**Phishing Attacks**

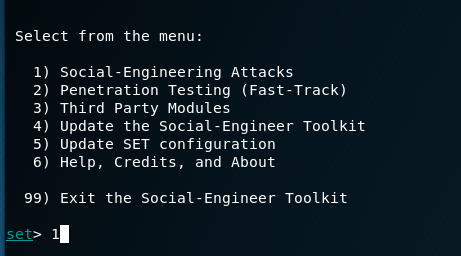
**With the help of kali linux:**

**Tools used: Social Engineering Toolkit**

**Steps:**

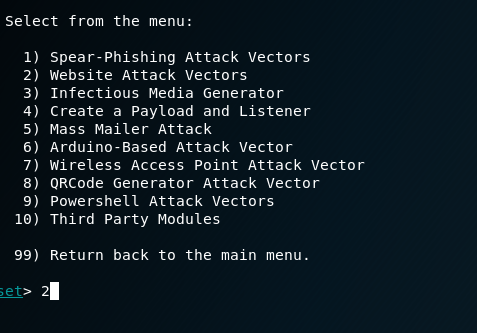
**1)execute command sudo setoolkit in Terminal in KaliLinux**

**2)the below shows the menu and the different options,since we are carrying out attacks we obviously pick 1**

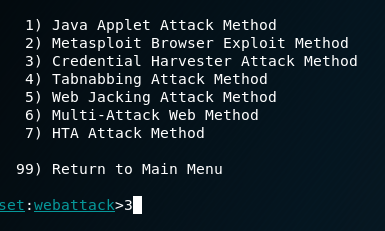
****

**3) As we are carrying out attacks based on website by cloning we choose 2**

**=Website Attack Vectors**

****

**4) As we are aiming to extract the user info we go for the credential harvesting method=3**

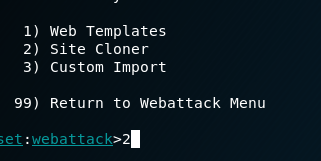
****

**5) for option1) we have already builtin templates but since they are very limited we don’t go for them**

**For option 2) we can get the toolkit to completely clone the website and make it ready for carrying out attacks**

**For option 3) if we have already created our very own clones we can just import them**

**For now the better option is to clone the site completely**

****

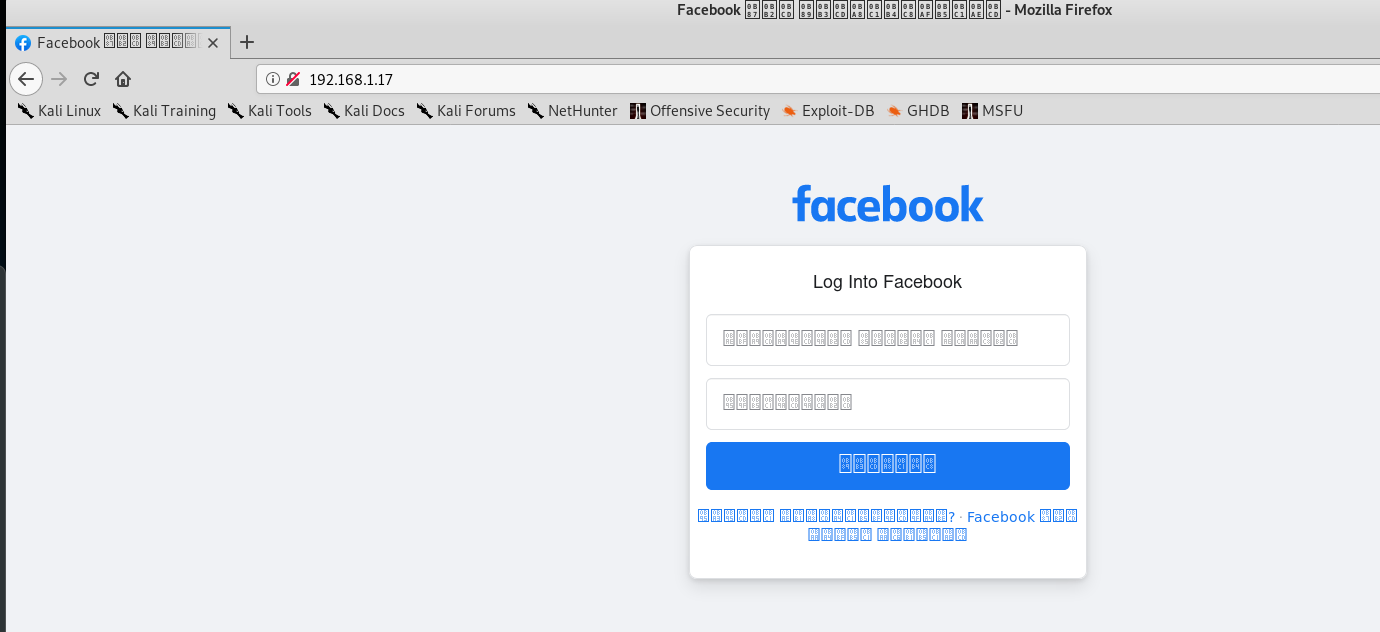
**6) next as shown below we make our own IP Address as the hosting website**

****

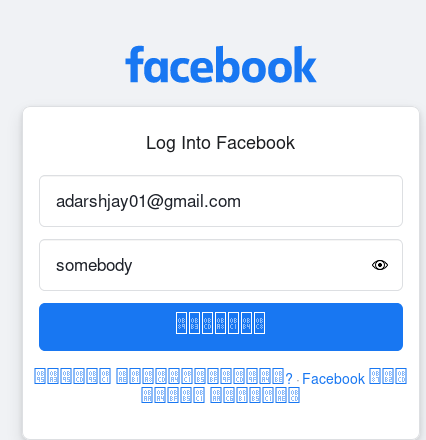
**7)as shown below we next copy the site we would like to clone which has a login form**

****

**8)as u can see the clone is completed**

****

**9) so for now entering some random credentials and test it.after we enter the credentials , the site will relocate to the original facebook site**

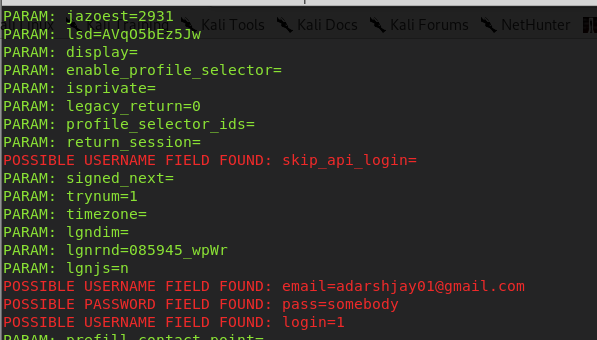
****

**10) now check in command prompt scroll up and find the fields marked in red as**

**POSSIBLE USERNAME FIELD FOUND: <USERNAME ENTERED>**

**POSSIBLE PASSWORD FIELD FOUND: <PASSWORD>**

**And there your username and password has been compromised!**

****

**#METHOD 2**

**Tool used:Social phish from github**

**Steps**

1. **Go to the site** [**https://github.com/xHak9x/SocialPhish**](https://github.com/xHak9x/SocialPhish)
2. **And copy the link provided**
3. **Then run these commands one after the other in command prompt**

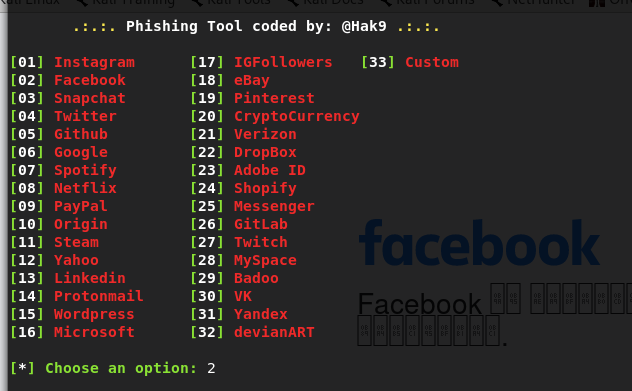
**git clone https://github.com/xHak9x/SocialPhish.git**

**cd SocialPhish**

**chmod +x socialphish.sh**

**./socialphish.sh**

1. **Next we choose the site u would like to clone the site on and harvest the credentials**

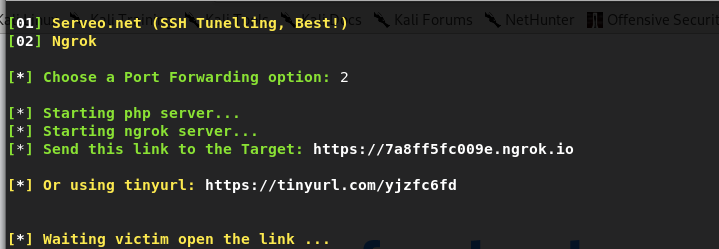
****

1. **Next we go for the ngrok option**

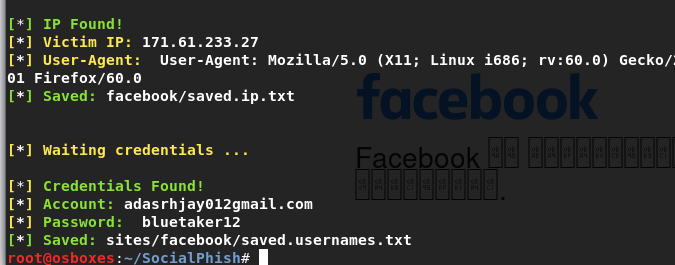
**What is Ngrok?**

**ngrok is a cross-platform application that enables developers to expose a local development server to the Internet with minimal effort**

1. **We will get links of our cloned website**

****

1. **Again on entering the credentials we will see that our username and password are taken by the cloned site**

****

**#METHOD 3**

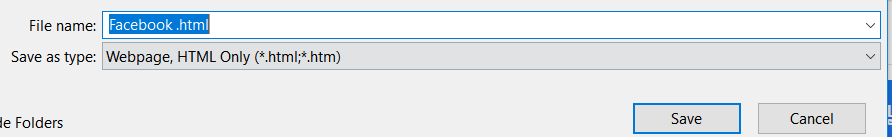
**Using computer hosted servers to carry out phishing attacks**

**Tools used: 1) WAMP server**

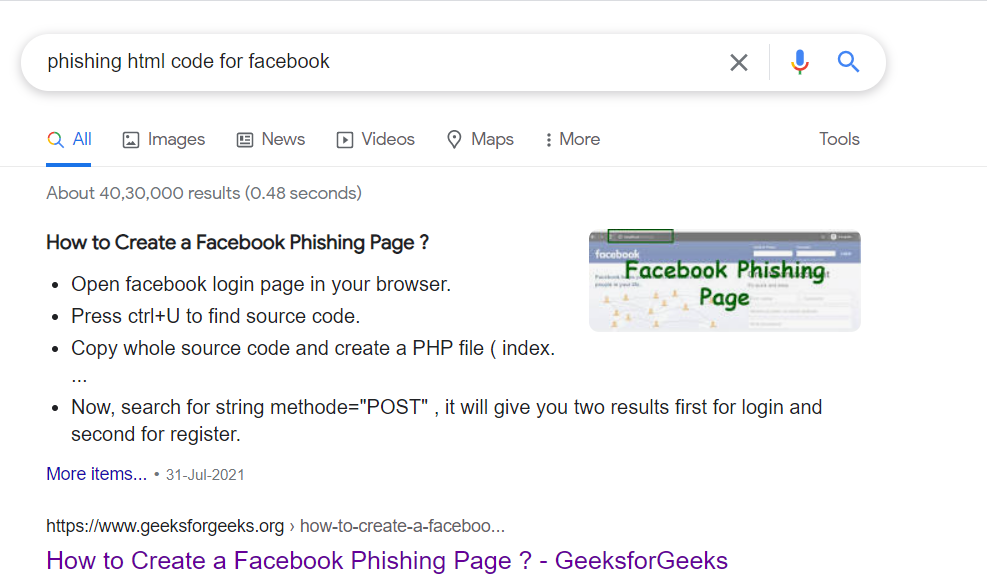
**2) Ngrok**

**Steps:**

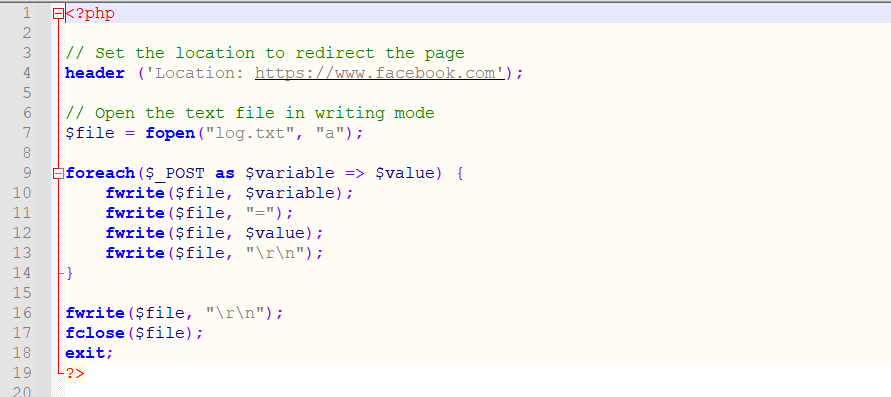
1. **First we go to the site where u want to clone ,and then right-click , you will then see the option to ‘Save As’, so save the file as HTML, and save as type as HTML only**

****

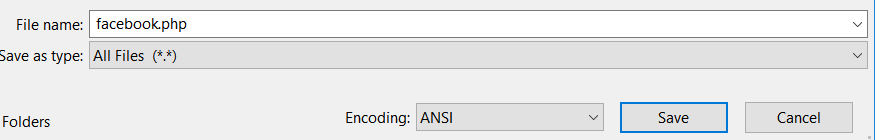
1. **Next go to your website and then search for php file for facebook**

****

1. **Next copy paste the php code present in the site to a notebook file, and change in ‘location’ change the file name to the site you are cloning this is so as to redirect to the original site**

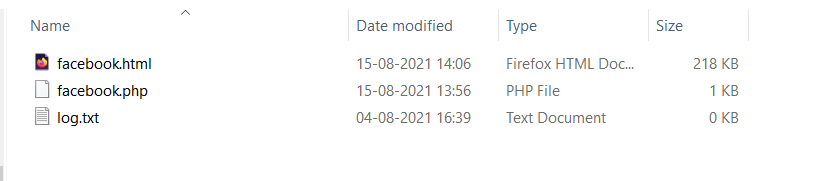
****

1. **Save the file name as the same name as u gave for the html file and in Save as type change txt to ‘All Files’**

****

**5)Next simply create a text file with same name as mentioned in the ‘fopen’ in the and save it as simple text file**

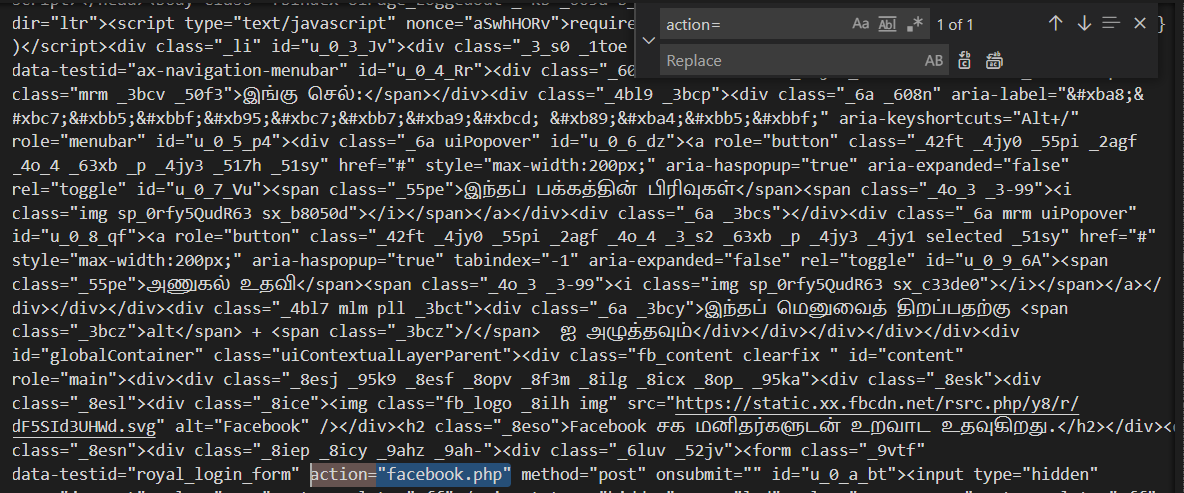
**In the end your folder should like this**

****

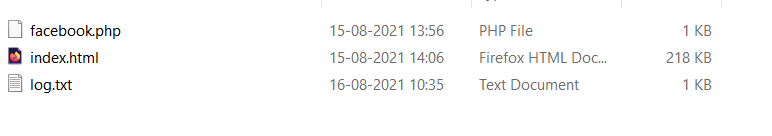
1. **Now go to your html with text editor(eg. Sablime Text Editor) and then go to**

**Edit-> Replace**

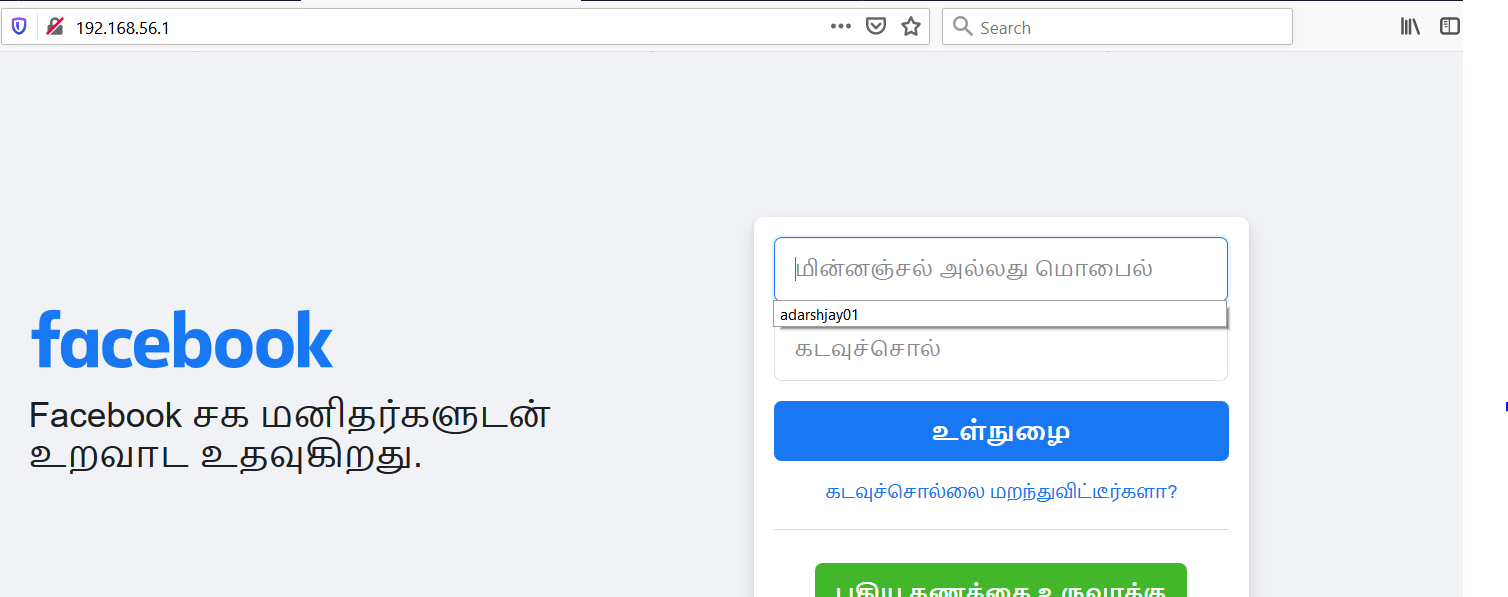
**Search for “action=” and then replace the link or whatever is present in action= to your php file that u just created and then save**

****

**6)Next we take all the files and put in wamp->www, delete all the files and paste the folders there, then rename the html file as index.html**

****

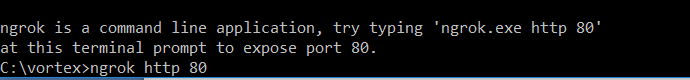
1. **Check if the server is active by going to your browser and search for your IP Address , if the page is opening and showing the cloned file then its working**

****

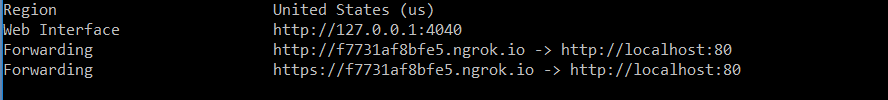
**7)Now to make your site more beleviable we use ngrok**

**After downloading we run the ‘ngrok.exe’ file and run the command**

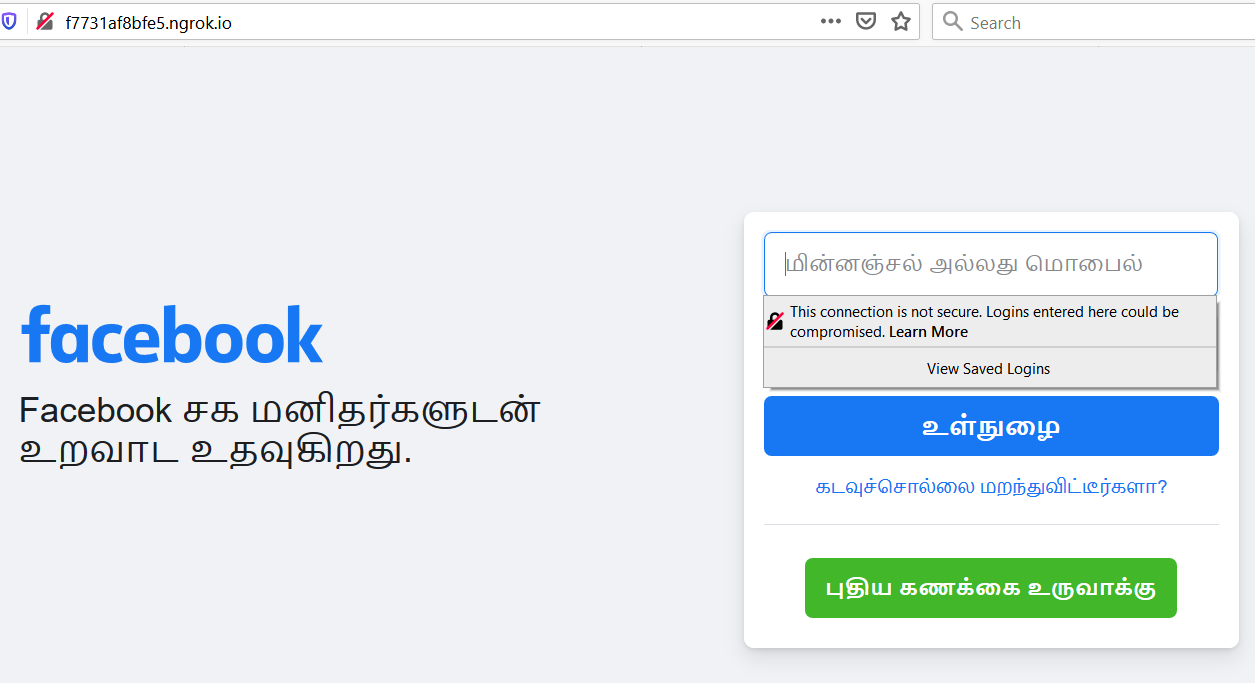
**🡪 ngrok http 80**

****

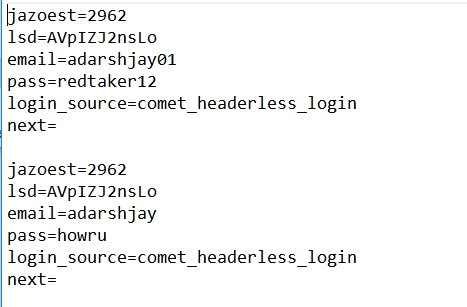
**8)click enter and we will see few links**

****

1. **Take any one of the links ending with ngrok.io and paste the link in browser**

****

**10)Type the credentials and check if its getting stored in the text file you have kept in wamp->www**

****

**Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. They may**

* **say they’ve noticed some suspicious activity or log-in attempts**
* **claim there’s a problem with your account or your payment information**
* **say you must confirm some personal information**
* **include a fake invoice**
* **want you to click on a link to make a payment**
* **say you’re eligible to register for a government refund**
* **offer a coupon for free stuff**

**How to protect?**

**1. Protect your computer by using security software. Set the software to update automatically so it can deal with any new security threats.**

**2. Protect your mobile phone by setting software to update automatically. These updates could give you critical protection against security threats.**

**3. Protect your accounts by using multi-factor authentication. Some accounts offer extra security by requiring two or more credentials to log in to your account. This is called multi-factor authentication.**