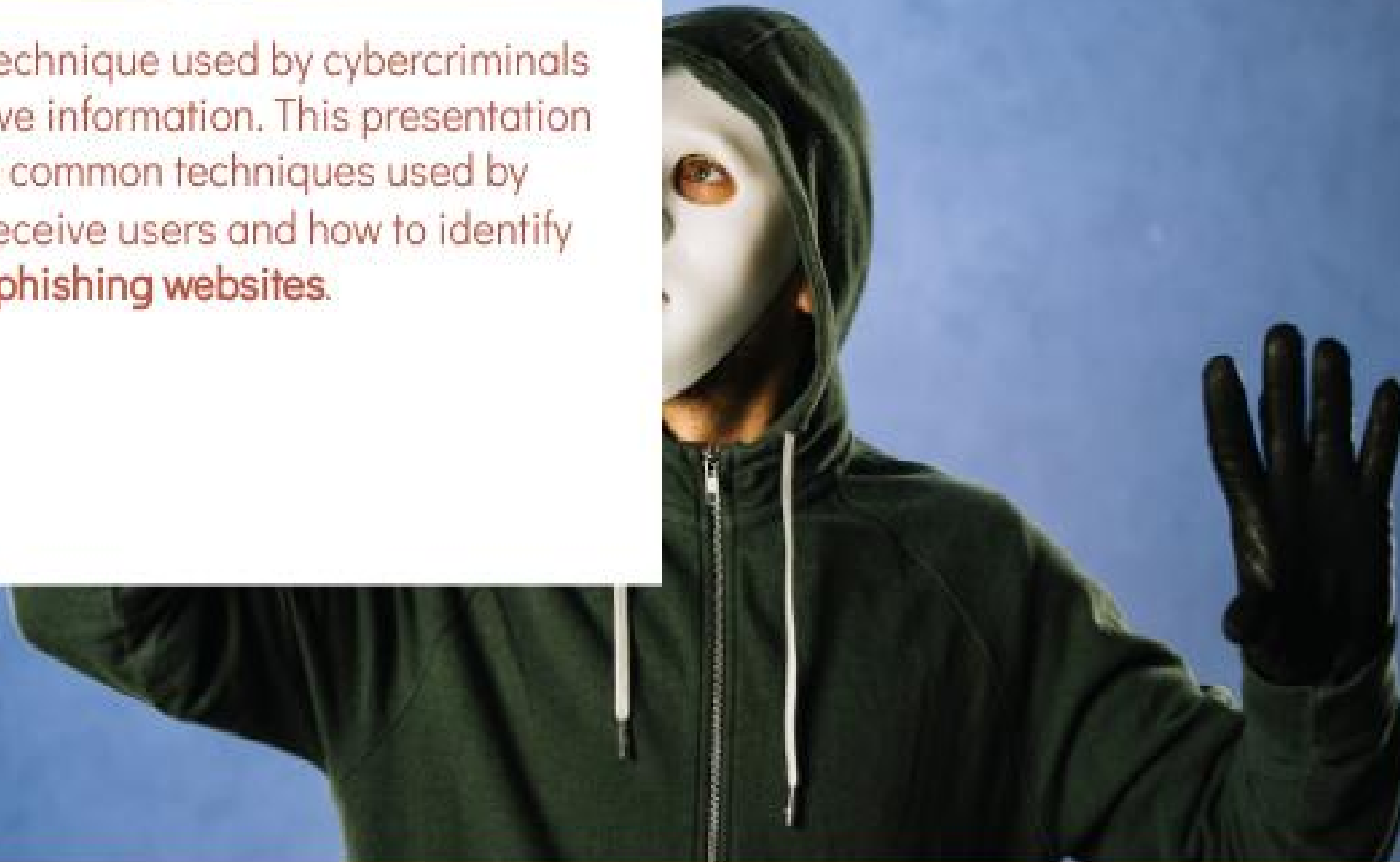




UNVEILING THE DECEPTIVE: TECHNIQUES FOR IDENTIFYING PHISHING WEBSITES

INTRODUCTION

Phishing is a technique used by cybercriminals to steal sensitive information. This presentation will explore common techniques used by phishers to deceive users and how to identify **phishing websites**.



WHAT IS PHISHING?

Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising oneself as a trustworthy entity in an electronic communication. It is usually carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website.



COMMON TECHNIQUES USED BY PHISHERS

Phishers use various techniques such as **spear phishing**, **whaling**, and **vishing** to trick users into revealing sensitive information. **Spear phishing** targets specific individuals, **whaling** targets high-profile targets such as executives, and **vishing** uses voice calls to deceive users.



IDENTIFYING PHISHING WEBSITES

Phishing websites often have **URLs** that are similar to legitimate websites or use **HTTPS** with a fake SSL certificate. They may also have a sense of urgency, contain spelling mistakes, or ask for sensitive information. Always verify the website's authenticity before entering any information.



Phishing Attacks

Phishing attacks are a serious threat as they can result in attackers obtaining important credentials that provide access to your bank accounts or other financial information. Attackers often use URLs that mimic the appearance of legitimate applications, making it difficult to distinguish between the real and fake websites.

DataSets

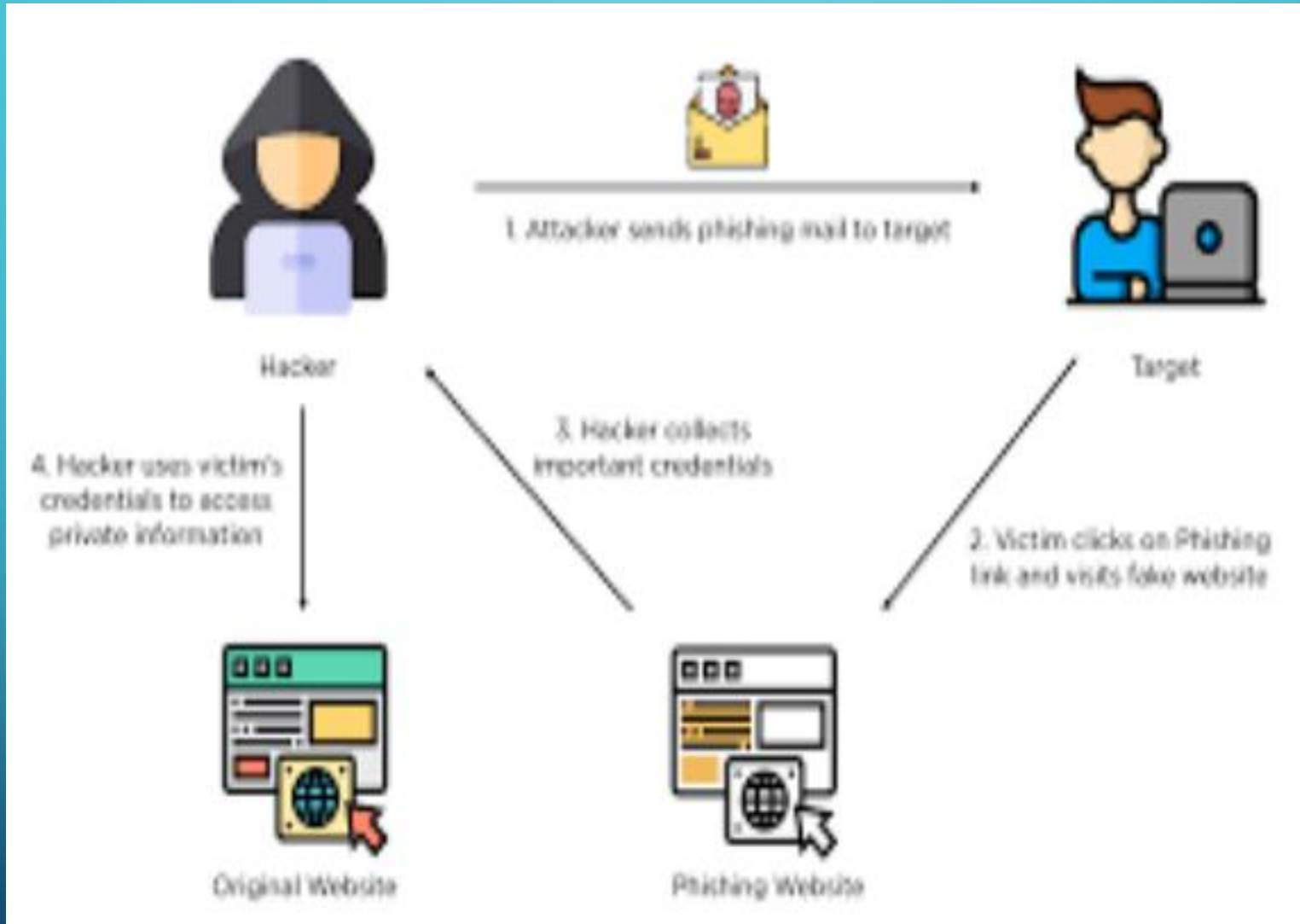
- 1>Genuine urls
- 2>Phishing urls
- 3>Train the Machine to Predict

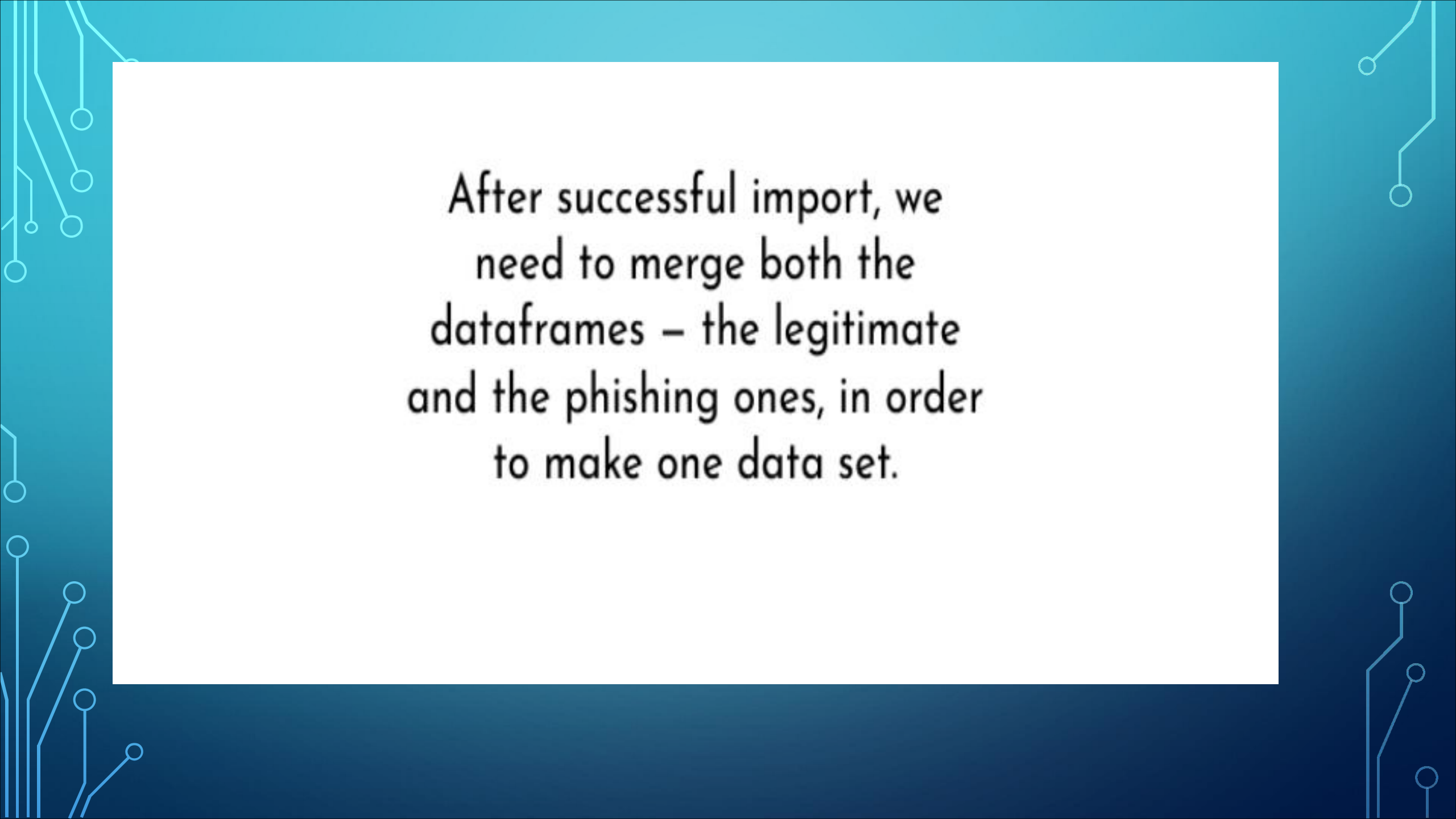
DataSet Description

The dataset for a ".txt" file is with no headers and has only the column values. The actual column-wise header is described above and, if needed, you can add the header manually if you are using '.txt' file. If you are using '.csv' file then the column names were added and given. The header list (column names) is as follows :['UsingIP', 'LongURL', 'ShortURL', 'Symbol@', 'Redirecting//', 'PrefixSuffix-', 'SubDomains', 'HTTPS', 'DomainRegLen', 'Favicon', 'NonStdPort',



Output:-



The background of the slide is a dark blue gradient. It is decorated with white, stylized circuit board traces that run along the top, bottom, and side edges. These traces connect to small white circles, resembling solder points or vias.

After successful import, we
need to merge both the
dataframes – the legitimate
and the phishing ones, in order
to make one data set.

PROTECTING YOURSELF FROM PHISHING ATTACKS

You can protect yourself from phishing attacks by using **two-factor authentication**, keeping your software up to date, and using an **antivirus** program. Be cautious when clicking on links or downloading attachments from unknown sources, and always verify the authenticity of the website.



CONCLUSION

Phishing attacks are becoming increasingly sophisticated and difficult to detect. By understanding common techniques used by phishers and knowing how to identify phishing websites, you can protect yourself and your sensitive information. Remember to always stay vigilant and cautious when online.

Phishing Attacks

Phishing attacks are a serious threat as they can result in attackers obtaining important credentials that provide access to your bank accounts or other financial information. Attackers often use URLs that mimic the appearance of legitimate applications, making it difficult to distinguish between the real and fake websites.

*Thank
you*

