NABA Recommendations for
Best Practices in an Effective Enterprise Anti-Phishing Programme

Phishing is a form of social engineering whereby threat agents attempt to deceive users or take advantage of a user's trust, in order to steal sensitive information, or to gain illegal access to credentials, internal networks, systems, databases, or other valuable enterprise assets.

The key to an effective enterprise anti-phishing programme is maintaining a high degree of staff awareness and training, on a continuous basis.

The following elements should be considered, in priority order:

1. With Respect to E-Mail:

1.1. Implement an On-Going Training Programme of Phishing Security Awareness

As noted, on-going employee awareness and training are key to any effective anti-phishing programme, instilling a healthy dose of suspicion in staff. Training should also include all executive staff as well, as spear-phishing is often directed at senior staff with higher credential levels. Simulated phishing attacks should be run throughout the enterprise on a regular basis to keep cyber awareness high and to monitor user responses in order to measure training effectiveness. Employees who are particularly vulnerable to such attacks will require increased and/or repeated training.

1.2. Employ Anti-Phishing Filtering to all Incoming E-mail

As e-mail is the key threat vector for phishing attacks, employ anti-phishing e-mail filtering, including spam filters, as an initial defense mechanism.

1.3. Employ Internal Security Resources

For e-mails with embedded hyperlinks, find the main URL for the enterprise that issued the incoming e-mail and verify that it matches their standard web addressing protocols. Employees should forward any e-mail they find questionable or suspicious to their internal Help Desk, Solution Centre or Security Team, as appropriate, so that it may be tested on an isolated computer.

1.4. Beware of Urgent Requests, Requests for Personal Information, Contests, Gifts or Money Offers

Urgent e-mail requests elicit an emotional user response to react swiftly, by clicking imbedded e-mail links or opening attachments, without thinking first. This impulse to react should be mitigated by employee training.

1.5. Beware of E-mail from Seemingly Reputable Organizations, e.g. Banks, Government, Social Media Platforms, Including Those from Their Own Organization

Such e-mail takes advantage of user's trust of large enterprise, social platforms and well-known brands.

2. Implement Multi-Factor Authentication (MFA)

In the event one security factor is compromised, there will be at least one additional layer of security before a user's account is fully compromised

3. **Implement Least-Privileged Access Rights**

   Least-privileged access rights is defined as the practice of restricting access rights for users, accounts and computing processes to an absolute minimum and only to those absolutely required to perform their routine, legitimate activities. This will ensure that, in the event of a successful phishing attack, the number of access rights compromised will be kept to a minimum.

4. **Limit Administrative Privileges**

   The number of staff in the enterprise with administrative privileges should be limited to only those whose job description requires such access. The number of people should be kept to an absolute minimum and the list of such people should be reviewed on a regular basis. Implement a Privileged Access Management (PAM) solution to control Administrative account activity and provide an audit trail of the tasks performed by those accounts.

5. **Implement a Regularly-Scheduled Software Update Program for all User Endpoint Devices**

   This will ensure the latest security provisions included in software updates will be implemented on all user endpoint devices and servers, to ensure System Administrators do not introduce any vulnerabilities into the system while they are performing maintenance on them.

6. **Implement an Endpoint Security Program for all Devices Accessing the Enterprise Network**

   This will allow the enterprise to access the security stance of all devices using the network and to deny access to those which are compromised. Devices can be separated between personal and corporate devices.

7. **Ensure the Enterprise Business Continuity Programme Includes the Mitigation of Successful Phishing Attacks**

   Simulate the various possible effects of a successful phishing attack and develop mitigation strategies in advance, as part of the written enterprise Business Continuity Programme. This should include maintaining and verifying backups so the Enterprise can recover, for example, from a ransomware incident caused by a phishing attack. These mitigation strategies should be exercised regularly.

8. **Adopt a Holistic Approach to the Enterprise Anti-Phishing Programme**

   Invest annually in counter-measures that include technology, training, employee awareness, software, etc. as an over-arching approach to mitigating phishing attacks.

January 7, 2020