Phishing Email Analysis Report

Sample Description:

This report analyzes an email purporting to be from Wells Fargo, warning the recipient about an expired security key and providing a link for reactivation.

Phishing Indicators:

- **Spoofed sender address:**
  The sender appears as `inmail-hit-reply@linkedin.com`, which is not a legitimate Wells Fargo email address. This is a classic case of email spoofing.
- **Header authentication failures:**
  As analyzed with MXToolbox, the message fails DMARC, SPF, and DKIM authentication. The mail originated from a suspicious domain (`example-payments.com`) and passed through unknown relays.
- **Suspicious link:**
  The email prompts the user to visit `http://cabinetkignima.com/Wellsfargo_keys_account5/page2.html` which, despite mentioning Wells Fargo, is clearly not affiliated with the bank. Hovering over the link reveals the mismatched domain.
- **Urgency/threatening language:**
  The email incites fear and urgency by claiming the account is at risk unless immediate action is taken.
- **Grammar/spelling errors:**
  The message contains multiple grammatical mistakes, such as "key your for your", which reduce the professionalism and legitimacy of the email.

Conclusion:

This message exhibits multiple classic phishing traits—sender spoofing, authentication failures, suspicious redirection links, urgent and manipulative language, and linguistic errors. These tactics together strongly suggest a phishing attack designed to steal user information.
