Security Not Guaranteed

Or, how to hold off the bad guys for another day.

A Presentation for B-Sides CLE

This Talk is NOT About…

A. Protecting Against Three Letter Agencies (KGB, FSB, CIA, NSA, FBI, DOJ)
B. Protecting Against a Targeted Attack
C. Protecting Your Corporation
D. How The Cloud Is Evil And Should Be Avoided At All Costs™

Would it surprise you if…

67% of consumers…

Don't have password protection on their devices.

(Sophos, August 2011)

Now, this *isn’t* a problem in itself…

But, it can be *disastrous* if your device is LOST or, STOLEN.

All devices can be

`Password Protected`

{ 9/10 }

The estimated number of **break-in** attempts that would be thwarted if people simply **locked** their computers.

And, it doesn’t have to be too **complicated**.

The password:

```
do graze irk
```

has **49 bits** of **entropy.**

It’s also a password that can be **remembered**, in some way.

And it can be typed fairly **quickly**.

It really takes about as much **effort** as:

`password1234`

But, is far more **secure**.

Now, you’re probably wondering about fingerprint unlocks:

My Friend Taylor Swift will talk about that.

Remember: Fingerprint locks are convenient, but they discard your ability to "forget" or refuse to unlock a device. They remove consent.

Used the hilarious ‘Swift on Security’.

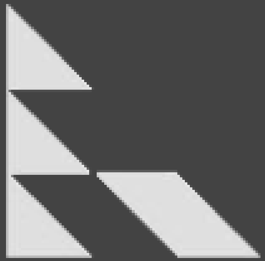
✓

Passwords are a start.

How do you keep your passwords together?

Believe it or not...

Some people still use pencil, and paper, or try to keep it in their heads.



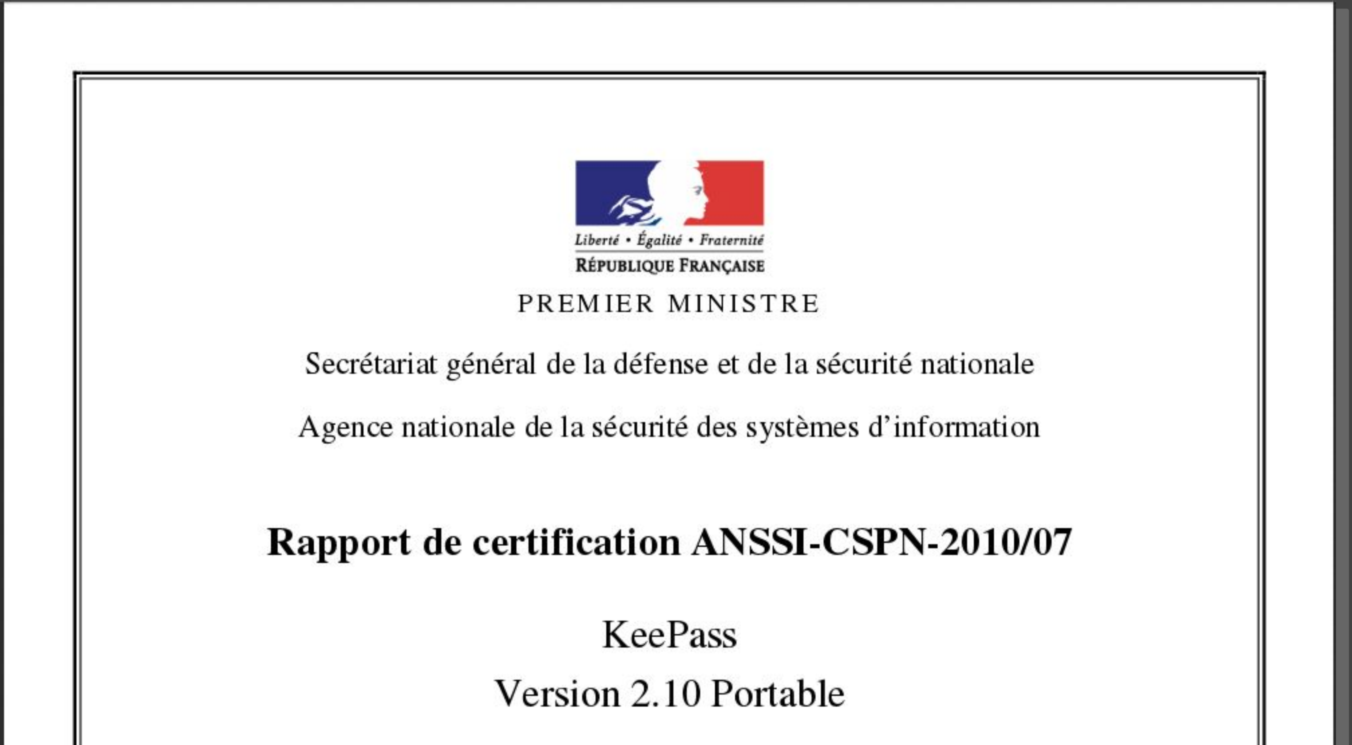
There are a lot of **good** password managers.

Raise your hand
if you’re using **KeePass**.

KeePass is very popular.

KeePass is also probably not secure.

The French ANSSI Did an Audit...



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

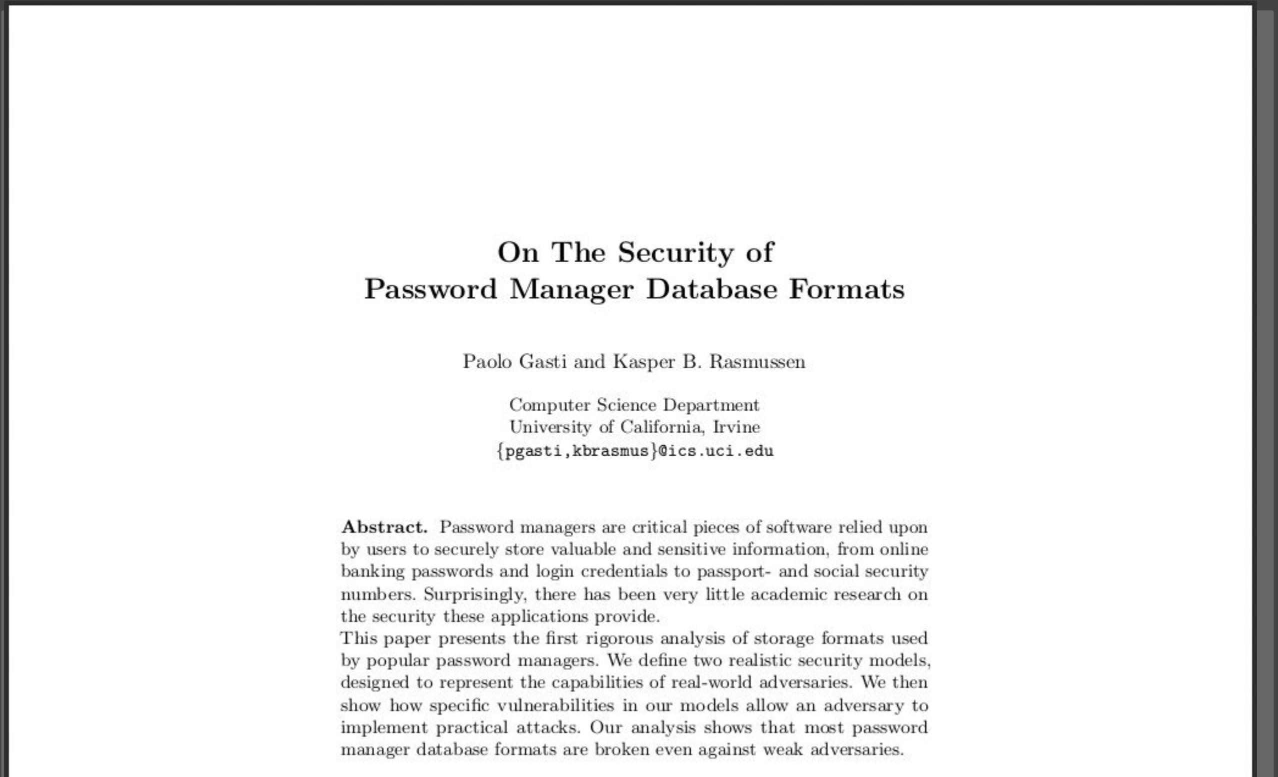
Rapport de certification ANSSI-CSPN-2010/07

KeePass

Version 2.10 Portable

And it **checked** out.

There’s a little more to it though.



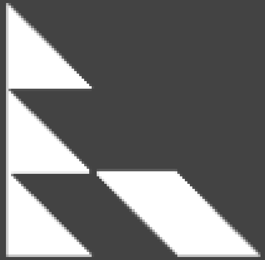
On The Security of Password Manager Database Formats

Paolo Gasti and Kasper B. Rasmussen

Computer Science Department
University of California, Irvine
{pgasti,kbrasmus}@ics.uci.edu

Abstract. Password managers are critical pieces of software relied upon by users to securely store valuable and sensitive information, from online banking passwords and login credentials to passport- and social security numbers. Surprisingly, there has been very little academic research on the security these applications provide.
This paper presents the first rigorous analysis of storage formats used by popular password managers. We define two realistic security models, designed to represent the capabilities of real-world adversaries. We then show how specific vulnerabilities in our models allow an adversary to implement practical attacks. Our analysis shows that most password manager database formats are broken even against weak adversaries.

KeePass has a lot of problems.



Which really apply to **all** of these.

Password managers are *flawed*.

It doesn’t often matter to the consumer which manager they use.

Just as long as it works.

For consumers stuff like LastPass is a good start.

Just as long as it’s not a notebook.

Mr. T. pities the fool who doesn’t have a password manager.

Used Mr. T. in a Serious Presentation

✓

Mentioning passwords...

Device **encryption** is an important security tool.

Many people fail to encrypt even the most important data.

Or, **overlook** critical points.

You can encrypt almost anything.

Desktops, phones, tablets; OS X, Windows, Linux, even BSD.

Device encryption starts fights.

If you do it, do it right.

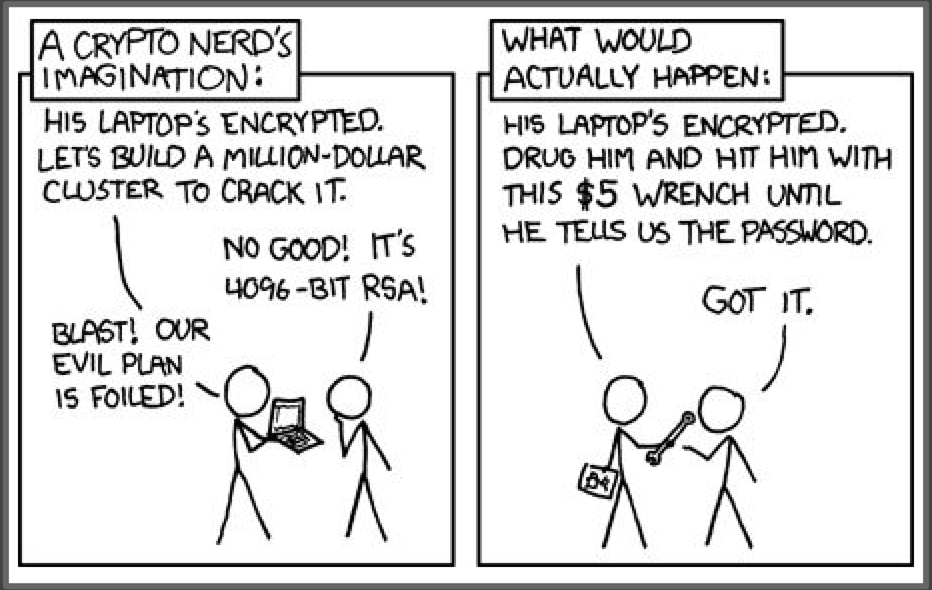
Hurricane Labs gave a presentation last year with pointers we all should know.

Self encrypting, is self decrypting.

Make sure the password is requested on boot.

Sometimes built in tools are the best you’ve got.

It’s still just a **deterrent.**


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Clichéd Use of XKCD in a Serious Presentation

Enough about passwords.

Let’s talk about two-factor authentication.

First off, what is it?

Something you know.	**Password.**
Something you have.	**RSA token.**
Something you are.	**Fingerprint.**

Something you pretend to be.

Happy.

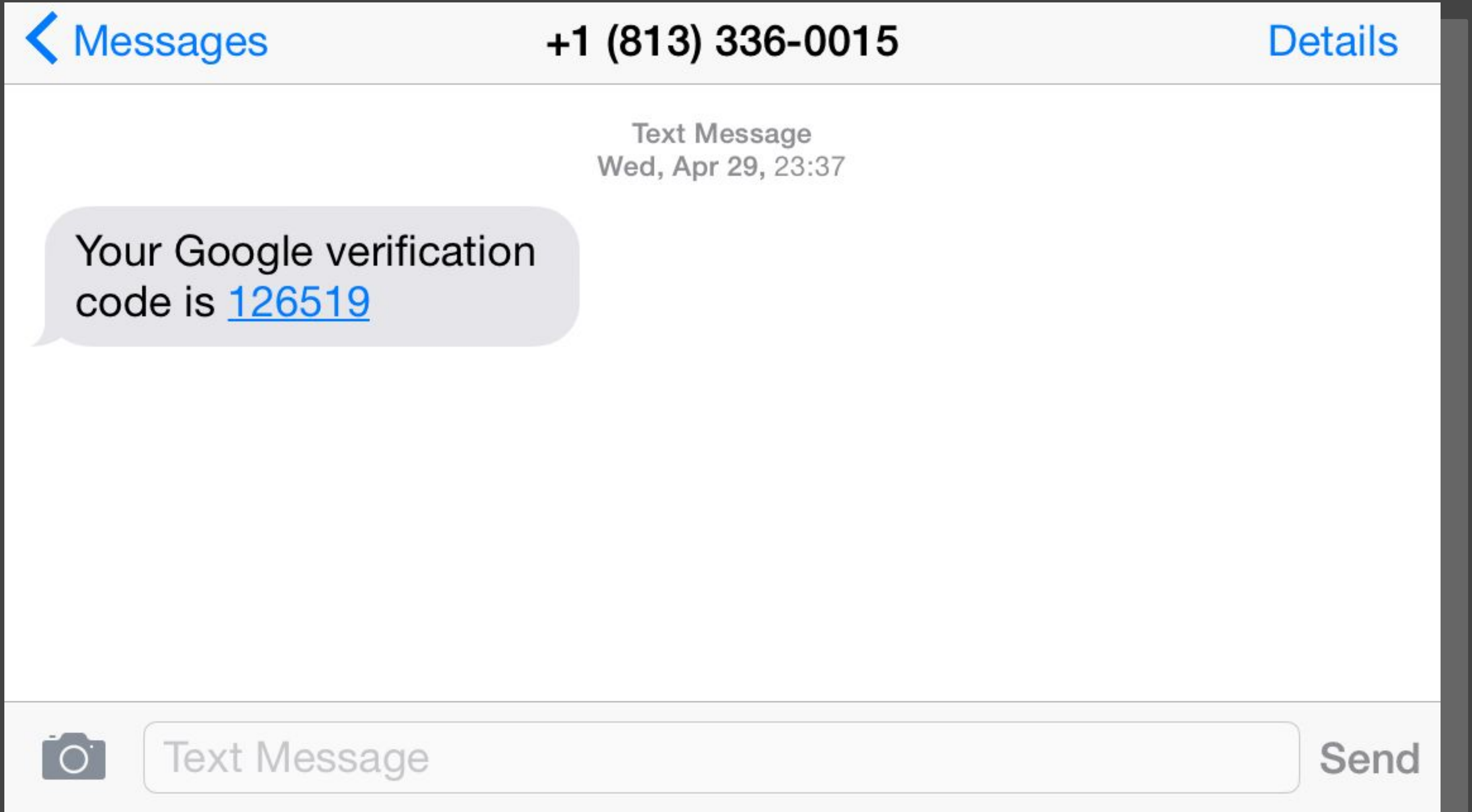
Now we know **what** it is...

Let’s talk about why.

It’s mostly to make your password half-useless.

There are many different “**tokens**”.

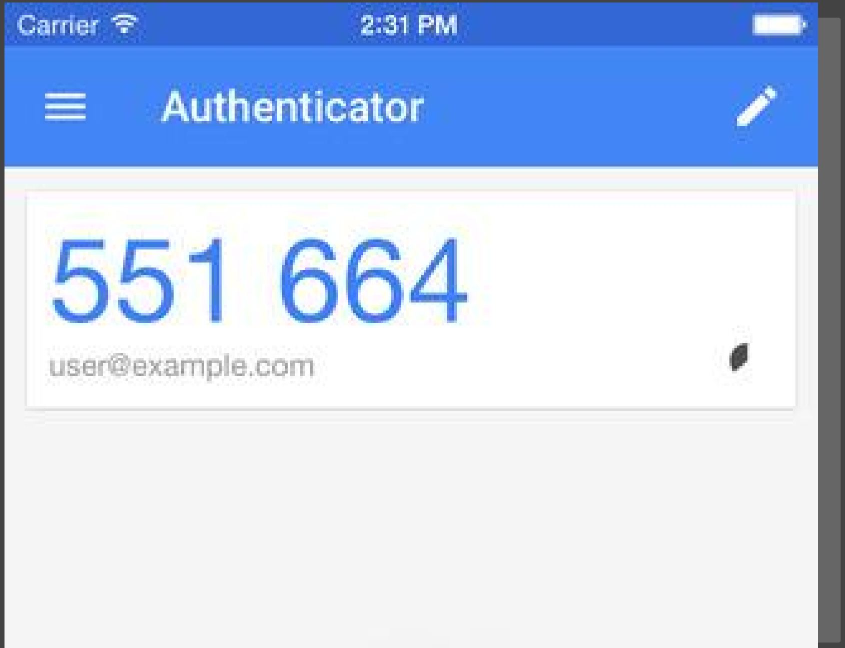
The Text Message



Text Message
Wed, Apr 29, 23:37

Your Google verification code is 126519

The App



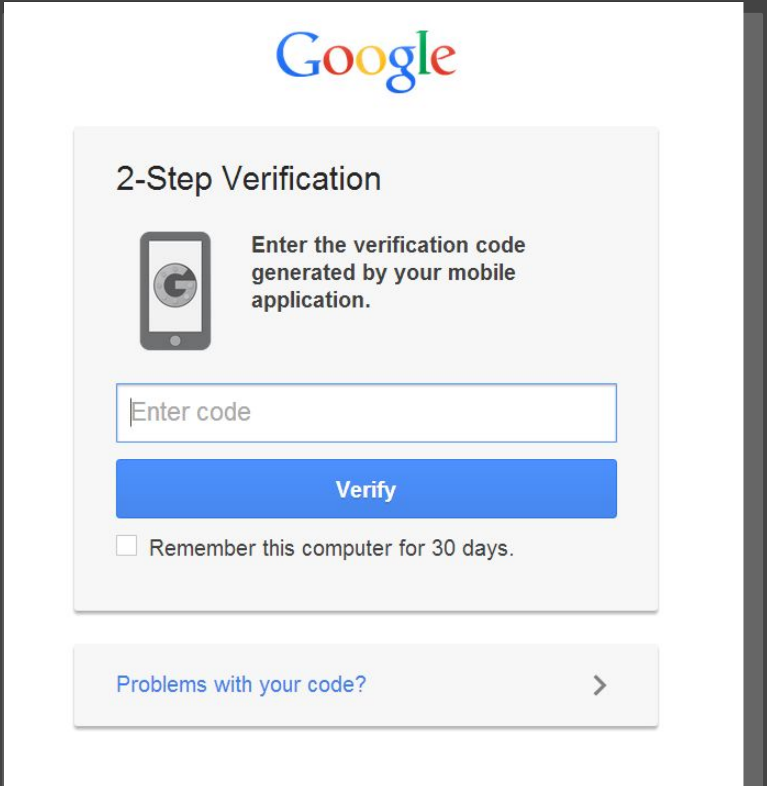
Carrier

2:31 PM

Authenticator

551 664

user@example.com

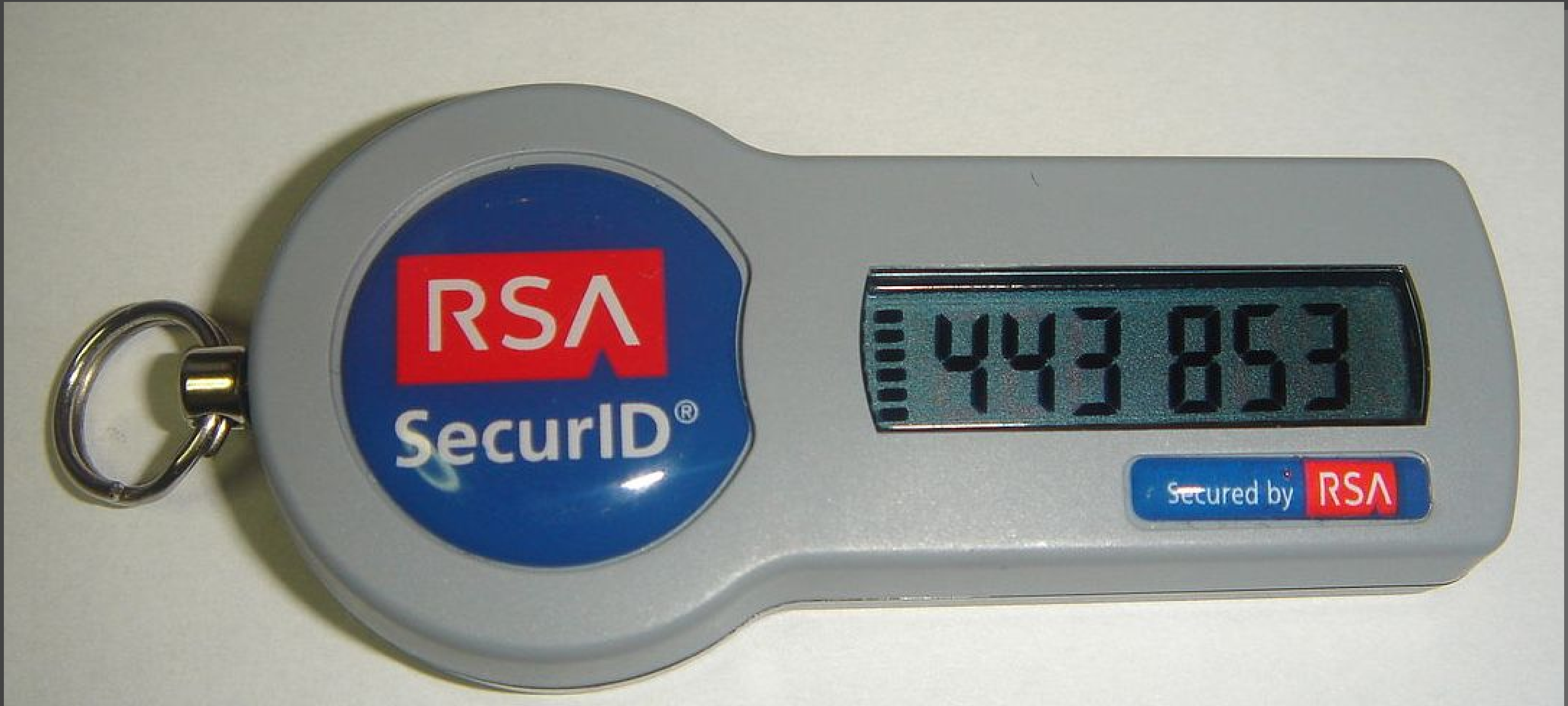


2-Step Verification

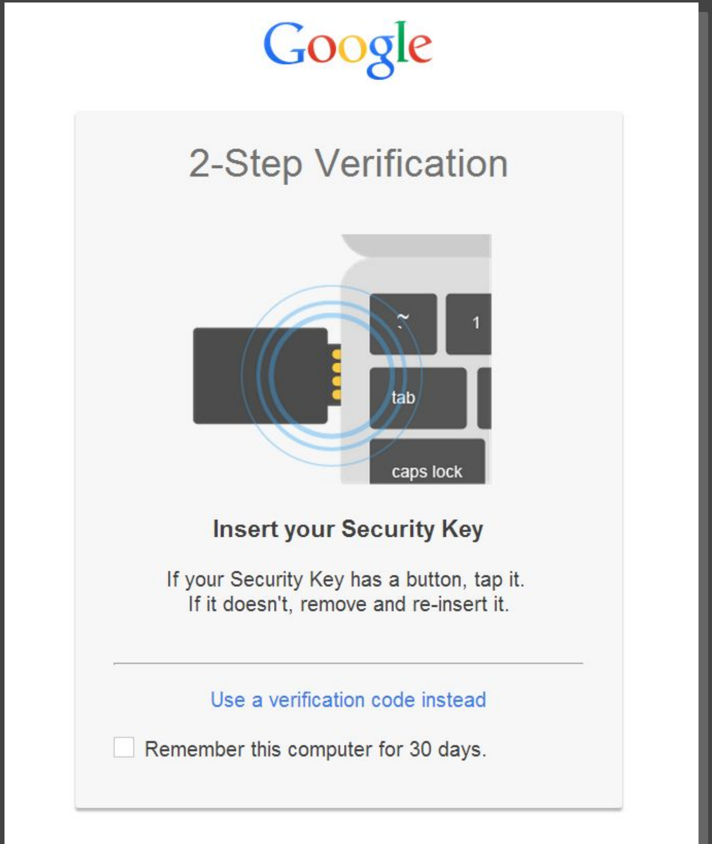
Enter the verification code generated by your mobile application.

□ Remember this computer for 30 days.

The RSA Token



The Hardware Token



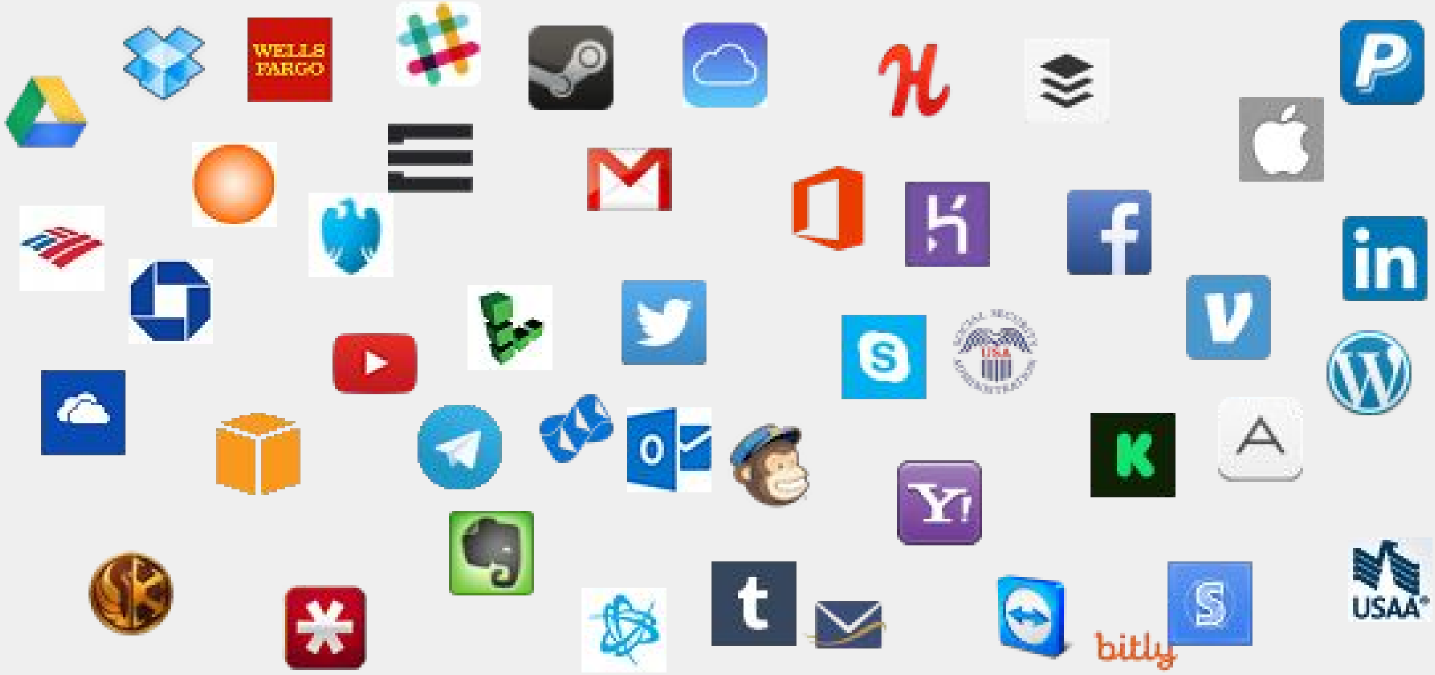
2-Step Verification

Insert your Security Key

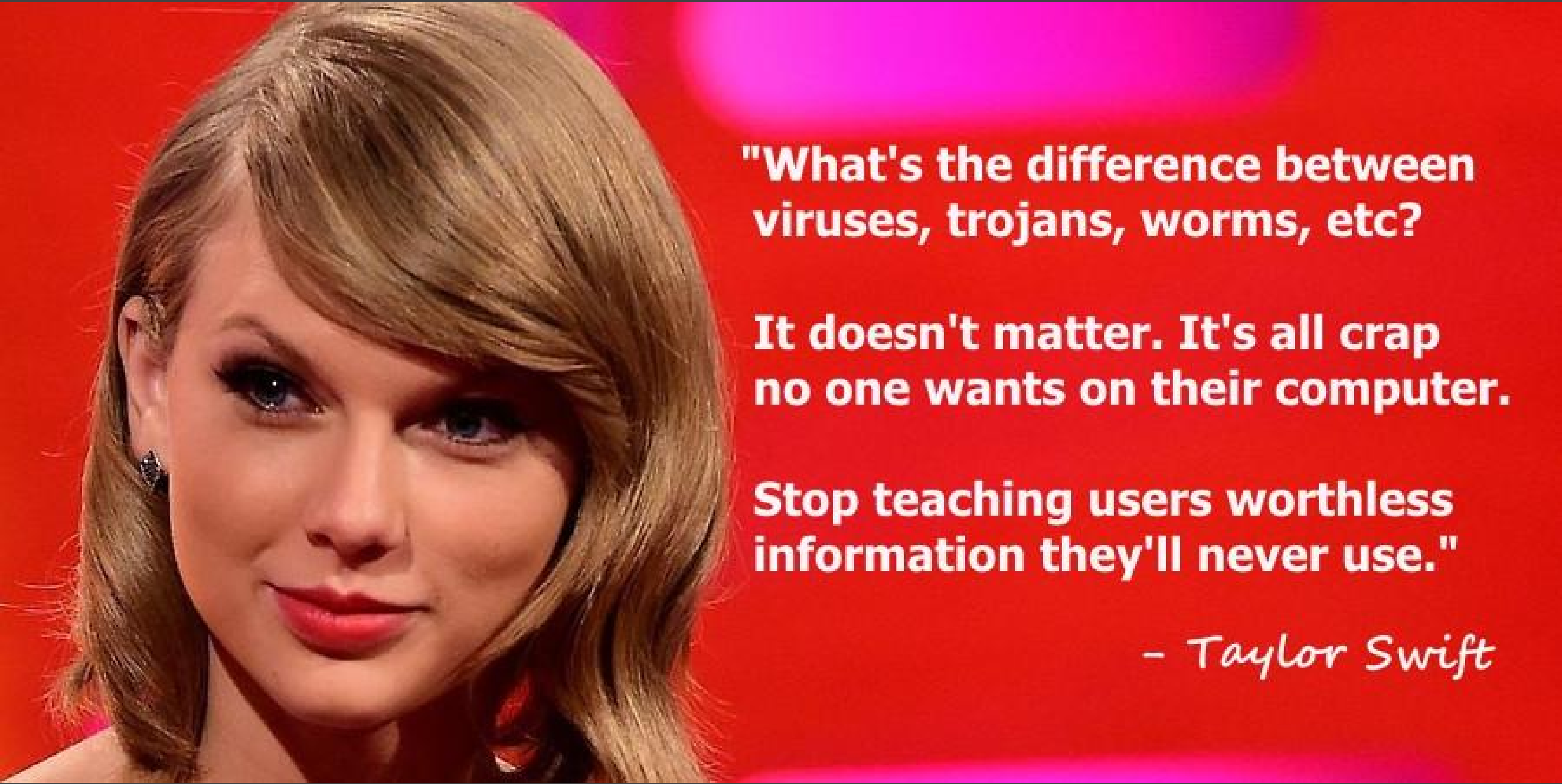
If your Security Key has a button, tap it.
If it doesn't, remove and re-insert it.

Use a verification code instead

□ Remember this computer for 30 days.


WELLS FARGO
USAA
bitly
Y!

Malicious Program Protection



"What's the difference between viruses, trojans, worms, etc?

It doesn't matter. It's all crap no one wants on their computer.

Stop teaching users worthless information they'll never use."

– Taylor Swift

Securi-Tay’s actually a little **wrong** there.

There are different kinds of threats, and different solutions.

Anti-Malware
Versus
Anti-Virus

It helps consumers to understand the threats out there.

It helps to have multiple lines of defense.

There are some fairly **decent** products.

And, some **questionable** services.

Product choice starts fights.

There are different measures of **success**.

Nothing’s **perfect**.

Remember how we said we don’t like Kaspersky?

Fin.

Resources page is at:

j.mp/SecurityNotGuaranteed