



LINUXDIARY 4.0

Explore the Linux Realm

LIMITED SEATS

19

August

COMPETITIVE WARGAMES

20

EXCITING PRIZES

REGISTER AT



- ▶ Session 01:
Open Source 101
- ▶ Session 02:
Echo Linux

- ▶ Session 03:
The File Maze
- ▶ Session 04:
NetVerse

• CONNECT WITH US •



Registration Fee:
Rs 199/-

Mr. D. N. Gangji
President
Walchand Linux Users' Group

Dr. M. A. Shah
HoD Computer Science
and Engineering

Dr. R. R. Rathod
HoD Information
Technology

Dr. A. J. Umbarkar
Staff Advisor,
Walchand Linux Users' Group

Dr. A. R. Surve
Assoc. Dean Student
Activities and Staff Advisor

Dr. U. A. Dabade
I/C Director
Walchand College of Engineering

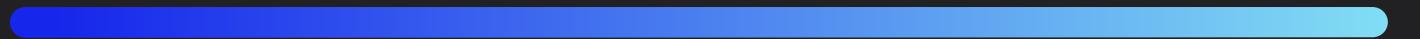
wcewlug.org

Venue:
Mini & Main CCF

For any query
84210 06401
99236 71592

LinuxDiary 4.0

2023





Day 2 | Session 2

Netverse

Basics of Networking

Linux Networking Commands

Nmap - Network Mapper

Phishing - Introduction & Demo

x x x x

Basics of Networking

- What is a Network ?
- IP Address
- Ports & Common Ports
- Socket Address
- The Internet

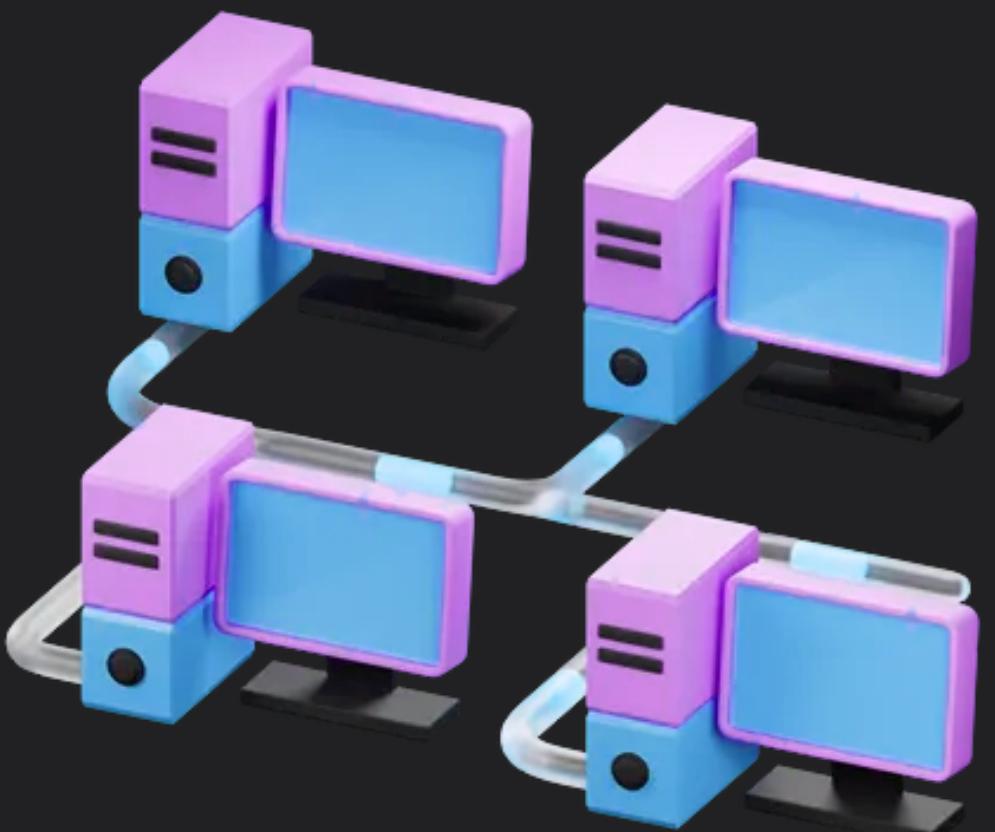


x x x x



What is Network?

- Collection of nodes that are connected together to enable communication and data exchange
- Nodes are devices that are connected to a network



IP Address

- IP stands for Internet Protocol
- Unique numerical identifier that is assigned to every device(node) on a network
- Used to identify devices logically and enable communication between them

192.168.1.16



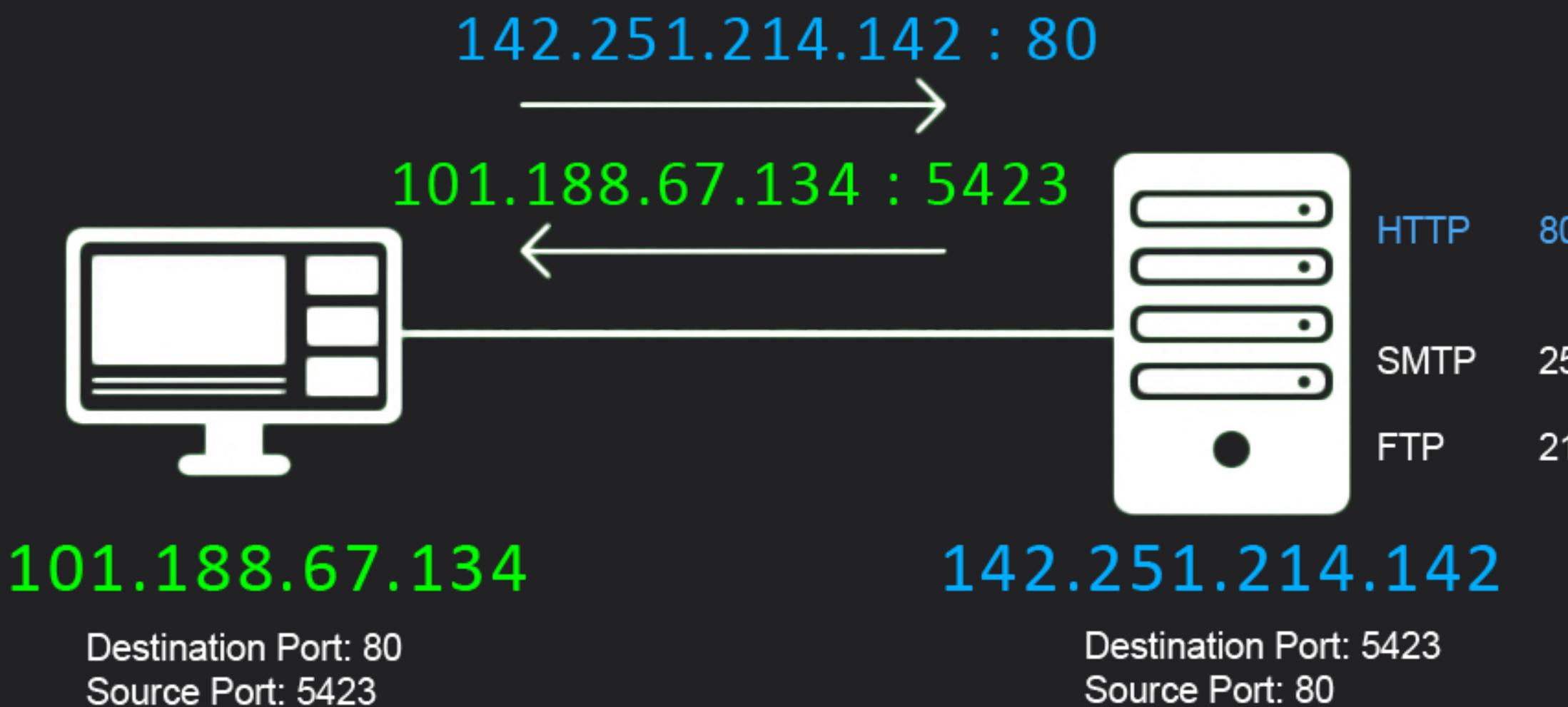
Ports

- A port is a virtual endpoint managed by a computer's OS for starting and ending network connections
- Each port is associated with a specific process or service
- Ports allow computer to easily distinguish between different kinds of traffic





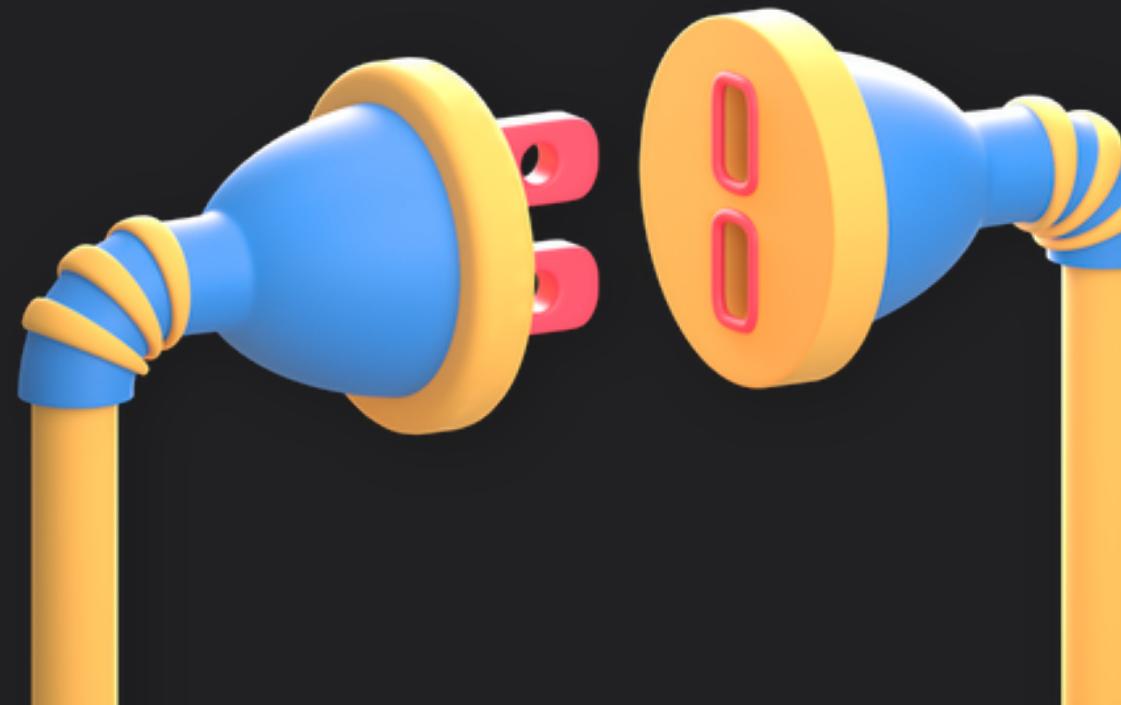
Common Ports



HTTP	80
HTTPS	443
SMTP	25
FTP	21
DNS	53
SSH	22

Socket Addresses

- A socket is one end point of the two way communication link between two programs running on internet
- Socket Address helps us to successfully send the message at the specified port of the specified machine
- Socket Address = IP Address + Port Number



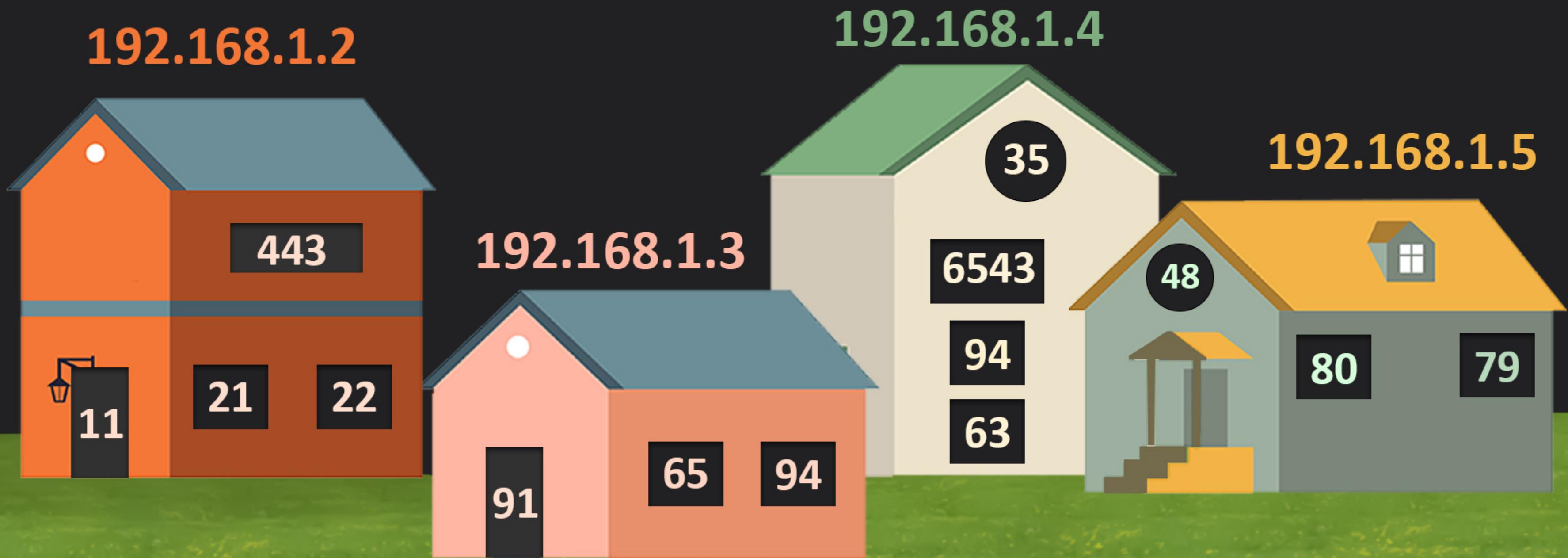
192.168.1.16 : 80

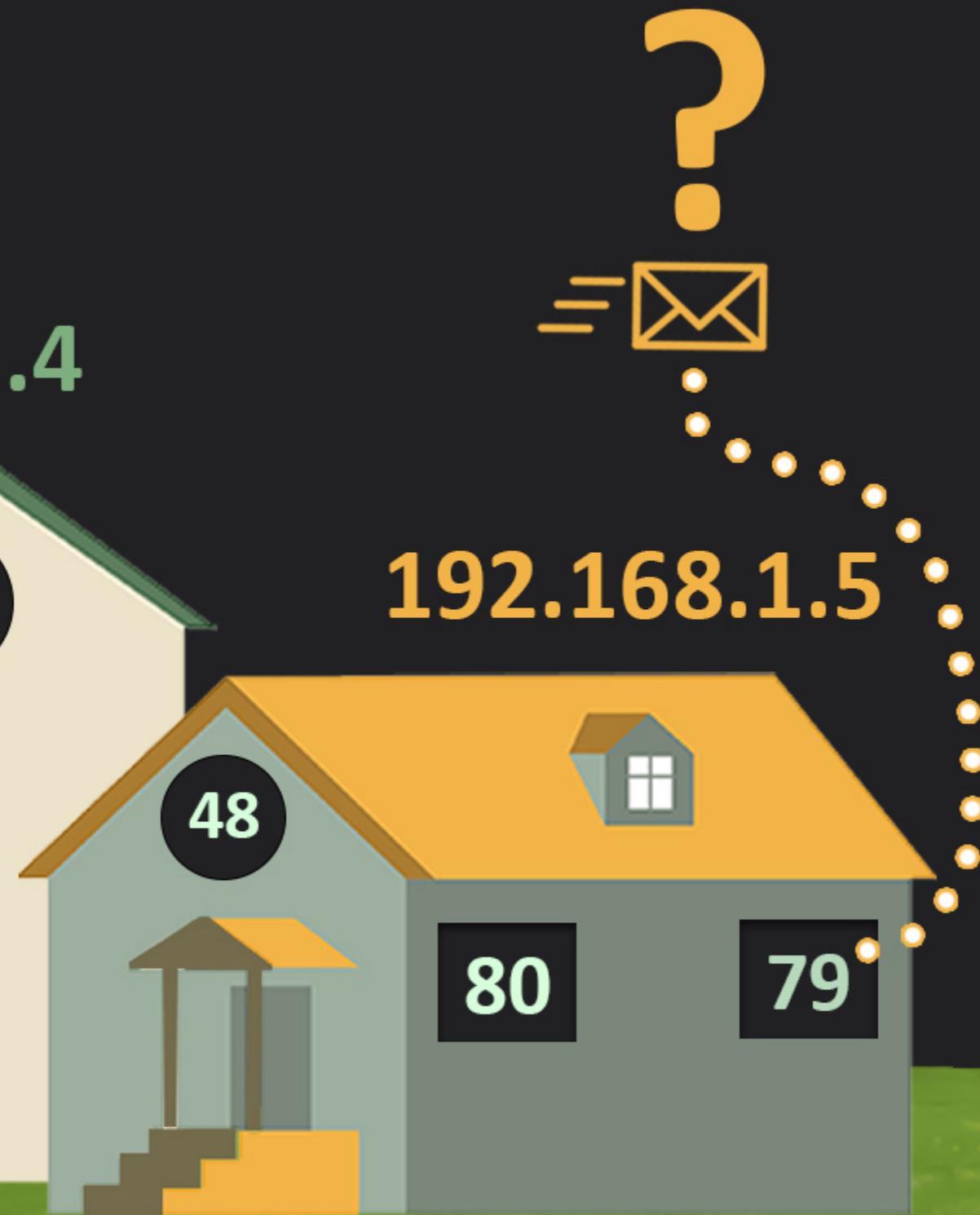
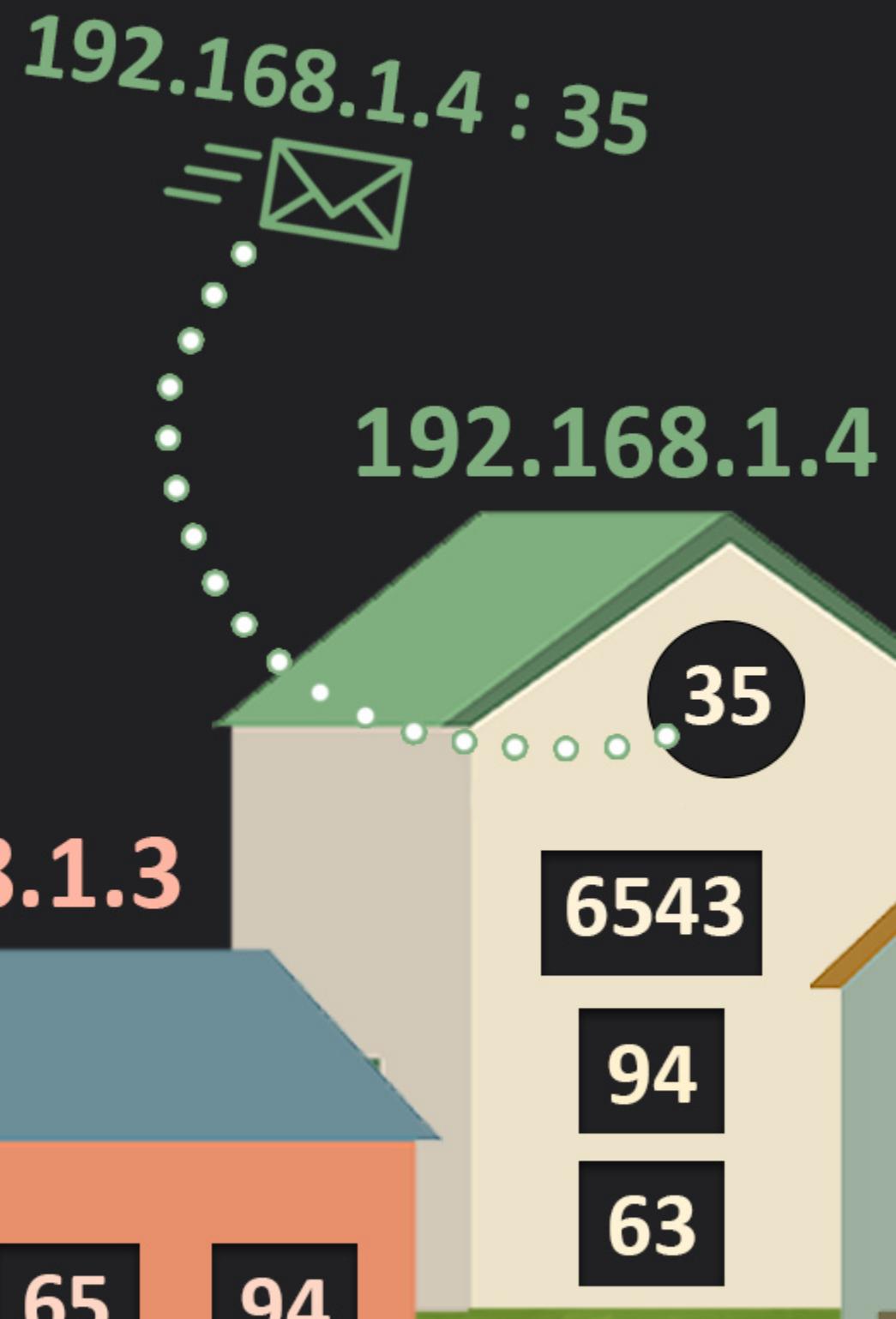
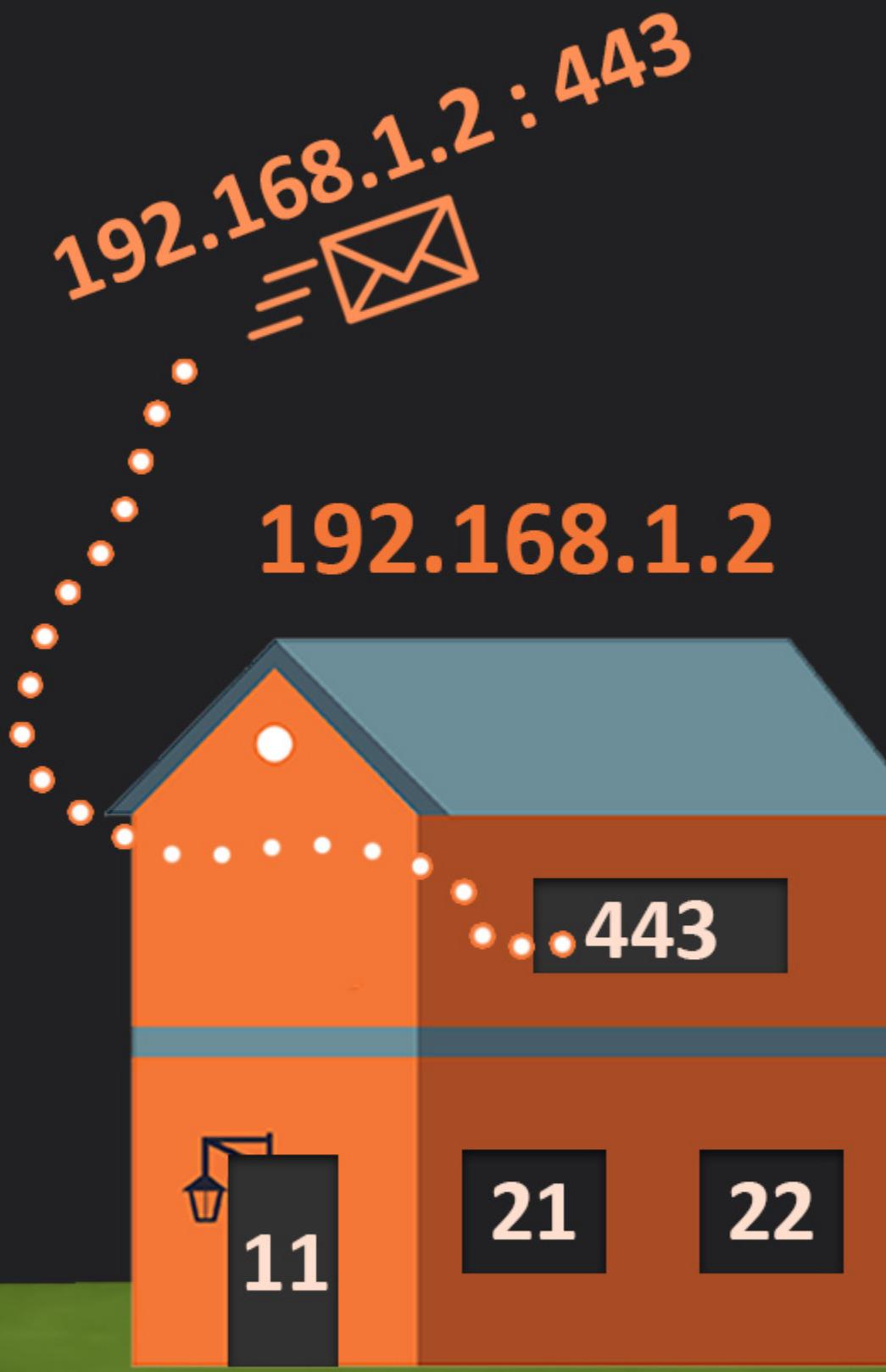


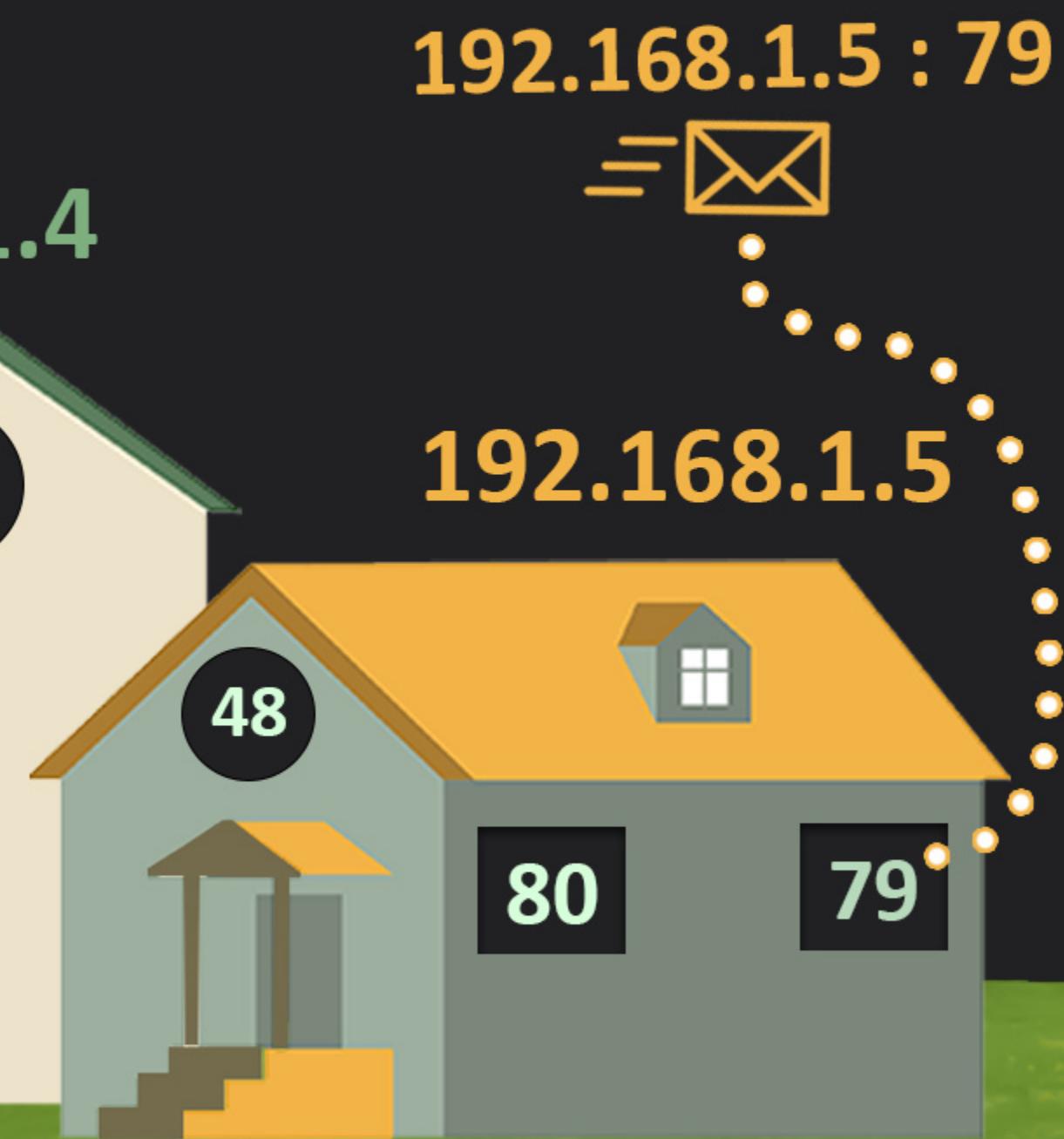
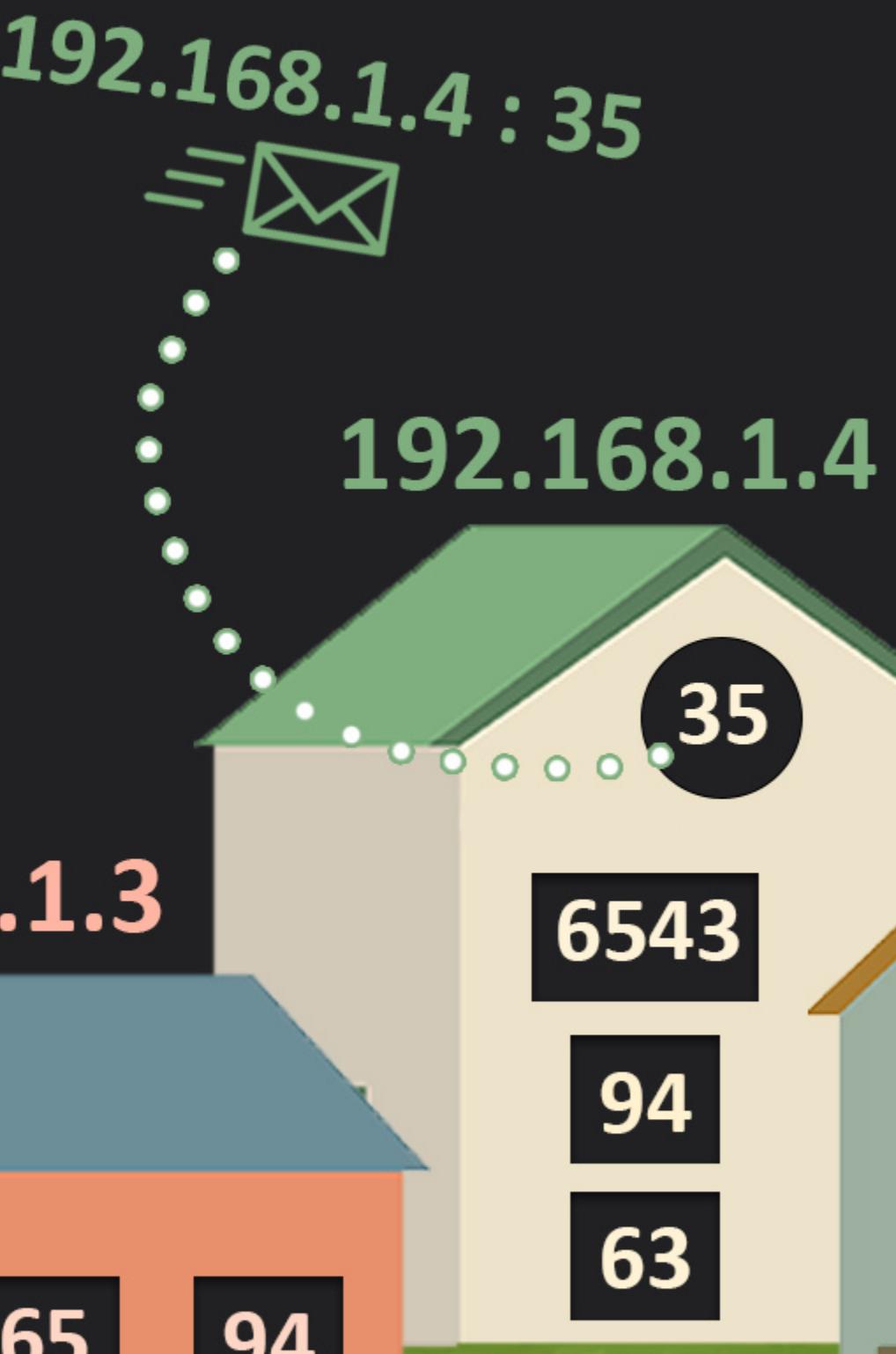
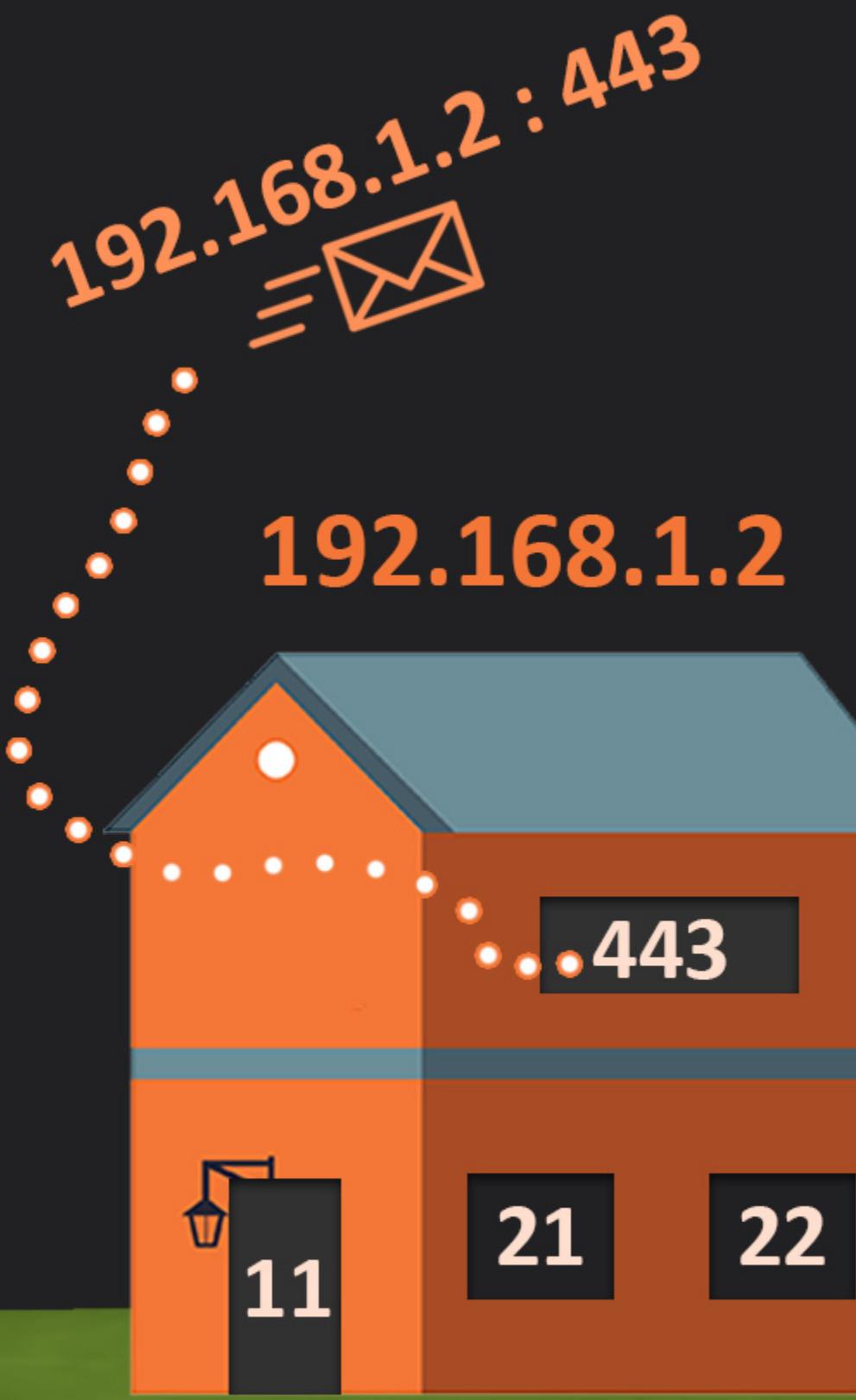
Gokuldham Society



Network: Gokuldham Society

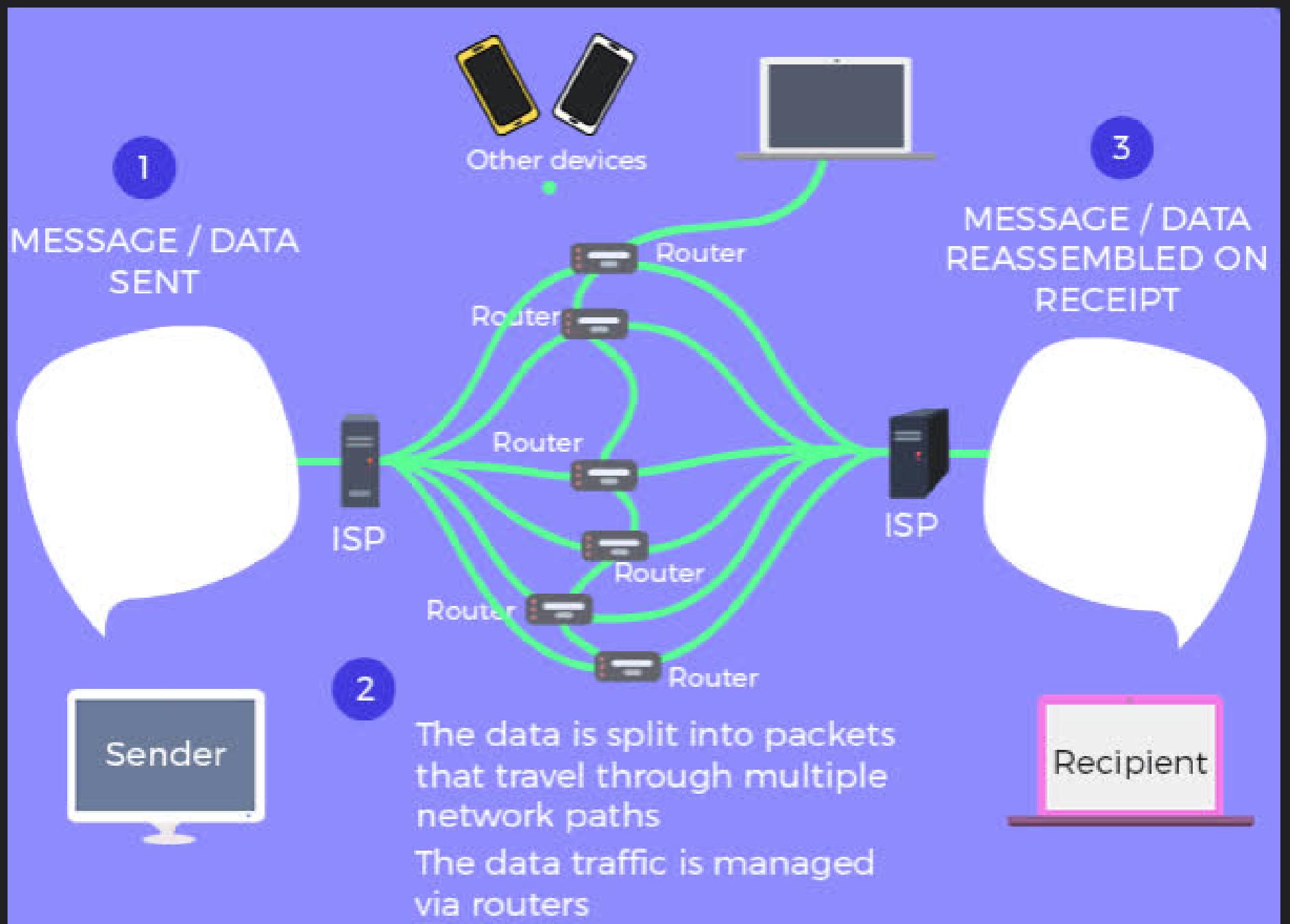






The Internet

- The Internet is a vast network that connects computers all over the world



TCP vs UDP

○ TCP: Transmission Control Protocol

- Slower
- Reliable messenger
- Safely and accurately delivers to their destination on the internet

TCP



○ UDP: User Datagram Protocol

- Faster
- Unreliable messenger
- It's like tossing a note into a sea-bottle, uncertain if anyone will discover it

UDP



Networking Commands

- ifconfig
- iwconfig
- ip
- ping
- host
- netstat
- whois
- curl

\$ ifconfig

- Configure a network interface
- Displays the status of the currently active interfaces



Syntax



```
$ ifconfig [flags]  
$ ifconfig [-v] [interface]
```



\$ iwconfig

- Similar to ifconfig command
- Displays wireless networking interfaces only



Syntax



```
$ iwconfig [interface] [options]
```

\$ ip

- Configure a network interface
- Displays or manipulate routers, devices, and tunnels



Syntax



```
$ ip [ OPTIONS ] OBJECT { COMMAND | help }
```

\$ ping

(Packet Internet Groper)

- Checks the network connectivity between host and server/host
- This command sends a data packet to the specified address with the message “PING” and get a response from the server/host

Syntax



```
$ ping [URL]
```

\$ host

- Displays domain name for given IP address or vice-versa
- Flags:
 - 4: It is used for IPv4 address only for the query
 - 6: It is used for IPv6 address only for the query

Syntax



```
$ host [website name/website ip address]
```

\$ netstat

- Netstat command displays various network related information
- Flags:
 - a: lists all the ports
 - at: lists all the tcp ports
 - au: lists all the udp ports

Syntax



```
$ netstat [flag]
```

\$ whois

- Displays information about a website's record
- Registration information
- Owner's information
- Server Names

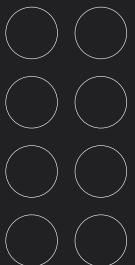
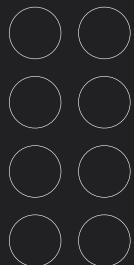
Syntax



```
$ whois [website name]
```

\$ curl

- A command-line tool to transfer data to or from a server, using any of the supported protocols (HTTP, FTP etc.)



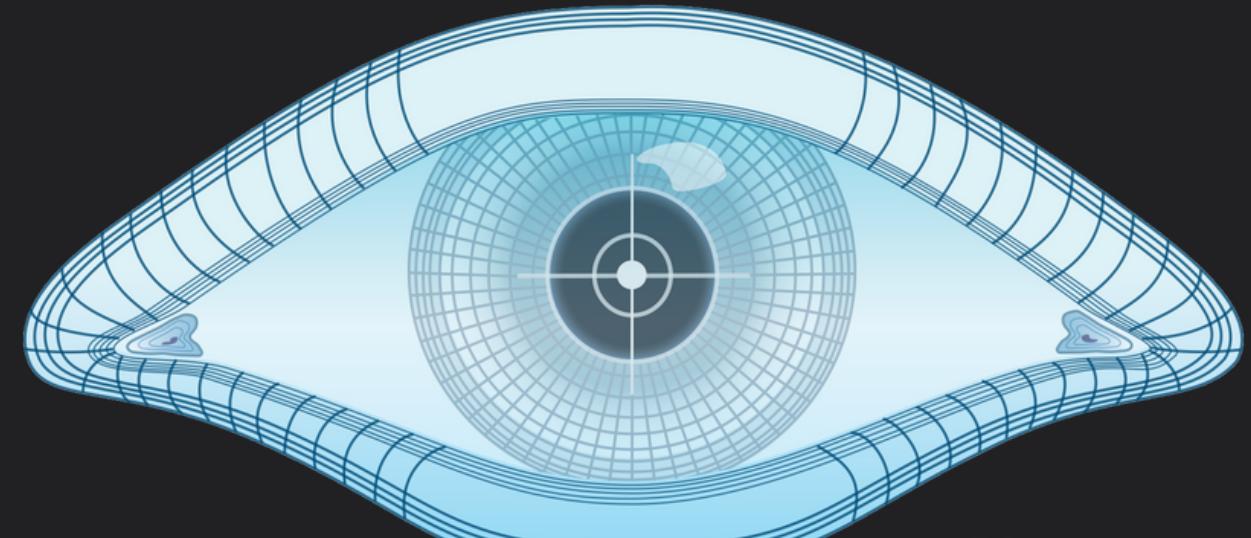
Syntax



```
$ curl [URL]
```

Nmap

- What is Nmap ?
- Port Scanning & Flags
- OS Detection
- Features
- Challenge !!!



NMAP.ORG

What is Nmap ?

- Stands for Network Mapper
- Open-source Linux command-line tool
- Scans IP Addresses and ports, discovers all open and it's services and detect vulnerabilities.



Features

- Open-Source
- Versatile
- Cross-Platform
- Scripting Engine
- Integration
- Well-maintained and Supported



NMAP

Port Scanning

- Scans ports on a target system to identify open ports, services running on those ports, and potential vulnerabilities
- Sending packets to specific ports on a target host and analyzing the responses to determine their state

Syntax



```
$ nmap <target IP>
$ nmap -p [port(s)] <target IP>
```

OS Detection

- Also known as operating system fingerprinting
- Identify the operating system running on a target system
- Helps to better understand the potential vulnerabilities of the system

Syntax



```
$ nmap -O <target IP>
```



NMap Flags

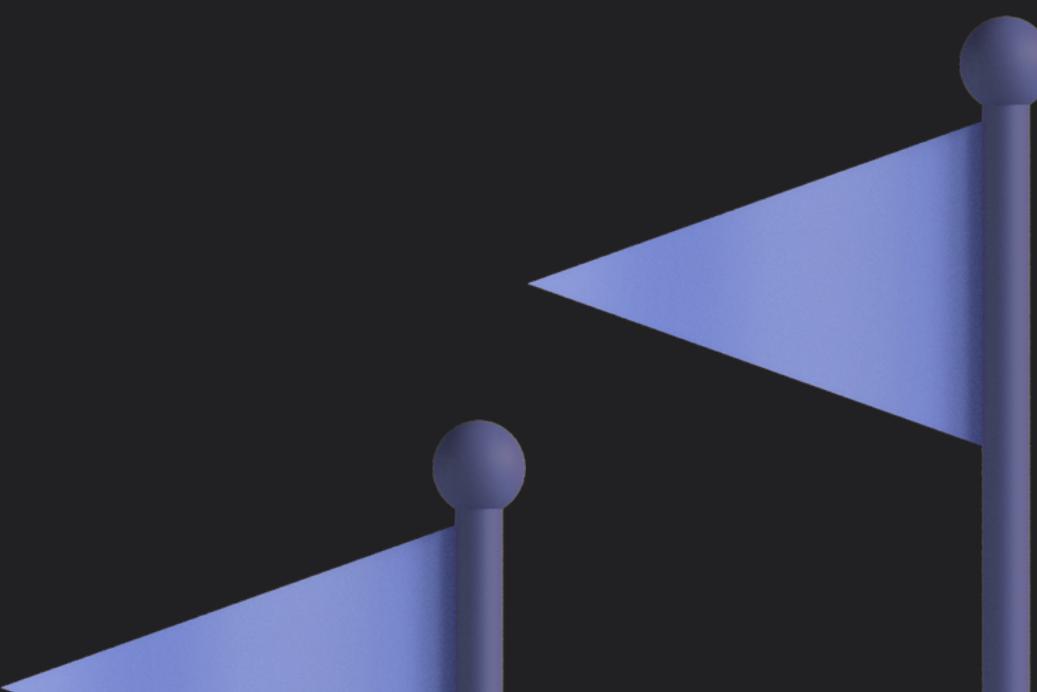
-sT : Invokes TCP Connect Scan, Comparatively Slow

-Pn : Treat all hosts as online (Skips host Discovery)

-sC : Scan using Scripts

-F : Fast Scan

-O : OS Detection



Phishing

- What is Phishing ?
- Examples
- Tools & Demo
- Detection and Prevention

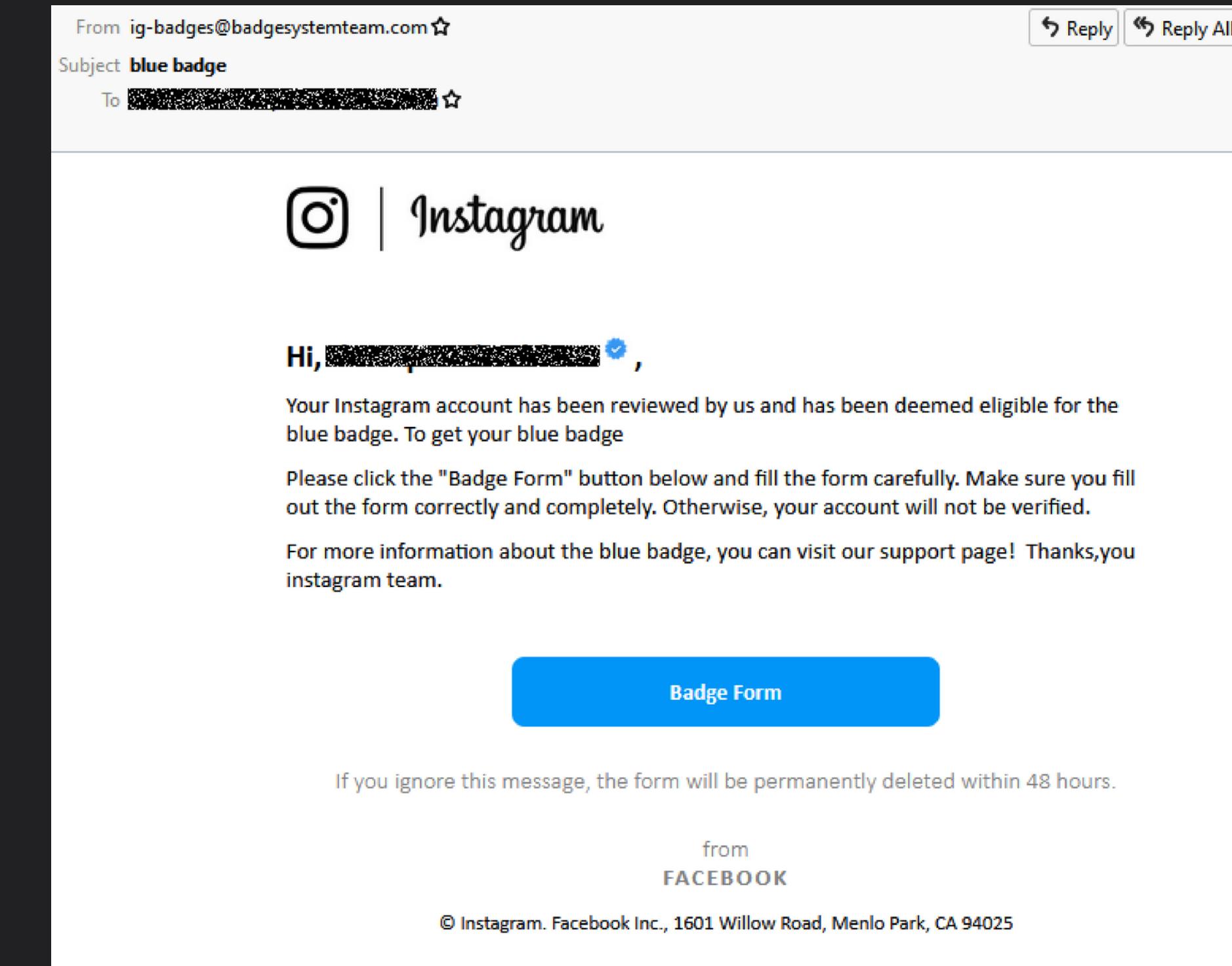
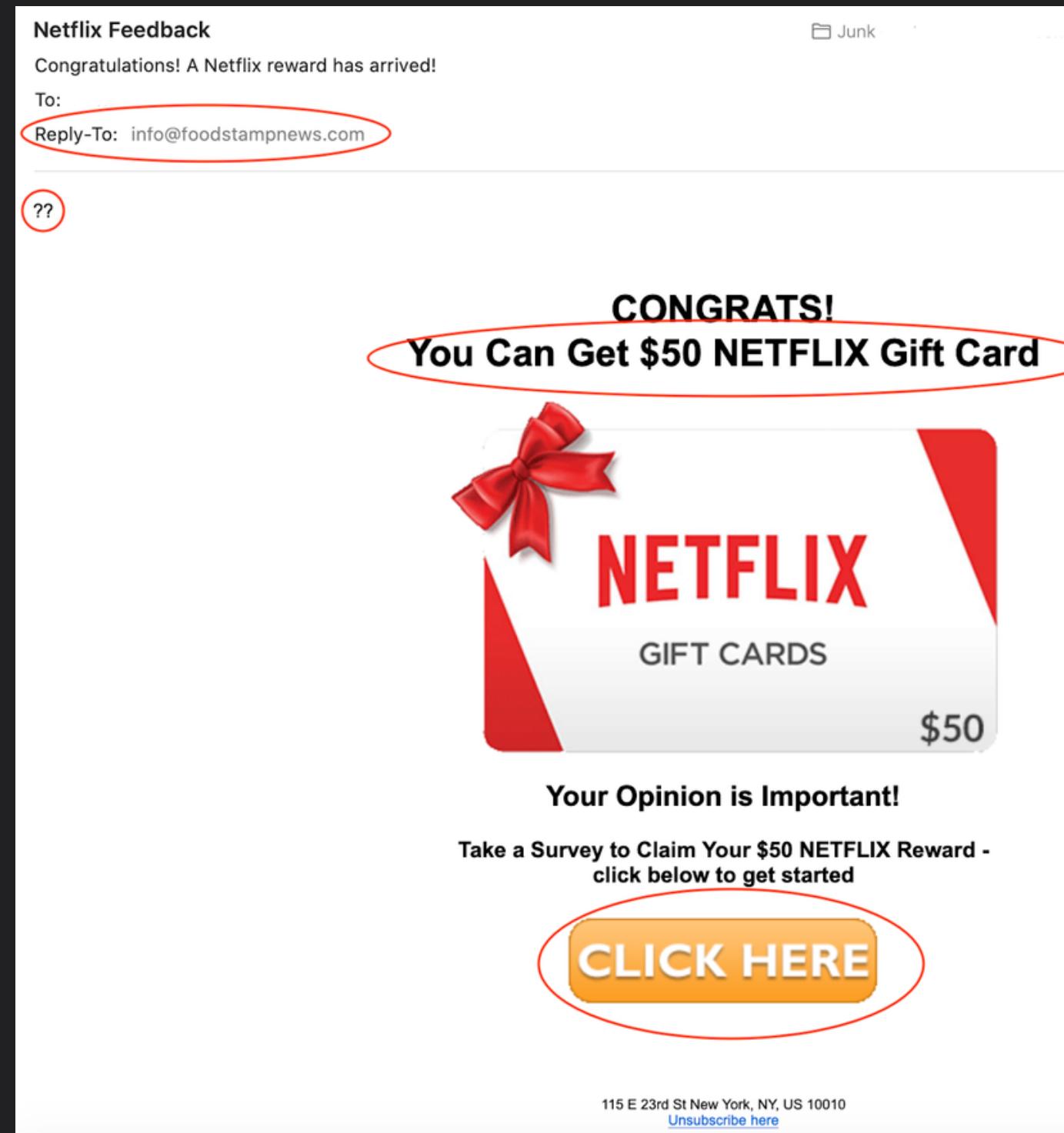


What is Phishing?

- Phishing attacks are fraudulent communications (emails, texts, calls or websites)
- Their aim is to trick users into revealing sensitive information or downloading malware
- These attacks put users at risk of cybercrime



Examples



LIVE DEMO

BRACE YOURSELF

IT IS TIME FOR ACTION



MATTHIAS CPTAIN

DISCLAIMER

This presentation is only for Educational Purposes.
Performing any types of hacking attempts
(without permission) on computers that you do not
own is illegal. WLUG does not promote any types of
Illegal activities.



This is how you might end up !



Tools

PyPhisher

- Written in Python, having 70+ login templates
- Highly Customized
- Stable Server i.e.: CloudFlare

PyPhisher - Installation



#Install dependencies

```
$ sudo apt install git python3 python3-pip php openssh-client -y
```

#Install PyPhisher

```
$ sudo pip3 install pyphisher --break-system-packages
```

#Run PyPhisher

```
$ pyphisher
```

Detecting Phishing

- There are grammatical mistakes
- Creates a sense of urgency e.g. Limited Time, Offer valid for only today, etc
- It includes suspicious attachments or links
- Website is misspelled e.g. go0gle.com, abibas.com, poma.com/login, etc



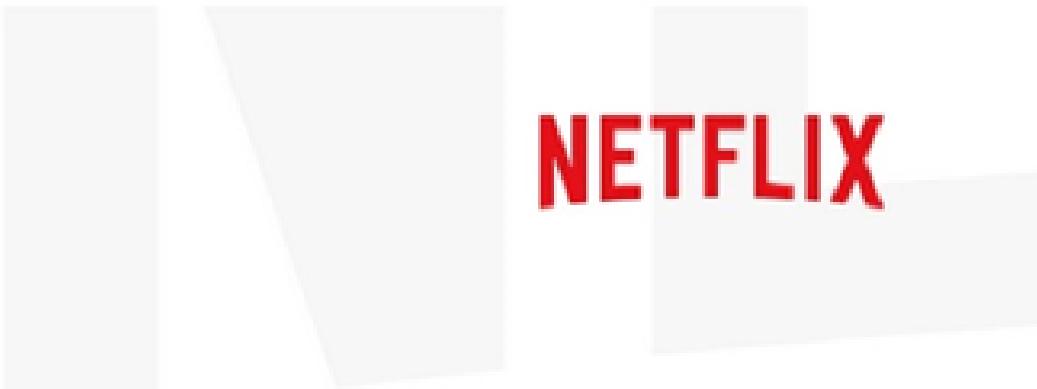
Detecting Phishing

From NETFLIX

Subject Invoice Failed - Account Blocked

27/3/19, 3:53 pm

To [REDACTED]



NETFLIX

Dears Customer,

We're having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your MASTERCARD in your payment details.

UPDATE ACCOUNT NOW

We're here to help if you need it. Visit the Help Center for more info or contact us.

Your friends at Netflix

MO MS Online Services Team
msonlineservices@microsoftonline.com

To You [REDACTED]

Wednesday, April 24, 1:09 PM

Attention: A user account was created or modified. Retrieve your user's temporary password. | [View this email in your browser.](#)



Microsoft

Your account password has expired.

The following contains password security guidelines.

Please note:

- A strong password consists of at least three of the following: uppercase letters, lowercase letters, numbers, symbols.
- For your protection and security, passwords are valid for 120 days.
- When distributing IDs and passwords, be sure to do so in a safe and secure manner.

To avoid service interruption, please change your password now.

Go to the sign-in page, <https://portal.office.com> and sign in with your User ID:
User Name: [REDACTED]

Once you have successfully signed in, you can create a new password by following the instructions on the si

We appreciate your prompt attention to this matter, and look forward to continuing to meet your business ne

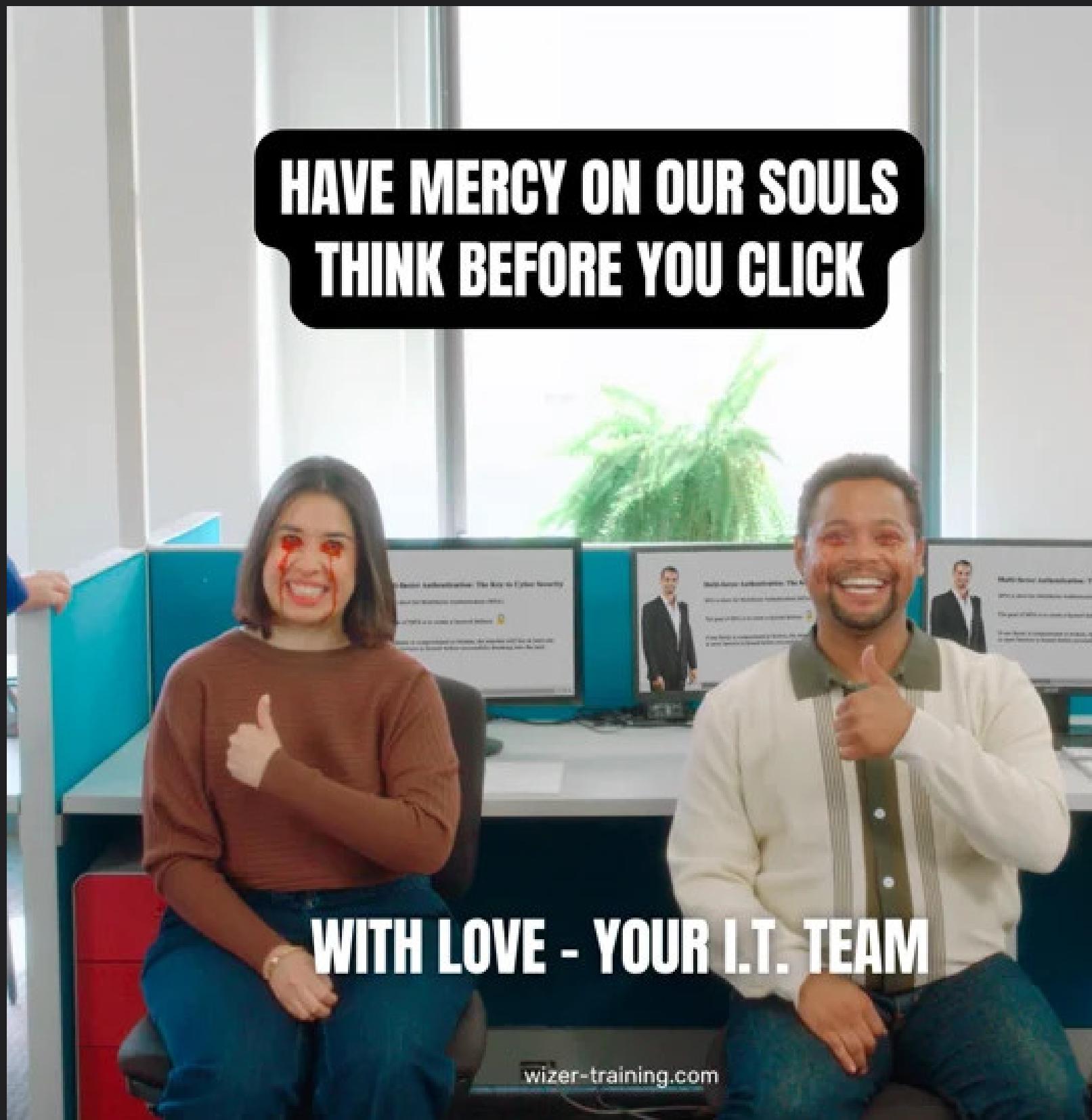
Thank you for choosing to host your IT solutions with Microsoft.

Sincerely,
The Microsoft Online Services Team

Preventing Phishing

- Think twice before you click
- Update your Browser
- Beware of Pop-Ups
- Get your firewall updated
- Install Ad Blocker extensions
- Avoid using public networks
- Check your online accounts often
- Use Anti-virus softwares





THANK YOU

COMMUNITY | KNOWLEDGE | SHARE