1. Motivation
- Significant growth in phishing threats (online theft of personal information)
- Cash cost per customer was 1800 USD to an organisation [2]
- Soft costs include reduced customer trust and satisfaction online, and damaged reputation

2. Project Description
- SSE: a simple email digital signing and verifying solution to reduce number of victims to phishing (figure 3)
- The system design was implemented in PHP and HTML scripting languages
- SSE was integrated into test website as an email security feature
- Source code is open for development: https://github.com/djames266/sse

3. Results of SSE Integration into Test Website
- SSE signing module replaced PHP mail and thus, added digital signing capabilities. Digital signatures were added to message body.
- 90% of users surveyed were able to verify and pass digitally signed messages sent to them
- 50% of users surveyed were made aware and understood how the tool protects them from phishing

4. Conclusion
- SSE Advantages: Simple integration into test website, requires no software installation/upgrade on recipient side, simple copy and paste verification process, confirms email message was as intended by sender.
- SSE Future Work: add message encryption, defend against drive-by email attacks, increase survey sample size to cover general population, improve verifier page design, expand digital signing capabilities to other email details, other SSE design improvements to cater for mail forwarding and mail attachments, integrate and test in websites written in different scripting languages to PHP

5. References

- Secure/Multipurpose Internet Mail Extensions (S/MIME)
  - Overview: S/MIME adds cryptographic security services to emails
  - Advantages: Can provide sender authentication, non-repudiation of sender and message confidentiality using encryption and digital signatures.
  - Disadvantages: S/MIME not supported by all email clients, email forwarding threatens sender’s privacy, must purchase digital signatures before use, not applicable to Webmail clients and requires user installation.
- Sender Policy Framework (SPF)
  - Overview: SPF details a protocol for domains to authorise the hosts allowed to send email using their domain names. The recipient host would check such authorisation.
  - Advantages: Reduces spammers forging domain names in the “From” header of an email, relatively easy record implementation in Domain Name System (DNS)
  - Disadvantages: Fails mail forwarding, no message privacy or integrity, cannot stop phishing attacks having fraudulent content.
- Domain Keys Integrated Mail (DKIM)
  - Overview: DKIM is based on cryptographic content signing. The sender adds a digital signature to the email header which is later verified by the recipient.
  - Advantages: Simplified key management using domain names, DKIM signatures transparent to non-supported users, wide range of deployment choices, enables authorised third party signing, can be used on top of other services like S/MIME.

4. Current Email Security Technologies
- Secure/Multipurpose Internet Mail Extensions (S/MIME)
  - Overview: S/MIME adds cryptographic security services to emails
  - Advantages: Can provide sender authentication, non-repudiation of sender and message confidentiality using encryption and digital signatures.
  - Disadvantages: S/MIME not supported by all email clients, email forwarding threatens sender’s privacy, must purchase digital signatures before use, not applicable to Webmail clients and requires user installation.
- Sender Policy Framework (SPF)
  - Overview: SPF details a protocol for domains to authorise the hosts allowed to send email using their domain names. The recipient host would check such authorisation.
  - Advantages: Reduces spammers forging domain names in the “From” header of an email, relatively easy record implementation in Domain Name System (DNS)
  - Disadvantages: Fails mail forwarding, no message privacy or integrity, cannot stop phishing attacks having fraudulent content.
- Domain Keys Integrated Mail (DKIM)
  - Overview: DKIM is based on cryptographic content signing. The sender adds a digital signature to the email header which is later verified by the recipient.
  - Advantages: Simplified key management using domain names, DKIM signatures transparent to non-supported users, wide range of deployment choices, enables authorised third party signing, can be used on top of other services like S/MIME.