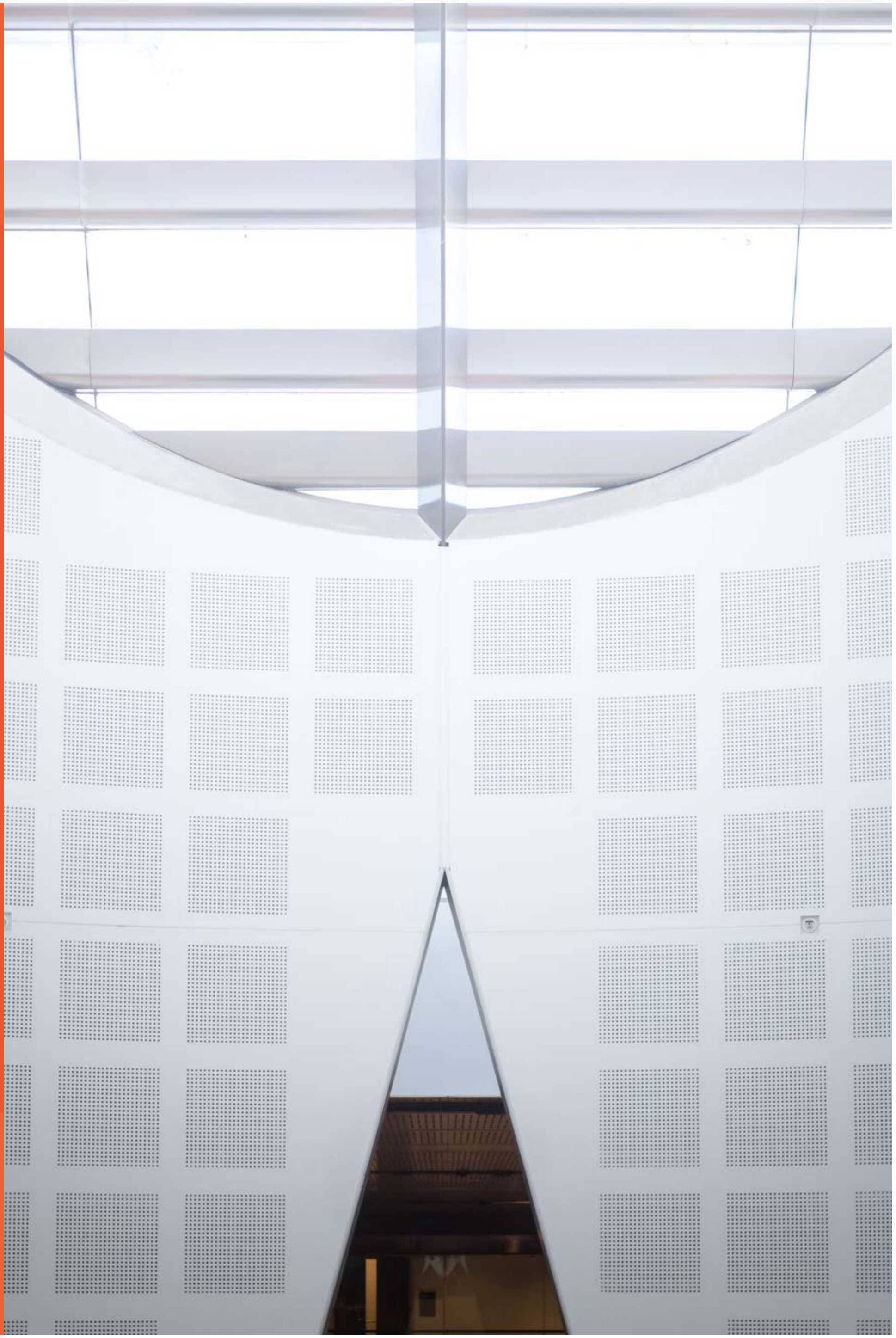
INFO2222

Operational Security and Authentication

Presented by

Luke Anderson



Overview

Today's Agenda

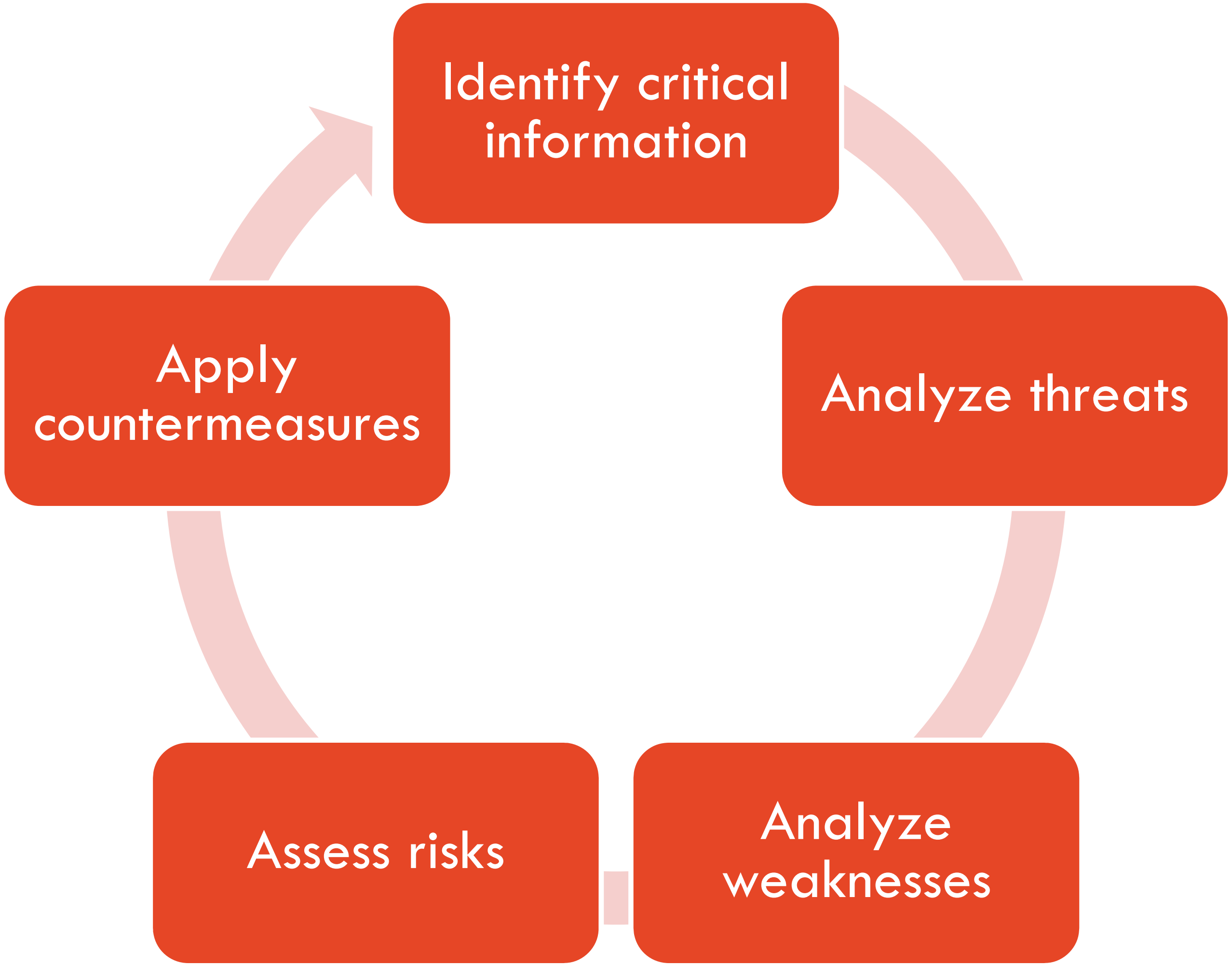
- Focused on the operation of your system in the context of the user
- Operational security:
  - Defences against:
    - Insider threats
    - Social Engineering
  - Physical security
  - Processes and policies (→ security management, later)
- AAA (Triple-A): Authentication, authorization, accounting
  - Authentication: "what you know, what you possess, what you are"

Operational Security

Definition

- Operational security's aim is to defend against attacks where **the primary attack is against procedures and processes, not so much technology**
  - Goal is to get your opponent to reveal mission-critical information
- Deception and trickery are incredibly effective
  - Often, they do not require much (or any!) technical investment – massively asymmetrical!
  - They often **bypass,** not attack, cryptographic and technical defences
  - They often attack psychological weaknesses in humans, which are deeply rooted and normally **beneficial in a social context**
- Many attacks against operational security fall into the category known as **Social Engineering:**
  - phishing/spear-phishing, pretexting, whaling, ...

Planning operational security: 5 stages



Identify critical information

Analyze threats

Analyze weaknesses

Assess risks

Apply countermeasures

Stage 1: Identifying critical information

- Critical information:
  - Facts about your own intentions and capabilities that an adversary would want to act against you effectively
- Examples:
  - Identities or personal information of your staff (→ social engineering!)
  - Movements or habits of your staff
    - E.g. unattended, unlocked screens during lunch break
  - Your planned next steps in some business deal
  - And of course, all business-critical information such as customer date, sales, etc.

Stage 2: Analyze threat

- **Systematic** analysis of your potential opponents
  - Identification of actors who have an interest in disrupting your business or processes
  - Identification of their motivation and goals
  - Identification of their capabilities (technical, staff, funding, …)
  - Identification of their determination and willingness to invest into action against you
- Examples:
  - Opponents for cybercriminals are law enforcement agencies
  - Opponents for businesses can be other businesses or agencies engaging in industrial espionage

- *Note: the use of the word "threat" here is not the same as in the technical phrase "Threat Modelling" – an unfortunate, but common ambiguity made popular over years of practice. "Threat" here refers to the non-technical analysis of opponent and their high-level capabilities. In the phrase "threat modelling", the word more commonly (but not always) refers to technical attacks against your (software) product. That should be better called "attack modelling", but the ambiguity persists.*

Stage 3: Analyze weaknesses

- In this stage, one tries to assume the opponent's role and think from their perspective
  - Which parts of your own organization show weaknesses?
  - Which practices does your organization have that could potentially be exploited?
  - What equipment do you use that could potentially harbour a weakness?
- This includes:
  - Physical security
  - Training of staff
  - Network defences
  - Analysis of software and hardware in use

Stage 4: Assess risks

- A threat can exploit a weakness
- Assign a risk level to each identified weakness
- This will guide your decision whether you need to invest to mitigate the risk

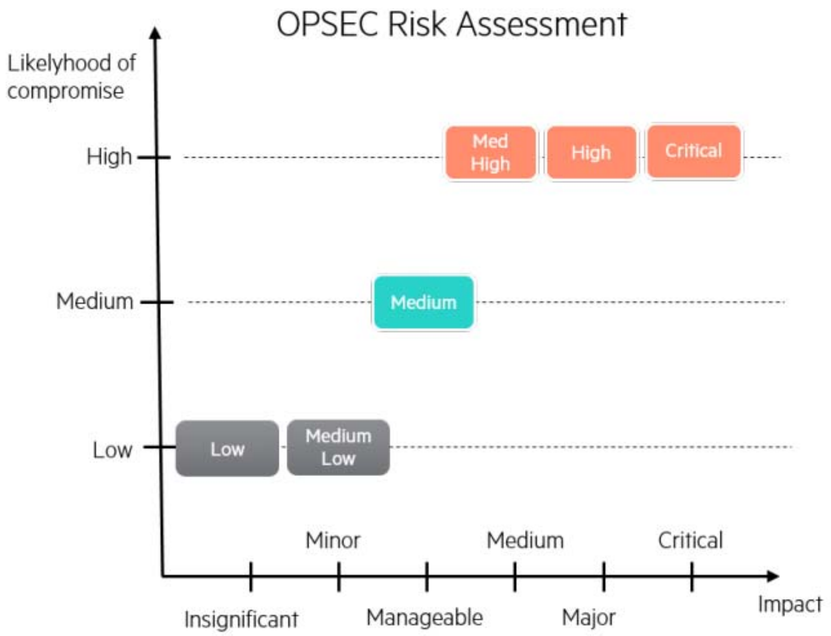


Figure: HP Enterprise Security Research: Cybercriminal OPSEC Practices. (https://techbeacon.com/sites/default/files/gated_asset/hpe-security-cybercriminal-opsec-practices.pdf)

Stage 5: Applying countermeasures

- In this stage, you prioritize the risks that you need to mitigate
  - Insight: your resources are limited. So are the attacker's resources!
- Development of mitigation plans take into account:
  - Technical and non-technical measures!
  - Mitigations to lower risk or eliminate it
- Countermeasures are a process
  - Remember: **security is a process, not a state**!
  - Countermeasures need to be continuously monitored for effectiveness and efficiency
  - Threats change! Your opponent develops and reacts to your countermeasures.
  - Your organization changes! New weaknesses develop.
- Security is expensive – this needs to be factored into business considerations

OPSEC: online world vs. real world

- Online setting is fundamentally different from the real world
- Online trickery is easier to do, and harder to stop
  - Online mechanisms and tools are not as usable or intuitive as the things we are familiar with on a daily basis
  - Online/remote setting gives us very few cues to verify a claim or identity

- Example: it is much easier to create a bogus website that imitates a bank and get victims to visit it than it is to rent a building and put a bogus bank branch in there with ATMs

Social engineering

- Social engineering is a particular risk for your OPSEC
- Aims at obtaining critical information
- Many different means are possible, depending on setting:
  - Personal or remote:
    - Baiting
    - Quid pro quo
  - Telephone/email contact:
    - Pretexting and impersonation
    - Phishing/spearphishing
  - Physical access:
    - Tailgating

Pretexting

- Presenting oneself as someone else to gain information.
  - Simple, very effective, bypasses all technical mechanisms

- Study in the UK:
  - Investigators trained hospital staff to identify and report false callers
  - Found 30 fake calls **per week**

- Very hard to defend against
  - Legitimate

Defences: Formal check-in and check-out systems for visitors, a culture where asking people who they are and who you can contact to verify them isn't seen as rude, education.

Defences against pretexting

- **Procedures/policy:**
  - Policy: no information revealed on the phone (not always applicable!)
  - Call-back: if caller claims to work for some organization, do not reveal information, but call back using the published phone number (not the attacker-supplied one!)

Defences: Formal check-in and check-out systems for visitors, a culture where asking people who they are and who you can contact to verify them isn't seen as rude, education.

Phishing

- Spoofed or malicious email attacks attempting to get a click, information, or some action
  - Often an email to many receivers
  - However, can also be incredibly sophisticated and trick even highly experienced security professionals
  - **Sometimes, a site visit is all that the attacker wants: malware drive-by download**

Spear phishing and whaling

- Spear phishing is targeted phishing
  - Email with just one (or very few) receivers
  - Custom-built to their expectations, imitates organization's protocols, style, corporate identity
  - Often makes use of the victim's publicly available data (Facebook!) or known position/contacts in the organization

- Particularly dedicated form: whaling
  - Targets receivers at the C-level (higher management)
  - Same goals e.g. get them to transfer money or disclose company secrets.
  - Effective!
  - Interestingly, some studies claim that C-level managers are particularly hard to train!

Defences against phishing

- **Training:**
  - Staff can be trained to detect phishing emails by looking for tell-tale signs or unusual requests
    - Anonymous receiver list, inspection of sender address, spelling errors or uncommon spelling
- **Procedures and policy:**
  - Disallow email-based processes for high-value transactions (require login to portal etc.)
  - TODO
- **Technical:**
  - **Not sufficient as a defence, but can be a useful aid**
  - Well-designed UI can be helpful, e.g. "this mail was not sent from within our company"
  - Email spoofing prevention (see INFO3616).

Baiting

- **Tricking someone into accepting/using a malicious gift**
  - Relies on the curiosity or greed of a victim rather than impersonation.
  - Distinguished by the promise of a item or good i.e. free movie.
- **Example:**
  - Leaving USB keys lying around – yes, most people are curious and will plug them in
  - Homer's story of the Trojan horse: the classic baiting story
- **Old tricks, yet they keep working:**
  - Promise people extraordinary return-on-invest, e.g. "send me money, I invest, and you get twice as much back"
  - advance-fee scam (in the online world: "Nigeria scam")

Defences: Education, strong security culture, openly discussing opportunities, healthy skepticism.

Tailgating

- Gaining access to a restricted area by walking behind someone who is authorized.
  - May pretend to be a delivery, or simply just follow.
  - Limited to a **physical** space.

Example: How many times have you let someone into a door at USYD with your swipe card? Would you be too nervous to confront someone?

Defences: A security culture where ‘no’ is okay, security guards, manned gates.

Quid pro quo

- The promise of a benefit in exchange for some information.
  - Different to baiting, as that is usually a good, this is any arbitrary benefit.

Example: Fraudsters who impersonate IT help, offering to fix computers in exchange for access to it.

Defences: Healthy skepticism, education, ensuring critical information flows are *need to know* rather than *need to withhold*.

Culture and rules

- It is **not enough** to have rules

- Staff must be continuously trained, so they are enforced
  - This may require a cultural change
  - Success stories (thwarted scams) make the rounds fast among staff, however, and can reinforce the training

- How effectively this can be enforced, is a matter of culture:
  - Employees of intelligence agencies are easier to train (and maintain the level of security) than corporations
  - Good corporate culture emphasizes the need for secrecy **in the right places**
  - We return to this in Week 12

Physical security

- Common attack: physical access to your premises and/or infrastructure makes the odds of defending successfully much worse
- Examples:
  - Tailgating – and then looking around, shoulder-surfing
  - Unlocked office and unlocked computer
  - Disposal of trash: no secret material may go out unshredded
- Defences depend on required security
  - Locks, sensors, walls, alarms for server rooms in data centre
  - But locks and walls can be sufficient for an office
  - Shredders for documents and media
  - Culture and policy for locking the screen
- Purpose can be both deterrence (cameras) as well as prevention (walls)

Information and information flows

- Many attacks can be defended against by designing policies that govern access to information
  - "Need to know" principle
- Multi-level security (e.g. security clearances): higher level may read everything below, but never in the other direction
  - Top Secret
  - Secret
  - Confidential
  - ...
- Systems can be built that support such security levels
  - Drawback: workplace workflows and culture must be compatible! Otherwise, users will find the systems clumsy to use and work around them.

Authentication & Authorization

AAA

- Computer systems exist for specific people and various tasks
  - Many systems are for multiple users (all servers are!)
  - Laptops, handhelds, and sometimes workstations are exceptions
- It is often essential that the system knows which user is active
  - Privileges may be assigned to users (what they are allowed to do)
  - System may need to log carefully who did what, and when
    - Auditing
    - Charging the user
  - System must be able to a) authenticate user and b) verify authorization to perform a task and c) do accounting

- Authentication is not always necessary:
  - It can be enough to just present authorization without any authentication

Authentication

- Interestingly, formal definitions for authentication are ***hard***

- Let's try: who can give a good definition of authentication?

Authentication

- Interestingly, formal definitions for authentication are ***hard***

- Common answer:
  - "Demonstrate/prove who I am"
  - Way too informal

- Common answers fail to include:
  - What is defined as my identity?
    (Biological? Photographic? Social security number?)
  - How is the proof done? Who can verify it?
  - Whose word do we trust? What is trust?
  - Who authenticates to whom?
  - Does it need to be live? Can I replay a proof?

Who are you?

- The less controlled and the more decentralized our system is, the harder authentication becomes

- E.g. can you really prove you aren't an impostor?
  - When there isn't an account you are tied to.
  - When you have only ever interacted online, or never before
  - When others can just replay some previous proof

- High-level fact (with deep implications):
  If two entities have never interacted before, and there is no third party that both would trust, there can be no way to define an authentication process between the two that would be secure against an attacker.

Authentication

- Authentication is the process of corroborating, by evidence, your identity to another party.
  - This is still far from a good, formal definition, but it suffices for our intuition. More in INFO3616 and COMP5617.
- Evidence can come in different forms

- Something you **know**
  - Some secret that no other entity can reveal
- Something you **have**
  - A physical thing no other entity possesses
- Something you **are**
  - A physical feature of your (human) body – biometrics

Authentication protocols

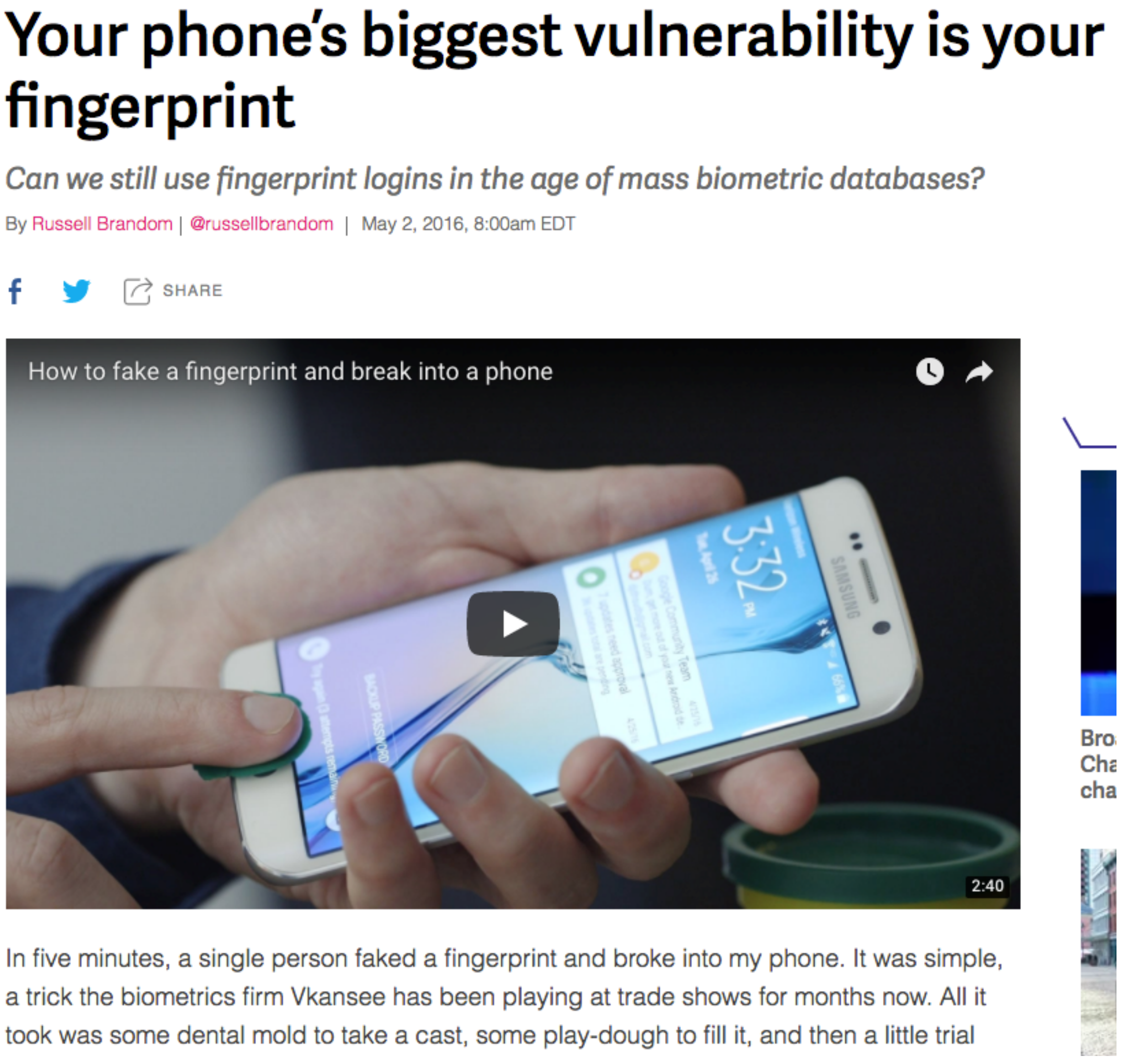
- All authentication is based on one or more links between a user and something they know/possess/are.

- Authentication protocols:
  - Define a series of messages between two parties who wish to authenticate
  - Can be mutual authentication or one-sided
  - The series of messages needs to be very carefully defined: attackers can replay parts or entire messages, craft carefully designed messages that are wrongly interpreted by the real users, etc.

Something you are - biometrics

- Special hardware can measure some (nearly?) unique feature of the user's body
  - E.g. Fingerprints, iris, face, voice
- **Advantages**
  - Resistant to many attacks (but not all)
  - Fingerprint readers, in particular, can be tricked
  - AI has made huge advances, but so have attackers
- **Disadvantages**
  - Recognition errors
    - Noise – no exact match
    - Faces and fingerprints change a bit with time and conditions
  - **Revocation – need to change authentication system if a breach does occur (e.g. someone manages to obtain a fingerprint)**
  - Biometrics is rarely used as the single factor in authentication

Beware of the fingerprint



Your phone's biggest vulnerability is your fingerprint

Can we still use fingerprint logins in the age of mass biometric databases?

By Russell Brandom | @russellbrandom | May 2, 2016, 8:00am EDT

SHARE

How to fake a fingerprint and break into a phone

In five minutes, a single person faked a fingerprint and broke into my phone. It was simple, a trick the biometrics firm Vkansee has been playing at trade shows for months now. All it took was some dental mold to take a cast, some play-dough to fill it, and then a little trial

Something you have

- Traditional physical security devices: key, identity card. A common example is, today, your mobile phone running so-called authenticator apps.
- **Advantages**
  - Intuitive
  - Authenticators are easy to customize & revoke; can run in software only
- **Disadvantages**
  - Hardware tokens are expensive to issue and change
  - Hardware tokens require corresponding hardware on-site, protected against physical attacks
  - Some devices are easily duplicated (e.g. swipe cards)
  - "Unforgeable" devices have **an extremely poor track record –** complexity of today's system makes "unforgeability" very very very hard.

Example: security tokens

- Small device or program that generates a frequently changing sequence of values
  - Hardware token: can give one to each user
  - Software: configure e.g. with QR code to assign secret value to each user
  - Smartphone apps by Microsoft, Google, and others

- Idea: "seed" secret, sometimes together with time, allows to create user-specific one-time values
  - Perhaps changed every second
  - Or perhaps changed by some events
  - Or on getting an SMS instruction

- Yubikeys are an example of a hardware token

Something you know

- The user provides knowledge only they know
  - This is the most common way to identify a user for an IT system
  - No special hardware needed and usually a ‘password’ or passphrase

- Advantages
  - Easy to use, very user friendly – users get to choose

- Disadvantages
  - Users get to choose: weak passwords, reuse, sharing…
  - Easily stolen
  - We are human, we forget

Usability and incorrect attempts

We have learnt that you should always tell the user explicitly what went wrong and how they can fix an error state.

But:

- If your website says "wrong password", it tells an attacker that the username they entered belongs to an account
- On the other hand, it helps the user remember their username
- Sometimes for security, no information should be given to the user and potential attacker for the state of the system. Just like debug information should be switched off.

Multi-factor Authentication

- You may have heard of this before. It simply means using at least two of the three categories.

- The most common ‘multi-factor’ setup today is:
  - Something you know = password.
  - Something you have = code sent to your mobile phone.

- This ‘common’ set up is often still breakable, the attacker can port the phone number and get the code.
  - But it raises the bar for the attacker – their time costs money, too

- Yubikeys are an example in widespread use of *something you have multifactor.*

Multi-channel Multi-factor Authentication

- Use two different communication channels between user and system.
  - A control that makes interception and man-in-middle more difficult.
- Combined with two-factor authentication
  - E.g. user has two passwords, one sent through internet and one by SMS
- An attacker needs to attack both factors.
  - Cost of attack is higher
  - Likelihood of successful attack is lower
- But also inconvenience to genuine user can be higher.

Passwords

- Passwords are currently the only basis of authentication that is intuitively understood
- Users are also very bad at choosing passwords
- There is an entire research direction on how to improve password security
- These were compiled by SplashData in 2017
- After every major data breach, such interesting lists are passed around

- 123456
- Password
- 12345678
- qwerty
- 12345
- 123456789
- letmein
- 1234567
- football
- iloveyou
- admin
- welcome
- monkey
- login
- abc123
- starwars
- 123123
- dragon
- passw0rd
- maste
- hello
- freedom
- whatever
- qazwsx
- trustno1

Empirical studies

- Study of compromised MySpace accounts in 2006
  - http://www.schneier.com/blog/archives/2006/12/realworld_passw.html
  - Average password was 8 characters
  - 28% were sequence of lower case letters followed by a single final digit
  - Less than 4% were a dictionary word

- Many such studies exist – every year

- We do not see much improvement in terms of the most popular passwords

Attackers can make educated guesses

- Insight: users do not choose arbitrarily
  - Many passwords are built around names of family, pets, sports teams etc.
  - If you know your victim, this is a great attack vector

- Dictionaries provide lists of suitable guesses.
  - Storage requirements are marginal today
  - Legitimate use (of course) in spellcheckers
  - Can modify for password guessing to also include variants (substitute 0 for O, 1 for I, 3 for e, 4 for A
    - note that you are not 1337 if you do this)
  - Password lists collated from breached data
    - lists of passwords really used
    - users are similar

Further educated guesses

- Some more common variants:
  - No password
  - Same as user ID or derived from user's name
  - Common word patterns (“qwerty”, “aaaaaa”..)
  - Complete English word list
  - Same with common capitalisations and substitutions..

Default passwords

- Another common password is simply the default password.

- Many systems come with a pre-installed account and default password.

  E.g. sysadmin account, initial password is "password".

  E.g. guest account, initial password is "guest".

- These are often available in (online) documentation

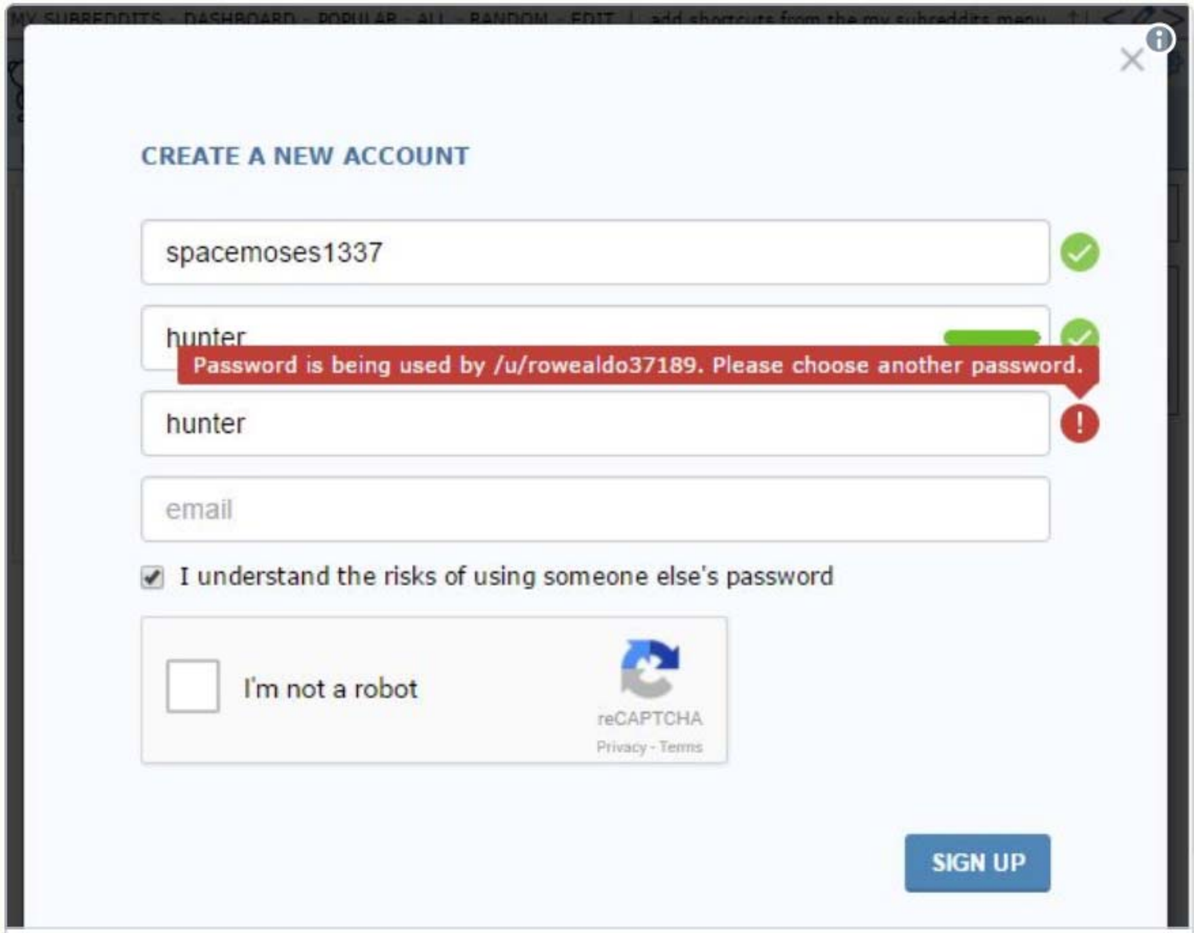
- So common that there are bots out there right now scanning websites and trying default credentials.

Don't laugh

- It is very easy as a security professional to laugh and joke about this… but it often misses the point.

- If a user does something harmful, it is important to understand **why** this behaviour occured.
  - E.g. user must remember the password, and people are not good at remembering long meaningless sequences. The fault is with the designer, then, and not the user!
  - People just want to be able to do their job or goal as easily as possible. If security stands in the way, users will work around it. They are more creative than any designer can assume, and hence the fault is again with the designer.
  - **The goal must be to design a system that strikes the correct balance at security and user inconvenience/support. That's hard.**

Companies get it wrong, too


MY SUBREDDITS · DASHBOARD · POPULAR · ALL · RANDOM · EDIT | add shortcuts from the my subreddits menu

CREATE A NEW ACCOUNT

spacemoses1337 ✓

hunter ✓

Password is being used by /u/rowealdo37189. Please choose another password.

hunter !

email

☑ I understand the risks of using someone else's password

□ I'm not a robot

reCAPTCHA
Privacy - Terms

SIGN UP

A helpful system.

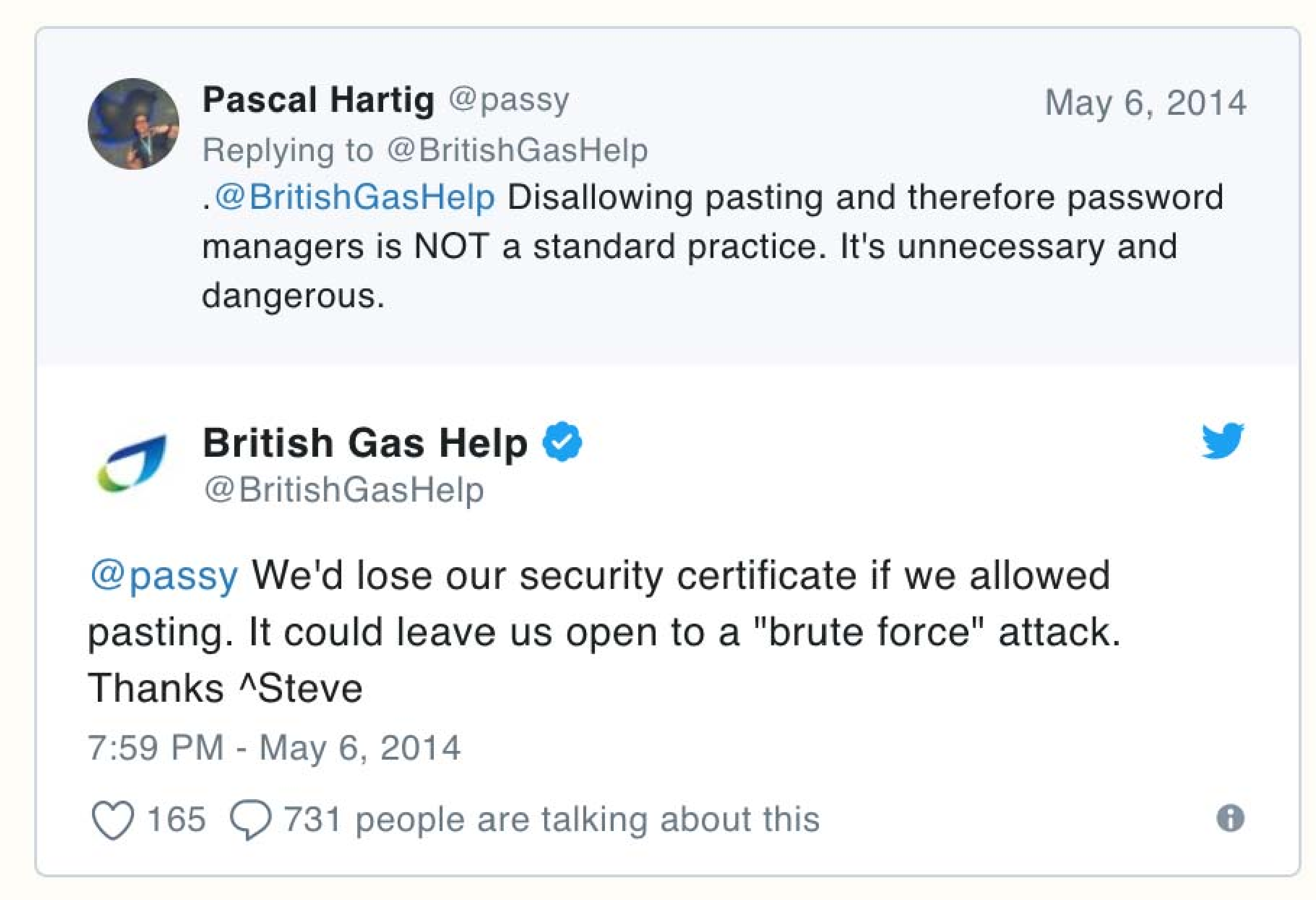
Brute Force

- Brute force is simply trying every combination.

- Assume the attacker knows some rules how password was created
  - Eg 6 characters, each from the keyboard
  - Or 8 alphabetic characters, all lower case

- Attacker tries all sequences of that shape, one after the other, until one succeeds (system allows access)
  - It's easy to write a program that generates all sequences

Stupid advice prevails



Pascal Hartig @passy May 6, 2014

Replying to @BritishGasHelp

.@BritishGasHelp Disallowing pasting and therefore password managers is NOT a standard practice. It's unnecessary and dangerous.

British Gas Help @BritishGasHelp

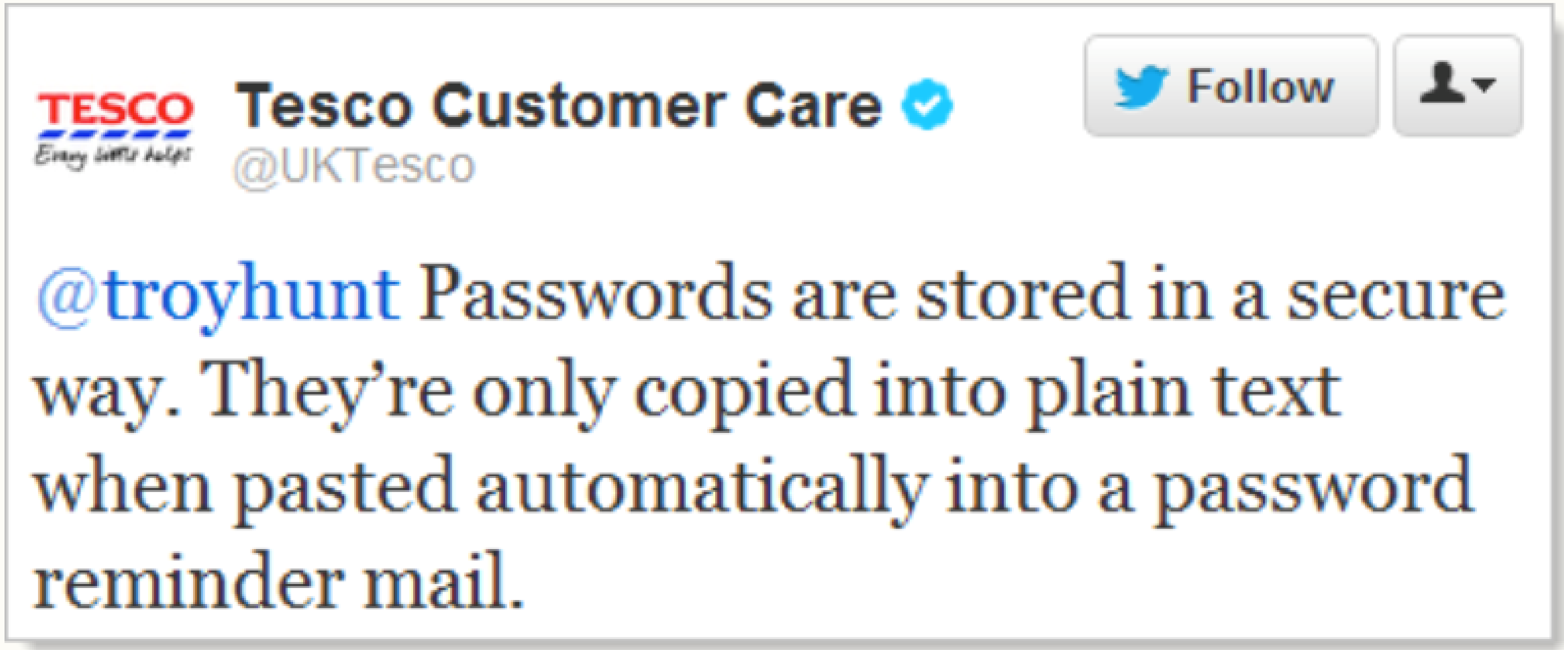
@passy We'd lose our security certificate if we allowed pasting. It could leave us open to a "brute force" attack. Thanks ^Steve

7:59 PM - May 6, 2014

♡ 165 731 people are talking about this

"Brute force" still possible: no attacker uses copy/paste. They can program.
At the same time, it prevents users from using password managers.

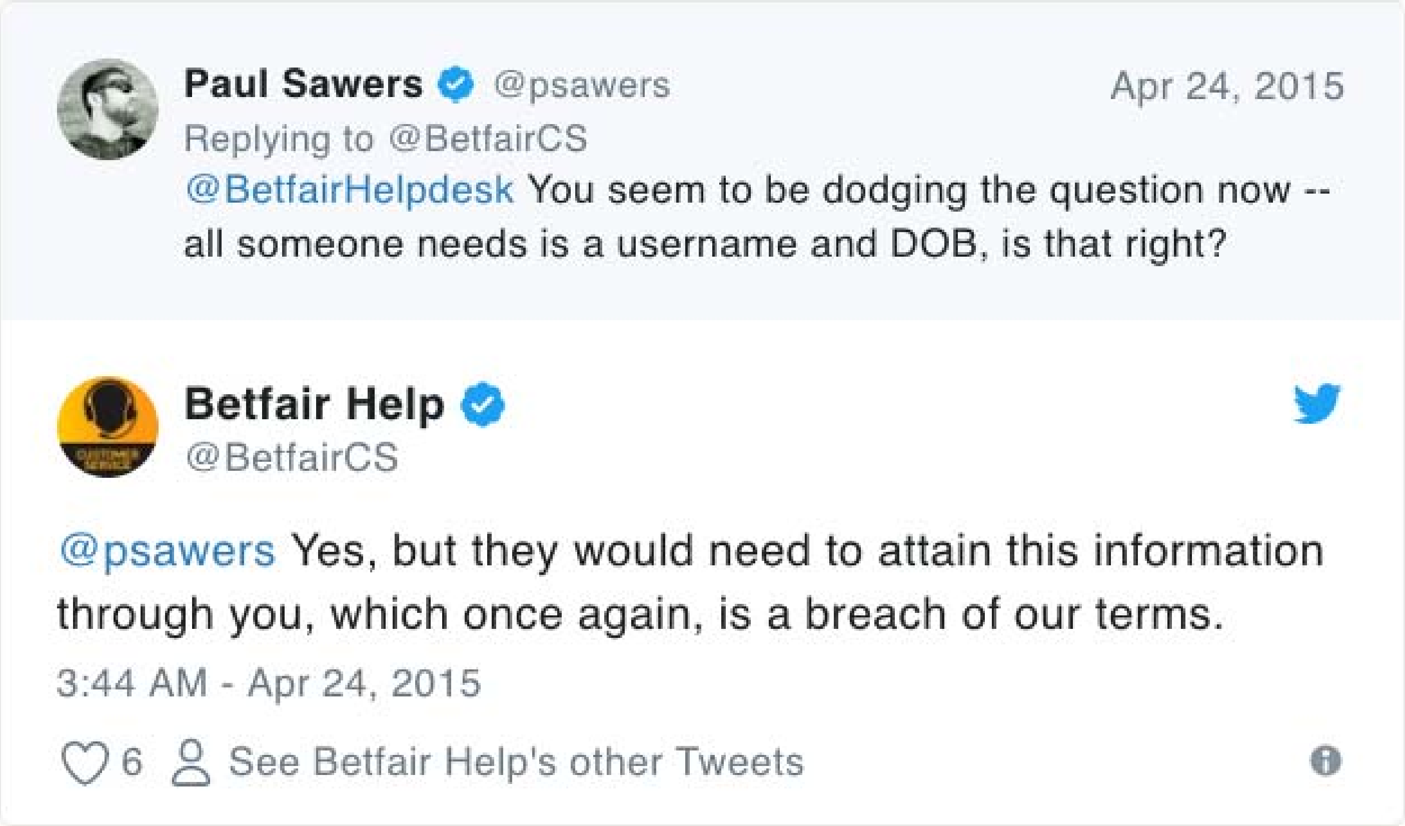
Don't panic.



Tesco Customer Care
@UKTesco

@troyhunt Passwords are stored in a secure way. They're only copied into plain text when pasted automatically into a password reminder mail.

Others don't even try



Paul Sawers @psawers Apr 24, 2015

Replying to @BetfairCS

@BetfairHelpdesk You seem to be dodging the question now -- all someone needs is a username and DOB, is that right?

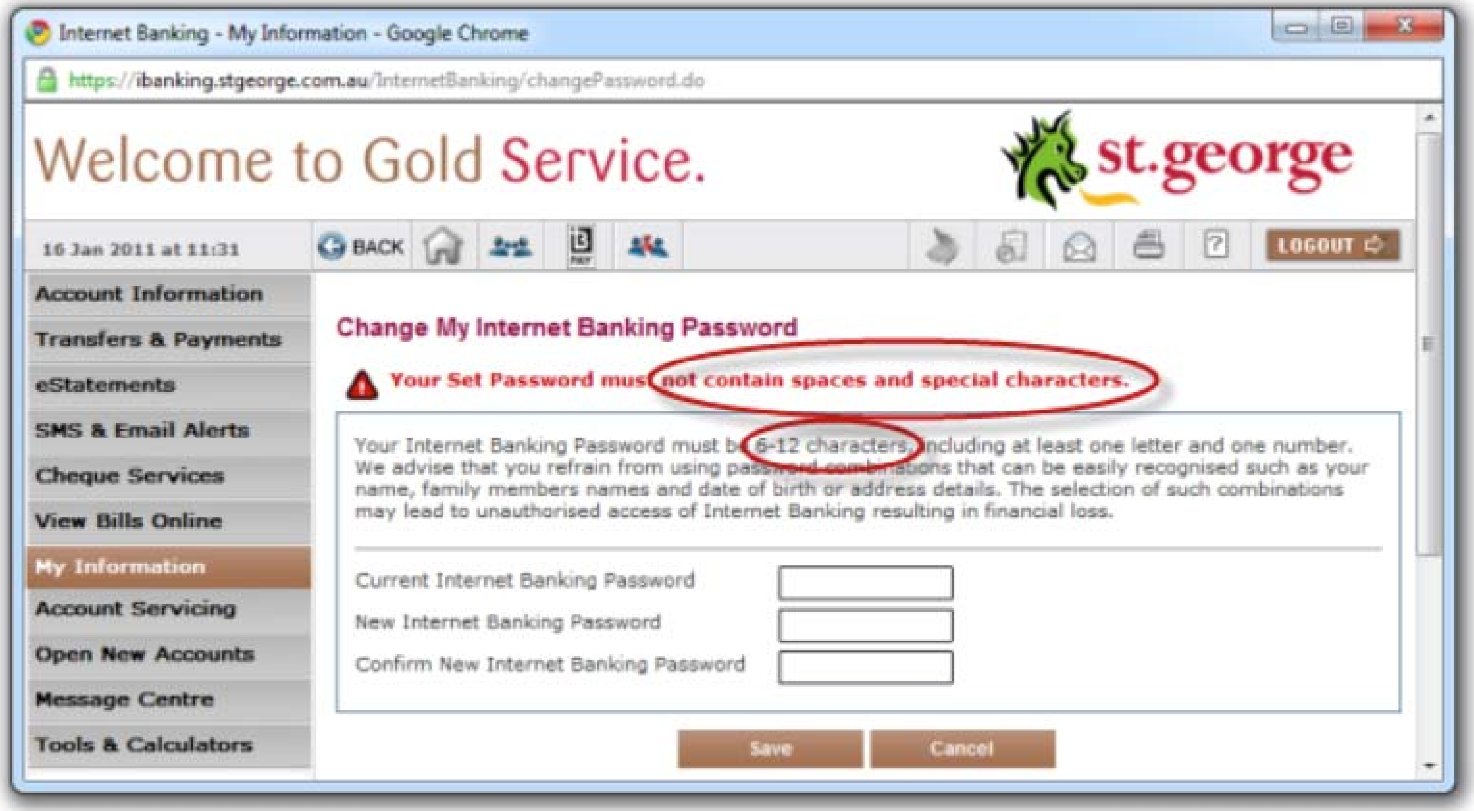
Betfair Help

@BetfairCS

@psawers Yes, but they would need to attain this information through you, which once again, is a breach of our terms.

3:44 AM - Apr 24, 2015

Make it easy on the developers or on the users?



Change My Internet Banking Password

⚠ Your Set Password must not contain spaces and special characters.

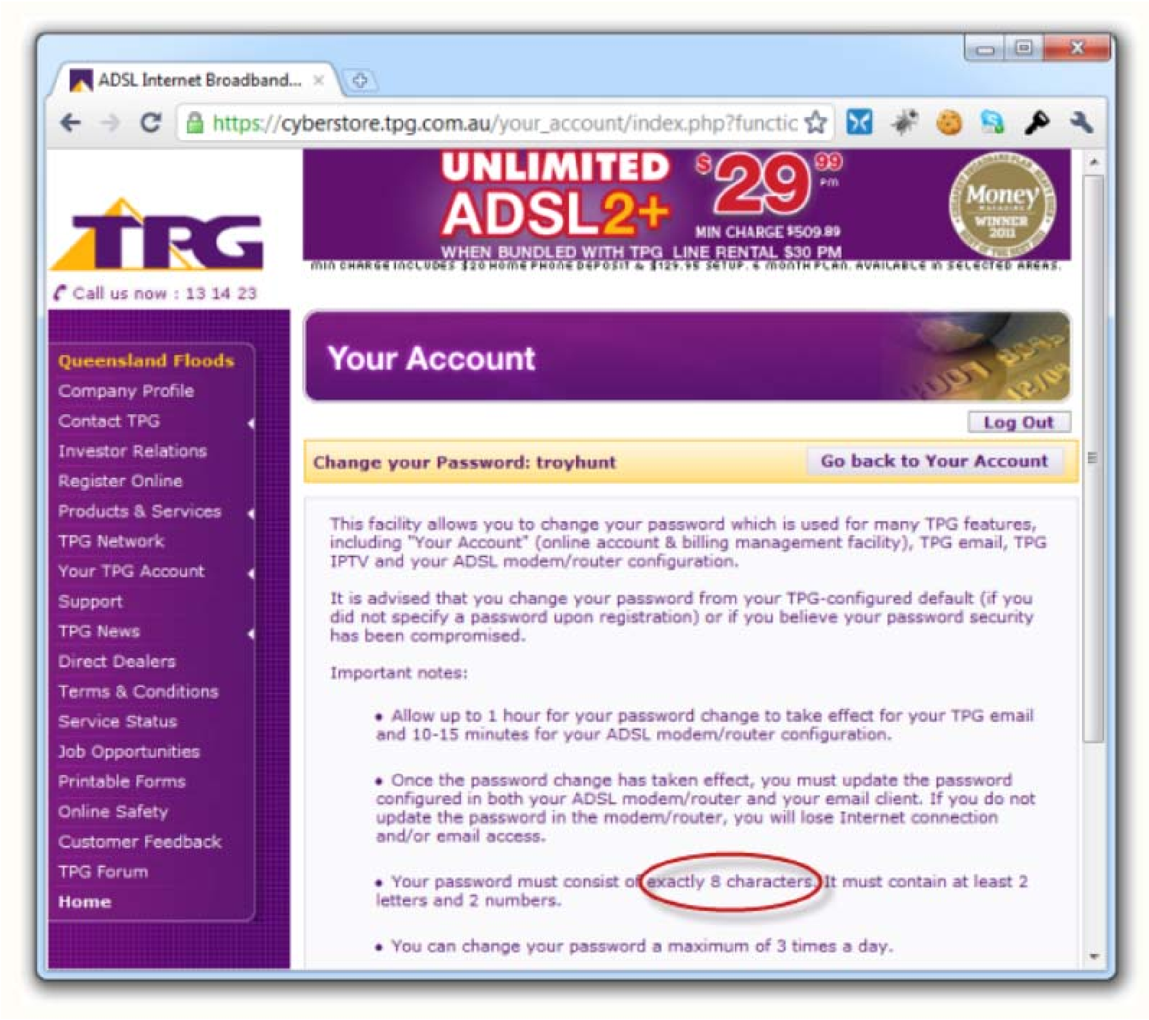
Your Internet Banking Password must be 6-12 characters, including at least one letter and one number. We advise that you refrain from using password combinations that can be easily recognised such as your name, family members names and date of birth or address details. The selection of such combinations may lead to unauthorised access of Internet Banking resulting in financial loss.

Current Internet Banking Password ▭

New Internet Banking Password ▭

Confirm New Internet Banking Password ▭

Unnecessary constraints, part 2



Your Account

Change your Password: troyhunt

This facility allows you to change your password which is used for many TPG features, including "Your Account" (online account & billing management facility), TPG email, TPG IPTV and your ADSL modem/router configuration.

It is advised that you change your password from your TPG-configured default (if you did not specify a password upon registration) or if you believe your password security has been compromised.

Important notes:

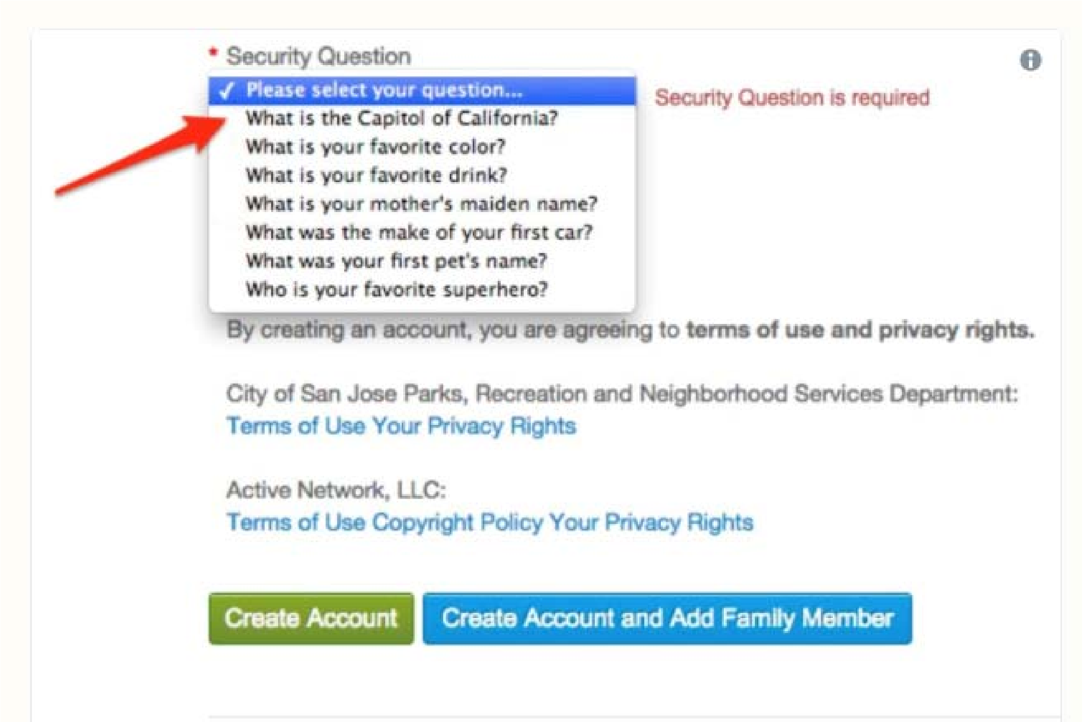
- Allow up to 1 hour for your password change to take effect for your TPG email and 10-15 minutes for your ADSL modem/router configuration.
- Once the password change has taken effect, you must update the password configured in both your ADSL modem/router and your email client. If you do not update the password in the modem/router, you will lose Internet connection and/or email access.
- Your password must consist of exactly 8 characters. It must contain at least 2 letters and 2 numbers.
- You can change your password a maximum of 3 times a day.

Security questions

- Commonly used to reset passwords if they have been lost
- Answers to security questions can be very common:
  - Mother's maiden name? Try "Smith", "Johnson", "Jones", "Miller", ...
  - Mother's date of birth? Age range can be guessed, as can be days
  - Pet names? See above.
  - First car driven? In Germany, try "Golf". In Australia, try "Corrolla" or "Mazda 3".
  - Favorite drink? Try "Margherita" or "Beer".

- Good practice, many websites now send an immediate email to a customer whenever a reset is requested
  - Can also geo-track: if request is from country other than known customer's address etc.

Security questions done wrong



* Security Question

✓ Please select your question...
What is the Capitol of California?
What is your favorite color?
What is your favorite drink?
What is your mother's maiden name?
What was the make of your first car?
What was your first pet's name?
Who is your favorite superhero?

Security Question is required

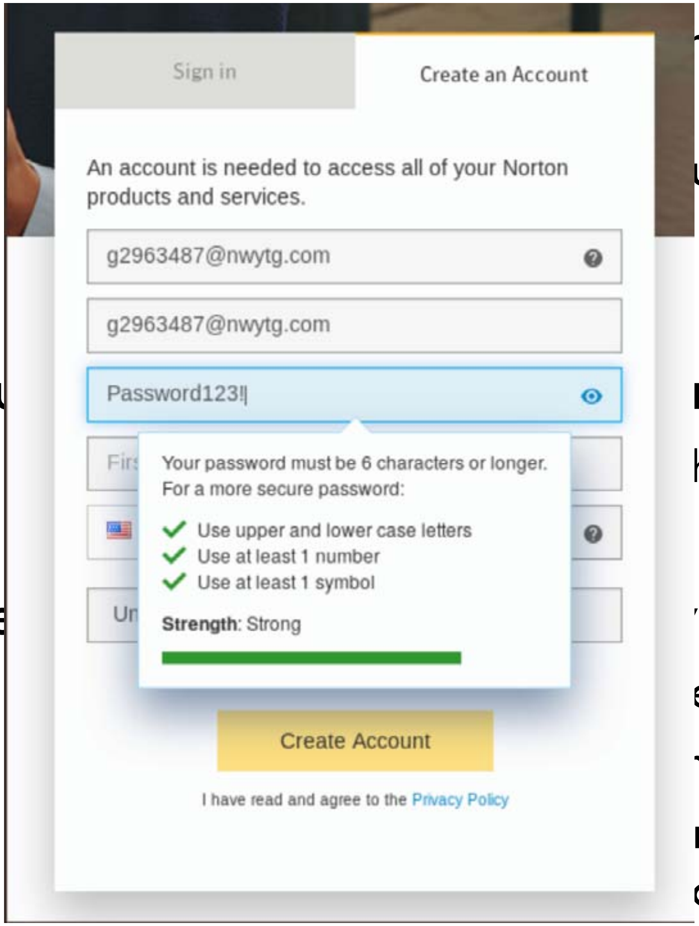
By creating an account, you are agreeing to **terms of use and privacy rights.**

City of San Jose Parks, Recreation and Neighborhood Services Department:
Terms of Use Your Privacy Rights

Active Network, LLC:
Terms of Use Copyright Policy Your Privacy Rights

Much bad advice out there

- E.g. "at least one punctuation character and one number"
  - k, " will
  - use
    se
- "Mu rs'
  - he
- "Ne or
  - e s 0s)
  - n P
  - n c t, is
    or



Sign in

Create an Account

An account is needed to access all of your Norton products and services.

g2963487@nwytg.com

g2963487@nwytg.com

Password123!|

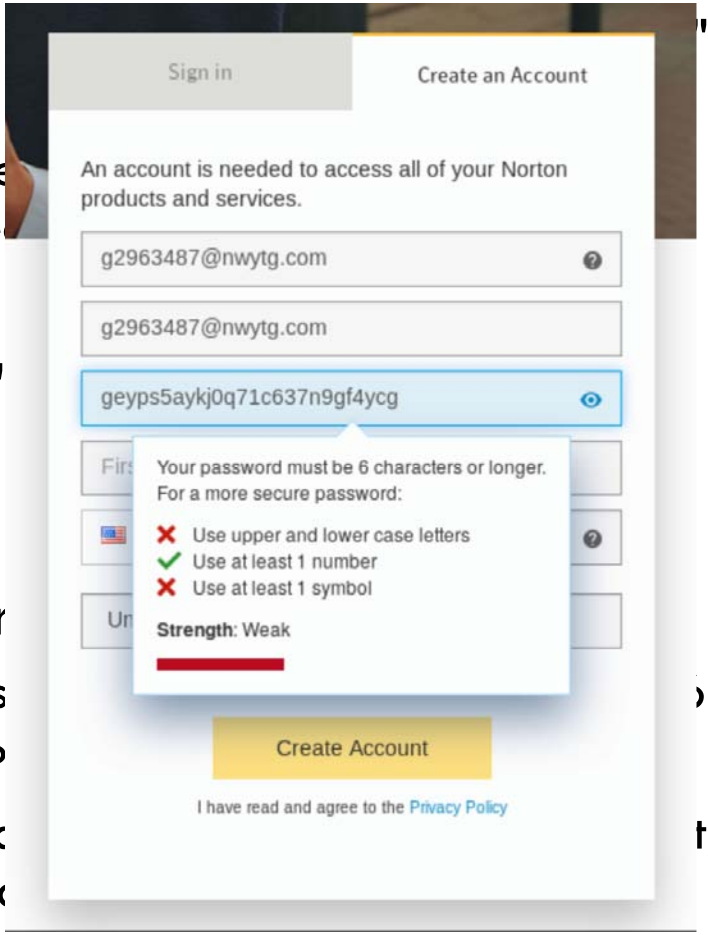
Your password must be 6 characters or longer.
For a more secure password:

✓ Use upper and lower case letters
✓ Use at least 1 number
✓ Use at least 1 symbol

Strength: Strong

Create Account

I have read and agree to the Privacy Policy



Sign in

Create an Account

An account is needed to access all of your Norton products and services.

g2963487@nwytg.com

g2963487@nwytg.com

geyps5aykj0q71c637n9gf4ycg

Your password must be 6 characters or longer.
For a more secure password:

✗ Use upper and lower case letters
✓ Use at least 1 number
✗ Use at least 1 symbol

Strength: Weak

Create Account

I have read and agree to the Privacy Policy

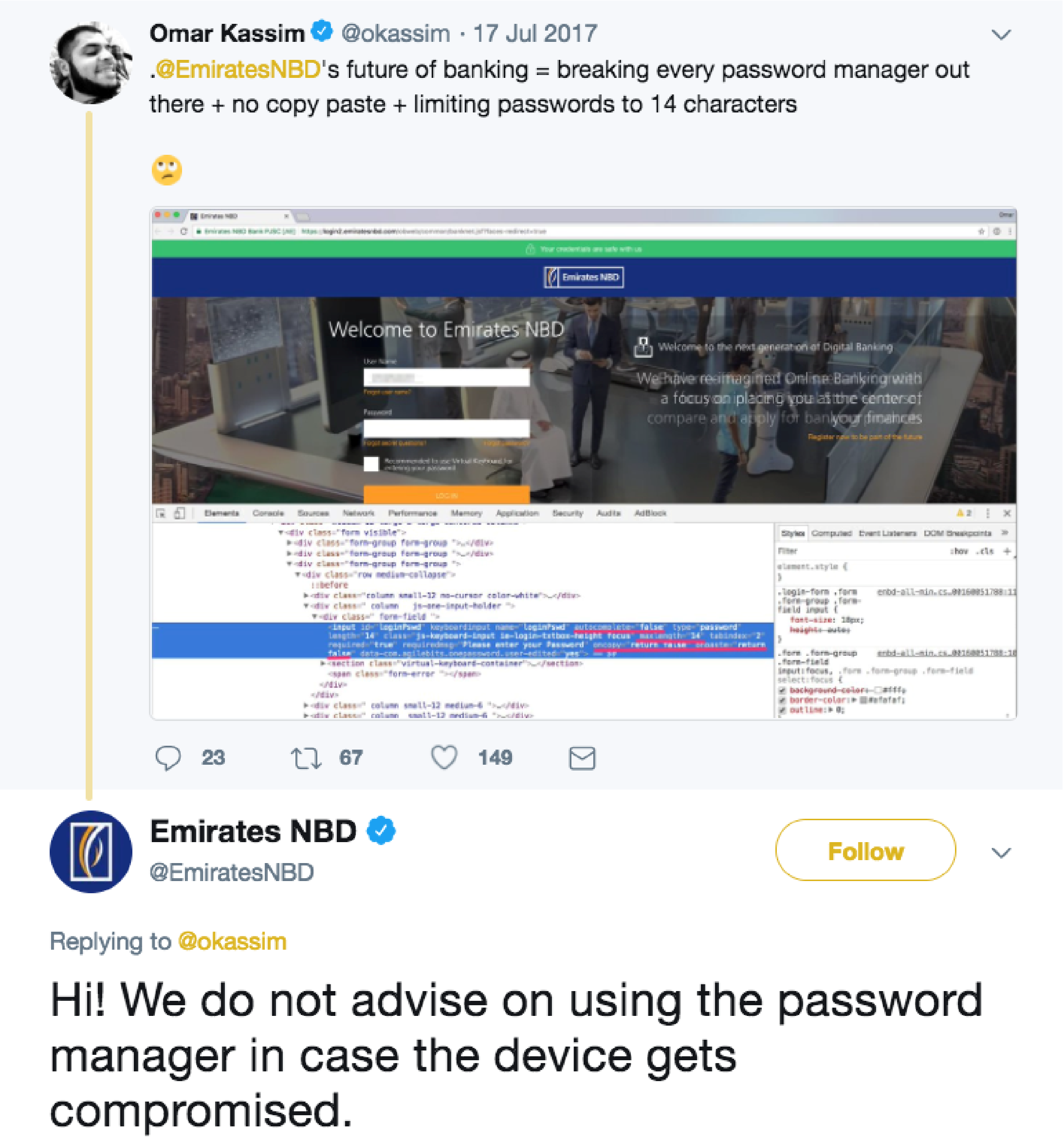
Password managers

- Many people have dozens of accounts – some have hundreds
- Password managers allow to store passwords for each website securely and copy/paste them to the browser
- They often integrate perfectly into the browser and allow you to create new passwords that you never need memorize
- You only need to remember your master password
  (and backup your password file)
  - Can of course print out the master password and keep at home

Not everyone got the memo

It is much less likely that a device gets compromised than a password guessed.

Especially if you forbid copy/paste.



Omar Kassim @okassim · 17 Jul 2017

.@EmiratesNBD's future of banking = breaking every password manager out there + no copy paste + limiting passwords to 14 characters

🙄

Emirates NBD
Your credentials are safe with us
Welcome to Emirates NBD
User Name
Password
LOG IN
Welcome to the next generation of Digital Banking
We have reimagined Online Banking with a focus on placing you at the center of compare and apply for bank your finances
Register now to be part of the future
Elements Console Sources Network Performance Memory Application Security Audits AdBlock
Styles Computed Event Listeners DOM Breakpoints

```
▼<div class="form visible">
  ▶<div class="form-group form-group ">…</div>
  ▶<div class="form-group form-group ">…</div>
  ▼<div class="form-group form-group ">
    ▼<div class="row medium-collapse">
      ::before
      ▶<div class="column small-12 no-cursor color-white">…</div>
      ▼<div class=" column   js-one-input-holder ">
        ▼<div class=" form-field ">
          <input id="loginPswd" keyboardinput name="loginPswd" autocomplete="false" type="password" length="14" class="js-keyboard-input ie-login-txtbox-height focus" maxlength="14" tabindex="2" required="true" requiredmsg="Please enter your Password" oncopy="return false" onpaste="return false" data-com.agilebits.onepassword.user-edited="yes"> == $0
          ▶<section class="virtual-keyboard-container">…</section>
          <span class="form-error "></span>
        </div>
      </div>
      ▶<div class=" column small-12 medium-6 ">…</div>
      ▶<div class=" column  small-12 medium-6 ">…</div>
```

23 67 149

Emirates NBD @EmiratesNBD

Follow

Replying to @okassim

Hi! We do not advise on using the password manager in case the device gets compromised.

Changing the password

- Outdated advice: change every month/quarter/twice a year
  - Even Australia's government guidelines still recommend that
  - Some organisations follow it slavishly

- Bad advice. Modern recommendations:
  - A strong password can remain in place for as long as the user wants to use it
  - Empirical studies have found that users are bad at creating new passwords when prompted: the passwords get weaker each time
  - Do not ask the user to change their password unless you suspect it has been compromised
  - Governments are slowly adopting this policy (e.g. the UK in 2017)

A really bad sign

- "Password must be between 8-12 characters"
  - Why would you want to restrict the user? To save space?
  - If you are storing the password in plain text: you lost already.
  - If you encrypt it: you still lost (more in a second)
  - Today, passwords are run through a hash function and only the (fixed length!) output is stored – same space requirements anyway!

Calculating the search space

- Suppose we know a password is 6 keyboard characters

- Each character is one of 46 keys, and either upper case or lower case, so 92 choices for each character

- So 92^6 possible passwords
  - About 600,000,000,000 choices to check

- How fast can we try a password?
  - People are slow: type about one per second
  - But computers are fast, so send as a message maybe 1 per microsecond (1,000,000 per second)

- Trying them all could take 600,000 seconds
  - About 7 days

Increasing the search space

- Suppose we know a password is 10 keyboard characters

- Each character is one of 46 keys, and either upper case or lower case, so 92 choices for each character

- So 92^{10} possible passwords
  - Now about 43,500,000,000,000,000,000 choices to check

- Let's keep this the same:
  - People are slow: type about one per second
  - But computers are fast, so send as a message maybe 1 per microsecond (1,000,000 per second)

- Trying them all could take 43,500,000,000,000 seconds
  - About 1.3 million years

- Four more characters significantly increased the time.

Length of the password

- Depends a bit on the use case
  - If you can employ a rate limit for password tries (e.g. you are running a website): 8 characters are minimum as of 2018
  - If the system can be accessed by an attacker without rate limit (e.g. an encrypted hard-drive they obtained): at least 14-16 characters as of 2018
  - With a password manager: you can use any length

- Character sets matter much less:
  - No need for complexity rules – just make sure the password is long and cannot be derived from a vocabulary

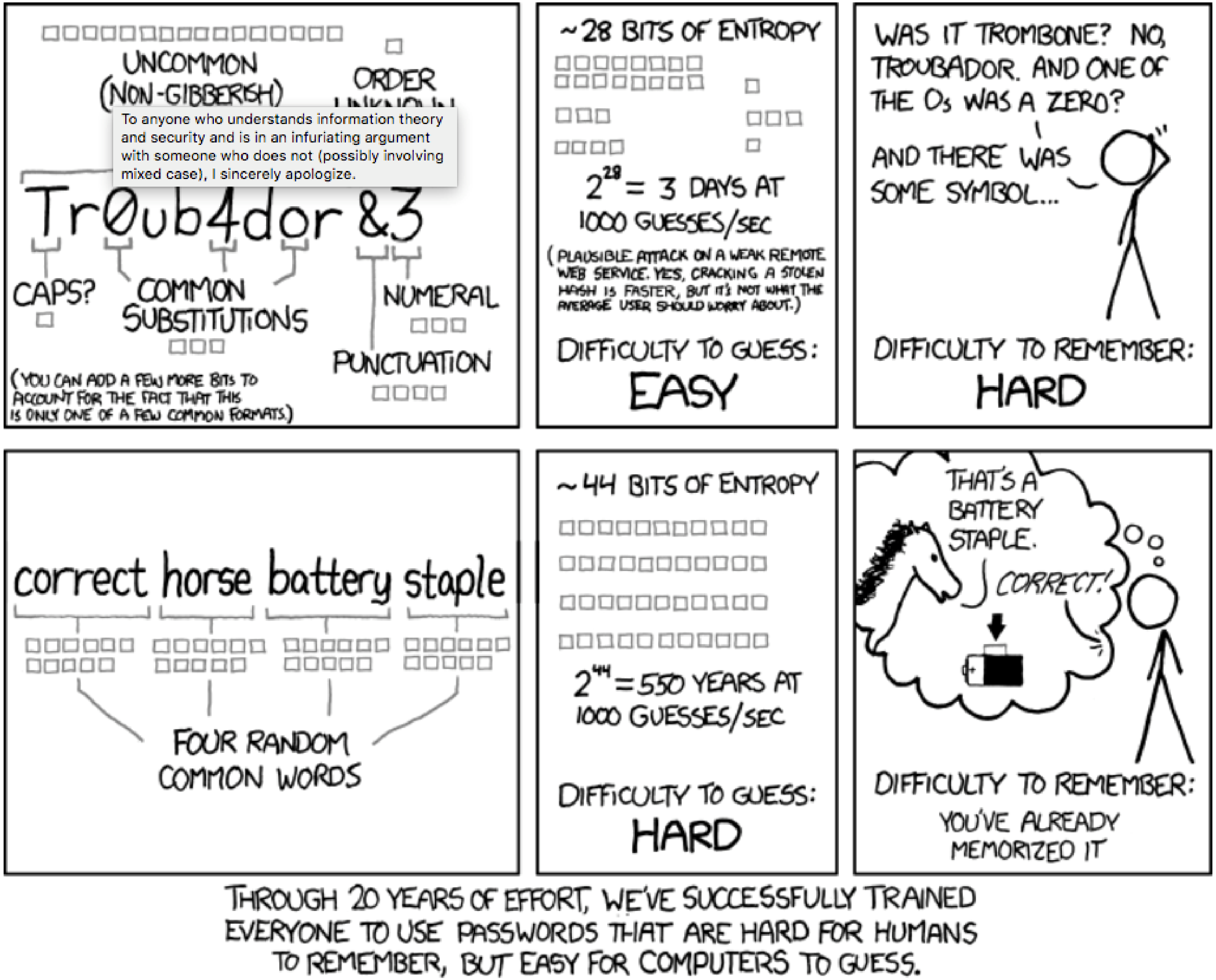
Password reuse

- Never re-use passwords across sites – if one is breached and has poor security practices, that password could be leaked. Email addresses can be leaked too, or they can be guessed.
- Again, password managers solve this.

Passphrases

- Passphrases can be a substitute for passwords, up to a certain level
- The idea is to use a sequence of unrelated words (ca. 6-7) instead of a password
  - General idea: choose randomly from long dictionary of plain words
  - Easy to remember, very reasonable security
  - Several dictionaries available, e.g. EFF wordlist
  - Simple generation methods exist (→ tutorial)
- With *n* words in the dictionary, and *k* chosen for passphrase, the adversary needs $n^k/2$ guesses
  - E.g. wordlist has 10k words, and you choose 6: attacker needs $500 * 10^{21}$ guesses

Passphrases



To anyone who understands information theory and security and is in an infuriating argument with someone who does not (possibly involving mixed case), I sincerely apologize.

UNCOMMON (NON-GIBBERISH)
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Storing passwords (repetition)

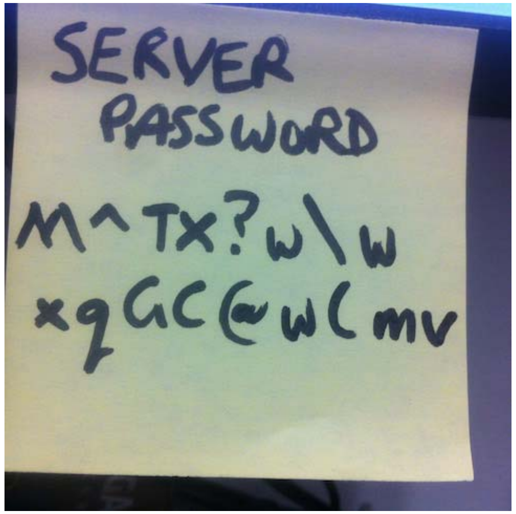
- **Never** store a password in plaintext
- The fundamental idea is to always salt and hash
  - Need for hashing is clear
  - Salting: prepend random, unique, but adversary-known string to password
- Why salting?
  - Otherwise, identical user passwords would hash to same value - attacker can spot that
  - Defend against rainbow tables: precomputed hash tables that can be downloaded freely and make password cracking (without salts) much more efficient
- Use available **tools/libraries:**
  - bcrypt and scrypt are good standards

Attack: interception

An attacker can try to find out the password by observing it.

- "On the wire" (in transit through a network) → never send unencrypted
  In the machine (see later discussion of "key loggers")
- In computer files where it is stored.

- From a physical record (Post It Note).
- As it is being used:
  - "Shoulder-surfing"
- By asking for it:
  - Phishing



Common defence: three chances

- Many software systems disallow further attempts after x number of failures (x often = 3)

- Many software systems deliberately:
  - Slow responses down after failed attempts
  - Lock out login for a time period, e.g. Apple iPhones
  - Present CAPTCHAs to stump bots
  - Email the user that someone has made multiple failed attempts

- This reduces the number of attempts per second, and reduces chance of brute-force or guided search succeeding in reasonable time.

Man In The Middle Attack

- A combination of interception and impersonation.

- Attacker intercepts messages from the user who thinks they are talking to the real system
  - But then attacker passes messages on to real system, and passes replies back to user

- User sees exactly what they expect from the real system
  - But attacker collects a lot of information (including password!)

- We will discuss such attacks in more detail in INFO3616

CAPTCHAs

- "Completely Automated Public Turing Test To Tell Computers and Humans Apart"
- Common task:
  - recognize characters in a visual image, or identify object in a picture
  - recognize types of image (e.g. distinguish signs from images)
  - In turn though, this generates data sets of classified data that can be fed into machine learning
  - Rule: machines get better at CAPTCHAs
- Attacks on CAPTCHAs
  - OCR software, image classification software etc.
  - Get humans to solve the task for the bot – cheap labour
  - Get the system to give you easier CAPTCHAs i.e. accessibility options...
- CAPTCHAs can slow down attacks; but they are no good as a stand-alone defence

Summary