PHISHING

BEYOND THE VEIL

Azhar Ghafoor

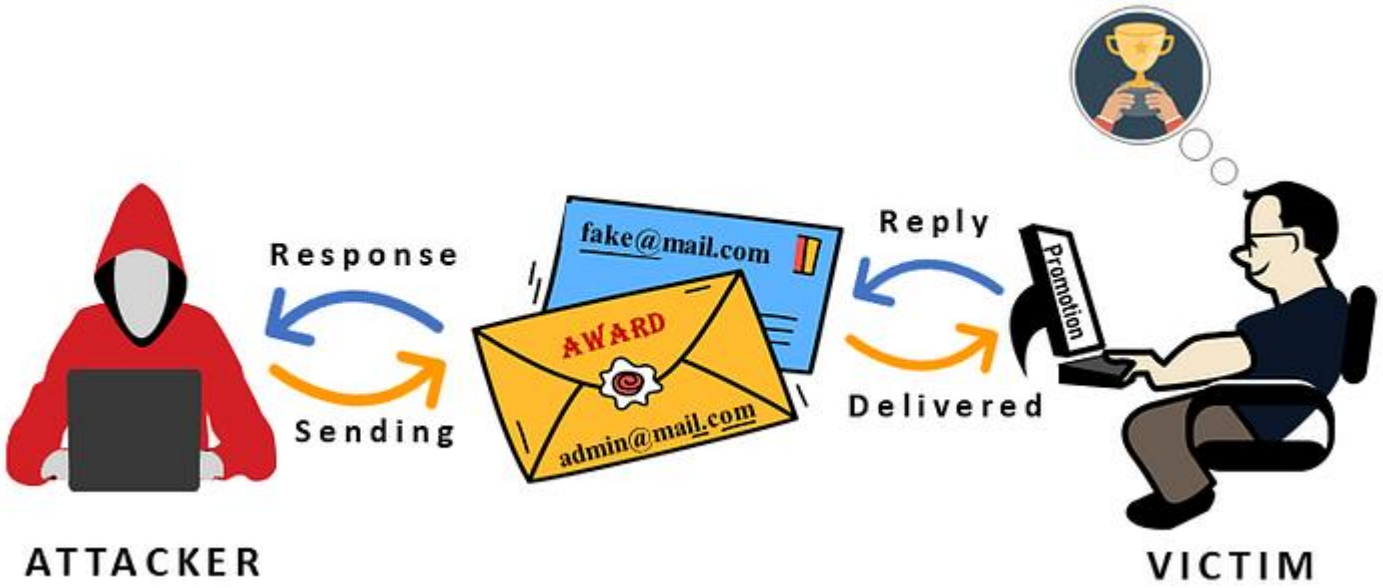
Azhar.Ghafoor@au.edu.pk

PHISHING

Phishing is a form of cyber attack where attackers deceive individuals into sharing sensitive information or performing actions through fraudulent emails, websites, or messages, often impersonating trusted entities.

Types

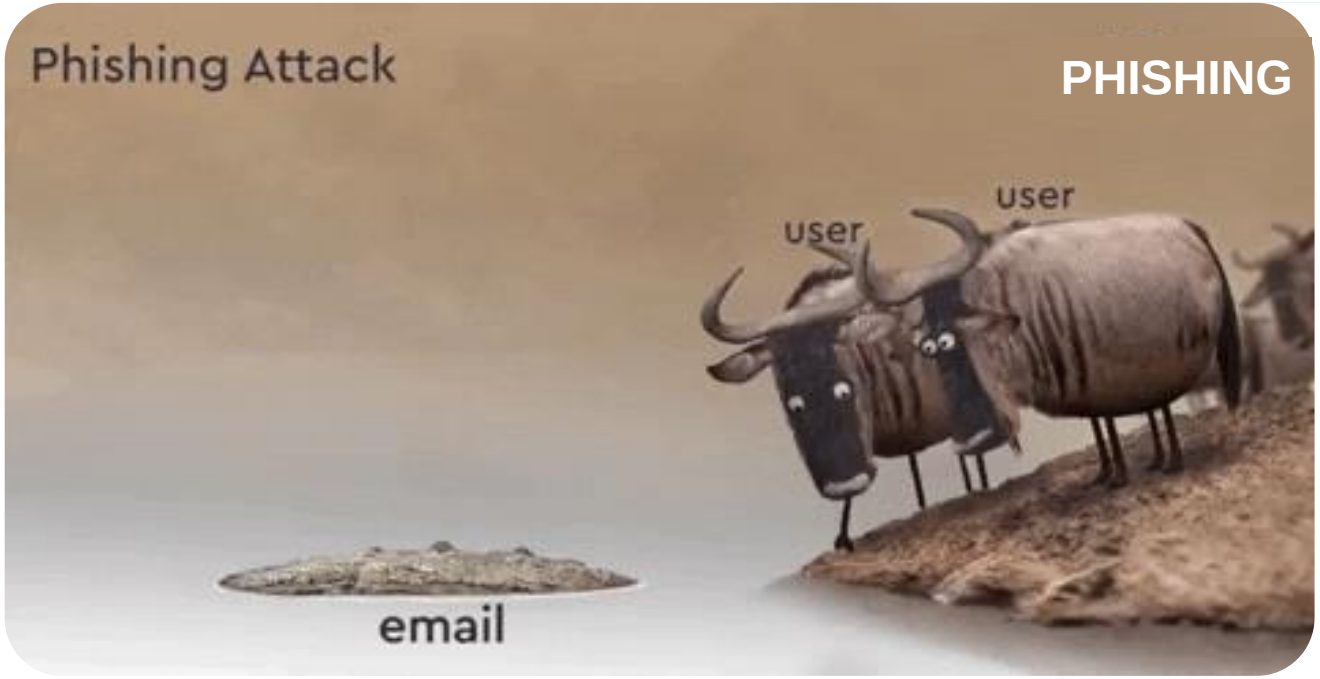
- Credential Phishing
- Spear Phishing
- Whaling
- Smishing
- Vishing



SOURCE: HTTPS://GHAFOORAZHAR.MEDIUM.COM/

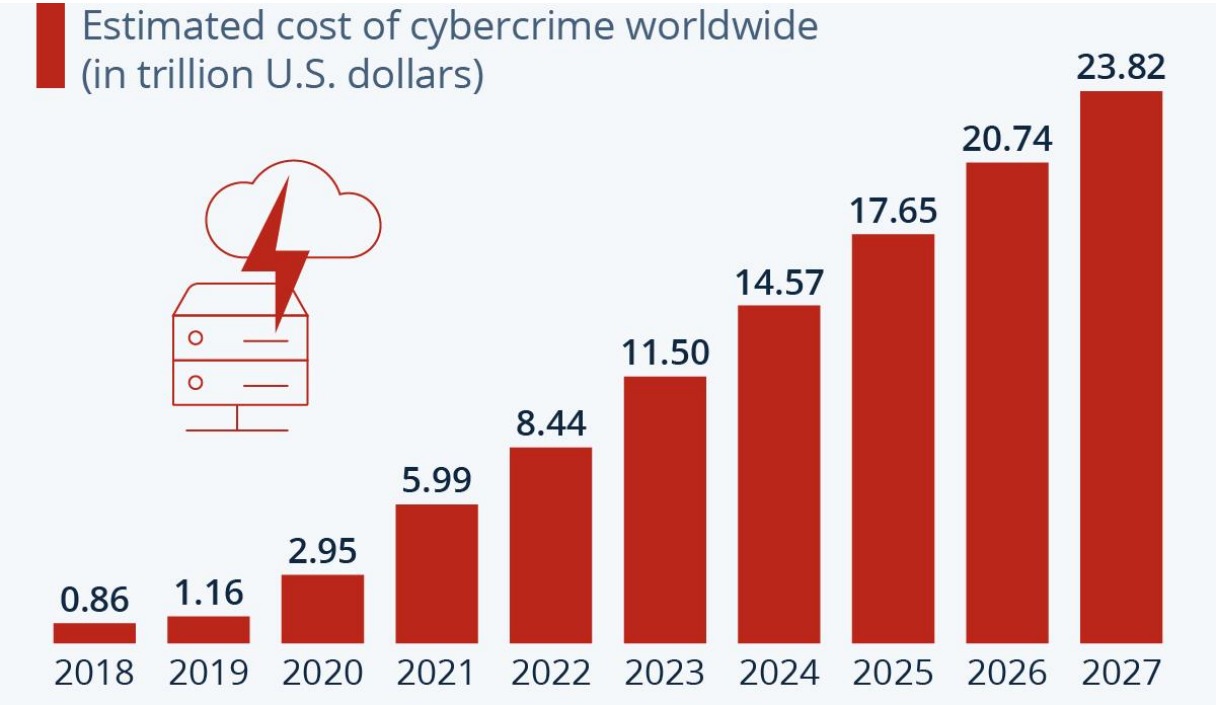
PHISHING

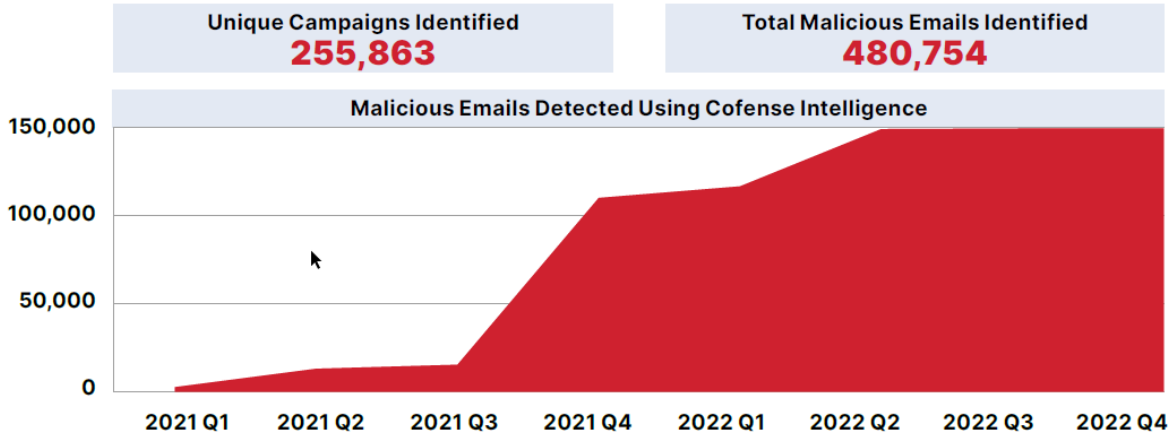
Phishing is a form of cyber attack where attackers deceive individuals into sharing their sensitive information.



WHY PHISHING?

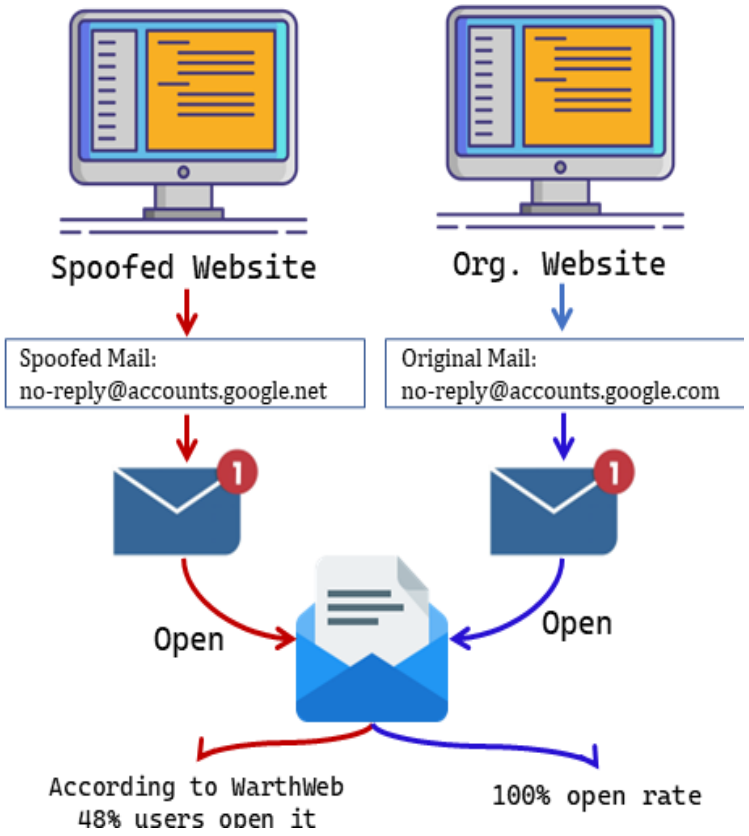
The recently published 'State of Email Security' report by Cofense has observed a significant 569% increase in phishing attacks, a 478% increase in the number of credential phishing incidents, and a 44% increase in malware attacks.





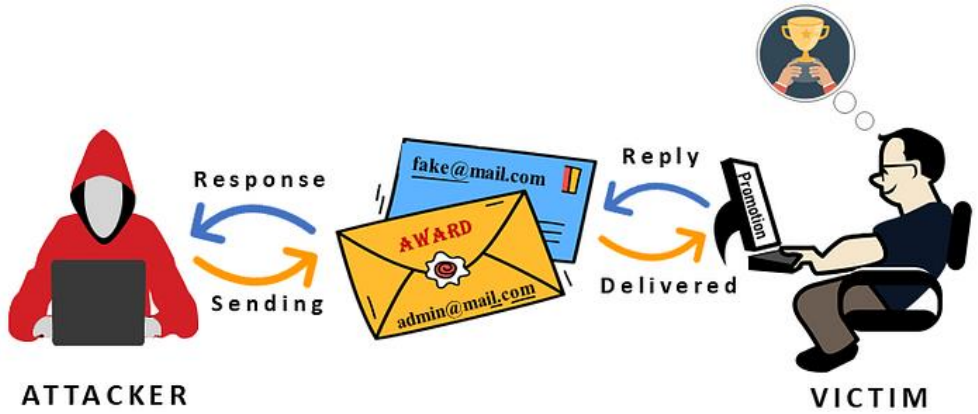
SOURCES:
https://www.statista.com/ | https://cofense.com/

NOOB PHISHING?



Spoofed Email

- Attackers often use email spoofing in phishing attacks by spoofing a domain name to convince users that the phishing email is legitimate.
- An email that seems to come from a company representative is more convincing at first glance than an email from some random domain.



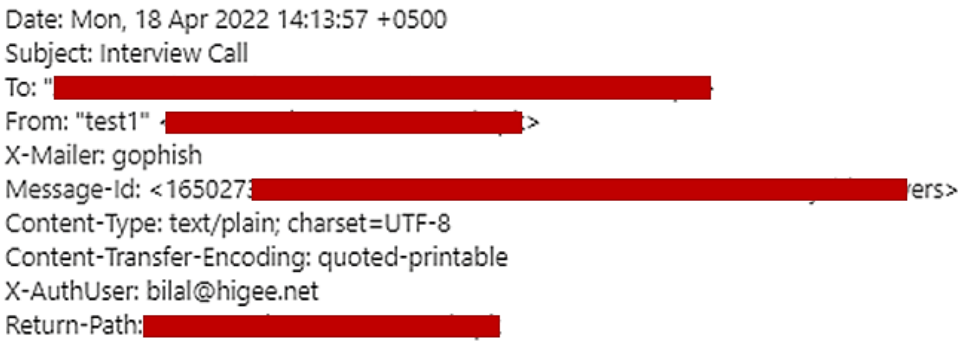
SOURCE: STAYING AHEAD OF THE PHISHING CURVE: A PIONEERING INVESTIGATION INTO EMERGING THREATS

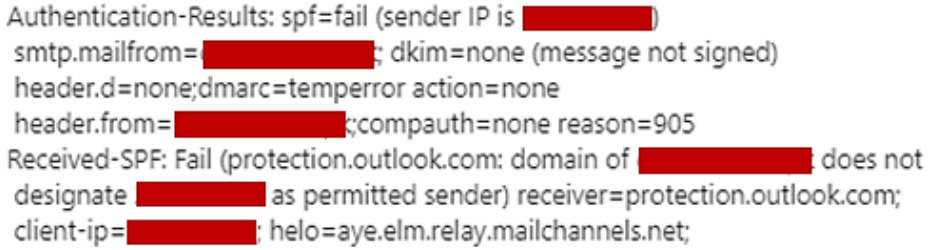
DETECTION

Majority of the phishing emails are easily caught by the SEG before they reach the inbox. But still some attackers manage to find some ways to infiltrate those controls. Then how one can detect these phishing emails?

Using Email Header

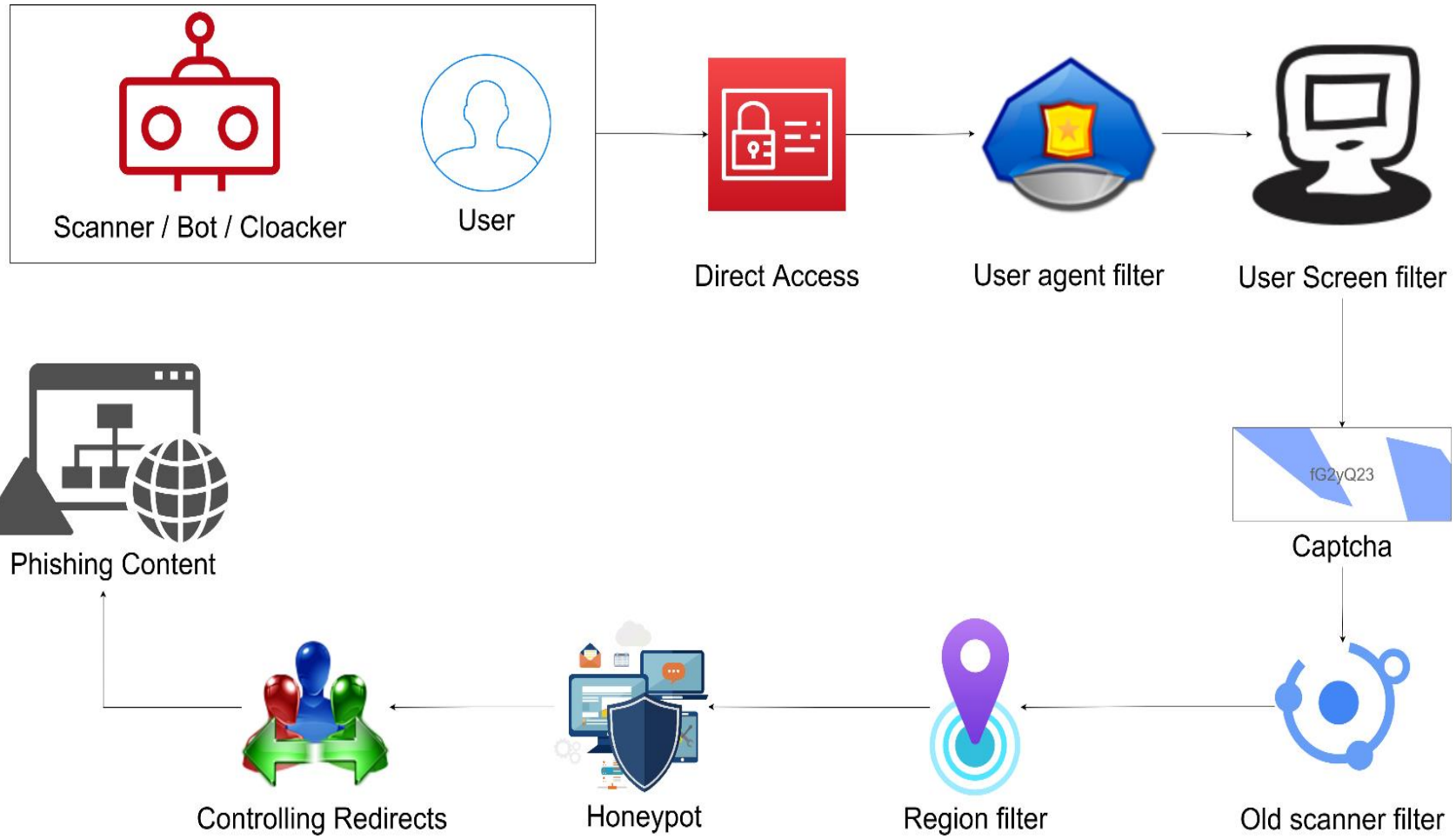
FROM: person who sent the email
TO: your email id
SUBJECT: first text recipients see after sender name
DATE: time when email was received /sent
SPF: to check if a mail server is permitted to deliver email for a certain domain
DKIM: a standard for preventing spam, spoofing, and phishing
DMARC: It is used to guard against domain spoofing
AUTHENTICATION-RESULTS: contains information about SPF, DKIM, and DMARC results
X-SENDER-ID: specifies the exchange key that was used to broadcast the message
X-MAILER: describes the mail client that was used to send the message
MESSAGE-ID: is used to extract information about original sender email address





ADVANCED PHISHING

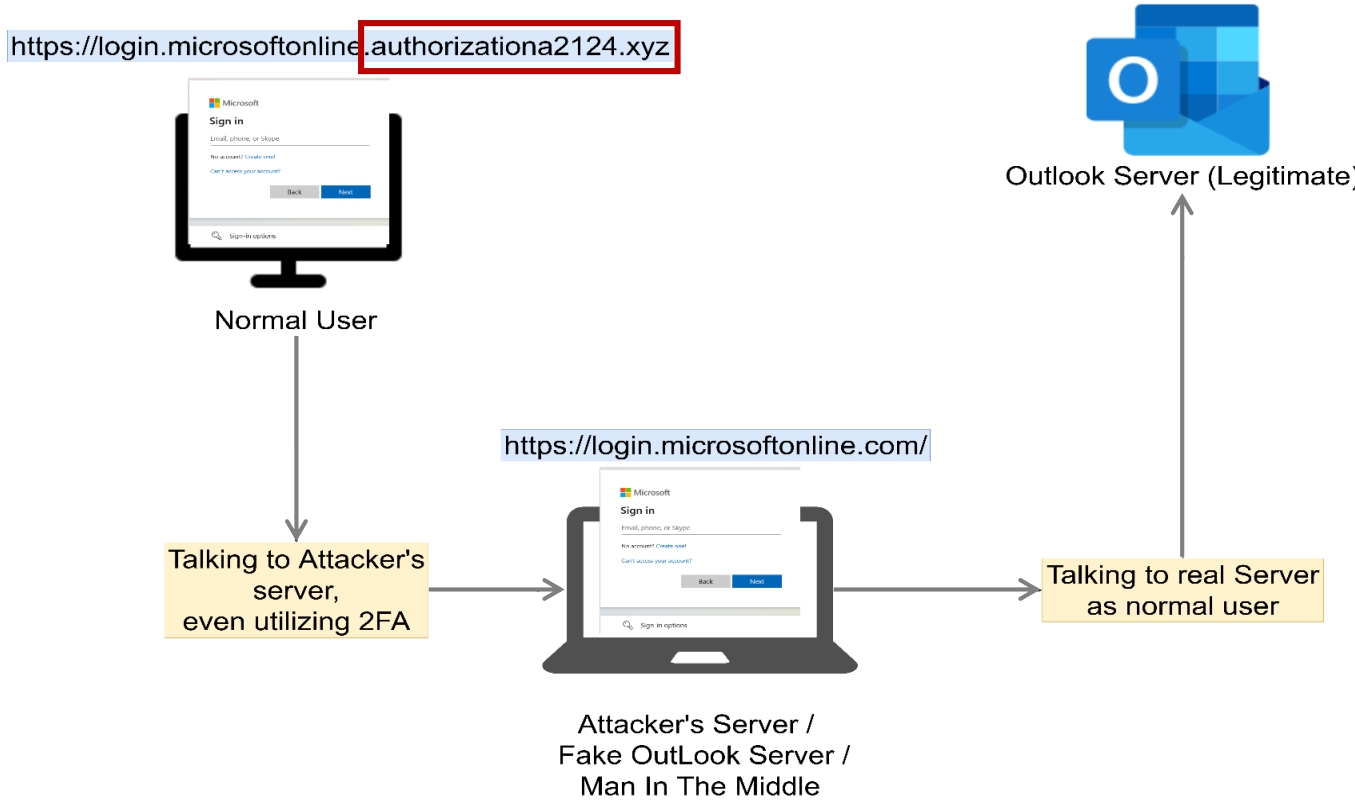
Combined Solution



MFA BYPASS

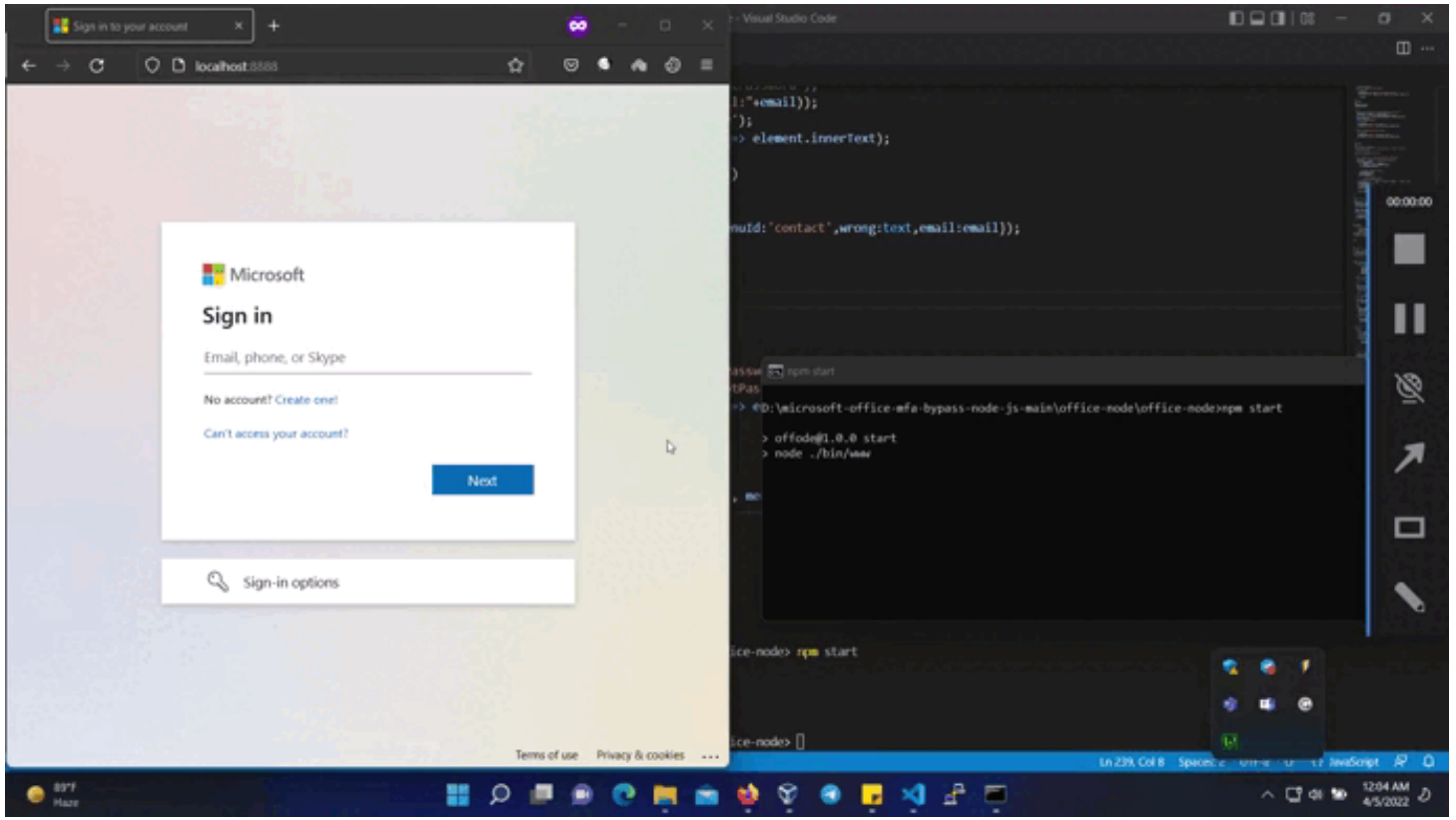
To Increase the security and provide protection against credential phishing attacks, organizations usually force employees to use Multi Factor Authentication.

Although MFA is a good practice but still it is bypass able +



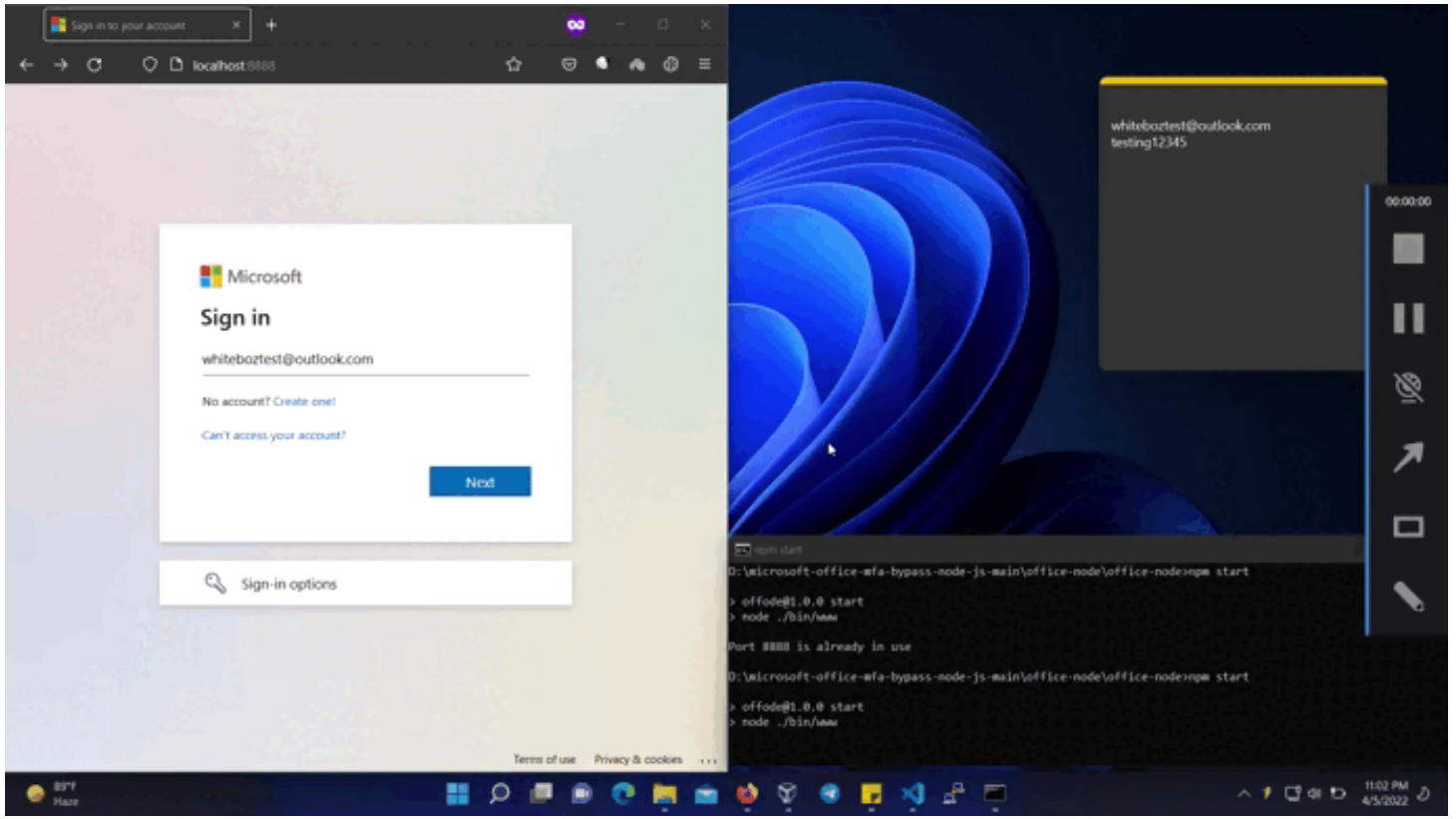
USE CASES

CASE-1 : Basic Email & Password



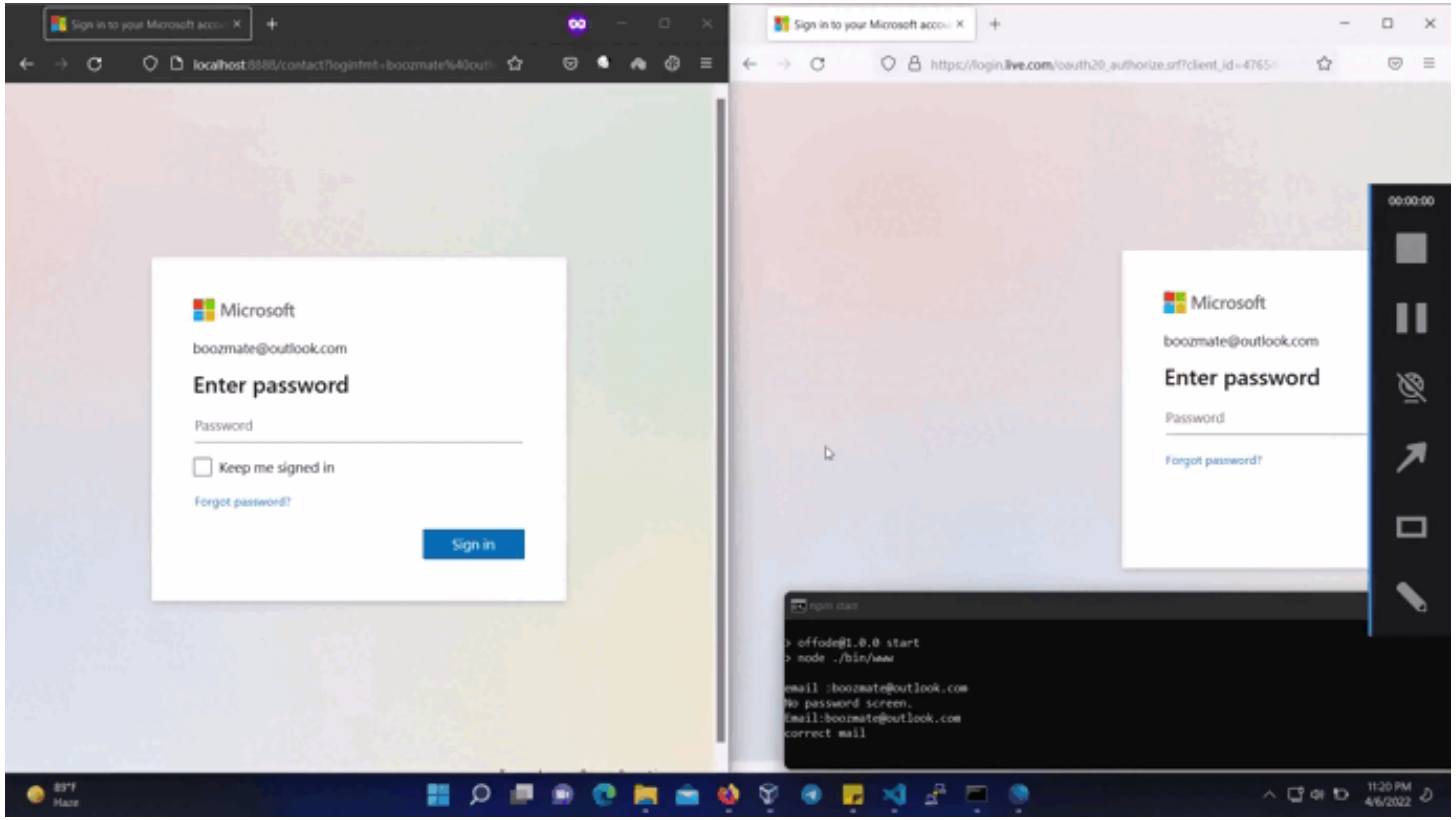
USE CASES

CASE-2 : Authenticator OTP



USE CASES

CASE-3: Phone Number OTP



ULTIMATE SOLUTION

Organizations can make use of advanced puzzle solving CAPTCHA's on login forms to avoid browser automation. Further, AI/ML enabled solutions can also be effective.

Best Practices

- The links or URLs provided in emails are not pointing to the correct location
- There's a request for personal information such as social security numbers or bank or financial information
- The message or the attachment asks you to enable macros, adjust security settings, or install applications.
- The sender address doesn't match the signature on the message itself. For example, an email is purported to be from Air University, but the sender address is john@evilcorp.com.
- There are multiple recipients in the "To" field and they appear to be random addresses.
- The page that opens is not a live page, but rather an image that is designed to look like the site you are familiar with.

To Dos

If you feel you've been a victim of a phishing attack:

- Contact your IT admin if you are on a work computer
- Immediately change all passwords associated with the accounts
- Report any fraudulent activity to your bank and credit card company

THANK YOU!

Azhar Ghafoor