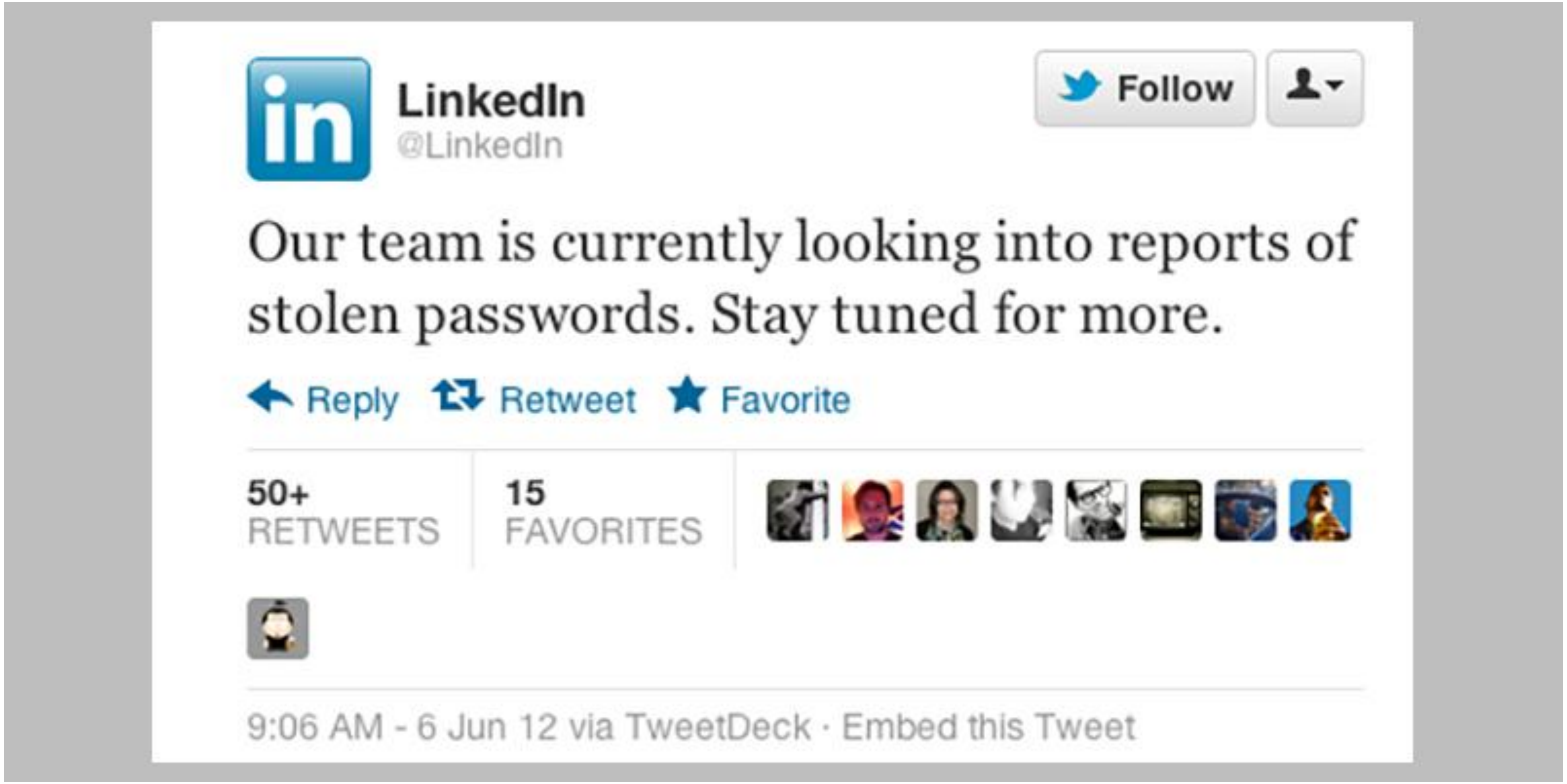
Be In, Be Passwordless

How to forget all your credentials



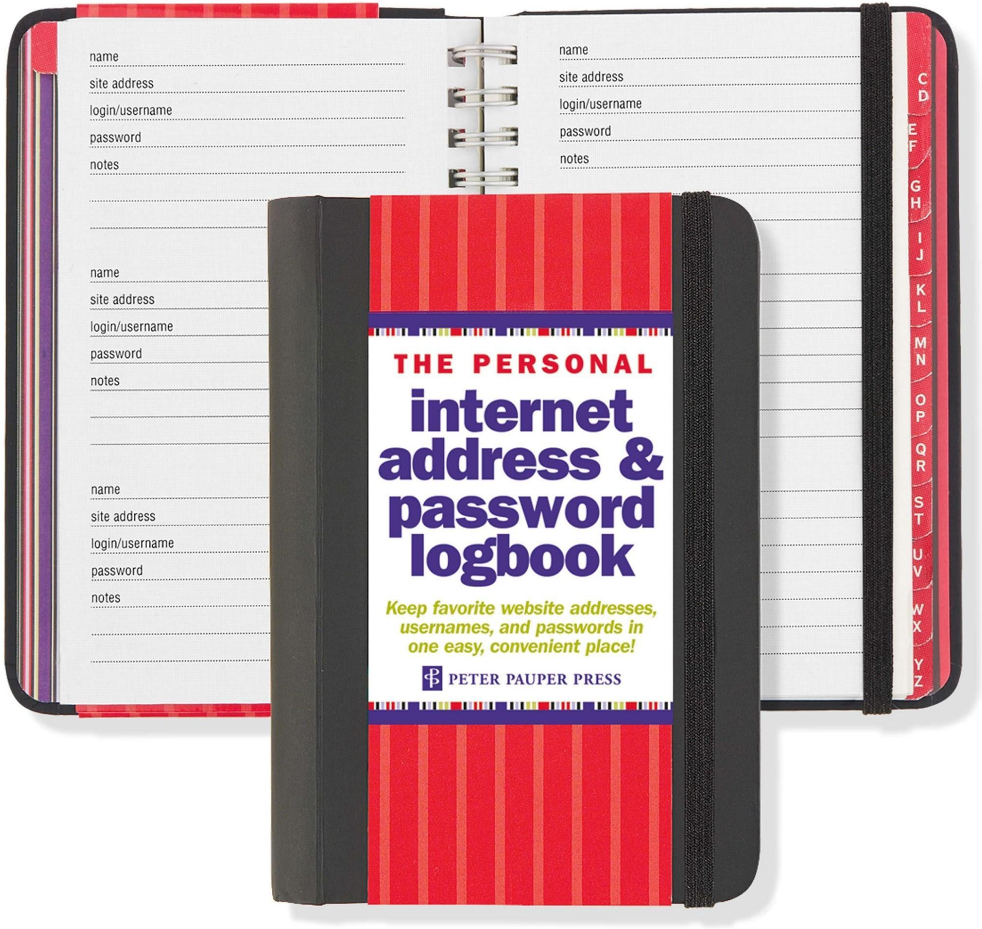
LinkedIn
@LinkedIn

Our team is currently looking into reports of stolen passwords. Stay tuned for more.

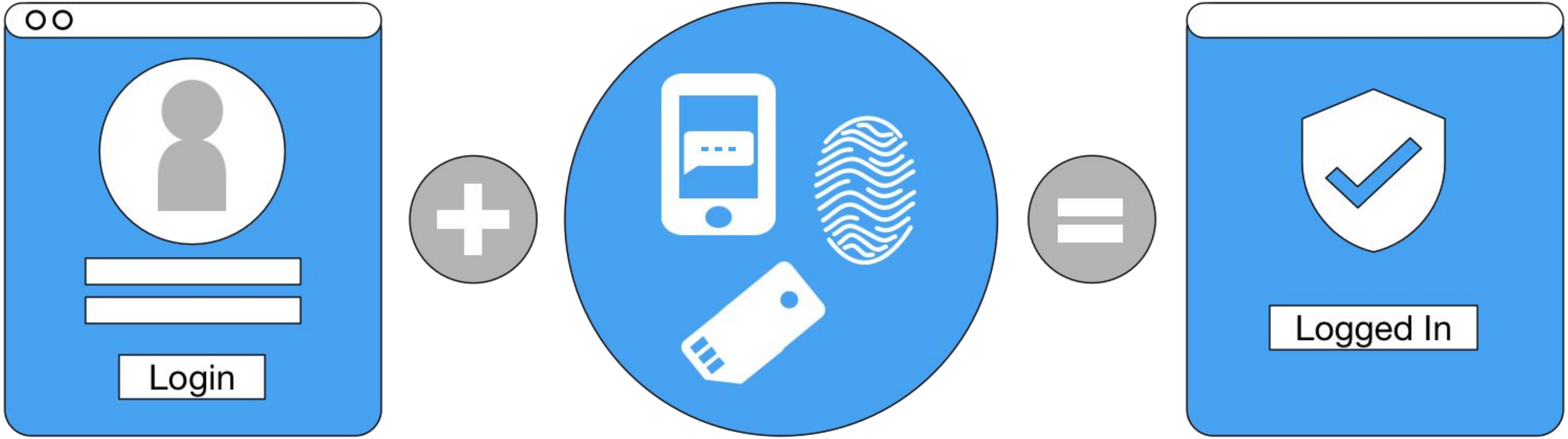
50+ RETWEETS

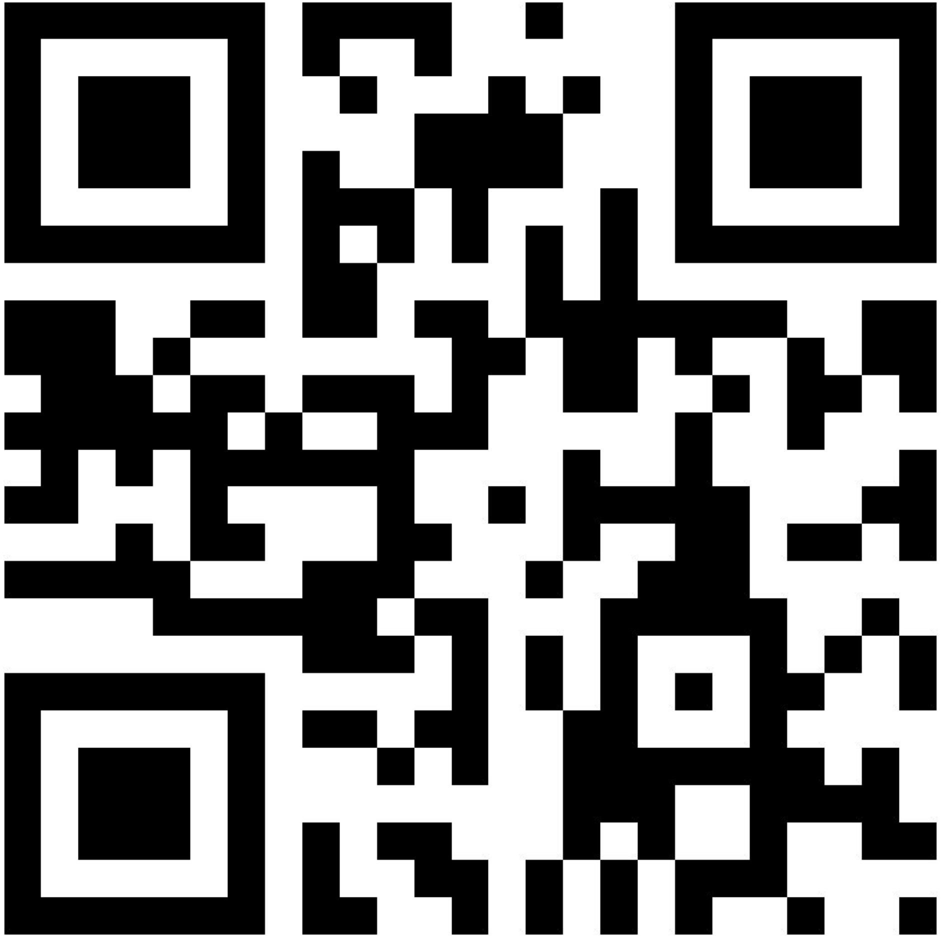
15 FAVORITES

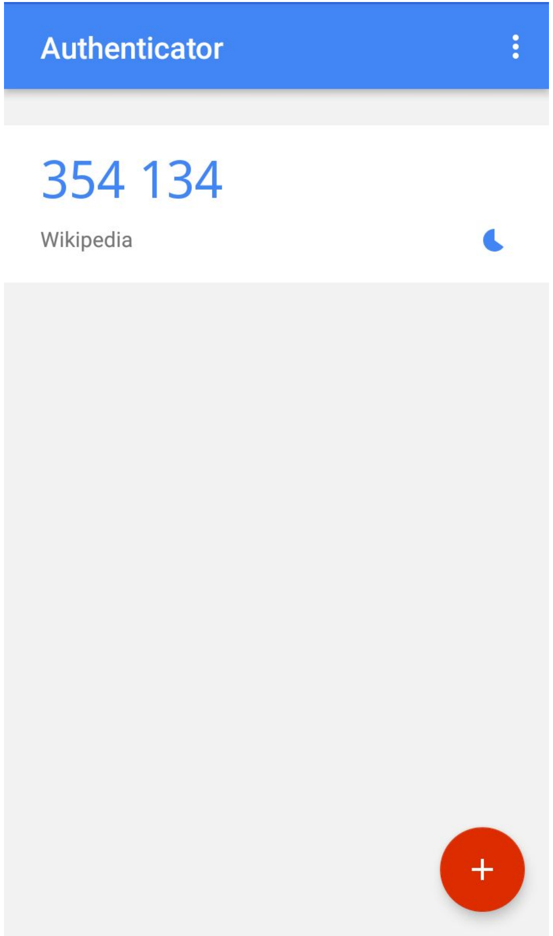
9:06 AM - 6 Jun 12 via TweetDeck · Embed this Tweet


THE PERSONAL
internet address & password logbook
Keep favorite website addresses, usernames, and passwords in one easy, convenient place!
PETER PAUPER PRESS
name
site address
login/username
password
notes
C D
E F
G H
I J
K L
M N
O P
Q R
S T
U V
W X
Y Z

Xebia


Login
Logged In





Authenticator

354 134

Wikipedia

BNP PARIBAS

La banque d'un monde qui change

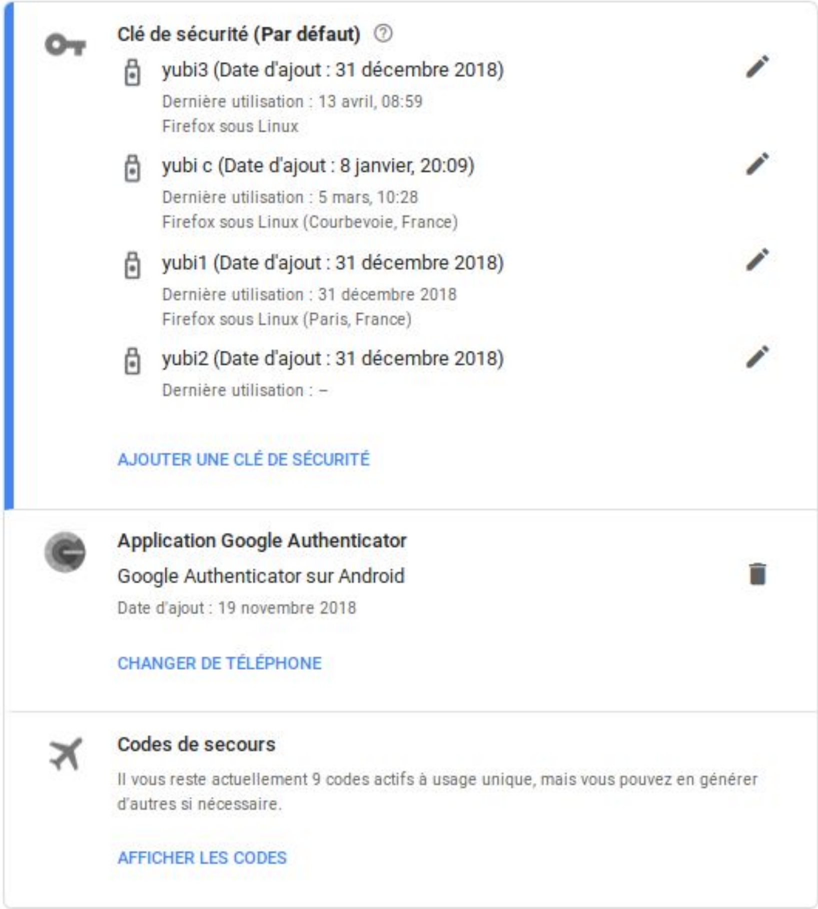
ÉLECTION PRÉSIDENTIELLE 22 AVRIL 2012
LE CHANGEMENT
C'EST MAINTENANT
MES 60 ENGAGEMENTS POUR LA FRANCE
FRANÇOIS
HOLLANDE

LastPass •••|

Can I Trust Them

- End-To-End encryption
- Require 2 secrets; Password and Secret Key
- Secret Key is generated on your device (Random)
- Secret Key never leave the device
- Password is Mixed with Secret Key (no password hash on the server)
- MFA (TOTP)

*https://1password.com/files/1Password%20for%20Teams%20White%20Paper.pdf



Clé de sécurité (Par défaut) ?

yubi3 (Date d'ajout : 31 décembre 2018)

Dernière utilisation : 13 avril, 08:59
Firefox sous Linux

yubi c (Date d'ajout : 8 janvier, 20:09)

Dernière utilisation : 5 mars, 10:28
Firefox sous Linux (Courbevoie, France)

yubi1 (Date d'ajout : 31 décembre 2018)

Dernière utilisation : 31 décembre 2018
Firefox sous Linux (Paris, France)

yubi2 (Date d'ajout : 31 décembre 2018)

Dernière utilisation : –

Application Google Authenticator

Google Authenticator sur Android

Date d'ajout : 19 novembre 2018

Codes de secours

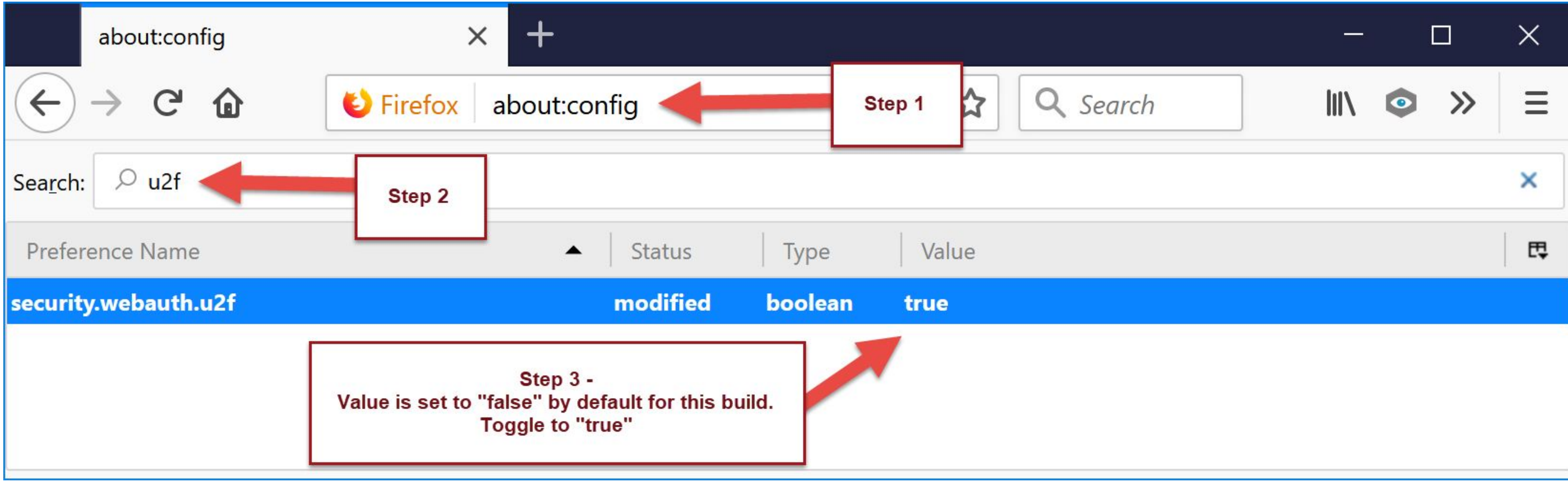
Il vous reste actuellement 9 codes actifs à usage unique, mais vous pouvez en générer d'autres si nécessaire.

Why U2F is secure

During registration with an online service, the user's client device creates a new key pair. It retains the private key and registers the public key with the online service. Authentication is done by the client device proving possession of the private key to the service by signing a challenge. The client's private keys can be used only after they are unlocked locally on the device by the user. The local unlock is accomplished by a user-friendly and secure action such as swiping a finger, entering a PIN, speaking into a microphone, inserting a second-factor device or pressing a button.

- Developed by google
- One secret for each site
- Challenge Response
- U2F token verifies the origin
- Session specific data is used as challenge

*https://security.stackexchange.com/a/71704

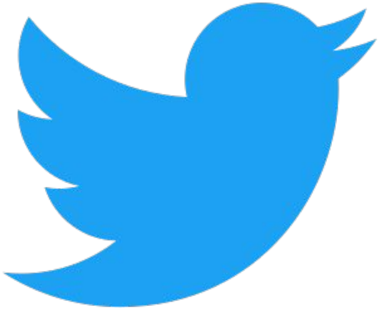


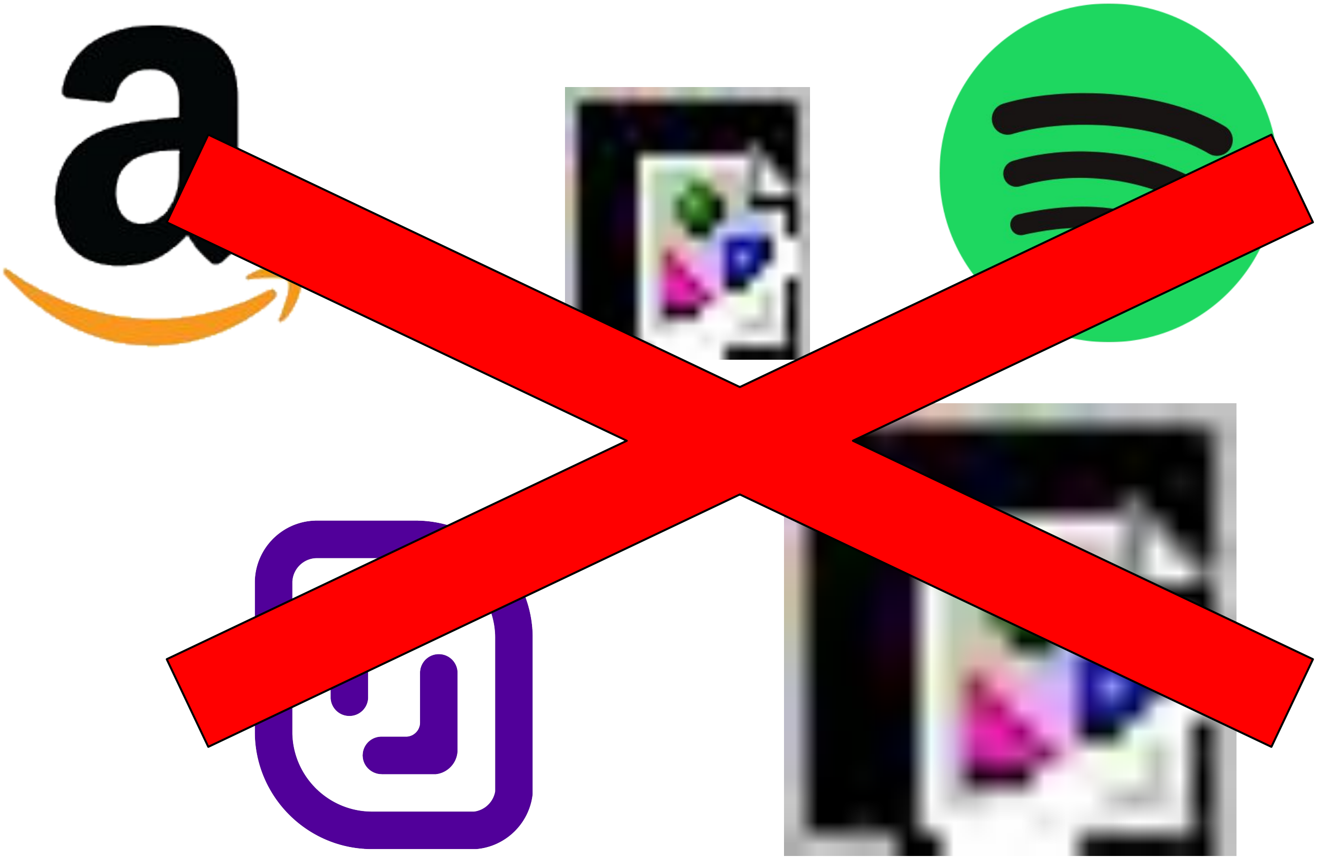
Step 1: about:config

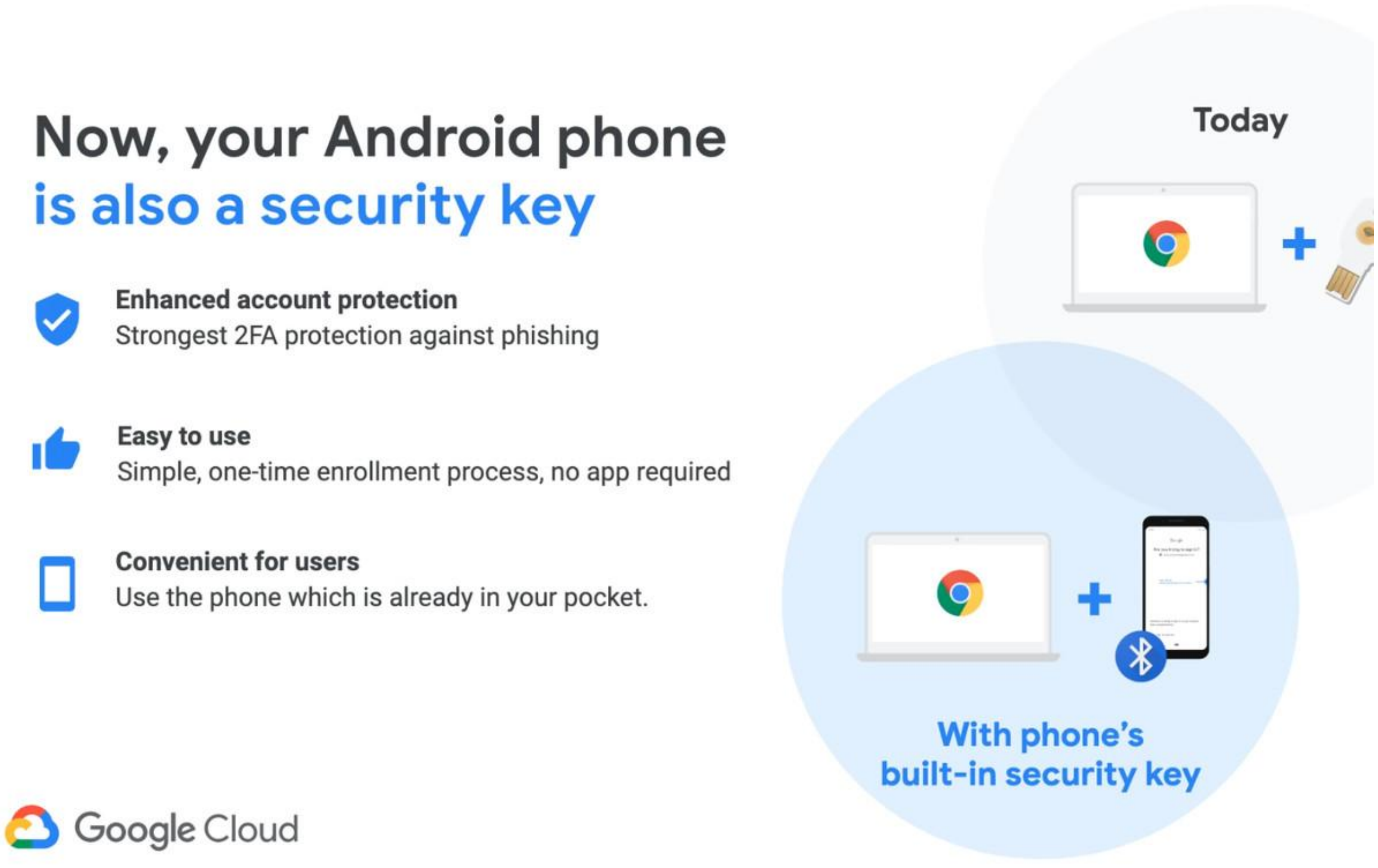
Step 2: Search: u2f

Preference Name	Status	Type	Value
security.webauth.u2f	modified	boolean	true

Step 3 -
Value is set to "false" by default for this build.
Toggle to "true"







Now, your Android phone is also a security key

Enhanced account protection
Strongest 2FA protection against phishing

Easy to use
Simple, one-time enrollment process, no app required

Convenient for users
Use the phone which is already in your pocket.

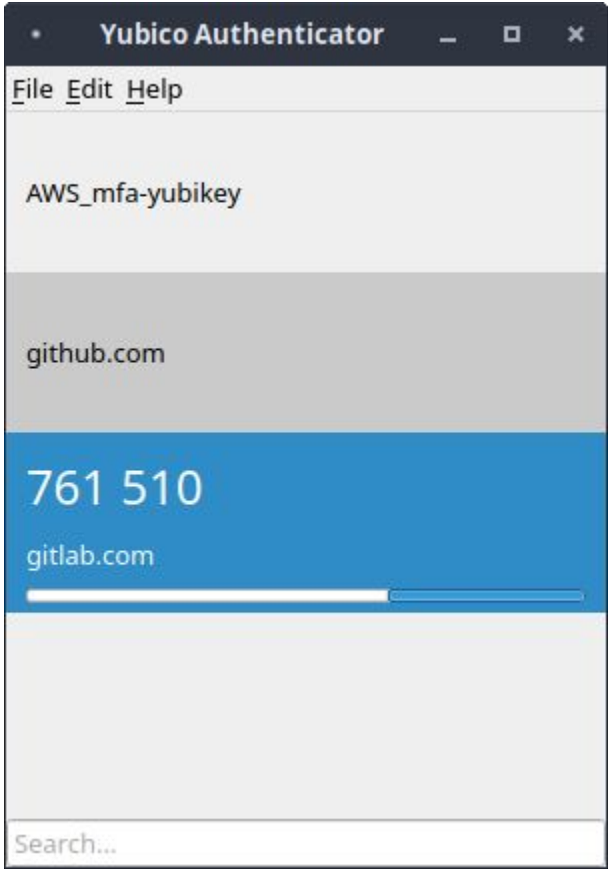
Today

With phone's built-in security key

Google Cloud

LORIEN
Celebrant

yubico



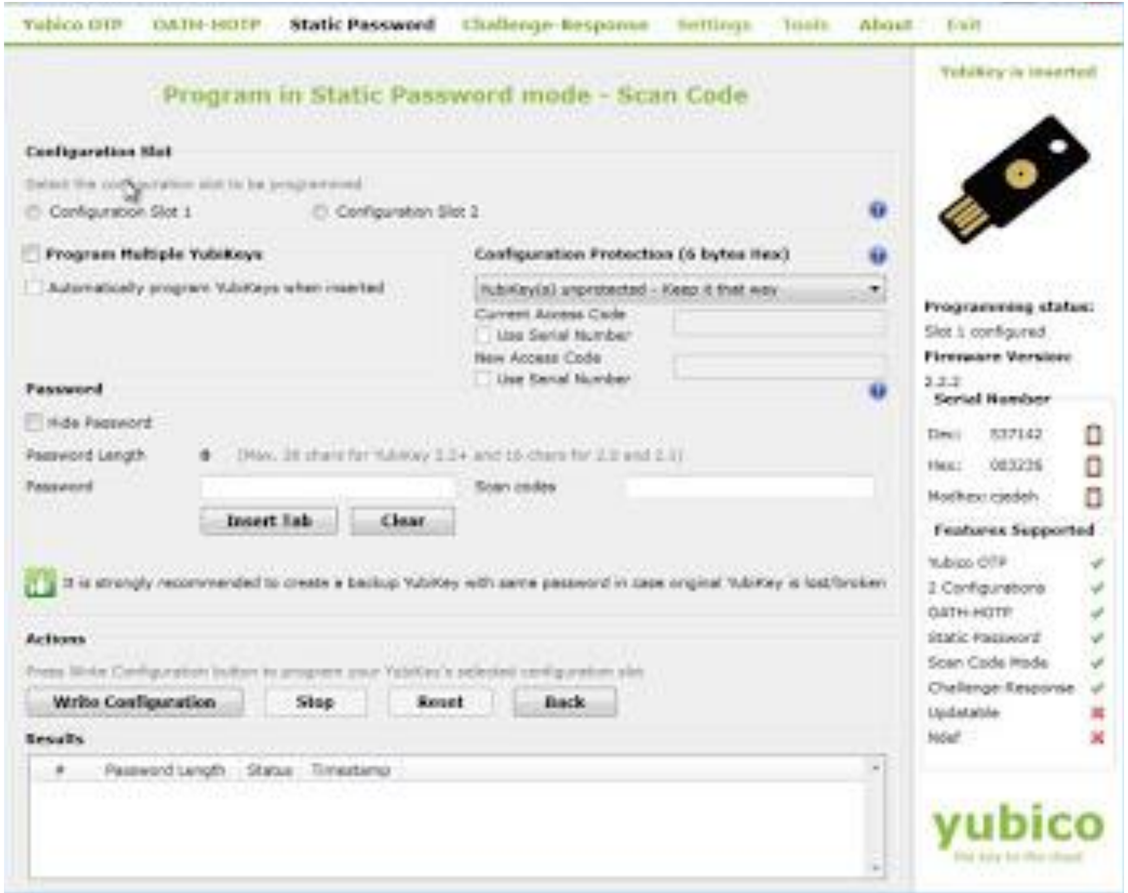
Yubico Authenticator

AWS_mfa-yubikey

github.com

761 510

gitlab.com



Program in Static Password mode - Scan Code

Configuration Slot

Select the configuration slot to be programmed

○ Configuration Slot 1 ○ Configuration Slot 2

□ **Program Multiple YubiKeys**

□ Automatically program YubiKeys when inserted

Configuration Protection (6 bytes Hex)

YubiKey(s) unprotected - Keep it that way

Current Access Code

□ Use Serial Number

New Access Code

□ Use Serial Number

Password

□ Hide Password

Password Length 8 (Max. 38 chars for YubiKey 2.2+ and 16 chars for 2.0 and 2.1)

Password

Scan codes

It is strongly recommended to create a backup YubiKey with same password in case original YubiKey is lost/broken

Actions

Press Write Configuration button to program your YubiKey's selected configuration slot

Results

#	Password Length	Status	Timestamp

YubiKey is inserted

Programming status:

Slot 1 configured

Firmware Version:

2.2.2

Serial Number

Dec:	537142
Hex:	083236
Modhex:	cjedeh

Features Supported

Yubico OTP	✓
2 Configurations	✓
OATH-HOTP	✓
Static Password	✓
Scan Code Mode	✓
Challenge-Response	✓
Updatable	✗
Ndef	✗

ModHex

cbdefghijklnrtuv

>_
SSH

This is Heaven but:

- Try to remember your most important password (email, bank)
- 1 = 0, 2 = 1, 3 = 2
- USB C-is the futur
- Some site only register one key (twitter wtf)
- save your PGP key offline (qrcode) before putting them on yubikey

Thanks

(This was not sponsored by yubico)

*this slides will be available in the XKE google drive and in my github account: https://github.com/scauglog/prez