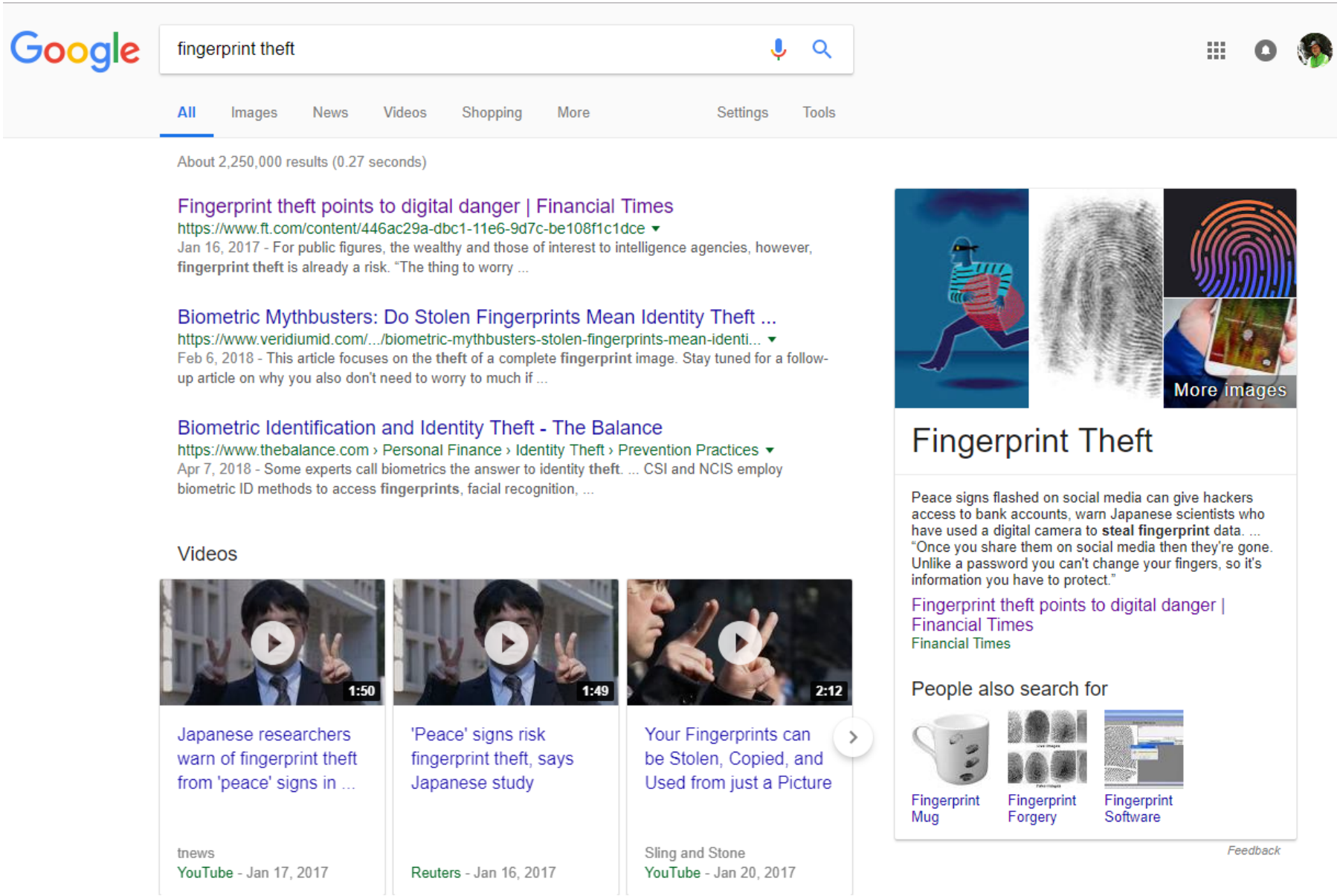
Can tech be biased?

More companies are ditching passwords and using fingerprints and other biometrics to stop hackers.

"We're seeing a very rapid evolution from what used to be passwords, then smart cards, and now to biometrics," said Alex Simons, director of program management in Microsoft's identity division.

Biometric authentication uses face, fingerprint or iris scans to quickly confirm a person's identity. You probably already use itap by touching the home button to unlock your phone.

Unfortunately…



“Dangerous Cyber World”

Secure | https://www.ft.com/content/446ac29a-dbc1-11e6-9d7c-be108f1c1dce

Apps For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...

HOME WORLD US COMPANIES MARKETS OPINION WORK & CAREERS LIFE & ARTS

Fingerprint theft points to digital danger

Japanese scientists fool biometric security system with off-the-shelf camera

Save

Security risk: a Japanese woman makes a V sign last week at a Tokyo amusement park © Reuters

Robin Harding in Tokyo JANUARY 16, 2017 4

Peace signs flashed on social media can give hackers access to bank accounts, warn Japanese scientists who have used a digital camera to steal fingerprint data.