



Phishing

"Phishing" es cuando se engaña a la gente para que entregue información secreta (como sus contraseñas o los datos de su tarjeta de crédito) en un sitio web falso que se disfraza para parecer un sitio web de confianza.

A la gente se le envían enlaces a estos sitios web de phishing falso en correos electrónicos o mensajes instantáneos. ¿Cómo pueden saber si es seguro hacer clic en un enlace?

En este proyecto, conocerás la investigación que se está realizando para entrenar a los sistemas de aprendizaje automático a fin de que puedan predecir si un enlace es a un sitio web de phishing o a un sitio web legítimo.



Esta hoja de trabajo de proyecto está bajo una licencia de Creative Commons Reconocimiento-Licencia de Compartir-Alike
<http://creativecommons.org/licenses/by-nc-sa/4.0/>

Empecemos por mirar algunas de las partes que componen una URL (dirección web):



número de puerto	<p>A qué puerto conectar.</p> <p>Si no se especifica, el navegador web utilizará el 80 (si el protocolo es "http") o el 443 (si el protocolo es "https").</p> <p>El 80 y el 443 son los números de puerto "estándar" que se utilizan casi siempre, pero los sitios web pueden utilizar otros puertos si lo desean.</p>
host	<p>host con el que se conectará el servidor web.</p> <p>Esta puede ser una dirección numérica con puntos (denominada "dirección IP") como 104.20.74.246</p> <p>O puede ser un nombre de host basado en texto (denominado un "nombre de dominio") como <code>machinelearningforkids.co.uk</code> que el navegador web utilizará para buscar la dirección IP de (llamada "búsqueda DNS").</p> <p>Puedes utilizar <code>https://whois.net</code> para buscar la dirección IP de un nombre de dominio. Esto también te permitirá averiguar cuándo se ha registrado un nombre de dominio y cuánto tiempo va a transcurrir antes de que caduque el registro de nombres de dominio.</p>
contraseña	<p>La contraseña que debe utilizarse para identificar al usuario</p> <p>Si no se especifica, el navegador de Internet no utilizará una contraseña.</p>
usuario	<p>El nombre de usuario a utilizar para identificar al usuario</p> <p>Si no se especifica, el navegador web no utilizará un nombre de usuario.</p>
protocolo	<p>El protocolo de comunicación que debe utilizar el navegador de Internet.</p> <p>Este será "https" para conexiones seguras, o "http" para conexiones inseguras.</p>

Otra cosa que entender es "redireccionar". A veces, una dirección web te enviará a otra dirección web. Por ejemplo, si visitas `https://bit.ly/39XEEfP` terminas en `https://machinelearningforkids.co.uk` porque la primera dirección es una redirección. Redireccionar oculta el destino real de una URL. Puedes unirte a varios. Por ejemplo, si visitas `https://bit.ly/35Jnlf8` terminas en `https://www.bbc.co.uk/noticias` después de 4 redirecciones.

`https://bit.ly/35Jnlf8` ➡ `https://tinyurl.com/wrcfg53` ➡ `https://bbc.in/2FICKBL` ➡ `http://news.bbc.co.uk` ➡ `http://www.bbc.co.uk/news`

Ahora mira este URL:

<http://login.bankofamerica.com@www.josueizagirre.com/wpcontent/cache/login.bankofamerica.com.uplogad/update.html>

La página web se parece a esto:

The screenshot shows a web page designed to look like the Bank of America online banking login page. At the top left is the Bank of America logo and a 'Sign In' link. At the top right is a 'Secure Area' link and a language selector 'En Español'. Below the header is a red banner that says 'Sign In to Online Banking'. The main content area is divided into two columns. The left column contains a form with the following fields: 'To Update Your Account, please enter the following.' followed by 'Your complete Social Security number (SSN) Numbers only' with an input field, 'ATM PIN' with an input field, 'Your complete card number. Use your ATM/Debit Card, Credit Card. Numbers only' with an input field, 'Expiry Date' with two dropdown menus (one showing '01' and the other '2020'), and 'Code Verification Number' with an input field and a note '3 or 4 digits AFTER the credit card number in the signature area of the card'. The right column contains links: 'Sign-in help', 'Forgot your Online ID?', 'Forgot your Passcode?', 'Not using Online Banking?', 'Enroll now', 'Learn more about Online Banking', and 'Service Agreement'. At the bottom of the page, there is a small link: 'POP Email Address Activation - Email Address for Alerts Delivery'.

Este sitio web no tiene nada que ver con el verdadero Banco de América.

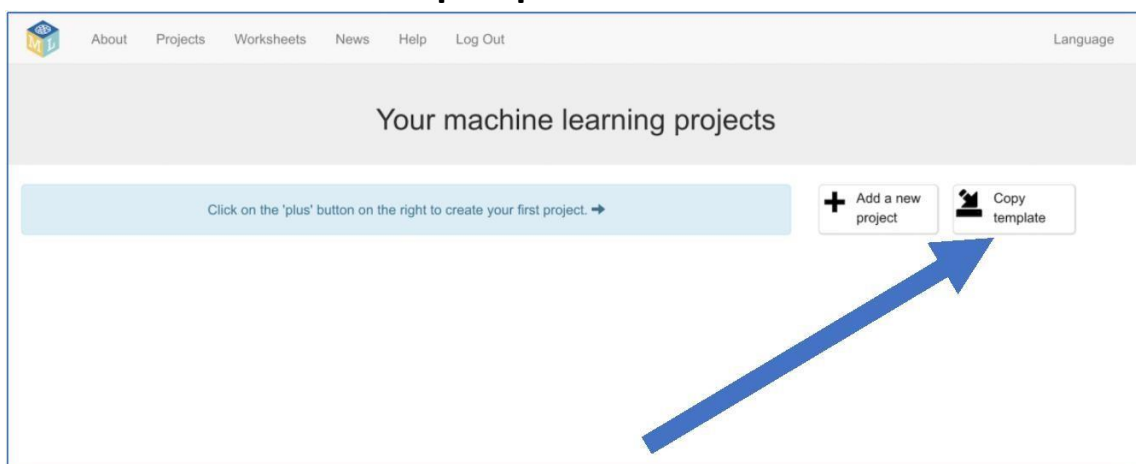
Esta es una URL de phishing

¿Cómo lo sabes?

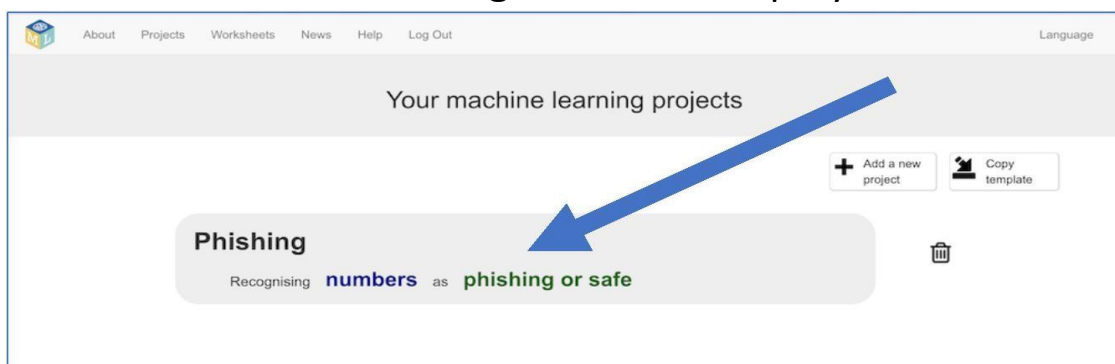
número de puerto	La página está utilizando el puerto 80-un sitio web de la banca real estaría usando el puerto estándar seguro 443.
host	El nombre de dominio para el sitio web es <code>www.josueizagirre.com</code> , que no es el verdadero dominio oficial para Bank of America.
nombre de usuario	La URL está dando el nombre de usuario " <code>login.bankofamerica.com</code> " aunque el servidor web ignora esto. Poner un usuario como este aquí es un truco para hacer que parezca que la dirección web es " <code>login.bankofamerica.com</code> "
protocolo	La página está usando " <code>http</code> "- un sitio web de la banca real estaría usando el protocolo seguro " <code>https</code> ".

¿Crees que una ordenador podría ser entrenado para predecir que esta URL era para un sitio web de phishing?

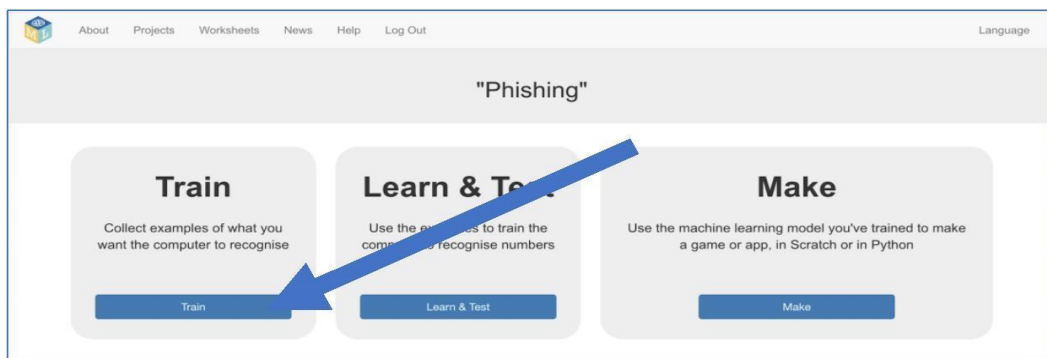
1. Ir a <https://machinelearningforkids.co.uk/> en un navegador web
2. Haz clic en "Empezar"
3. Haz clic en "**Iniciar sesión**" y escribe tu usuario y contraseña.
Si no tienes un usuario, pídele a tu profesor o jefe de grupo que te cree uno.
Si no recuerdas tu usuario o contraseña, pídele a tu profesor o líder de grupo que la reinicie.
4. Pulsa en "**Proyectos**" en la barra de menú superior
5. Haz clic en el botón "**Copiar plantilla**".



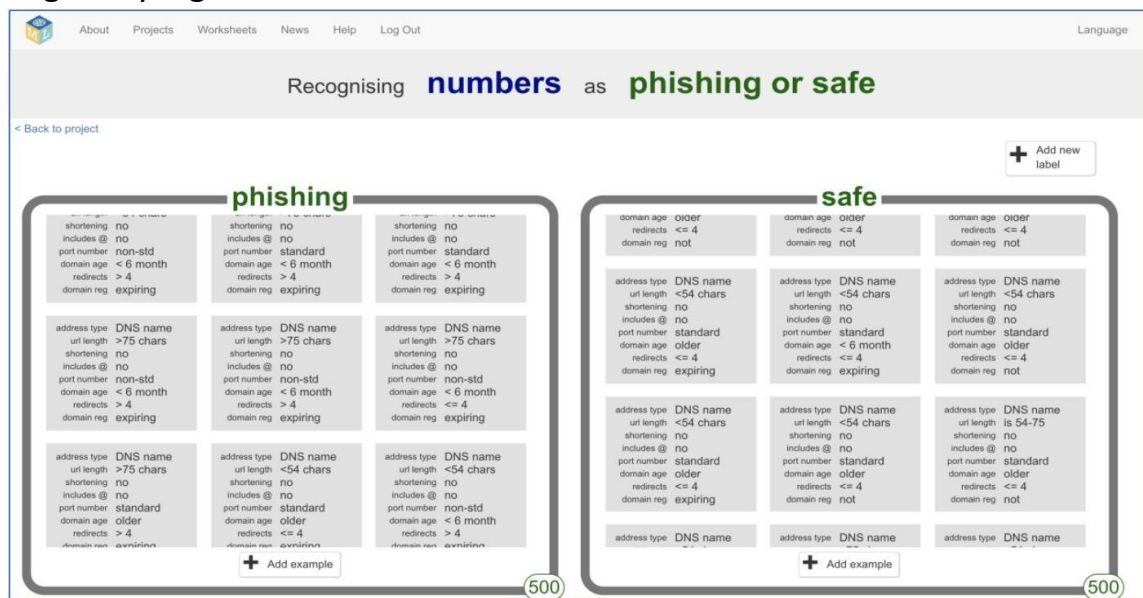
6. Busca la plantilla Phishing y luego haz clic en "**Import**".
7. Ahora deberías ver "**Pishing**" en tu lista de proyectos. Haz clic en él.



8. Esta plantilla incluye un conjunto de datos de aprendizaje de ejemplo para ayudarte a ahorrar tiempo. Haz clic en el botón **"Entrenar"** para revisar los datos de entrenamiento.



Los datos de entrenamiento de muestra incluyen detalles sobre 1000 URL. 500 fueron identificados como sitios web de phishing, y 500 fueron identificados como sitios web seguros y legítimos.



Cada URL se ha descrito utilizando los atributos siguientes:

atributo	descripción	posibles valores	motivo
tipo de dirección	¿Se ha proporcionado la dirección del host en la URL como una dirección IP numérica, o un nombre de dominio basado en texto?	Nombre del DNS si la URL tenía un nombre de dominio basado en texto (como "machinelearningforkids.co.uk") Dirección IP si el URL tenía un nombre de host numérico (como "104.20.75.246")	El uso de direcciones IP es inusual, y a veces una forma de ocultar el destino real de una dirección web
atributo	descripción	posibles valores	motivo

longitud de URL	¿Qué tan larga es la URL?	<54 caracteres si la URL tiene menos de 54 caracteres. entre 54-75 si la URL tiene entre 54 y 75 caracteres. >75 caracteres si la URL tiene más de 75 caracteres.	Las URL de phishing en los correos electrónicos tienden a ser más largas, ya que es más fácil ocultar la parte sospechosa de la dirección si la URL es muy larga.
abreviación	¿Utiliza la URL un servicio de abreviación, como bit.ly o tinyurl.com? Los servicios de acortamiento usan redirecciones para hacer una versión corta de una dirección web larga.	sí si la URL utiliza un servicio de acortamiento reconocido no si la URL no utiliza un servicio de acortamiento reconocido	Los servicios de acortamiento, como cualquier redireccionamiento, hacen difícil saber el verdadero destino de una URL, por lo que son útiles para disfrazar un enlace de phishing.
incluye @	¿Incluye la URL el símbolo @?	sí si la URL incluye una @ no si el URL no incluye @	Los enlaces legítimos con usuario/contraseñas son inusuales. Los enlaces de phishing aprovechan el hecho de que muchos usuarios no se dan cuenta de que nada antes de una @ es un usuario/contraseña y ponen una dirección web falsa en su lugar.
número de puerto	¿Utiliza la URL los números de puerto estándar para las páginas web?	estándar si el URL utiliza el puerto estándar 80 o 443 no estándar si el URL utiliza un número de puerto personalizado y no estándar	El uso de números de puerto no estándar es inusual.
edad de dominio	¿Cuánto tiempo hace que se registró el nombre de dominio? Por ejemplo, machinelearningforkids.co.uk se registró el 17 de abril de 2017, lo que puede comprobarse en whois.net	< 6 meses si el nombre de dominio se registró hace menos de 6 meses más antiguo si el dominio fue registrado hace más de 6 meses	Los sitios web de phishing a menudo no existen hace mucho tiempo. Son reportados y descubiertos rápidamente, así que los atacantes crean nuevos sitios y registran nuevos dominios. Esto significa que un enlace a un dominio que se registró hace mucho tiempo puede ser más probable que sea legítimo.
redireccionar	¿Cuántas redirecciones tiene que seguir el navegador para llegar a la página final?	<= 4 si hay cuatro o menos redirecciones desde el URL a la página web final > 4 si hay más de cuatro redirecciones para llegar a la página web final	Una o dos redirecciones es común para ayudar a los desarrolladores de sitios web a administrar su sitio, pero más que eso es posiblemente sospechoso como señal de que se está tratando de ocultar el verdadero destino de una URL.

atributo	descripción	posibles valores	motivo
----------	-------------	------------------	--------

registro de dominio	¿Se ha registrado el dominio durante muchos años, o va a expirar pronto?	expira si el nombre de dominio va a expirar en el próximo año no si el nombre de dominio no va a expirar en el próximo año	Los sitios web de phishing a menudo no existen por mucho tiempo. Se denuncian y se descubren rápidamente, por lo que los atacantes sólo registran los nombres de dominio durante un corto período de tiempo para ahorrar costes. Es más probable que las grandes organizaciones de buena reputación registren nombres de dominio durante varios años.
---------------------	--	---	--

Por ejemplo:

<http://login.bankofamerica.com@www.josueizagirre.com/wpcontent/cache/login.bankofamerica.com.upload/date.html>

se mostrarán en los datos de entrenamiento como:

```
address type  DNS name
url length   >75 chars
shortening    no
includes @    yes
port number   standard
domain age    older
redirects     <= 4
domain reg    expiring
```

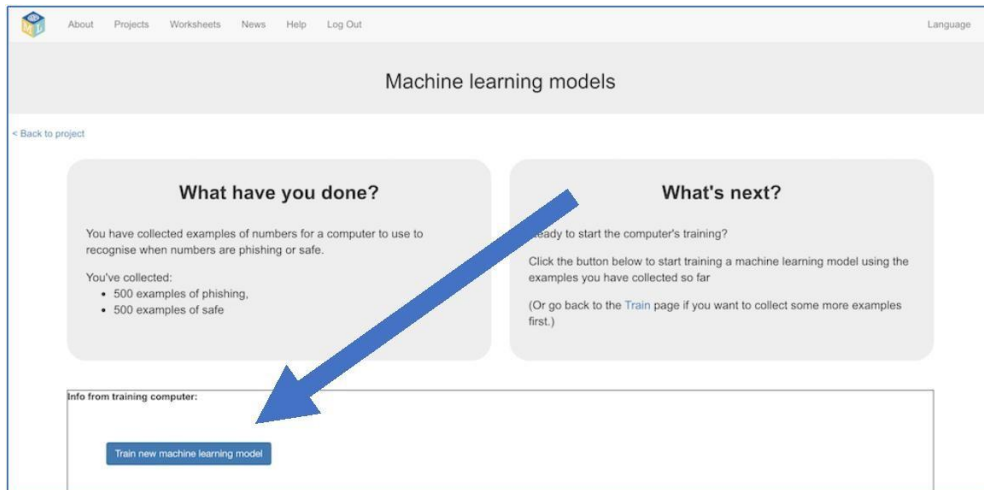
Desplázate por el resto de los datos de entrenamiento que has importado.

Las URLs de phishing del proyecto de ejemplo fueron reportados por los usuarios de todo el mundo al sitio web <https://phishtank.com> ya que es una fuente confiable para obtener un gran número de enlaces de phishing. Los atributos elegidos para describir las URL son sólo un ejemplo para el primer proyecto de inicio. Después de haberlo intentado, observarás algunos otros atributos que se pueden utilizar para entrenar mejores modelos de aprendizaje automático.

9. Pulsa el enlace "<Volver al proyecto" en la parte superior izquierda.

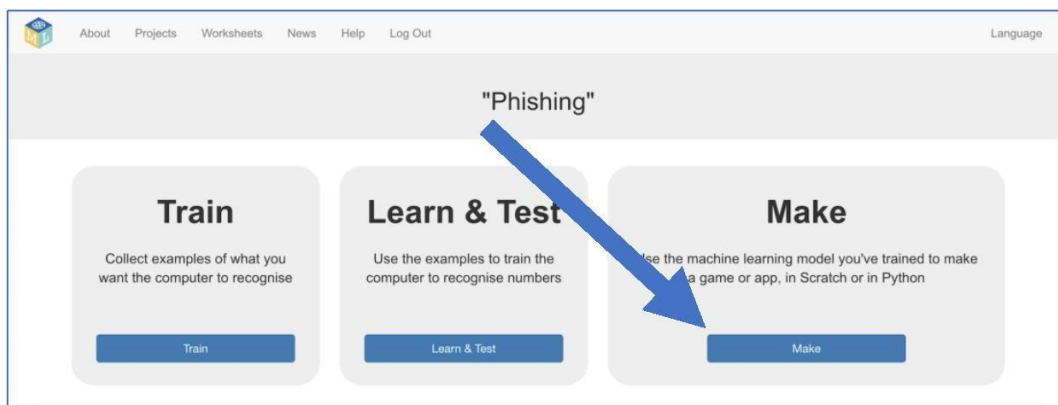
10. Haz clic en el botón "Aprender & Probar".

11. Haz clic en el botón "Entrenar un nuevo modelo".

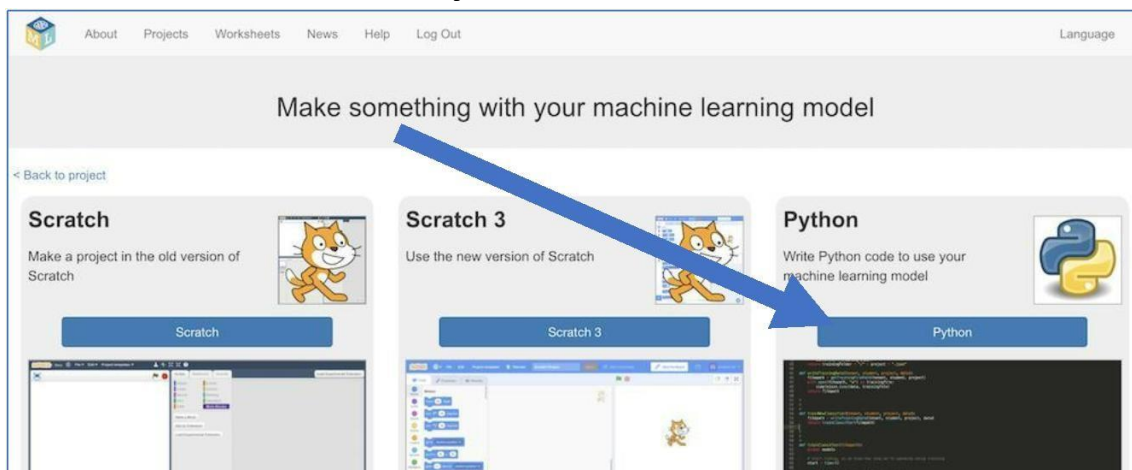


12. Pulsa el enlace "<Volver al proyecto" en la parte superior izquierda.

13. Haz clic en el botón "Crea".

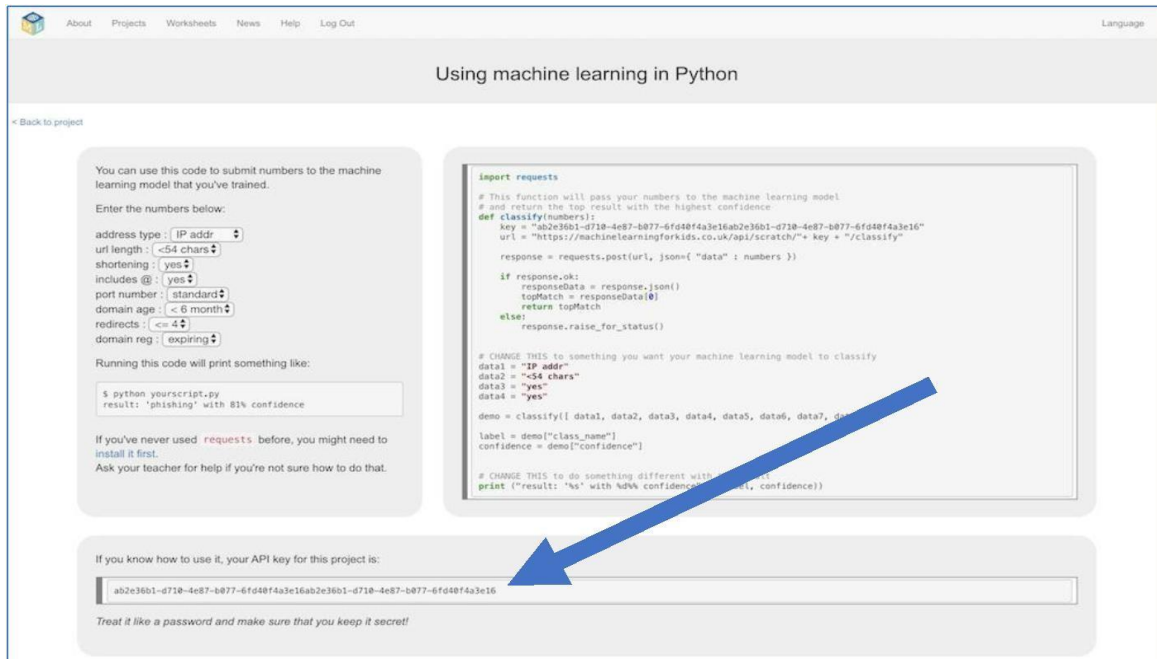


14. Haz clic en el botón "Python".



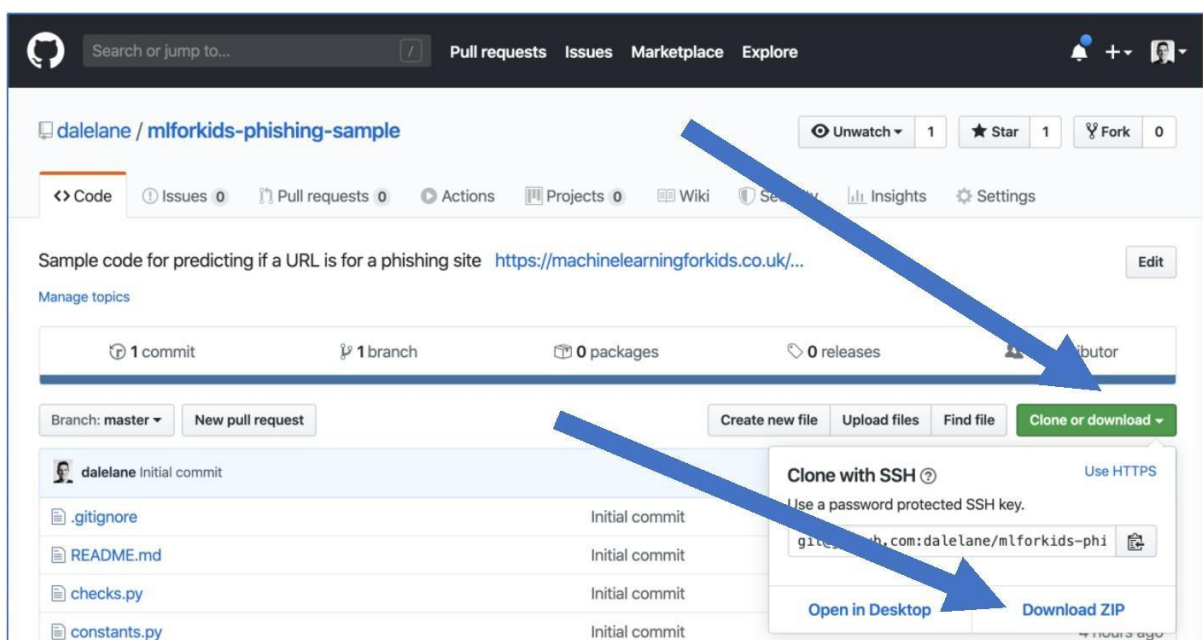
15. Toma nota de tu "clave de API"

Esto es como un código secreto que tu programa Python podrá utilizar para acceder a tu modelo de aprendizaje automático.



Nota: la clave de API en la captura de pantalla anterior es falsa. Las claves API son las contraseñas de like. Yo no compartiría mi clave de API real, y tú no deberías compartir la tuya.

16. Accede a <https://github.com/dalelane/mlforkids-phishing-sample> y descargar un zip con el proyecto Python de ejemplo



17. Descomprime el archivo zip del proyecto

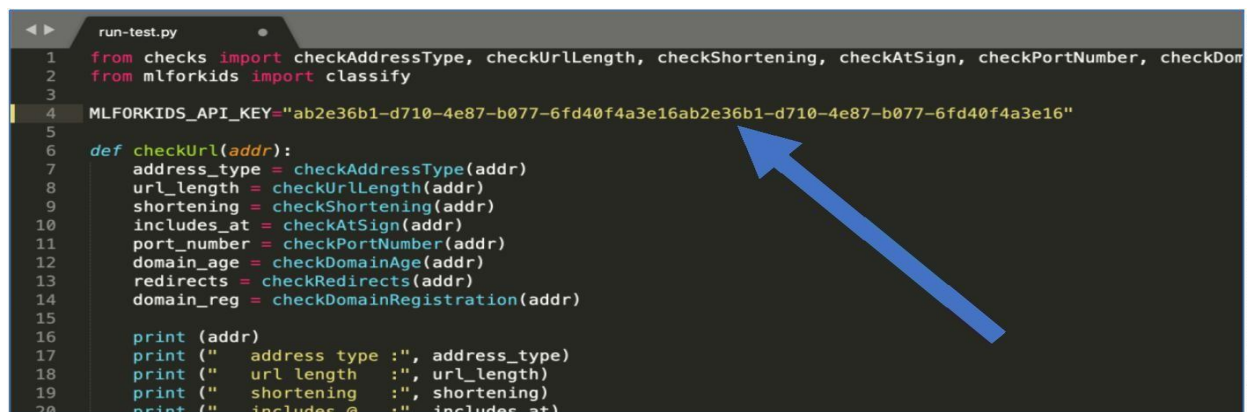
- 18.** Abre una línea de comandos en la carpeta en la que has descomprimido el código del proyecto.
- 19.** El archivo requirements.txt enumera las bibliotecas de terceros que necesitará para ejecutar el código. La forma más sencilla de instalar todo esto es ejecutar el comando:

```
pip3 install -r requirements.txt
```

Pídele a tu profesor o líder de grupo que te ayude si no estás seguro de cómo hacer esto.

```
Dales-MBP-2:mlforkids-phishing-sample-master dale$ pip3 install -r requirements.txt
Collecting certifi==2019.11.28 (from -r requirements.txt (line 1))
  Using cached https://files.pythonhosted.org/packages/b9/63/df58cac98ead5b06c55a399c3bf1db9da7b5a24de7890bc9cfd5dd9e99/certifi-2019.11.28-py2.py3-none-any.whl
Requirement already satisfied: chardet==3.0.4 in /Library/Frameworks/Python.framework/Versions/3.7/lib/python3.7/site-packages (from -r requirements.txt (line 2)) (3.0.4)
Requirement already satisfied: future==0.18.2 in /Library/Frameworks/Python.framework/Versions/3.7/lib/python3.7/site-packages (from -r requirements.txt (line 3)) (0.18.2)
Requirement already satisfied: idna==2.8 in /Library/Frameworks/Python.framework/Versions/3.7/lib/python3.7/site-packages (from -r requirements.txt (line 4)) (2.8)
Collecting python-dateutil==2.8.1 (from -r requirements.txt (line 5))
  Using cached https://files.pythonhosted.org/packages/44/70/d60450c3d448ef87586924207ae8907090de0b306af2bce5d134d78615cb/python_dateutil-2.8.1-py2.py3-none-any.whl
Requirement already satisfied: python-whose==0.7.2 in /Library/Frameworks/Python.framework/Versions/3.7/lib/python3.7/site-packages (from -r requirements.txt (line 6)) (0.7.2)
Requirement already satisfied: requests==2.22.0 in /Library/Frameworks/Python.framework/Versions/3.7/lib/python3.7/site-packages (from -r requirements.txt (line 7)) (2.22.0)
Collecting six==1.13.0 (from -r requirements.txt (line 8))
  Using cached https://files.pythonhosted.org/packages/65/26/32b8464df2a97e6dd1b656ed26b2c194606c16fe163c695a992b36c11cdf/six-1.13.0-py2.py3-none-any.whl
Collecting urllib3==1.25.3 (from -r requirements.txt (line 9))
  Using cached https://files.pythonhosted.org/packages/b4/4b/d837291310ee1ccc242ceb6efbd9eb21539649f193a7c8c86ba15b98539/urllib3-1.25.3-py2.py3-none-any.whl
Installing collected packages: certifi, six, python-dateutil, urllib3
Found existing installation: certifi 2019.6.16
Uninstalling certifi-2019.6.16:
  Successfully uninstalled certifi-2019.6.16
Found existing installation: urllib3 1.25.3
Uninstalling urllib3-1.25.3:
  Successfully uninstalled urllib3-1.25.3
Successfully installed certifi-2019.11.28 python-dateutil-2.8.1 six-1.13.0 urllib3-1.25.3
```

- 20.** Abre el archivo "run-test.py" en el editor de código favorito y actualiza MLFORKIDS_API_KEY en línea 4. Introduce la clave de API que ha encontrado en el paso 15.



```
run-test.py
1 from checks import checkAddressType, checkUrlLength, checkShortening, checkAtSign, checkPortNumber, checkDomain
2 from mlforkids import classify
3
4 MLFORKIDS_API_KEY="ab2e36b1-d710-4e87-b077-6fd40f4a3e16ab2e36b1-d710-4e87-b077-6fd40f4a3e16"
5
6 def checkUrl(addr):
7     address_type = checkAddressType(addr)
8     url_length = checkUrlLength(addr)
9     shortening = checkShortening(addr)
10    includes_at = checkAtSign(addr)
11    port_number = checkPortNumber(addr)
12    domain_age = checkDomainAge(addr)
13    redirects = checkRedirects(addr)
14    domain_reg = checkDomainRegistration(addr)
15
16    print(addr)
17    print("    address type :", address_type)
18    print("    url length    :", url_length)
19    print("    shortening    :", shortening)
20    print("    includes @    :", includes_at)
```

- 21.** Ejecutar el programa
- ```
python3 run-test.py
```

El programa utilizará el modelo de aprendizaje automático que has entrenado para predecir si una variedad de URL es segura o phishing:

**<https://machinelearningforkids.co.uk/ayuda>**

Esperemos que se prediga que esto es seguro, ya que yo envío este enlace a la gente muy a menudo!

**<https://www.bbc.co.uk>**

Se trata de un sitio web muy antiguo y respetable, registrado en agosto de 1996. Esperemos que piense que es un enlace seguro.

**[https://en.wikipedia.org/wiki/Machine\\_learning](https://en.wikipedia.org/wiki/Machine_learning)**

La página de Wikipedia de Aprendizaje Automático es otro enlace seguro.

**[https://91.198.174.192/wiki/Machine\\_learning](https://91.198.174.192/wiki/Machine_learning)**

Esta es la misma dirección que arriba - es la dirección de la página de Wikipedia sobre Aprendizaje Automático, pero usando la dirección IP para guardar el navegador web que necesita para buscar la dirección del nombre de dominio de Wikipedia. Es un enlace seguro a visitar, pero es inusual describirlo usando la dirección IP, así que el modelo de aprendizaje automático podría (¿incorrectamente?) pensar que es sospechoso.

**<https://mickey@bit.ly/35Jnlf8>**

Esto realmente apunta al sitio web de la BBC News <https://www.bbc.co.uk>, pero utiliza varias redirecciones para esconder eso, así que el modelo de aprendizaje automático probablemente prediga que es sospechoso.

**<https://login.bankofamerica.com@www.josueizagirre.com/wp-content/cache/login.bankofamerica.com.uplogad/update.html>**

Este es un sitio web de phishing que pretendía ser una página del Bank of America. Esperemos que el modelo de aprendizaje automático prediga correctamente que es sospechoso.

**<http://flinxdeicdccc.com/2612aa892d962d6f8056b195ca6e550d/tnFBsV27sc3kIMJg0Z8snqenra mMHIXz.php?country=US-United%20States&lang=en>**

Este es otro sitio web de phishing que esperamos que el modelo de aprendizaje automático reconozca correctamente.

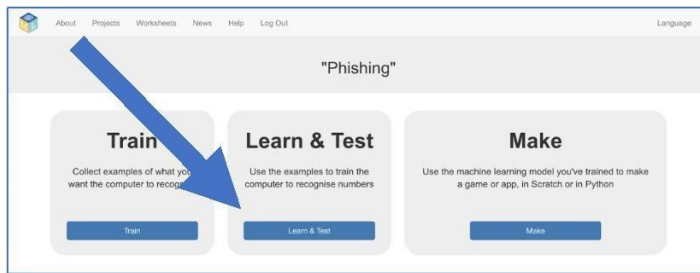
## **22.** Edita el archivo "`run-test.py`" en un editor de código para probar otras URL.

*Consulae cómo se probaron las URL de ejemplos anteriores para aprender a utilizar el `checkUrl` función.*

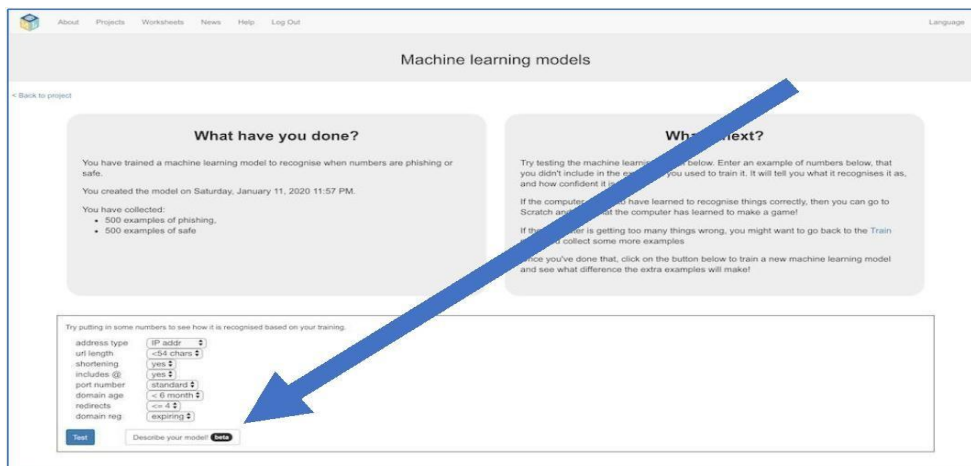
*Prueba las direcciones de sitios web legítimos que utilices y confíes para ver si el modelo predice que están a salvo.*

*Prueba las direcciones de los sitios web de phishing para ver si el modelo predice que no se puede confiar en ellos. Si necesitas encontrar URLs para phishing, <https://phishtank.com> es un buen lugar para mirar. Busca las nuevas URL que sólo se han notificado como sitios de phishing para ver cómo se puede hacer frente a los modelos ML.*

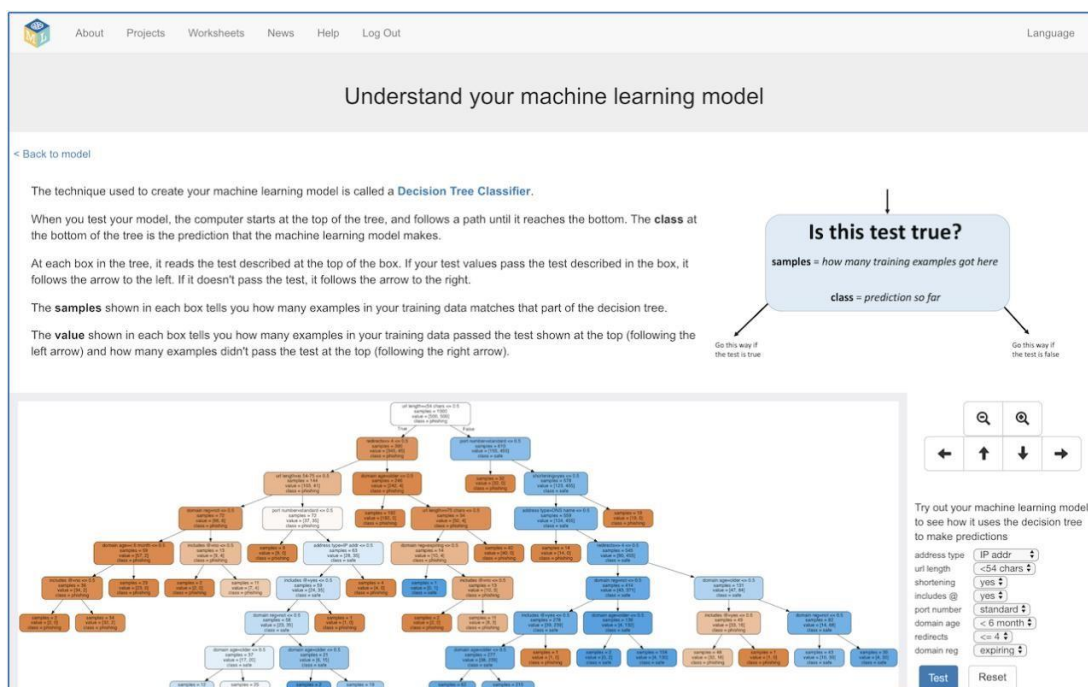
23. Haz clic en el botón "**Aprender & Probar**" de Machine Learning for Kids.



24. Haz clic en el botón "**Describe your model**".



25. Examina la visualización para el modelo de aprendizaje automático. Esto muestra cómo el modelo está realizando predicciones. Utiliza el botón **Test** para ver cómo funciona.



## ¿Qué has hecho?

Has utilizado un conjunto de datos prepreparados para entrenar un tipo de modelo de aprendizaje automático llamado "clasificador de árbol de decisión" para que pueda predecir si una URL va a ser un sitio web legítimo o un sitio web de phishing.

Has utilizado el modelo de aprendizaje automático de un programa de Python, que has modificado para que pueda hacer predicciones sobre tus propias direcciones web.

## 26. ¡ Planifica tu propio proyecto!

*La importación de la plantilla significa que no tienes que decidir qué características debe utilizar el modelo de aprendizaje automático.*

*El proyecto ha utilizado ocho características (descritas en el paso 8 anterior).*

*Piensa en cómo podría mejorar el modelo de aprendizaje automático añadiendo características adicionales. ¿Qué otros atributos acerca de los sitios web crees que ayudarán al modelo de aprendizaje automático a ser mejor al reconocer las URL de phishing? Las siguientes páginas incluyen enlaces a algunos proyectos de investigación sobre este tema que podrían ayudar a darles algunas ideas.*

## Investigación de aprendizaje automático sobre Phishing

Los modelos de aprendizaje automático para reconocer las URL de phishing es un tema activo en la investigación ML.

Intenta ver algunos de los documentos que se listan a continuación.

Incluso si no entiendes todo lo que dicen, la ejecución de tu propio experimento debería ayudarte a conseguir la idea general.

¿Alguna de estos papeles te da una idea para tu propio proyecto?

### **<https://ibm.biz/phishing-hassan>**

En este artículo se describe la investigación de Hassan sobre 30 atributos diferentes de los enlaces de phishing. Doce de estos se basan en atributos de la URL, como hiciste en el proyecto. Algunos atributos que se describen se basan en la forma en que se visualizó el enlace. Por ejemplo, si el enlace de phishing estaba en un correo electrónico, ¿se visualizaba el URL cuando se pasa el puntero del ratón por encima del enlace?

### **<https://ibm.biz/phishing-rajab>**

En este artículo se describe la investigación de Rajab sobre cómo decir qué características son las más útiles para reconocer las URL de phishing. Identificaron el protocolo (si la página se inicia con http o https) y si el certificado SSL para un sitio web está firmado por un origen de confianza como dos de los atributos más significativos que se deben utilizar.

### **<https://ibm.biz/phishing-joshi>**

Joshi & Pattanshetti describe 48 atributos que encontraron para ser útiles, incluyendo si la página contiene formularios seguros, si los formularios en la página tratan de enviar correos electrónicos, si el icono de la barra de direcciones parece válido, y muchos más.



### **<http://ibm.biz/phishing-basnet>**

Basnet, Sung & Lui describen cómo revisaron 177 atributos diferentes de URL's para identificar el más útil para entrenar un modelo de aprendizaje automático.

Algunos de ellos revisaron el contenido de las páginas web, no sólo la dirección URL, como contar el número de enlaces en la página, si la página contiene iframes, si tiene campos de contraseña en ella, etc.

### **<https://ibm.biz/phishing-mohammad>**

Mohammad, Thabtah y McCluskey describen una variedad de características que se identifican como útiles, algunas basadas en URL como lo han hecho, pero algunas basadas en el uso de JavaScript en páginas web, y algunos usando datos de fuentes externas como Google, PhishTank, Alexa, y otros.

Describen los atributos que han utilizado muy claramente, y debes reconocer varias de estas características de las características del proyecto.

### **<https://ibm.biz/phishing-shirazi>**

Shirazi, Haefner & Ray se basan en el artículo Mohammad et al descrito más arriba, y dicen cómo identificaron los 10 atributos más útiles que usaban para hacer "Fresh-Phish".

Uno de ellos fue el ranking de Google para una URL, confiando en Google para tener un rango alto para sitios web legítimos.

### **<https://ibm.biz/phishing-whittaker>**

Whittaker, Ryner & Nazif describen cómo Google ha evaluado las URL para identificar las páginas de phishing.

Describen características como la presencia de términos como "customerservice" en la URL, que se descubrió que eran más comunes en los sitios de phishing.