There are various phishing prevention systems with different functions, as mentioned in the last chapter: some for phishing detection and prevention, some for data encryption, and some for authentication strength. This section will discuss how to deploy a phishing detection and prevention platform using IPS and IDS as an example. Host-based IDS and Network-based IDS: A. Efe and İ. N. Abaci compared two kinds of IDS: host-based intrusion detection systems and network-based intrusion detection systems [32]. ¨ Host-based intrusion detection system (HIDS) HIDS operates on personal devices or terminal servers and has been in use since the early 1980s. Back then, it was primarily used to store logs of dangerous network activities. Nowadays, HIDS has become more sophisticated, and it can not only store risk logs but also detect various types of cyber-attacks and send alerts. ¨ Network-based intrusion detection system (NIDS) NIDS is normally deployed behind the firewall in the Demilitarized Zone (DMZ) to detect all traffic entering and leaving the network. It has two main components: sensors and monitors. The sensor captures and analyzes the traffic to determine its classification, while the monitor displays the analysis results and triggers alarms for further processing by the network administrator. The authors also pointed out in their research that detection systems can be classified into two types according to the detection methods: blacklist-based and anomaly-based. The blacklist based method uses a database containing known phishing or attack information to detect suspicious traffic. The anomaly-based method classifies traffic by analyzing its features to identify potential threats [32]. Nowadays, both methods are integrated to combat the evolving and frequently occurring cyber attacks more effectively. Out-of-band and inline deployment: N. Pappas analyzed the two deployment ways for IPS and IDS and compared their differences. The IPS or IDS can be deployed as out-of-band or inline [33]. In most situations, IDS adopts out-of-band deployment, while IPS uses the inline method. ¨ Out-of-band deployment The detection system's sensor is not typically installed in the backbone network. It is usually connected to an interface on a router or switch. The traffic does not pass directly through the 25 sensor. Instead, the sensor gains a duplicate of the traffic by configuring the router or switch to mirror the traffic. The sensor can only monitor and detect malicious traffic but cannot prevent it. The entire network can continue to operate normally if the detection system meets some issues in this setup. ¨ Inline deployment The detection system's sensor is directly installed in the backbone network. All external traffic must pass through the sensor before reaching the internal network. The sensor inspects all traffic and can not only detect abnormal traffic but also automatically block malicious activities. In this model, the entire network will not operate if the detection system experiences a failure. ¨ Hybrid deployment N. Pappas suggested using hybrid deployment for a modern company network. Deploy IDS and IPS in the same network because most IPS use anomaly-based detection and filter methods. This method may cause false positives. The IPS will lead to more false positives if the level of security is configured too high. However, if the security level is too low, it will miss many malicious traffic and phishing websites. Therefore, the author suggests to deploy the IDS and IPS at the same time [33]. The following figure shows how to deploy the IDS and IPS in the same network. Figure 7: Hybrid deployment with IDS and IPS 26 As shown in Figure 7, the firewall performs basic filtering after the traffic enters the company's network from the Internet. Then, the IPS prevents malicious traffic from progressing further. The filtered traffic flows through the core router and switches into the internal network. The IDS continues to detect

and analyze the traffic that has passed through the IPS. All network logs are sent to the SIEM for storage and display. The cybersecurity staff can monitor abnormal traffic through the IDS and SIEM to protect the network. All traffic reaching the end users has been filtered by the IPS and analyzed by the IDS, with cybersecurity staff overseeing the process through the SIEM. An anti-phishing system can be used instead of the IDS and IPS in this suggested topology.