



BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE DEPUTY GOVERNOR | FINANCIAL SUPERVISION SECTOR

MEMORANDUM NO. M-2022-043

To : **ALL BSP SUPERVISED FINANCIAL INSTITUTIONS (BSFIS)**

Subject : **Email Security Control Recommendations**

As BSP Supervised Financial Institutions (BSFIs) continue to accelerate their digital transformation initiatives, email remains to be the primary means of communication in conducting core business operations from marketing and sales, and customer support services, to logistics and supplier contracting, among others. This is also used as one of the main verification and/or authentication factors linked to a bank, financial, or e-payment account in providing electronic payments and financial services (EPFS).

Given the central role of email in digital communications, cyberthreats ranging from spam, phishing, ransomware and other malware attacks targeting email platforms and communications continue to confront BSFIs. Among the most prevalent and costly cyberattacks for financial clients globally is Business Email Compromise (BEC), a type of cyberattack that utilizes seemingly legitimate email accounts from another organization to fraudulently trick employees of another business into giving their credentials, money, personal information, financial details or other sensitive data. Most BEC attacks leverage on spoofing of a corporate or individual's identity whereby the email address of the legitimate sender is impersonated to mislead the recipient on the sender of the email, thereby making the fraud attempt more effective.

In view of this, BSFIs are advised to reinforce email security through the adoption of robust and layered security controls and industry best practices as provided under Section 148 of the Manual of Regulations for Banks (MORB) and Sections 147-Q/145-S/142-P/126-N of the Manual of Regulations for Non-Bank Financial Institutions (MORNBFI). To further enhance email security, BSFIs should adopt, as warranted, the security controls and best practices in safeguarding both incoming and outgoing emails, as follows:

1. Set up a secure Simple Mail Transfer Protocol (SMTP) authentication method on the mail server to control user access.
2. Encrypt emails end-to-end using industry-accepted encryption standards and versions.

3. Enforce thresholds and rate-limit SMTP connections to prevent distributed denial-of-service (DDoS) attacks against the mail server.
4. Activate Reverse Domain Name System (rDNS) to ensure that the Internet Protocol (IP) addresses of incoming emails map to a valid domain name.
5. Use DNS/Email reputation-based blacklists and local IP address filtering to cut down on received spam.
6. Enable content-filtering, anti-spam, and anti-virus features and/or employ sandbox technologies to detect and block incoming emails with invalid or malicious links and attachments.
7. Put in place layered security controls such as firewalls and intrusion prevention systems (IPS).
8. Secure outbound email traffic by imposing sending quotas and scanning outbound messages.
9. Configure mail server relay options to be very restrictive. This is to prevent the mail server from being used as a gateway by threat actors in sending malicious or spam emails.
10. Activate Sender Policy Framework¹ (SPF), Domain-based Message Authentication Reporting and Conformance² (DMARC), and DKIM³ (DomainKeys Identified Mail) to prevent sender address spoofing.

The controls specified in this memorandum are not exhaustive. BSFIs should employ security controls and approaches appropriate to the setup of email platforms. For cloud-based or hybrid email platforms, additional security controls such as multifactor authentication and/or advanced threat protection may be explored with their cloud service providers. To thwart advanced threats and implement a defense-in-depth approach, BSFIs should integrate email security solutions with enterprise fraud management systems, privilege access management, data leak protection, and mobile device management, among others. BSFIs may likewise adopt other generally accepted email security practices which may not have been captured in the above-cited recommendations.

Aside from technical controls, another important activity for preventing email-based attacks is to ensure adequate user education and awareness of the measures to take in case suspicious emails are received. As

¹ The Sender Policy Framework (SPF) is an email authentication protocol and part of email cybersecurity used to stop phishing attacks. It allows an organization to specify who is allowed to send email on behalf of its domain.

² DKIM (DomainKeys Identified Mail) is a protocol that allows an organization to take responsibility for transmitting a message by signing it in a way that mailbox providers can verify. DKIM record verification is made possible through cryptographic authentication. Implementing email authentication technology like DKIM is one of the best ways to protect employees and customers from targeted email attacks.

³ Domain-based Message Authentication Reporting and Conformance (DMARC) is an open email authentication protocol that provides domain-level protection of the email channel. DMARC authentication detects and prevents email spoofing techniques used in phishing, business email compromise (BEC) and other email-based attacks. The domain owner can publish a DMARC record in the Domain Name System (DNS) and create a policy to tell receivers what to do with emails that fail authentication.

such, BSFIs should also consider incorporating the following activities in the enterprise cybersecurity awareness campaign:

1. Identify and cascade whether a virus or malware infection may spread by just opening or selecting an email. While this is not true for most email clients, an assessment should be conducted on the current email platform and version used especially if it enables scripting or automatic downloads and execution, which may heighten the risk of infection.
2. Inspect the Email Header Information:
 - a. The 'Received' information includes 'from' (sender) and 'by' (receiver) which shows the message path from the message sender to the final recipient. This may show multiple records depending on the number of hops within the email system, but the real sender will be identified by checking the last 'received from' information in the email header.
 - b. The 'From' information shows the sender's name and email address.
 - c. The 'Reply-To' refers to the email address that will receive replies to the email. If the reply-to address does not match the sender's email that the sender claims to be representing, there is a good chance that it is a spoofed email.
 - d. The 'Return-Path' defines where bounced emails will be processed. While it is possible to forge the return-path in a message header, it is not done with great frequency.

Note that 'From', 'Reply-To', and 'Return-Path' can be spoofed to show a false name and email.

An example of the email header of a spoofed email:

```
From: "Wally A. Malay" <wamalay@agency.gov.ph>  
Reply-To: "Wally A. Malay" <wamalay@agency.gov.ph>  
Return-Path: "Wally A. Malay" <wamalay@agency.gov.ph>  
Received: from unknown (10.xx.xxx.x) by <fakeemail@scammer.net>
```

In this sample, the sender shows a spoofed legitimate email address. Replies to this email and bounce notifications will be sent to the legitimate email address.

In some cases, spam messages use a similar email address such as wamalay@agencygov.ph which may not be easily detected at first glance.

3. Scrutinize the content of the email. Phishing emails oftentimes have generic greetings and contain unfamiliar links or attachments or unsolicited requests for personal information. These emails are also unexpected and usually contain a sense of urgency that pushes

the recipient to act quickly. It is advisable not to click any attachments or links unless the communication is verified.

4. Contact the sender of the message through a different/trusted channel to verify the validity of the email.
5. Provide guidance on how to report and handle suspicious or malicious emails based on the entity's policies.
6. Conduct regular phishing simulations or exercises.

BSFIs are expected to promptly report to the BSP major email-related cyber incidents/crimes pursuant to the event-driven report and notification (EDRN) and report on crimes and losses (RCL) requirements defined in Section 148 and 173 of the MORB and Sections 147-Q/145-S/142-P/126-N of the MORNBF. In certain instances, BSFIs may need to seek assistance and cooperate with appropriate law enforcement authorities for prompt resolution of cybercrime cases, especially if cases involve public safety and security, pursuant to the Cybercrime Prevention Act of 2012 and other relevant laws and regulations.

For information and guidance.

 Digitally signed by
Chuchi G. Fonacier
Date: 2022.10.07
16:46:22 +08'00'

CHUCHI G. FONACIER
Deputy Governor

07 October 2022