



***2019 June 06: You be what?***

## *What is a YubiKey?*

The YubiKey is a hardware authentication device manufactured by Yubico that supports one-time passwords, public-key encryption and authentication, and the Universal 2nd Factor (U2F) and FIDO2 protocols developed by the FIDO Alliance. It allows users to securely log into their accounts by emitting one-time passwords or using a FIDO-based public/private key pair generated by the device. YubiKey also allows for storing static passwords for use at sites that do not support one-time passwords. Facebook uses YubiKey for employee credentials, and Google supports it for both employees and users. Some password managers support YubiKey. Yubico also manufactures the Security Key, a device similar to the YubiKey, but focused on public-key authentication.

- Wikipedia

Linux-Ottawa  
linux-ottawa.org

# YubiKey Offerings

## YubiKey 5 Series

*strong two-factor, multi-factor and passwordless authentication, and seamless touch-to-sign. Supports FIDO2, FIDO U2F, one-time-password (OTP), and smart card; choice of form factors for desktop or laptop.*

*Comes in 4 formats:*

*YubiKey 5 NFC*

*YubiKey 5C*

*YubiKey 5 Nano*

*YubiKey 5C Nano*



# YubiKey Offerings

## Yubico Security Key

*Comes in two variants:*

*Security Key*

*Security Key NFC*

*Combines hardware-based authentication, public key cryptography, and U2F and FIDO2, along with USB and NFC capabilities*

*Inexpensive (for a YubiKey)*



Linux-Ottawa  
linux-ottawa.org

# YubiKey Offerings

## Yubico FIPS

*FIPS (Federal Information Processing Standards) are a set of standards that describe document processing, encryption algorithms and other information technology standards for use within non-military government agencies and by government contractors and vendors who work with the agencies.*

*You probably do not need this one.*



## *What do I have?*

**I have 4 YubiKey 4s, two Security Key NFC keys, two YubiKey 5s and a HyperFIDO Mini arriving any time now.**

*I don't have a lot configured with them, I did my first real usage at a conference and just used it for my GPG keys.*

*I also have my Mac configured to use that one for logins.*

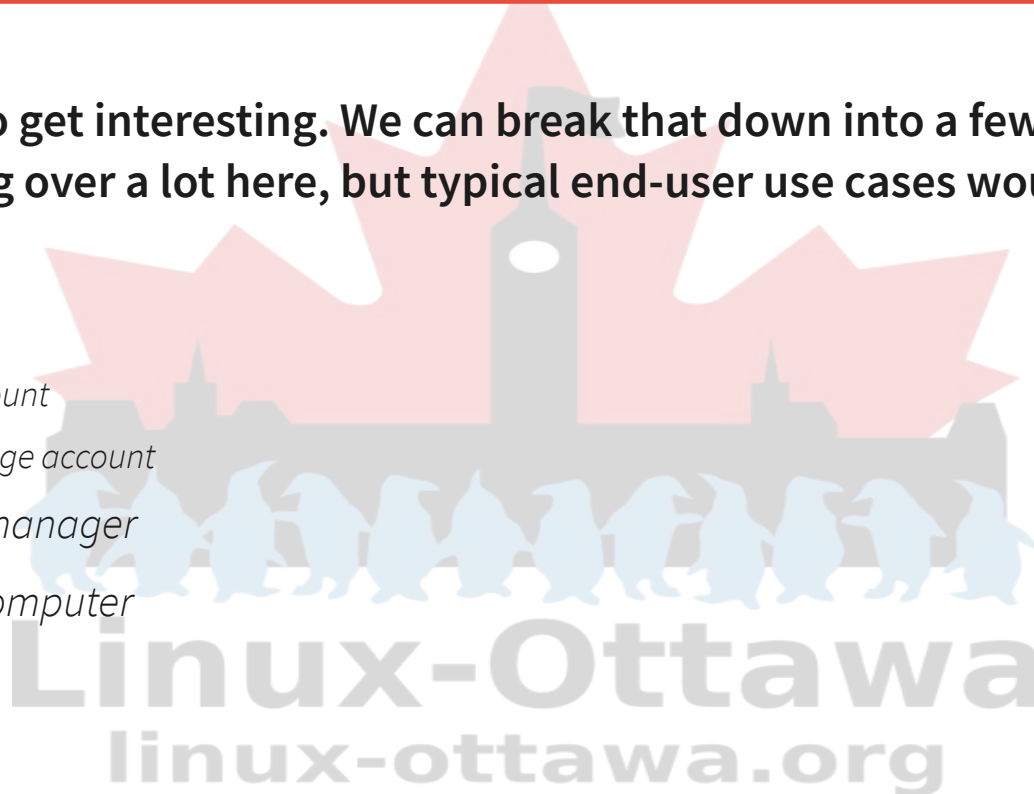
*There are a lot of other options and we will discuss some of them as we go through the talk.*

**Linux-Ottawa**  
linux-ottawa.org

## *OK, so what do we do with one?*

That is where it starts to get interesting. We can break that down into a few main cases for most users. I'm skipping over a lot here, but typical end-user use cases would include:

- *Protect access to*
  - *My social media account*
  - *My \$BigCo webmail account*
  - *My cloud based file storage account*
- *Protect my password manager*
- *Protect access to my computer*
- *Store my GPG keys*
- *Etc.*



# Protecting Your Access

## Social Media

*Do you have a facebook account? You might want to secure access to it.*

*How about*

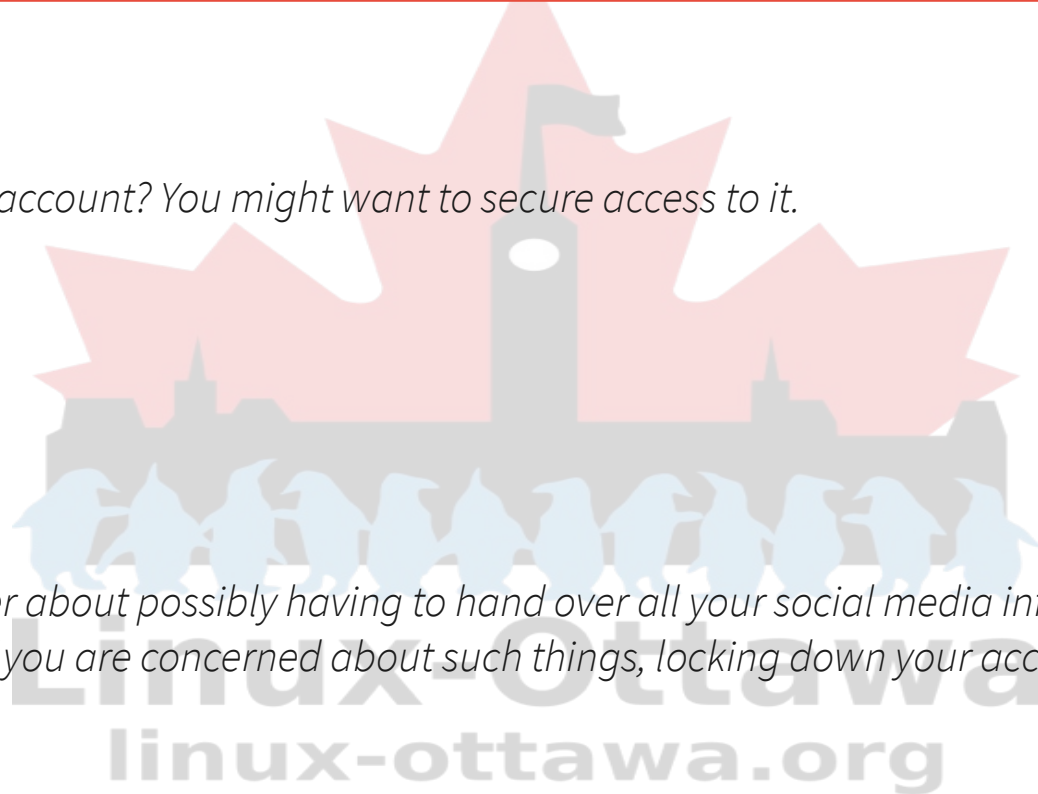
*Twitter?*

*Instagram?*

*Reddit?*

*YouTube?*

*I saw some recent chatter about possibly having to hand over all your social media information if you want a VISA to work in the U.S. If you are concerned about such things, locking down your accounts may be a good thing.*





# Protecting Access - Twitter



## Twitter Example

*I have a twitter account. I mostly follow other people and use it as a “interesting things” aggregator from people I know or wish to know what they are discussing. However, if I lost control of my account, I could be posting all manner of things I wouldn’t want associated with me.*

*Let’s go through the exercise of getting this set up.*

Linux-Ottawa  
linux-ottawa.org

# Protecting Access - Twitter

## Twitter Example

*In the top menu, click your profile icon, then click Settings and privacy.*

*Click on the Account tab.*

*Under Security and next to Login verification, click the Review your login verification methods button to get started.*

*Enter your password and click Confirm.*

*From the selections, click Set up next to Security key.*

*Enter your password and click Confirm.*

*From the selections, click Set up next to Security key.*

*Read the instructions and then click Start.*

*If you're asked to verify your password, enter it and click Verify.*

*You will see a pop-up window asking you to register your key by inserting it into your computer's USB port. Once inserted, press the button located on your key. Then verify the key by pressing the button one more time.*



# Protecting Access - Twitter

Twitter

https://twitter.com

Home Moments Notifications Messages Search Twitter Tweet

Profile and settings

What's happening?

Elizabeth K. Joseph Retweeted

**Kuberkus** @fuzzychef · 7h  
Hey, frequent conference organizer here. Thread to educate the other white boys in my followers about diversity and conferences, because there's a lot of BS going around and I'm tired of it. (1)

1 26 37

Show this thread

**TheHighNibble** @TheHighNibble · Jun 2  
The #IMSAI 8080 Replica kit I've been working on for some time now will start to ship this month! I recently assembled the first production kit, pictured here. If it interests you, head over to [thehighnibble.com](http://thehighnibble.com) for more details and how to order.

IMSAI 8080

IMSAI 8080

Scott Murphy @ovsage  
Tweets 1,282 Following 215 Followers 175

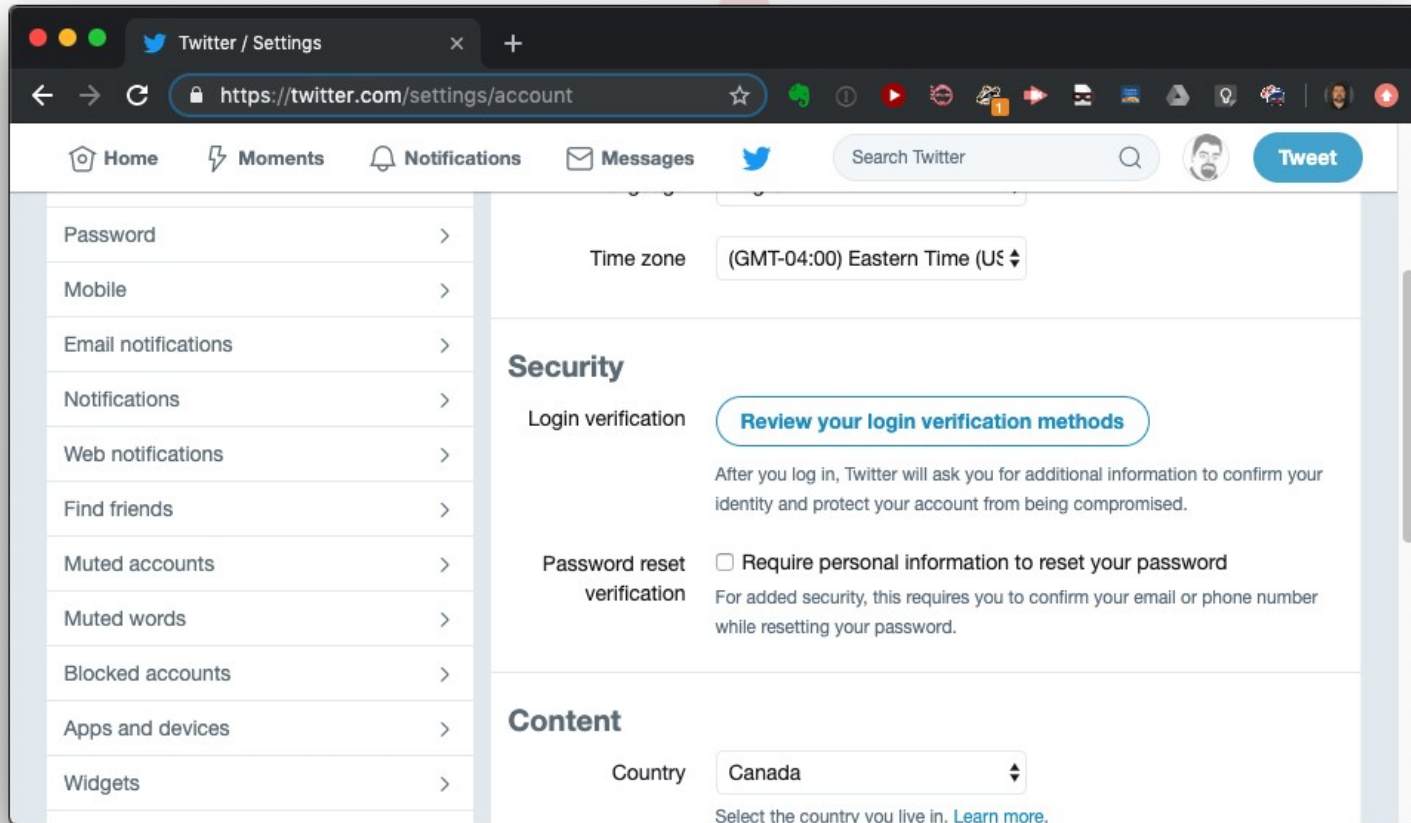
Who to follow · Refresh · View all  
Followed by Denise and others  
I am Gareth's Smirking ...  
Follow  
HintonburgPublicHous @...  
Follow

https://twitter.com/settings

# Protecting Access - Twitter

The image shows a browser window displaying the Twitter profile of Scott Murphy (@ovsage). The browser's address bar shows the URL <https://twitter.com>. The navigation bar includes Home, Moments, Notifications (with a badge), Messages, and a search bar. The profile header shows the name Scott Murphy, handle @ovsage, and statistics: 1,282 Tweets, 215 Following, and 175 Followers. Below the header is a 'Who to follow' section with a 'Follow' button for 'I am Gareth's Smirking ...'. The main content area shows a tweet from Kuberkus (@fuzzychef) and a tweet from TheHighNibble (@TheHighNibble) mentioning the #IMSAI 8080 kit. A settings menu is open over the right side of the page, listing options: Profile, Lists, Moments, Promote Mode, Twitter Ads, Analytics, Settings and privacy (highlighted), Help Center, and Keyboard shortcuts. The browser's address bar at the bottom of the window shows <https://twitter.com/settings>.

# Protecting Access - Twitter



The screenshot shows the Twitter account settings page in a web browser. The browser's address bar displays the URL `https://twitter.com/settings/account`. The page features a navigation bar with icons for Home, Moments, Notifications, Messages, and a search bar. A left-hand sidebar lists various settings categories, including Password, Mobile, Email notifications, Notifications, Web notifications, Find friends, Muted accounts, Muted words, Blocked accounts, Apps and devices, and Widgets. The main content area is divided into sections: 'Time zone' is set to '(GMT-04:00) Eastern Time (US)'; the 'Security' section includes 'Login verification' with a 'Review your login verification methods' button, and 'Password reset verification' with an unchecked checkbox for 'Require personal information to reset your password'; the 'Content' section shows the 'Country' set to 'Canada'.

Twitter / Settings

https://twitter.com/settings/account

Home Moments Notifications Messages Search Twitter Tweet

Password >

Mobile >

Email notifications >

Notifications >

Web notifications >

Find friends >

Muted accounts >

Muted words >

Blocked accounts >

Apps and devices >

Widgets >

Time zone (GMT-04:00) Eastern Time (US)

### Security

Login verification [Review your login verification methods](#)

After you log in, Twitter will ask you for additional information to confirm your identity and protect your account from being compromised.

Password reset verification  Require personal information to reset your password

For added security, this requires you to confirm your email or phone number while resetting your password.

### Content

Country Canada

Select the country you live in. [Learn more.](#)

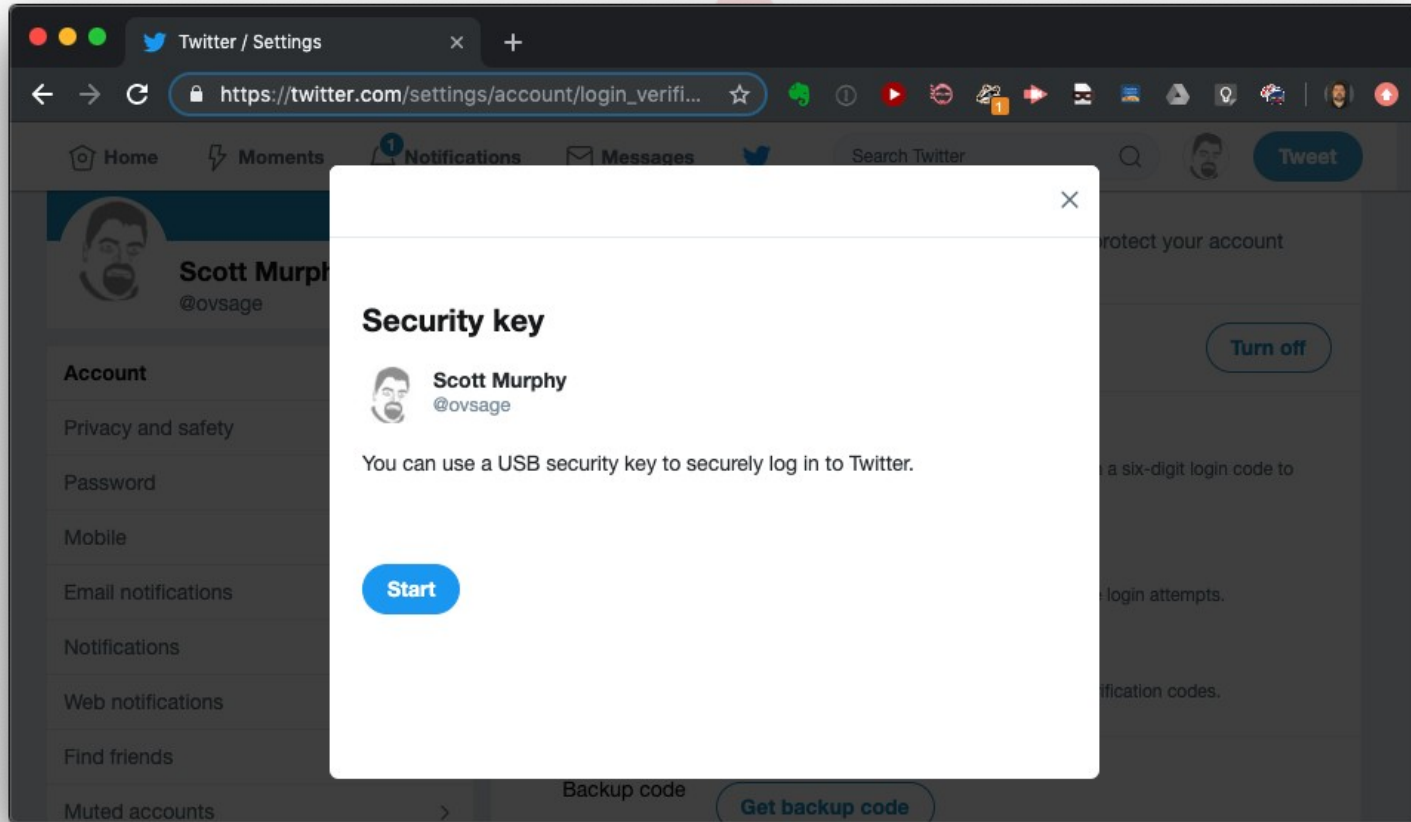
# Protecting Access - Twitter

The screenshot shows a web browser window with the Twitter settings page for login verification. The browser's address bar shows the URL `https://twitter.com/settings/account/login_verifi...`. The Twitter navigation bar at the top includes Home, Moments, Notifications (with a badge), Messages, and a search bar. The user's profile information, Scott Murphy (@ovsage), is visible on the left. The main content area is titled "Login verification" and explains that after login, Twitter will ask for additional verification. A "Turn off" button is present. Below this, there are four settings:

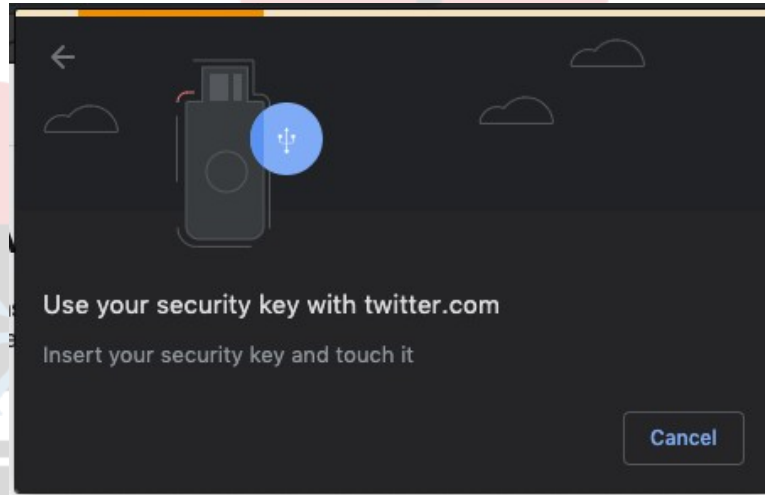
- Text message** with an **Edit** link. Description: "Twitter will send a text to your mobile phone with a six-digit login code to enter."
- Security key** with a **Set up** link. Description: "You can use a physical electronic key to approve login attempts."
- Mobile security app** with a **Set up** link. Description: "You can use a separate app to generate your verification codes."
- Backup code** with a **Get backup code** button.



# Protecting Access - Twitter

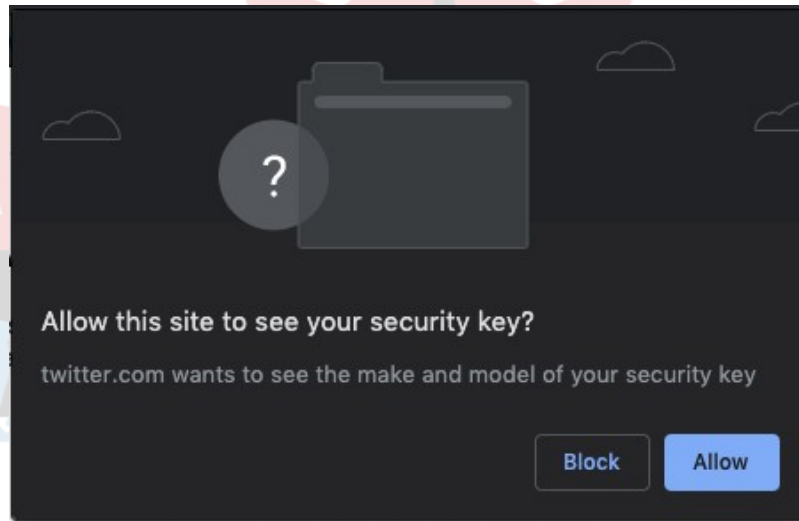


## Protecting Access - Twitter

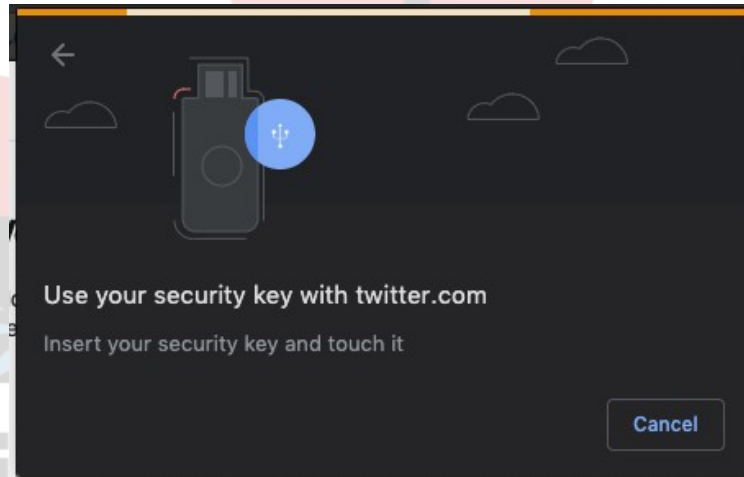




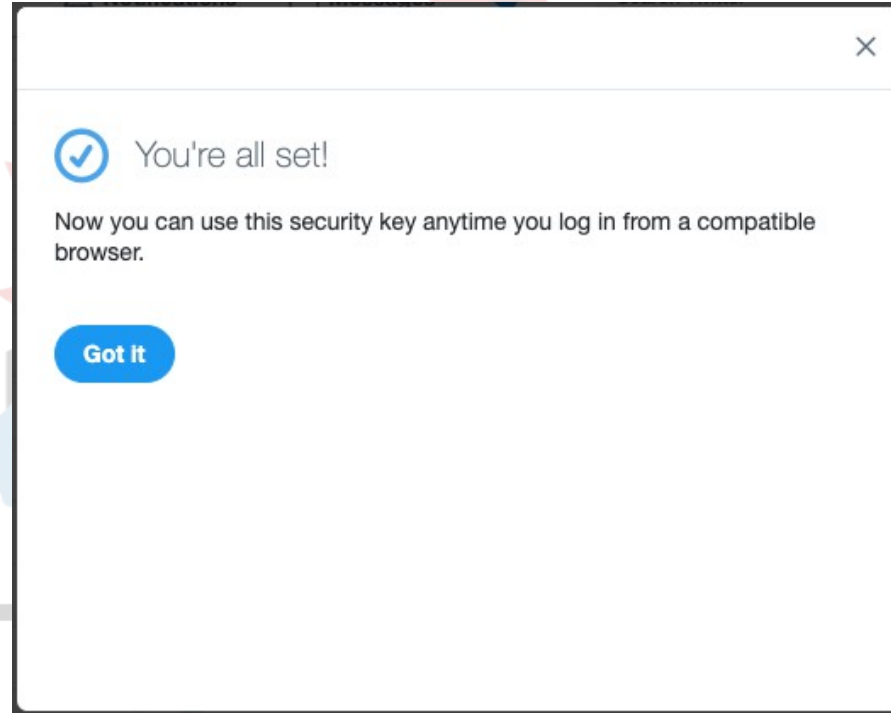
## Protecting Access - Twitter



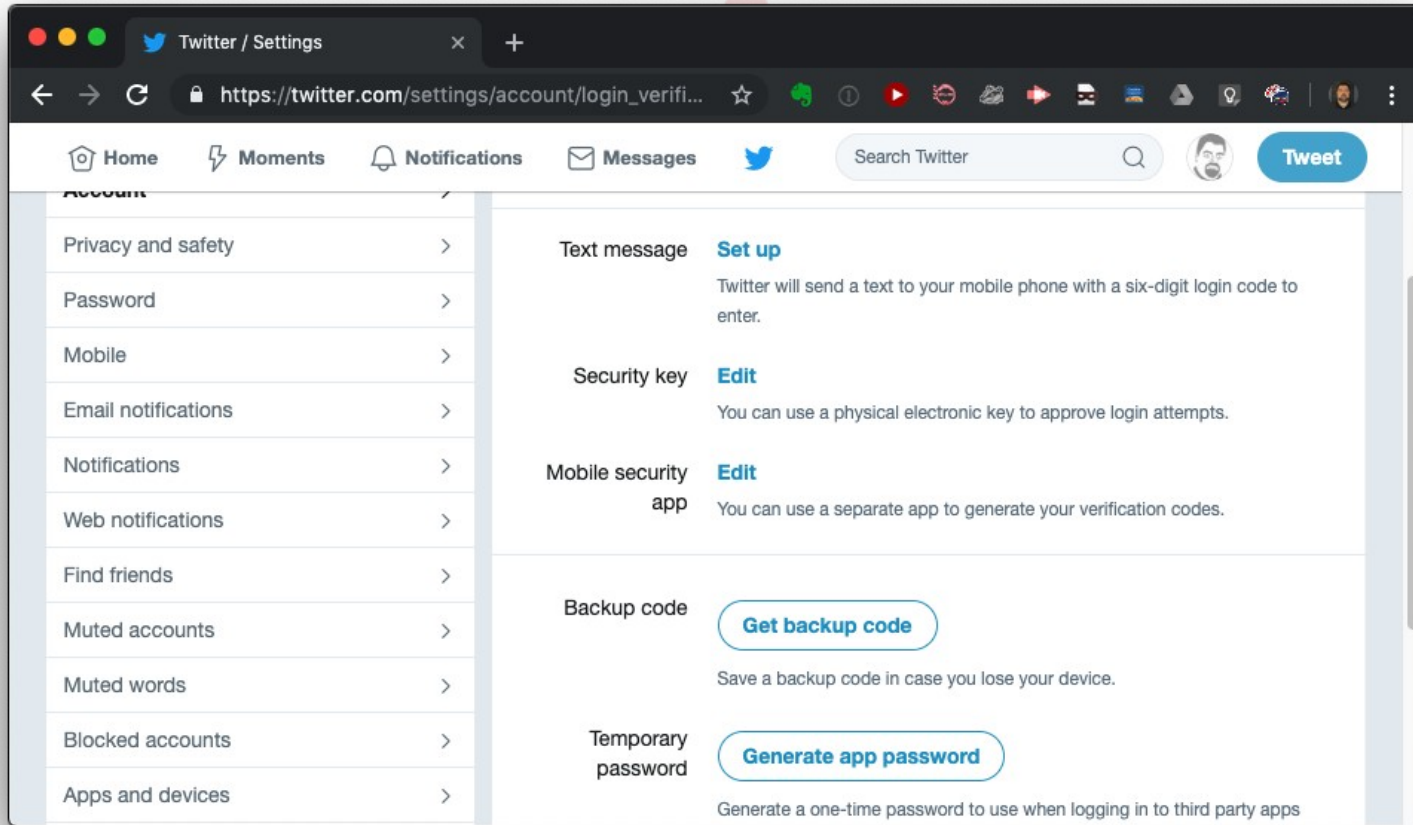
## Protecting Access - Twitter



# Protecting Access - Twitter



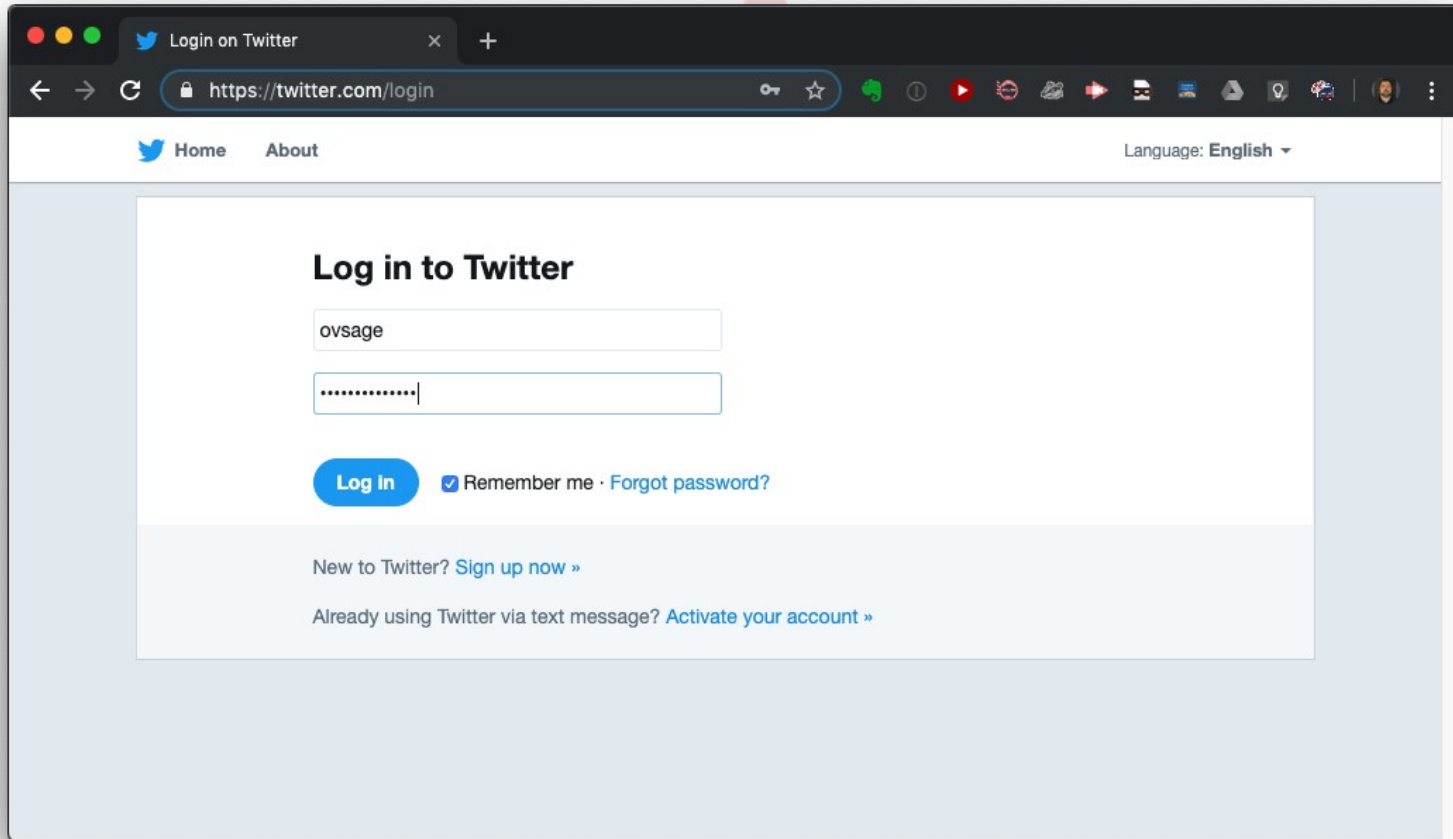
# Protecting Access - Twitter



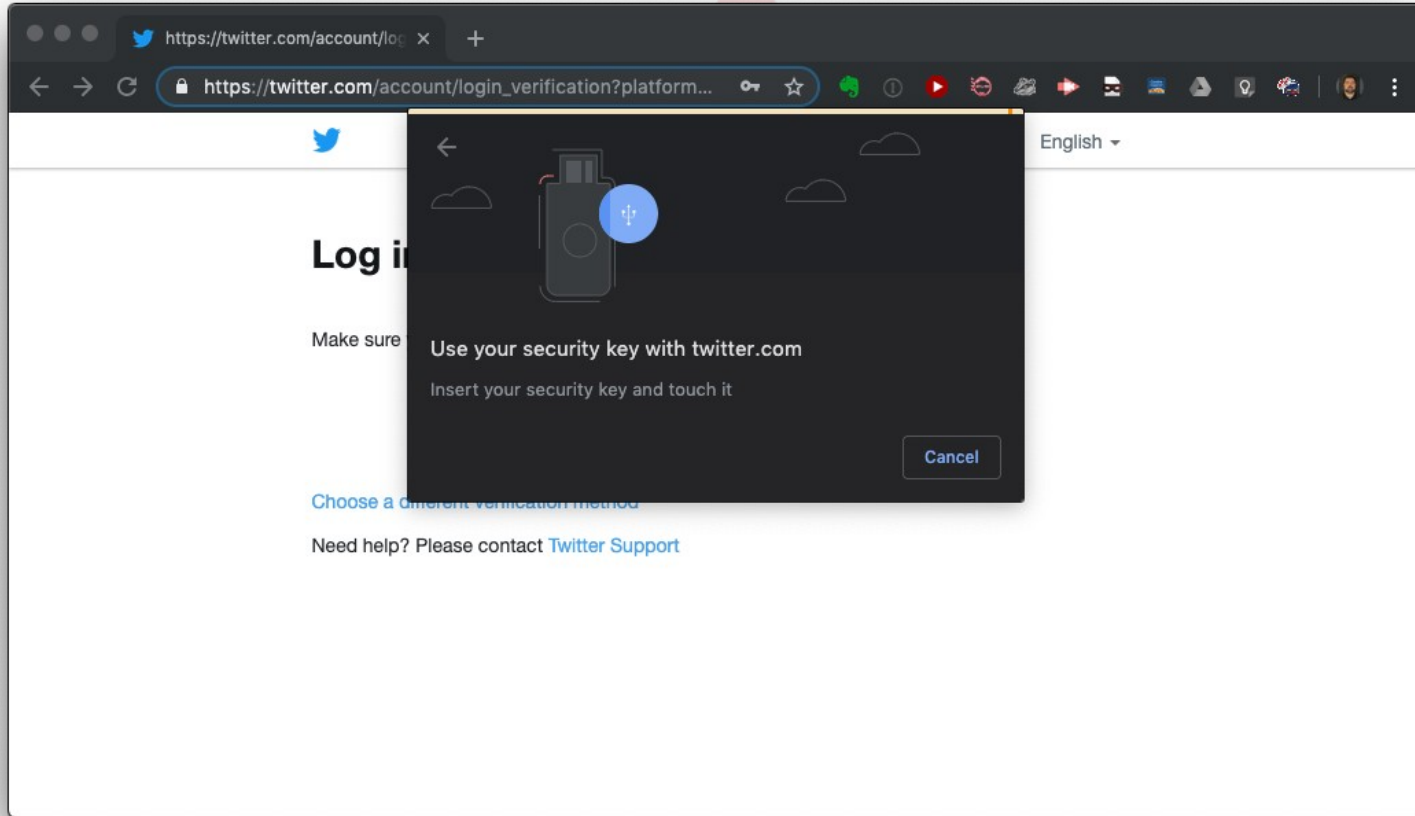
The screenshot shows the Twitter account settings page for login verification. The browser address bar displays the URL [https://twitter.com/settings/account/login\\_verifi...](https://twitter.com/settings/account/login_verifi...). The navigation bar includes Home, Moments, Notifications, Messages, and a search bar. The left sidebar lists various settings categories, with 'Account' selected. The main content area shows the following options:

- Text message** [Set up](#)  
Twitter will send a text to your mobile phone with a six-digit login code to enter.
- Security key** [Edit](#)  
You can use a physical electronic key to approve login attempts.
- Mobile security app** [Edit](#)  
You can use a separate app to generate your verification codes.
- Backup code** [Get backup code](#)  
Save a backup code in case you lose your device.
- Temporary password** [Generate app password](#)  
Generate a one-time password to use when logging in to third party apps

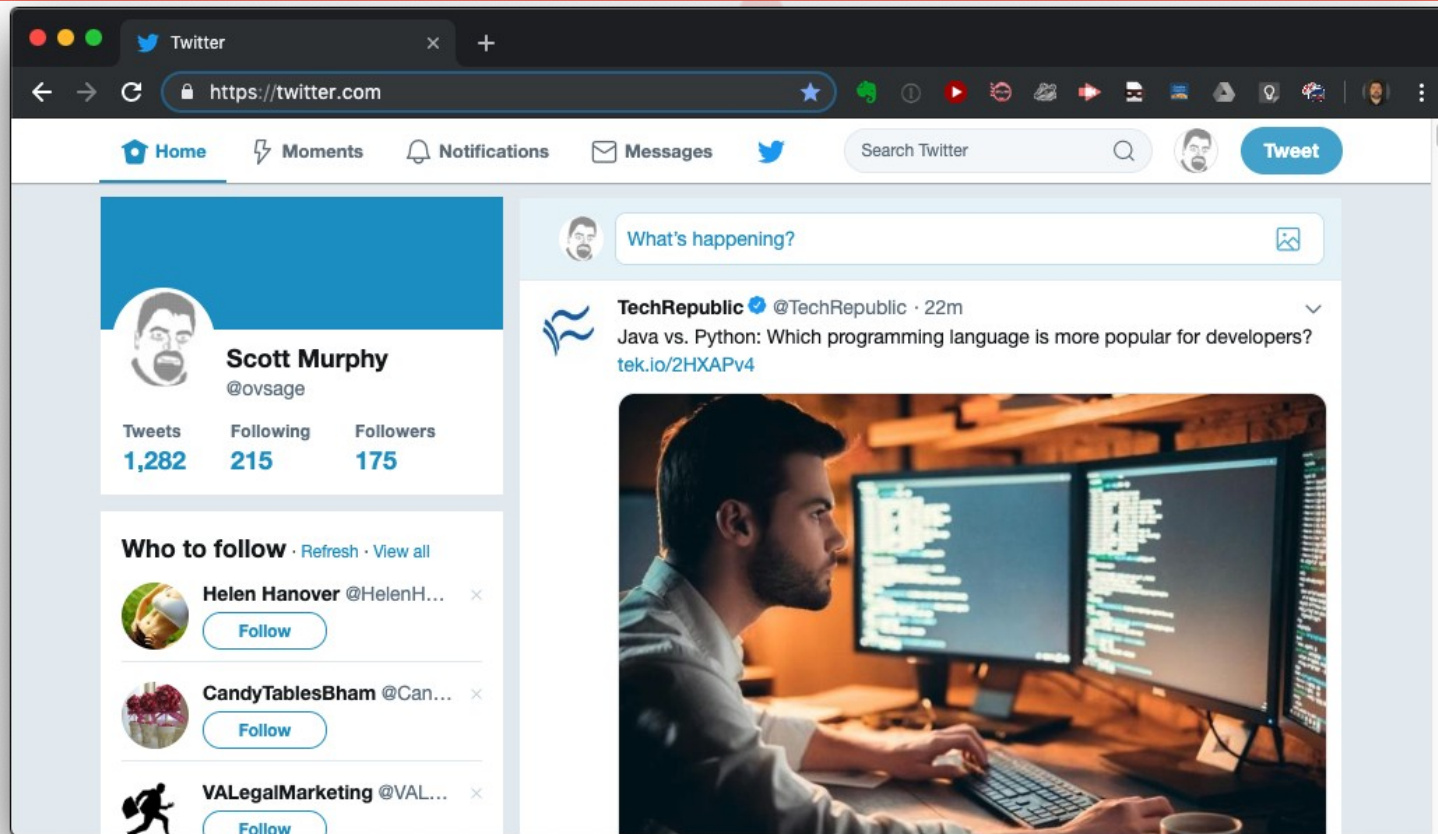
# Protecting Access - Twitter



# Protecting Access - Twitter



# Protecting Access - Twitter



## Protecting Access - GitLab



### GitLab Example

*I also have a GitLab account. It is used mostly for messing around with things. I prefer it over GitHub because you can have private repositories. I am not a professional coder and having my dirty laundry hanging out there is not something I want to do. I have no issue with sharing things, just not my rough scripts, etc.*

Linux-Ottawa  
linux-ottawa.org



# Protecting Access - GitLab

## GitLab Process

*Log in to your GitLab account.*

*Go to your Profile Settings.*

*Go to Account.*

*Click Enable Two-Factor Authentication.*

*Plug in your U2F device.*

*Click on Set up New U2F Device.*

*A light will start blinking on your device. Activate it by pressing its button.*

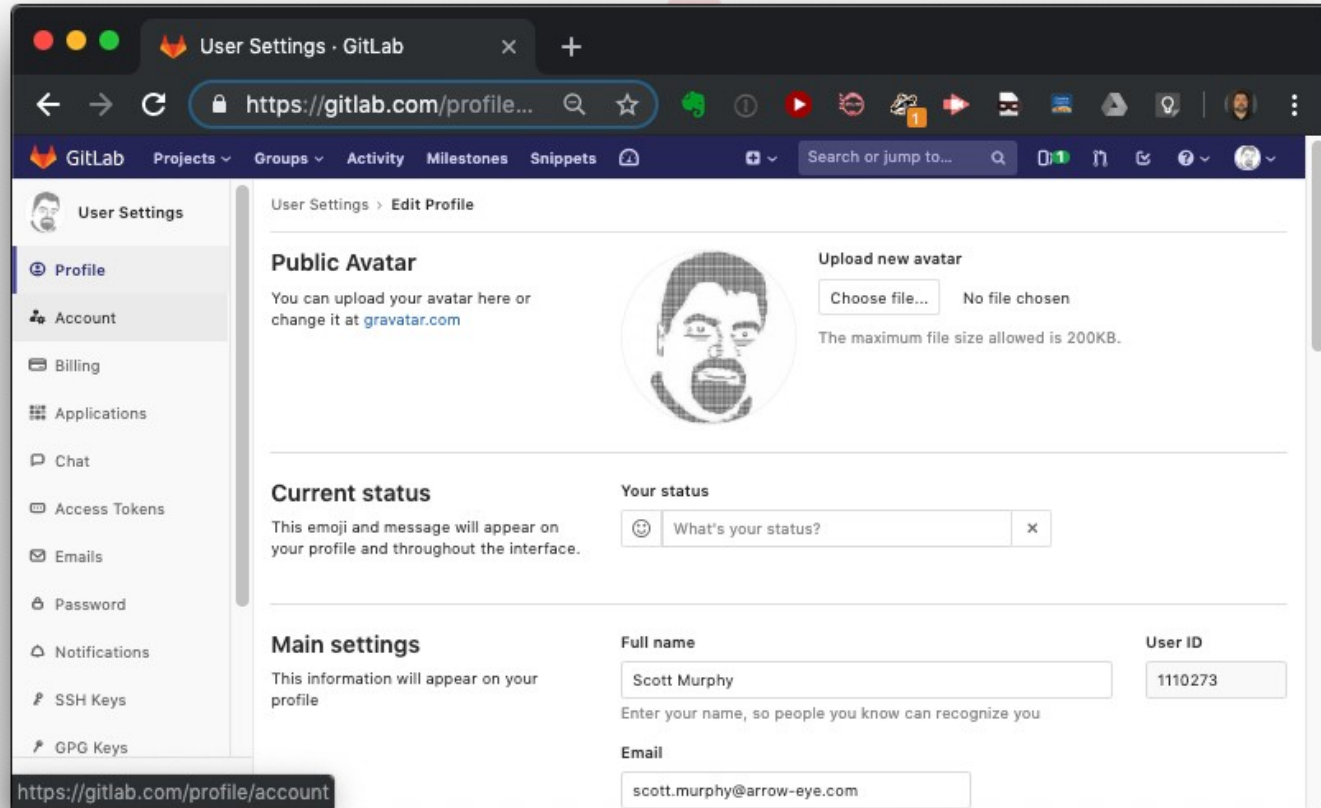


# Protecting Access - GitLab

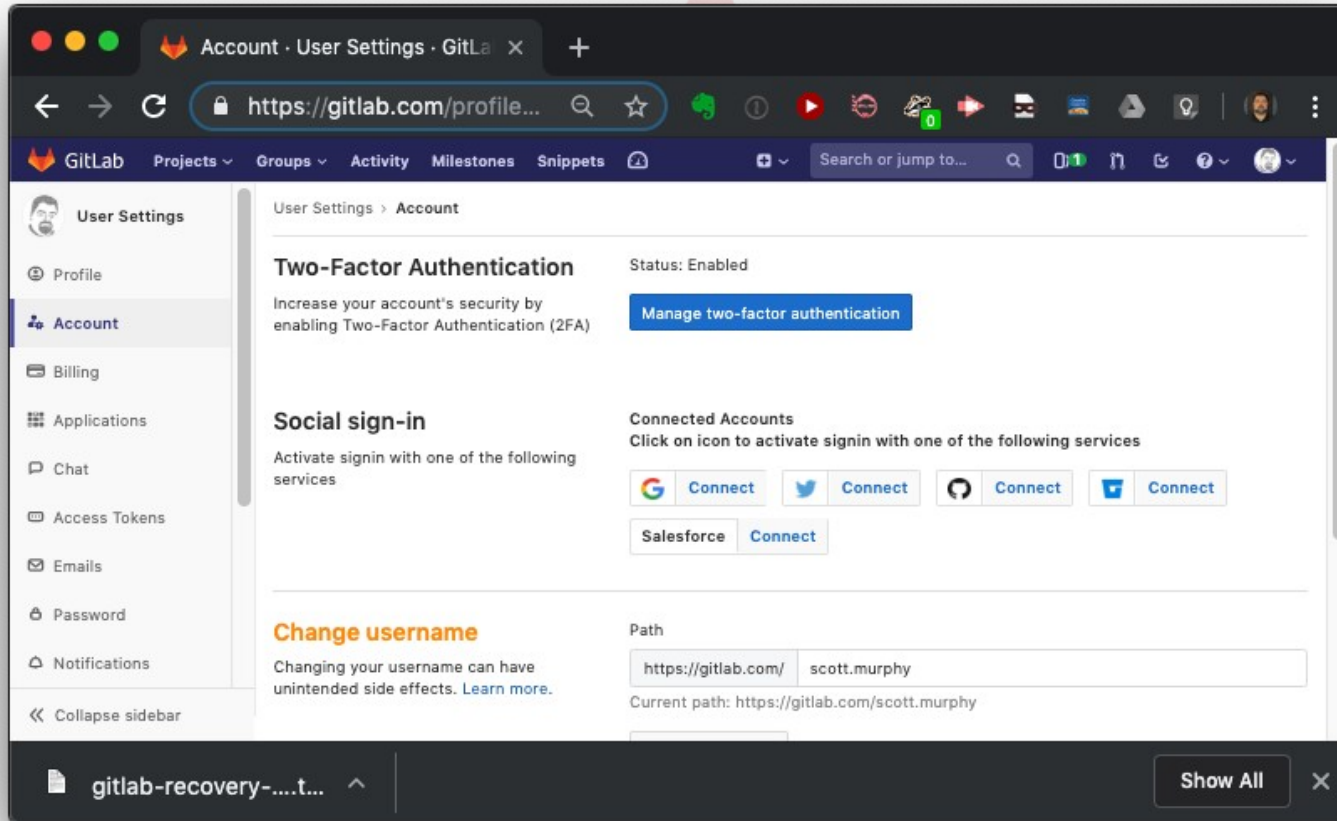
The screenshot shows the GitLab Projects Dashboard. The browser address bar displays `https://gitlab.com/?nav_s...`. The navigation bar includes links for Projects, Groups, Activity, Milestones, and Snippets, along with a search bar and user profile icon. The main content area is titled "Projects" and shows a list of projects under the "Your projects" section. A user profile menu is open, showing options like "Set status", "Profile", "Settings", and "Sign out".

Project Name	Role	Stars	Forks	Issues	Commits	Updated
Scott Murphy / Linux-Ottawa Wiki	Maintainer	0	0	0	0	
Scott Murphy / Arrow-Eye Web Site	Maintainer	0	0	0	0	Updated 2 months ago
lopsa / secretary	Owner	0	0	0	0	Updated 4 months ago
Scott Murphy / utilities-catchwire-kalitap	Maintainer	0	0	0	0	Updated 4 months ago
Scott Murphy / u-boot-2014.04-catchwire-kalitap	Maintainer	0	0	0	0	Updated 4 months ago

# Protecting Access - GitLab



# Protecting Access - GitLab



The screenshot shows the GitLab user settings page for account security. The browser address bar shows the URL `https://gitlab.com/profile...`. The page title is "Account · User Settings · GitLab". The left sidebar contains navigation options: Profile, Account (selected), Billing, Applications, Chat, Access Tokens, Emails, Password, and Notifications. The main content area is titled "User Settings > Account" and features three sections:

- Two-Factor Authentication:** Status is "Enabled". A blue button labeled "Manage two-factor authentication" is present. Below the text "Increase your account's security by enabling Two-Factor Authentication (2FA)", there is a blue button labeled "Manage two-factor authentication".
- Social sign-in:** Text reads "Activate sign-in with one of the following services". Under "Connected Accounts", it says "Click on icon to activate sign-in with one of the following services". There are five "Connect" buttons for Google, Twitter, GitHub, Facebook, and Salesforce.
- Change username:** Text reads "Changing your username can have unintended side effects. [Learn more.](#)".

At the bottom, there is a "Path" field containing `https://gitlab.com/scott.murphy` and a "Current path" label with the same value. A "Show All" button is visible in the bottom right corner of the settings area.

# Protecting Access - GitLab

The screenshot shows a web browser window with the URL `https://gitlab.com/profile...`. The page title is "Two-Factor Authentication · Account". The left sidebar contains "User Settings" with options for Profile, Account (selected), Billing, Applications, Chat, Access Tokens, Emails, Password, and Notifications. The main content area is titled "User Settings > Two-Factor Authentication > Account".

**Register Two-Factor Authenticator**

You've already enabled two-factor authentication using one time password authenticators. In order to register a different device, you must first disable two-factor authentication.

If you lose your recovery codes you can generate new ones, invalidating all previous codes.

[Disable two-factor authentication](#) [Regenerate recovery codes](#)

**Register Universal Two-Factor (U2F) Device**

Use a hardware device to add the second factor of authentication.

As U2F devices are only supported by a few browsers, we require that you set up a two-factor authentication app before a U2F device. That way you'll always be able to log in - even when you're using an unsupported browser.

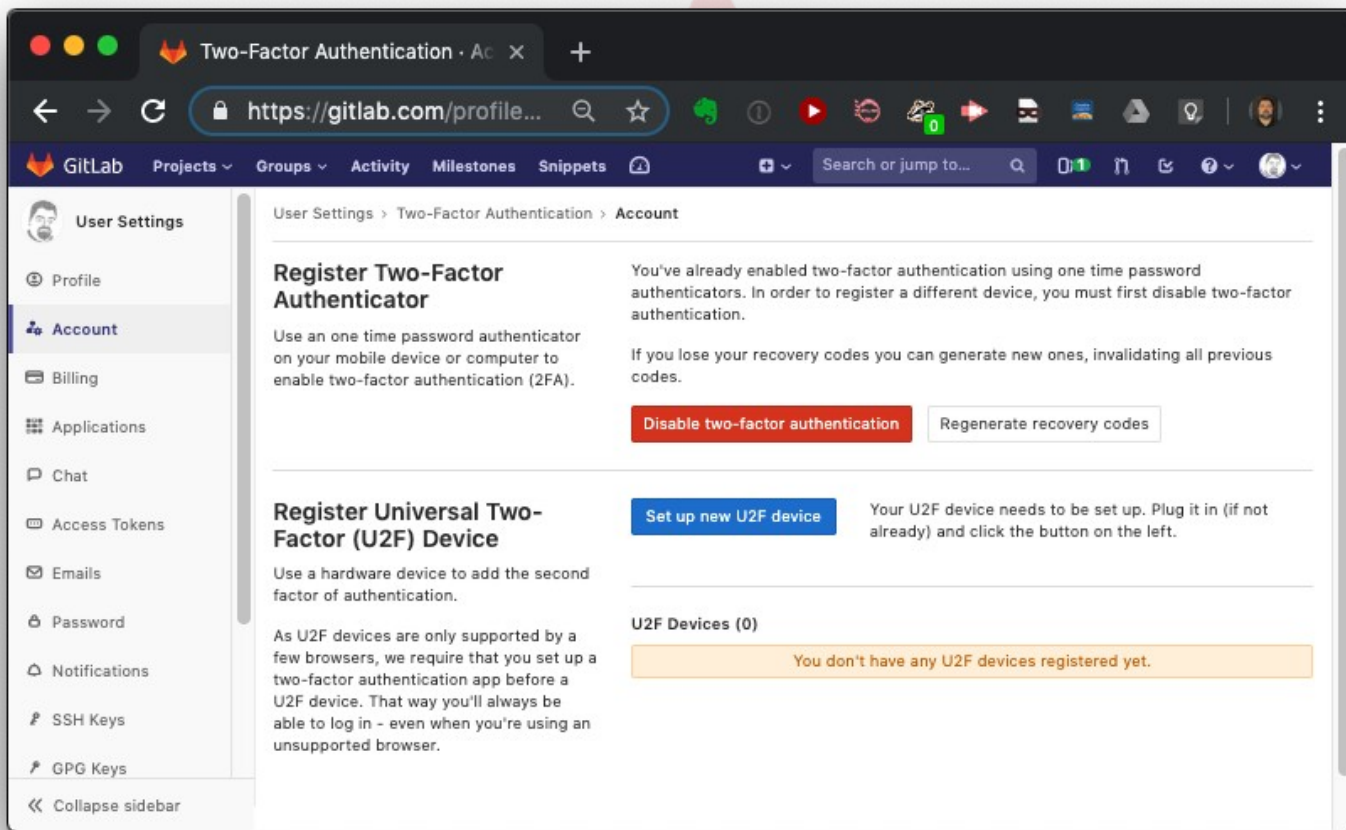
[Set up new U2F device](#) Your U2F device needs to be set up. Plug it in (if not already) and click the button on the left.

**U2F Devices (0)**

You don't have any U2F devices registered yet.

At the bottom of the browser window, a file named "gitlab-recovery-....t..." is open, and a "Show All" button is visible.

# Protecting Access - GitLab



The screenshot shows a web browser window with the URL `https://gitlab.com/profile...`. The page title is "Two-Factor Authentication · Account". The left sidebar contains "User Settings" with a sub-menu including Profile, Account (selected), Billing, Applications, Chat, Access Tokens, Emails, Password, Notifications, SSH Keys, GPG Keys, and Collapse sidebar. The main content area is titled "User Settings > Two-Factor Authentication > Account".

### Register Two-Factor Authenticator

Use an one time password authenticator on your mobile device or computer to enable two-factor authentication (2FA).

You've already enabled two-factor authentication using one time password authenticators. In order to register a different device, you must first disable two-factor authentication.

If you lose your recovery codes you can generate new ones, invalidating all previous codes.

[Disable two-factor authentication](#) [Regenerate recovery codes](#)

---

### Register Universal Two-Factor (U2F) Device

Use a hardware device to add the second factor of authentication.

As U2F devices are only supported by a few browsers, we require that you set up a two-factor authentication app before a U2F device. That way you'll always be able to log in - even when you're using an unsupported browser.

[Set up new U2F device](#) Your U2F device needs to be set up. Plug it in (if not already) and click the button on the left.

**U2F Devices (0)**

You don't have any U2F devices registered yet.



# Protecting Access - GitLab

The screenshot shows a web browser window with the URL `https://gitlab.com/profile...`. The page title is "Two-Factor Authentication · Account". The left sidebar contains a "User Settings" menu with options: Profile, Account (selected), Billing, Applications, Chat, Access Tokens, Emails, Password, Notifications, SSH Keys, GPG Keys, and Collapse sidebar. The main content area is titled "User Settings > Two-Factor Authentication > Account".

### Register Two-Factor Authenticator

You've already enabled two-factor authentication using one time password authenticators. In order to register a different device, you must first disable two-factor authentication.

Use an one time password authenticator on your mobile device or computer to enable two-factor authentication (2FA).

If you lose your recovery codes you can generate new ones, invalidating all previous codes.

[Disable two-factor authentication](#) [Regenerate recovery codes](#)

---

### Register Universal Two-Factor (U2F) Device

Trying to communicate with your device. Plug it in (if you haven't already) and press the button on the device now.

Use a hardware device to add the second factor of authentication.

U2F Devices (0)

You don't have any U2F devices registered yet.

# Protecting Access - GitLab

The screenshot shows a web browser window with the URL `https://gitlab.com/profile...`. The page title is "Two-Factor Authentication · Account". The left sidebar contains "User Settings" with a sub-menu including Profile, Account (selected), Billing, Applications, Chat, Access Tokens, Emails, Password, Notifications, SSH Keys, GPG Keys, and Collapse sidebar. The main content area is titled "User Settings > Two-Factor Authentication > Account".

### Register Two-Factor Authenticator

Use an one time password authenticator on your mobile device or computer to enable two-factor authentication (2FA).

You've already enabled two-factor authentication using one time password authenticators. In order to register a different device, you must first disable two-factor authentication.

If you lose your recovery codes you can generate new ones, invalidating all previous codes.

[Disable two-factor authentication](#) [Regenerate recovery codes](#)

---

### Register Universal Two-Factor (U2F) Device

Use a hardware device to add the second factor of authentication.

Your device was successfully set up! Give it a name and register it with the GitLab server.

[Register U2F device](#)

**U2F Devices (0)**

You don't have any U2F devices registered yet.



# Protecting Access - GitLab

The screenshot shows the GitLab user settings page for Two-Factor Authentication. The browser address bar shows the URL `https://gitlab.com/profile...`. The page has a navigation sidebar on the left with options like Profile, Account, Billing, Applications, Chat, Access Tokens, Emails, Password, Notifications, SSH Keys, and GPG Keys. The main content area is titled "Your U2F device was registered!" and contains two sections: "Register Two-Factor Authenticator" and "Register Universal Two-Factor (U2F) Device".

**Register Two-Factor Authenticator**

You've already enabled two-factor authentication using one time password authenticators. In order to register a different device, you must first disable two-factor authentication.

If you lose your recovery codes you can generate new ones, invalidating all previous codes.

[Disable two-factor authentication](#) [Regenerate recovery codes](#)

---

**Register Universal Two-Factor (U2F) Device**

[Set up new U2F device](#) Your U2F device needs to be set up. Plug it in (if not already) and click the button on the left.

Use a hardware device to add the second factor of authentication.

As U2F devices are only supported by a few browsers, we require that you set up a two-factor authentication app before a U2F device. That way you'll always be able to log in - even when you're using an unsupported browser.

**U2F Devices (1)**

Name	Registered On	
YSK1	Jun 6, 2019	<a href="#">Delete</a>

## What else?

### **I use 1Password on my Mac and phones. I have a family license.**

*Supports YubiKey if I use the cloud based 1Password ecosystem*

*I'm a little cheap there. I'd prefer to do my own storage, so I don't want to keep paying for a service that might vanish one day with all my passwords.*

### **I was going to set up KeyPassXC for YubiKey access (but my existing key has issues)**

*KeypassXC runs on MacOS and Linux*

*Can use a few items as decryptors – password, keyfile, and YubiKey*

**Linux-Ottawa**  
linux-ottawa.org

## *GPG encrypted email on my mac*

The process of adding your GPG keys is a little convoluted. I had to find a walkthrough the first time I did it and I'm not sure I really did it correctly. It works, but I have not tried it again. We can go through it as an exercise and load keys on another YubiKey.

The process of sending an email will be a demo item using the original key.



Linux-Ottawa  
linux-ottawa.org

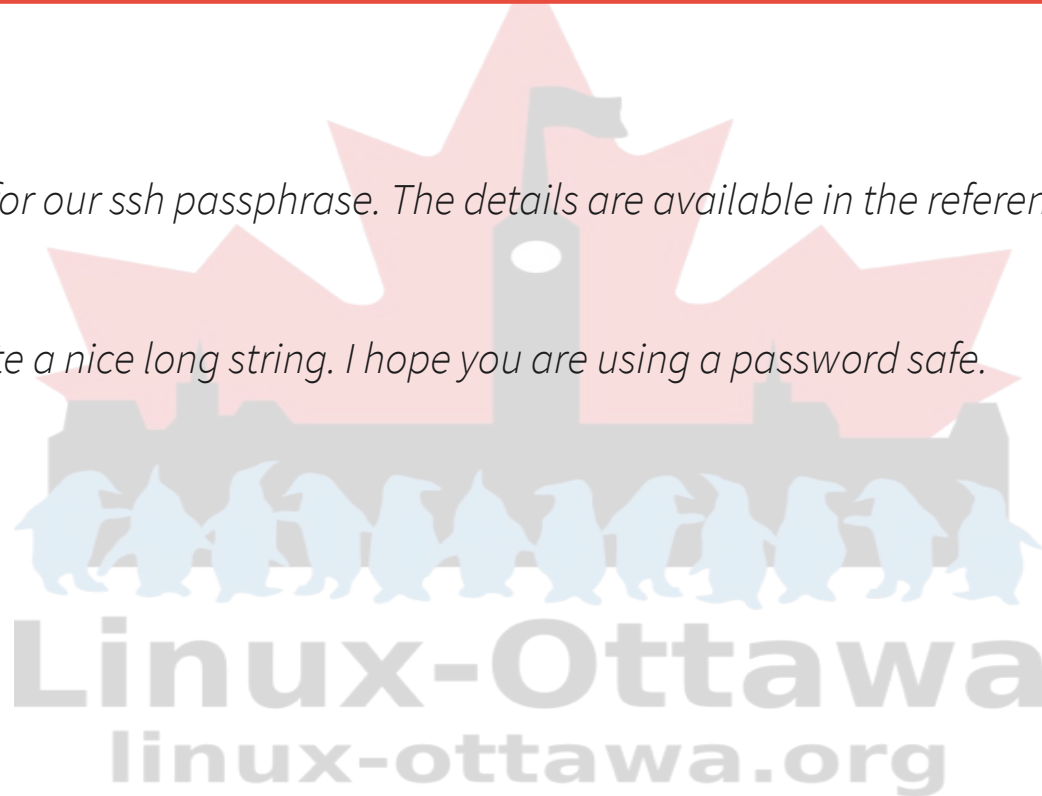
## *Other things we can do*

### **SSH Keys**

*We can use the YubiKey for our ssh passphrase. The details are available in the references*

### **Password Generator**

*Hit the button to generate a nice long string. I hope you are using a password safe.*



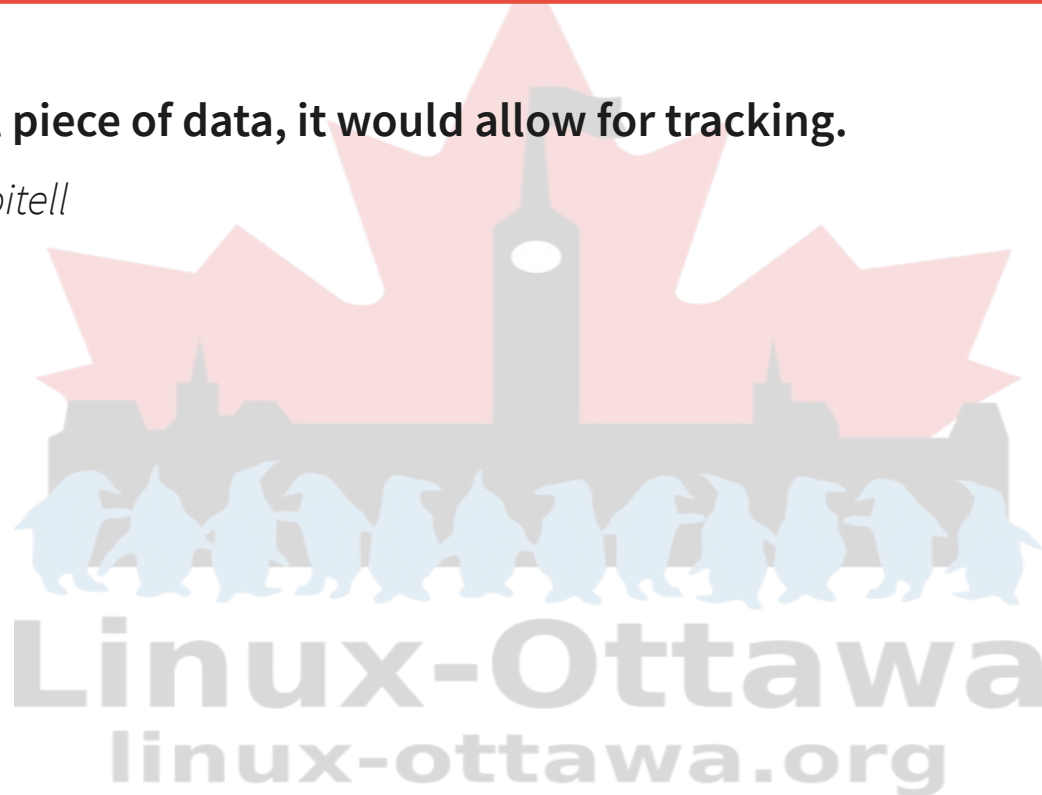


Demo Time

## *Leaking of YubiKey serial number*

While not exactly a vital piece of data, it would allow for tracking.

*<https://ssg.github.io/yubitell>*



## ***Sending encrypted email***

Not having to leave your private keys on the computer is a good thing.

Not having to remember a passphrase is also nice.

One thing of note – this device is a roach motel for private keys. They can get installed, but they can not be extracted.

*Wiped, yes.*

*Extracted, no!*



**Linux-Ottawa**  
linux-ottawa.org

## *A Recommendation...*

If you have anything you want to protect, using one of these devices (not just YubiKey) would be a good idea.

Buy two. Having a backup is also a good idea, a very good idea



**Linux-Ottawa**  
linux-ottawa.org



## *References/Links for more information*

<https://en.wikipedia.org/wiki/YubiKey>

<https://help.twitter.com/en/managing-your-account/two-factor-authentication#security-key>

<https://hackernoon.com/avoid-leaking-your-identity-with-yubikey-92539b6608a>

Using your yubikey

<https://www.engineerbetter.com/blog/yubikey-all-the-things/>

<https://www.yubico.com/2018/07/5-simple-ways-to-get-started-with-your-yubikey-2-2/>

<https://medium.com/@kamushadenes/making-the-most-out-of-your-yubikey-4-b64a1d19a56b>

<https://ocramius.github.io/blog/yubikey-for-ssh-gpg-git-and-local-login/>