Security Tokens

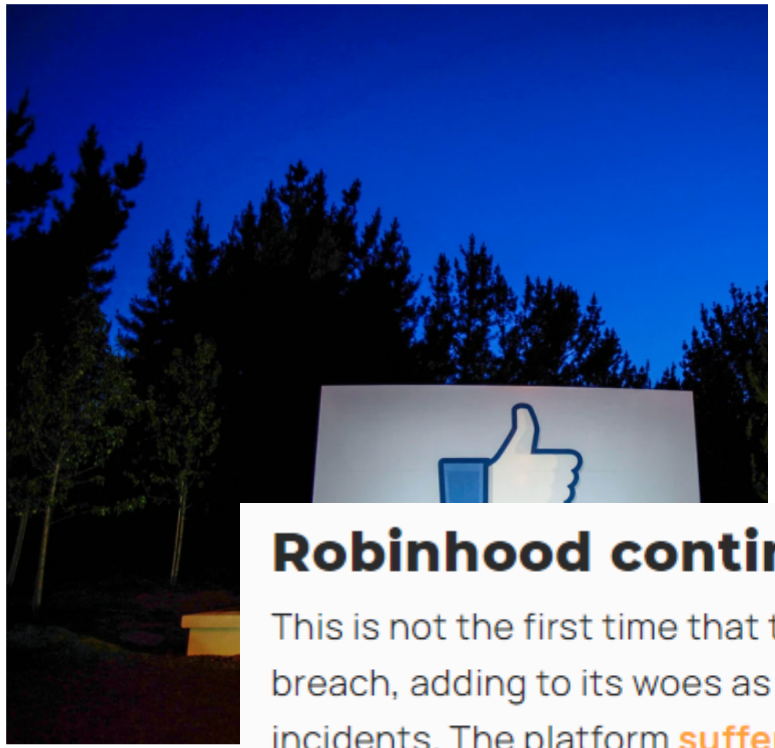
Security without remembering the password.

Problem with traditional passwords

- Password reuse
- Passwords are hard to remember
- Forces you to have to trust third parties

Facebook admits it stored 'hundreds of millions' of account passwords in plaintext

Zack Whittaker @zackwhittaker / 5:58 PM GMT+2 • March 21, 2019



Google Has Stored Some Passwords in Plaintext Since 2005

On the heels of embarrassing disclosures from Facebook and Twitter, Google reveals its own password bugs—one of which lasted 14 years.

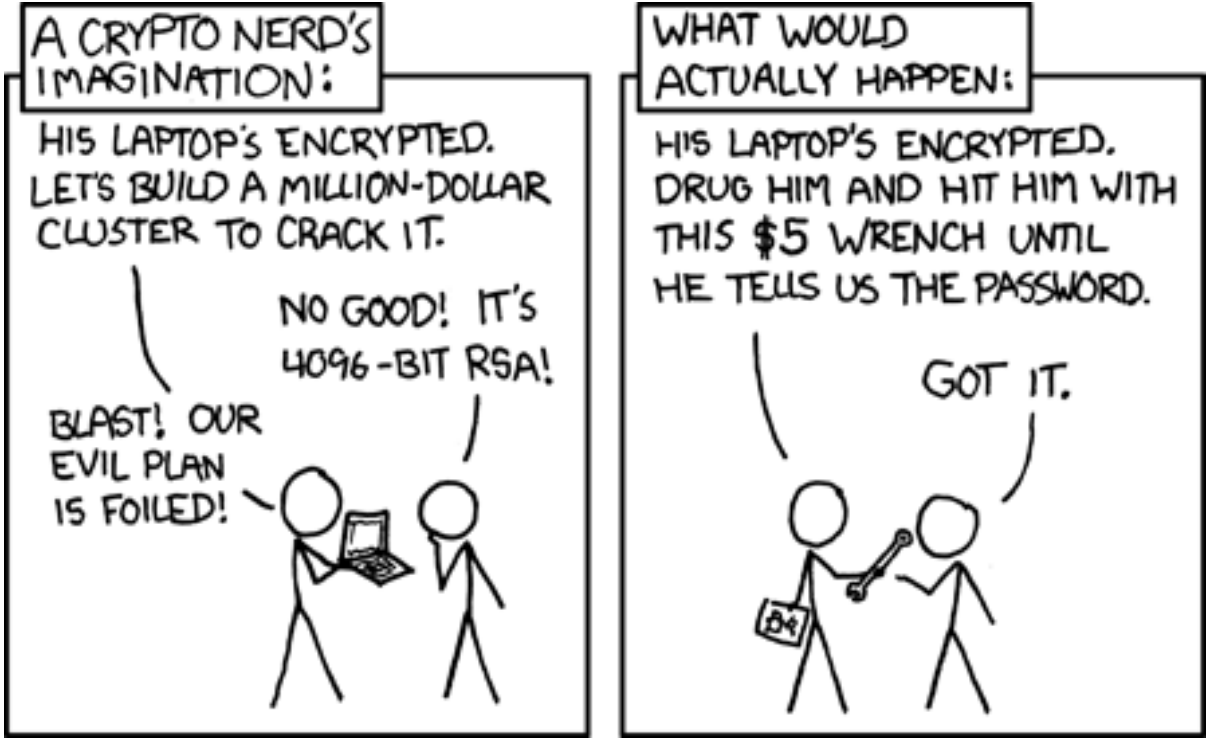
Robinhood continues to take reputational hits

This is not the first time that the popular trading platform has suffered a data breach, adding to its woes as it suffers from reputational hits for this and other incidents. The platform suffered a major breach in 2019 — which was a result of passwords being stored in plaintext.

Problem with traditional passwords

- Password reuse
- Passwords are hard to remember
- Forces you to have to trust third parties
- The user (You) knows the passwords

Problem with traditional passwords



Problem with traditional passwords

- Password reuse
- Passwords are hard to remember
- Forces you to have to trust third parties
- The user (You) knows the passwords

Problem with traditional passwords

- Password reuse
- Passwords are hard to remember
- Forces you to have to trust third parties
- The user (You) knows the passwords

Alert Message from Amazon.com

A

amazon<accounts@mazon.com>
Fri 6/28/2019 3:16 AM

Dear Customer,

We are contacting you to remind you that on 20th June 2019 we identified some unusual activity coming from foreign IP address 265.456.23.1 (located in Africa).

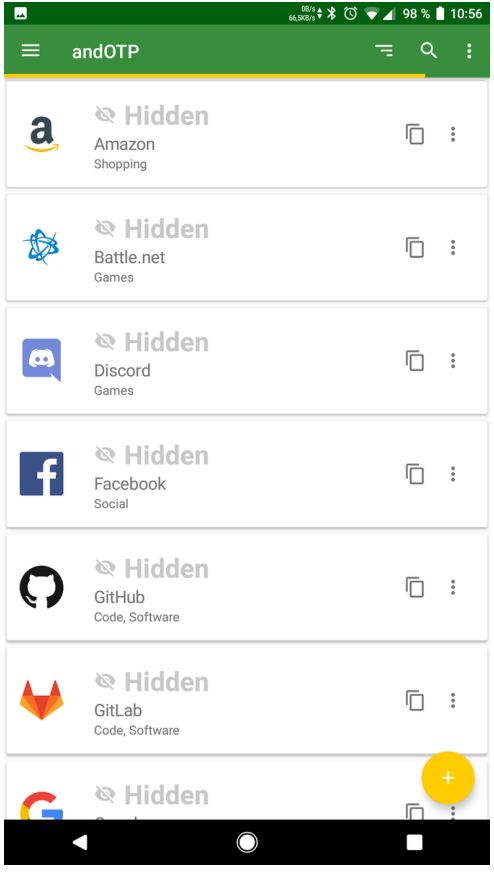
In order to prevent any fraudulent activity from occurring we are requiring to open investigation into this matter. According to site policy you will have to confirm that you are the real owner of amazon account by completing the following form or else your account will be marked as fraudulent, and we will have to terminate the account.

https://www.amazon.com/userdata/accounts/security/fraud-prevention

https://bit.ly/2XCDhQD

We hope you found this message to be useful. However, if you'd rather not receive future e-mails or this sort from Amazon, please visit the opt-out link below
https://www.amazon.com/gp/gss/o/4337ddfds.32hdhd

Security Tokens



Security Tokens

What are Security Tokens(a.k.a. Authentication device)

- Peripheral devices that allow us to login to a restricted electronic resource(PC, Server, Electronic Wallet, Password Storage)
- Some of them store a cryptographic key that is used to generate a signature, or biometric data. Others store passwords.
- Although you can create your own security key, you can can also buy one. Bought keys usually have anti-tampering mechanisms.
- Might incorporate features like USB, NFC,RFID,Bluetooth.

Token Types

- Static

  Device contains the password. Said device is required for each authentication.
- Synchronous

  Relies on the system clock to generate a token, device and server must have synchronized time.
- Asynchronous

  A One time password is created without the use of a clock.
- Challenge response

  Proving someone has the Private key by using the Public Key.

- Connected/Disconnected
- SmartCards
- Programmable
- Contactless
- → Bluetooth,RFID,NFC…

There are many types of security tokens for various uses…

Security Keys - Like unlocking your door

- Typically they require you only plug the device.
  (Note: plugging your device is not necessary in some cases)
- Authentication information is transmitted to your device and you are in.
- More advanced devices my include support for freatures like FIDO2, OTP, U2F
- You can easily make your own out of any USB stick but it will be inherently less secure

Security Key example

```
[09:30] ~ -> su usbuser
* pam_usb v0.5.0
* Authentication request for user "usbuser" (su)
* Device "USBKEY" is not connected.
* Access denied.
Password:
su: Authentication failure
[09:32] ~ -> su usbuser
* pam_usb v0.5.0
* Authentication request for user "usbuser" (su)
* Device "USBKEY" is connected (good).
* Performing one time pad verification...
* Regenerating new pads...
* Unable to update pads.
* Access granted.
[usbuser@T440s john]$
```

USBKEY connected

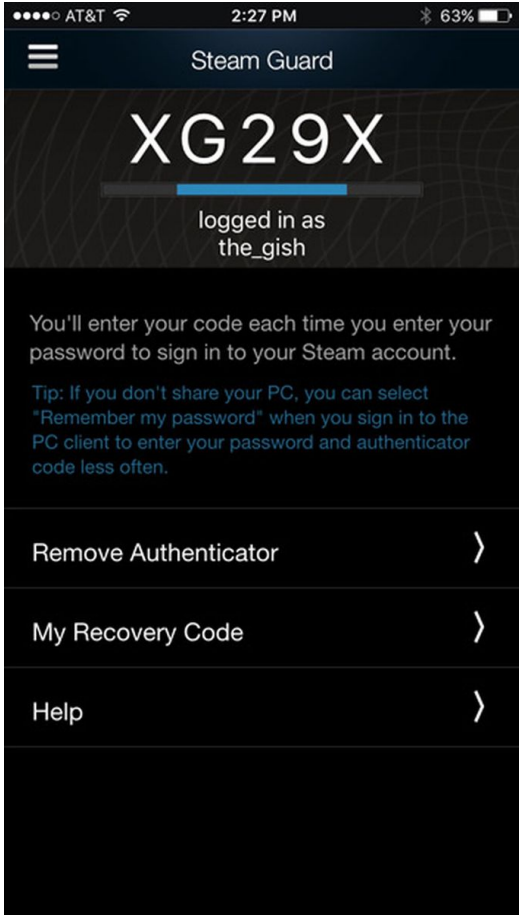
```
[09:38] ~ -> sudo su usbuser
* pam_usb v0.5.0
* Authentication request for user "usbuser" (su)
* Device "USBKEY" is not connected.
* Access denied.
[usbuser@T440s john]$
```

One Time Password - Useless after a minute.

One Time Password(OTP) make use of (pseudo)randomness to generate a code you can use to login.

- They can take the form of Synchronous tokens(TOTP),Asynchronous Tokens, and even Challenge responses
- Can come in the form of SMS messages, specific applications(Soft Tokens) or even specific Hardware devices.

E-Mail	GabeN@valvesoftware.com
Password	MoolyFTW



Smart Card - The name's Bond, James Bond

- Extremely cheap to make
- Not really secure
- Perfomance limited due to the fact they are low power
- Also can be contactless

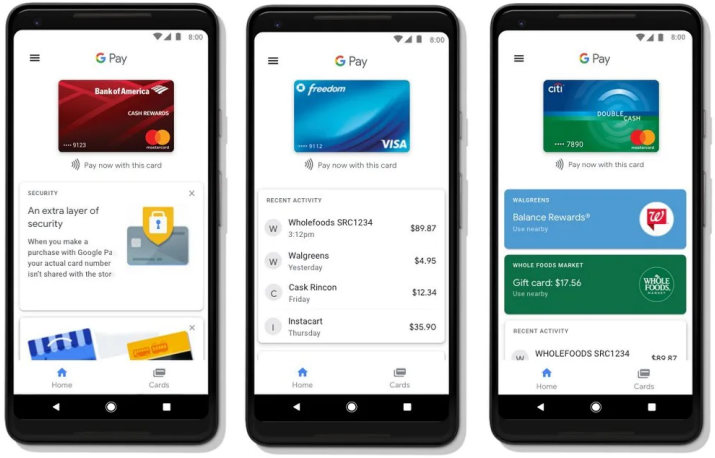
Complex Card - This isn't even my final form

- Unlike Smart Cards they have way more features including RFID Blocking,OTP,and whatnot.
- Are way more expensive
- Used to be cards with batteries
- For all intents and purposes are now probably part of your phone for extra security

Programmable - Your Phone

It is safe to assume majority of people own complex high performance computing devices in their pocket.

- We can program these devices to do all our magic security stuff.
- These devices do have various security features already like filesystem encryption, advanced login systems, etc.
- Advanced features can be easily implemented using high level programming languages



That's nice, but where can I use them?

Uses of security tokens

- Unlocking the password store on your computer
- Unlocking external password managers(Bitwarden,Keypass,LastPass etc.)
- Computer user Logins
- Extra authentication layer in case of a malicious login
- Access to specific “Smart“ home appliances

Nothing is perfect.

As with any other computing module there are ways to break it.

- Many of these devices rely on old or insecure hardware
- Vast majority of “smart“ devices lack critical security updates, this also includes your phone
- Backdoors have been documented in the past

As always the best solution is to make it so the was never anything useful for someone malicious.

Dont let this be you ->

533 million Facebook users' phone numbers and personal data have been leaked online

Aaron Holmes
Apr 3, 2021, 5:41 PM

That’s all folks!

PDF can be found at:
https://github.com/SViN24/Security-Tokens-2021