

Security on the Internet



Overview

- Intro to cybersecurity
- What's your data worth?
- Who is responsible for security online?
- Protecting your data online

A large, heavy-duty metal vault door is shown open, revealing its intricate locking mechanism. The door is made of thick steel and features a complex arrangement of gears and bolts. A sign on the door provides technical specifications. The interior of the vault is visible through the circular opening, showing a metal grate and a red carpeted floor.

What makes something secure?

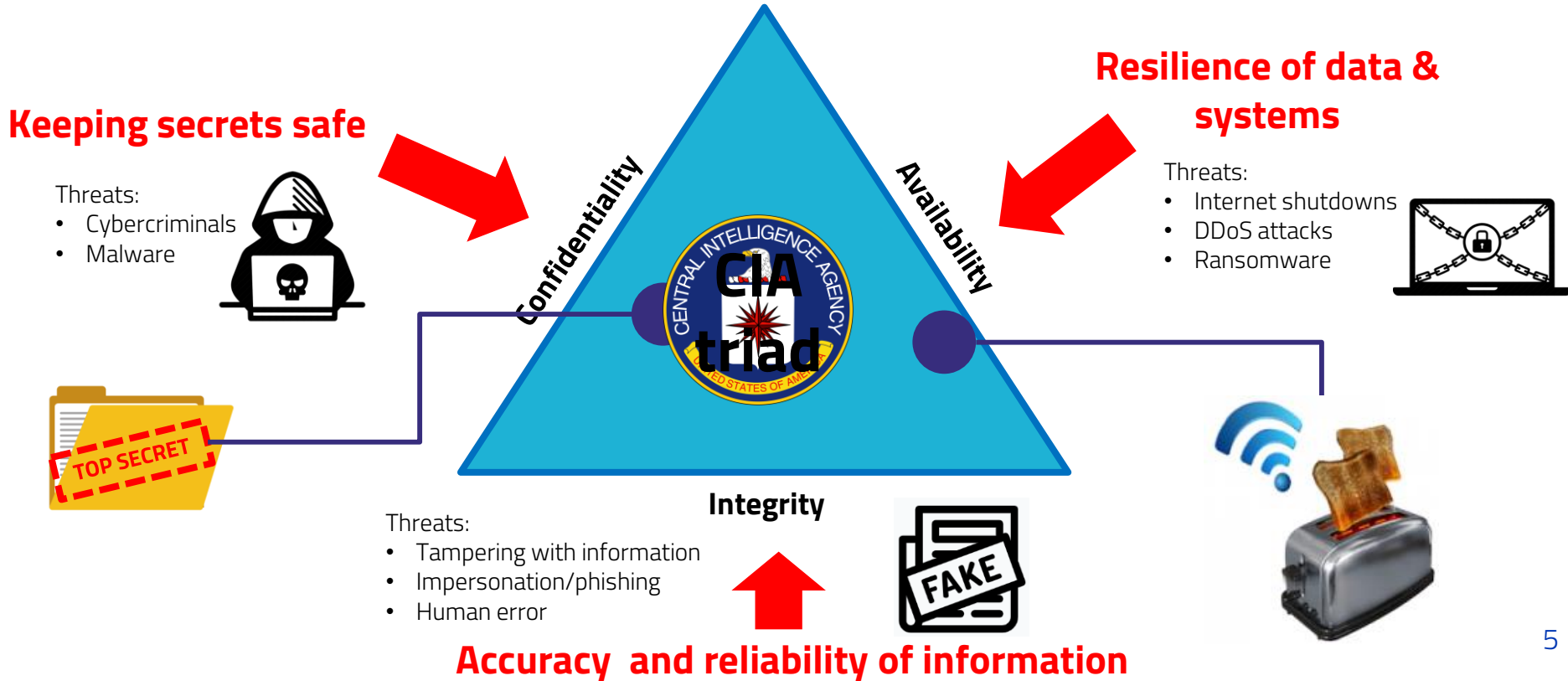
VAULT DOOR


WEIGHT: 22 1/2 Tons
THICKNESS: 22 Inches
STEEL: 11 Layers of Special
Cutting and Drill Resistant
LOCKS: 4 Hamilton Watch
Movements for Time Locks



Cybersecurity is the practice of protecting systems, networks, programs and data from attacks.

Basics of cybersecurity



A close-up photograph of a person's hands holding a large stack of US one hundred dollar bills. The bills are fanned out, showing the front side with the portrait of Benjamin Franklin. The person is wearing blue denim jeans. The background is dark and out of focus.

**What is the
most valuable
thing you own?**

The world's most valuable resource is no longer oil, but data

The data economy demands a new approach to antitrust rules



2017 – The Economist

Capital One data breach: What you can do following the bank hack

The latest banking data breach exposed the records of almost 106 million

UK mass surveillance laws do not breach human rights, tribunal rules

Facebook to be fined \$5bn for Cambridge Analytica privacy violation - reports

The \$5bn fine would be the largest Commission fine against a tech company

TECHNOLOGY INFORMATION SECURITY

'Massively negligent': children's photos, audio recordings released after toymaker VTech breach

Improving facial recognition software requires thousands of faces. But did they consent?

Share on Facebook | Share on Twitter | Email | Print

BC Science | By techn... | Posted 25 July 2019 at 3:4

Fitness tracking apps expose activity on sensitive military bases

THESE maps were supposed to be a bit of promotional fun but they could potentially reveal very compromising in

Facebook Admits It Was Used to Incite Violence in Myanmar

FBI called in to investigate FaceApp over privacy concerns

The hugely popular FaceApp has taken the world by storm, but the FBI is involved.

Bias in AI: A problem recognized but still unresolved

Curus Radfar | 1 week ago

Comment

'I felt disgusted': inside Indonesia's fake Twitter account factories

'Buzzer teams' are a growing part of politics, helping to churn up religious and racial divides

Chinese surveillance company tracking 2.5m Xinjiang residents

UK hospitals hit with massive ransomware attack

Sixteen hospitals shut down as a result of the attack

By Russell Brandom | May 12, 2017, 11:36am EDT

Domestic Abusers Are Increasingly Weaponising Smart Home Tech

Melanie Ehrenkranz

Jun 26, 2018, 2:00pm - Filed to: domestic abuse

Share | Facebook | Twitter | LinkedIn | StumbleUpon | RSS

news | JANUARY 30, 20

target list for cyber-



Capital One data breach: What you can do following the bank hack

The latest banking data breach exposed the records of almost 106 million

UK mass surveillance laws do not breach human rights, tribunal rules

Rights groups brought case against CCHQ after Snowden revelations

Facebook to be fined \$5bn for Cambridge Analytica privacy violation - reports

The \$5bn fine would be the largest Commission fine against a tech company

TECHNOLOGY INFORMATION SECURITY

'Massively negligent': children's photos, audio recordings released after data breach

Improving facial recognition software requires thousands of faces. But did they consent?

Share on Facebook Share on Twitter

technology gadgets > wearables

BC Science By technologist posted 25 July 2019 at 3:4

Fitness tracking apps expose activity on sensitive military bases

THESE maps were supposed to be a bit of promotional fun but they could potentially reveal very compromising information

Facebook Admits It Was Used to Incite Violence in Myanmar

Bias in AI: A problem recognized but still unresolved

Curus Radfar 1 week ago

Comment

FBI called in to investigate FaceApp over privacy concerns

The hugely popular FaceApp has taken the world by storm, but the FBI is investigating

'I felt disgusted': inside Indonesia's fake Twitter account factories

Deep fakes/fake news

'Deep fakes' are a growing part of politics, helping to churn up anger and racial divides

Bias and discrimination

Chinese surveillance company tracking Xinjiang residents

Political interference

TECH CYBERSECURITY

Massive ransomware attack

Sixteen hospitals shut down as a result of the attack

By Russell Brandom May 12, 2017, 11:36am EDT

Freedom of choice

Abusers Are Increasingly Weaponising Smart Home Tech

Abuse and cybercrime

Domestic abuse

Share f t in

news JANUARY 30, 20

target list for cyber-



What do these websites have in common?



2008 - 360 million accounts

2014 - 4.6 million accounts breached



2013 - 153 million accounts breached

Adobe



2014 - 3200 accounts breached



2012 - 43 million accounts breached



2016 - 164 million accounts



2017 - 57 million accounts



2018 - 29 million accounts



2012 - 3 billion accounts

2018 - 100 million accounts



2013 - 50 million accounts



2014 - 145 million accounts



2013 - 65 million accounts



2014 - 5,176,463 accounts breached



2017 - 17 million accounts breached

The Cloud – Someone else's computer



Google data centre – Iowa, USA

- Anyone can start a cloud service, website or application
- Data protection laws in different countries
- The company may sell or access your data

>100 million users

A Russian-owned company



CEO – 40-year old Yaroslav
Goncharov
Team of 12 people

What data is collected?

Photos, Analytics information, Cookies



FaceApp



Where is the data?

United States and countries in which FaceApp,
its Affiliates or Service Providers maintain
facilities



What are they doing with the data?

Sharing with FaceApp Affiliates, Service Providers,
third-party advertising partners.
Perpetual licence to the data.



How are they securing the data?

“We use commercially reasonable safeguards”
“FaceApp cannot ensure the security of any
information you transmit to FaceApp or guarantee
that information on the Service may not be
accessed, disclosed, altered, or destroyed.”



The Treacherous 12

1. Data breaches
2. Insufficient identity, credential, and access management
3. Insecure interfaces and APIs
4. System vulnerabilities
5. Account hijacking
6. Malicious insiders
7. Advanced persistent threats
8. Data loss
9. Insufficient due diligence
10. Abuse and nefarious use of cloud services
11. Denial of service
12. Shared technology issues



How much is your data worth?

- Driver's licence - \$20
- Netflix account - \$4
- Credit card details - \$5-110
- PayPal credentials: \$20-200
- Email addresses and passwords: \$0.70-\$2.30
- Medical record - up to \$1000
- Passports - \$1000-2000

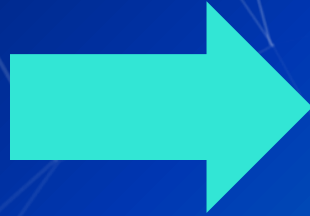
The screenshot displays several listings for data breaches on an online marketplace. The listings include:

- Uber Account:** [MS] Uber 0.5 cheap RANDOM country, 100% CC attached, AUTO. Item # 15697 - Accounts & Bank Drops - PissedM0f0 (1961). Buy price: USD 0.40 (0.0016 BTC). Views: 944 / Bids: Fixed price. Quantity left: Unlimited.
- Ebay Accounts:** Selling Ebay Accounts With Low And HIGH Feedback.. Item # 2544 - Accounts & Bank Drops - Dwaze (342). Buy price: USD 0.00 (0.0000 BTC). Views: 3441 / Bids: Fixed price. Quantity left: Unlimited.
- Zomato Database Breach:** Zomato Database Breach (17 millions entries, md5 encryption). Price: USD 1,001.45 (including 1.45 transaction fee). In stock. Shipping options: Please select an option... Vendor: nclay (+0) [Level 1 (9)]. Class: Digital.
- Myspace 360M:** Myspace 360M. By peace_of_mind (100.0%) [Level 1 (14)]. Price: 0.60000 / BTC 6.0000. A red circle highlights the price "0.60000 / BTC 6.0000". To the right, a red text overlay reads "6BTC = \$2800 (2013)". Postage Option: [dropdown]. Escrow: Yes, escrow by RealDeal is available. Class: Digital.

IDENTITY THEFT

Short Term

- Fraud
- Financial Loss
- Reputational Damage
- Personal Security risks
- Rise in other crimes



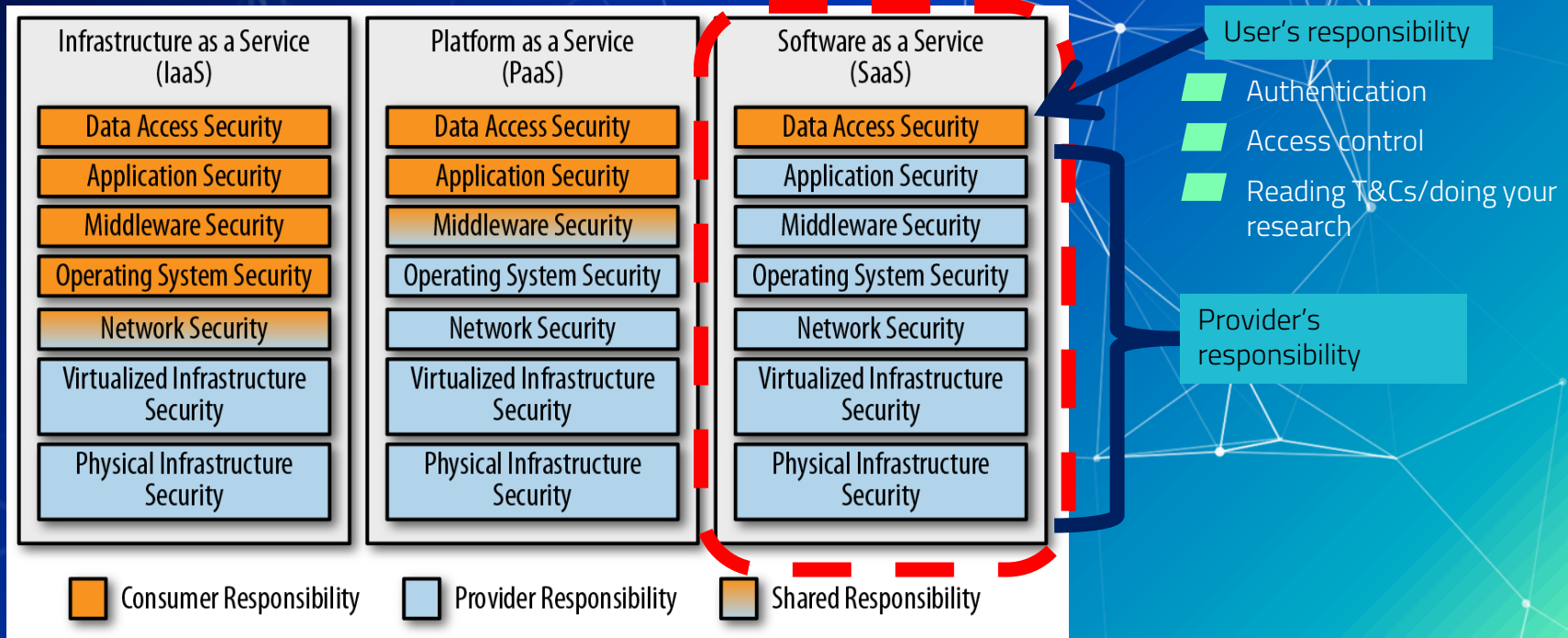
Long Term

- Issues with background checks
- Difficulty getting loans
- Damage to credit score



**Who is responsible
for security on the
internet?**

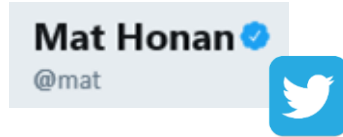
Shared responsibility model



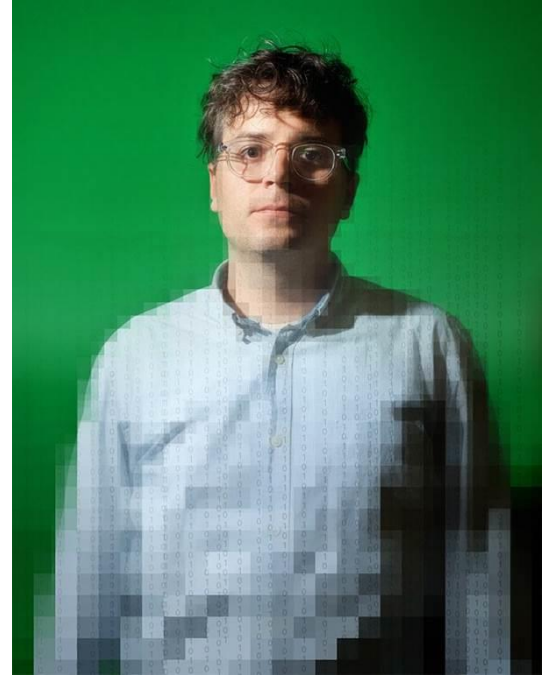
One hour to destroy a digital life

One hour to compromise iCloud, Google, Amazon and Twitter accounts.

The target:



1. The hacker collected name, address and email from public websites online.
2. Hacker called Amazon, using online information to impersonate Honan and add a credit card number to his account, then called a second time and used that card as identification to add a new email address.
3. On Amazon, he could see Honan's credit cards and had enough information to reset his Apple iCloud account.



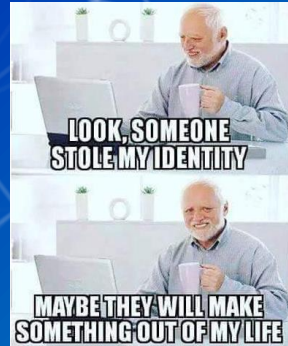
Mat Honan, Wired Magazine Technical Writer



Personal information
is like money. Value it.
Protect it.



Own your online
presence



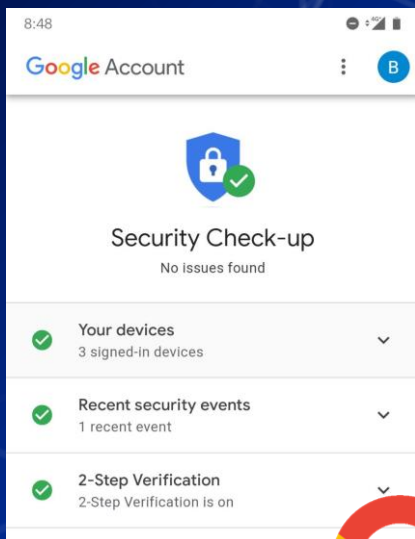
Lock down your login



Quick wins for securing your accounts

Google Security Checkup

<https://myaccount.google.com/intro/security>



Download a password manager



Search yourself and adjust your privacy settings



What if I have been hacked?

How will I know?

- Suspicious activity on your email, bank account or application
- Notification from the website owner
- Check Have I been Pwned and sign up to be notified

What to do?

- Change passwords or contact the website if you can't access your account
- Check logged on sessions
- Notify your bank if financial information is involved
- Inform the police if you have been a victim of identity theft

<https://haveibeenpwned.com/>

';--have i been pwned?

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

example@example.com

pwned?

Oh no — pwned on 2 sites!

Are you creating strong, unique passwords on all sites?



Adobe

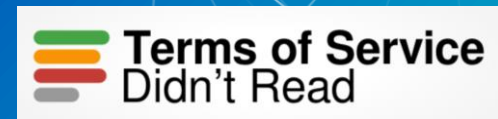
The big one. In October 2013, 153 million accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.



Stratfor

In December 2011, "Anonymous" attacked the global intelligence company and consequently disclosed a veritable treasure trove of data including hundreds of gigabytes of email and tens of thousands of credit card details which were promptly used by the attackers to make charitable donations (among other uses). The breach also included 860,000 user accounts complete with email address, time zone, some internal system data and MD5 hashed passwords with no salt.

More information



THANKS!

What is valuable to you and how are you going to protect it?

