○ ICICI Bank Phishing Case Study

• Phishing Threat Overview (example)

ICICI Bank is one of India's leading private sector banks with millions of customers. In 2020, many ICICI Bank customers were targeted through phishing attacks via email and SMS. These messages were crafted to look like official communication from the bank, tricking users into revealing sensitive information.

•The Attack

The phishing emails and SMS messages claimed that the recipient's account had suspicious activity or needed KYC verification. The messages included a link that redirected to a fake ICICI Bank login page. The attackers used ICICI's branding and design to make the page look real.

•Impact

- Users who entered their login details on the fake page unknowingly gave access to their bank accounts.

- Several cases of unauthorized transactions were reported.

- ICICI Bank had to issue warnings and reminders to customers, advising them not to click on unknown links or share their credentials.

•Lessons Learned

This case shows how effective phishing attacks can be when they use social engineering tactics. Even customers of major banks can fall victim to realistic-looking fake emails or messages. It highlights the need for

public awareness and the importance of tools that can automatically detect phishing attempts before users fall for them.

.Relevance to Our Project

Our phishing email detection tool addresses this exact threat. If such a system had been in place, users could have analyzed suspicious emails before clicking on them. With machine learning, our tool can classify messages as phishing or legitimate, helping to prevent fraud and protect user data.