NABA Recommendations on Best Practices to Mitigate Social Engineering

Social engineering has become more commonplace in the enterprise and increasingly complex to address. Cyber criminals have become very adept at manipulating employees into handing over sensitive or valuable enterprise information.

Social engineering is predicated on psychological manipulation of the employee. Typically, it involves email (i.e. “phishing”) or some other form of communication that invokes a sense of fear, pressing need, response to authority, elation, etc., in the employee, motivating him/her to take action by clicking on a phishing e-mail, a malicious link or by revealing sensitive information. Social engineering can also be attempted over the phone (i.e. “vishing”) or even in face-to-face communications, when the cyber criminal has breached the physical barriers of an enterprise building.

Social engineering operates on the psychological level of the employee. As every employee is different, social engineering has become a pernicious threat to the enterprise to mitigate. Cyber criminals need only to deceive one employee in order to be successful in launching malware, receiving sensitive information, gaining access to the enterprise building or network, etc. Cyber criminals have been known to research the social media presence of individual employees in advance in order to make their phishing emails more personal and relevant.

Some of the steps that have proven to help the enterprise mitigate the risk are as follows.

In all cases, when in doubt, employees should contact their internal IT resources or internal security team before taking any action.

1. Train

Employee training on ways to detect and mitigate social engineering is critical. Comprehensive Security Awareness should be undertaken in the enterprise on a reoccurring basis and should include social engineering testing and simulated phishing attacks. Training should focus on implementing enterprise-wide behavioural change on the part of the employee and should be performed on an on-going, proactive basis.

Further, employees should be trained to adopt a “zero-trust” attitude toward external requests. In fact, employees can be encouraged to “think like a cyber criminal” to reinforce their preparedness.

2. Delete requests for personal information or passwords

Although this would appear to be obvious, cyber criminals sometimes offer bogus rewards or other false incentives in return for personal information, or even passwords. In addition, they might send emails impersonating a government department, law office, bank or insurance company, as examples. Since the payload of some of these email requests may contain malware, they should either be deleted or routed to the enterprise cyber security team for analysis, as mentioned.

3. Limit information released to third parties

Some cyber criminals will contact the enterprise IT team posing as software or hardware salespeople. In order to better tailor their bogus unsolicited offer, they will ask for information on the hardware or software an enterprise is using, i.e. firewalls, routers, security software, etc. The more information they receive, the better position they are in to exploit latent vulnerabilities.

When faced with such requests, it is recommended to route these questions to a designated central point of contact in the enterprise, someone who is responsible for vetting the requestor and the need for the requested information. Employees should be trained that the default response to such requests is never to release any information.

4. Secure your devices, network and software

As a general IT best practice, ensure all required software patches are installed promptly and security software updates are set to be installed automatically.

5. Use multi-factor authentication

One of the main targets of cyber criminals are credentials, as they facilitate their access to internal enterprise networks and assets. Using multi-factor authentication can help to mitigate this risk.

6. Reject requests for help or offers for help

Legitimate external companies and organizations do not contact an employee for help. If an employee did not specifically request assistance from the sender, an email offer of such assistance is most likely a scam. Delete email requests from charities or other organizations with which your organization does not have a relationship.

7. Always escort guests when physically visiting an enterprise

Physically accessing enterprise facilities through “tail-gaiting” or “piggy-backing” provides the cyber criminal with direct access to internal networks and devices. Guests should always be escorted from the point of legal entry into the building to the visited employee and then escorted out. All visits should be logged in advance with security and credentials should be validated by enterprise security before access is granted.

8. Question people in the enterprise you don’t know

It is not improper to politely challenge the credentials of unescorted people in the enterprise that are not recognized. If their status is circumspect, enterprise security should be immediately involved.

9. Learn to react slowly

As the majority of social engineering attacks are attempted by phishing, cyber criminals try to motivate the employee to react emotionally and quickly to offers for help, gifts, false demands by senior management, etc. Employees must learn to react slowly and review the request thoroughly, when confronted by a reported sense of urgency. When such requests are received, they should either be deleted or routed to the enterprise cyber security team for analysis.

In general, there are four steps that can be used to help mitigate social engineering:

- Verify the requester is who they say they are;
- Verify that the requestor is an employee of the stated company;
- Verify that the requester is authorized to make the request;
- Whenever in doubt, employees should route such requests to the enterprise cyber security team for analysis.

June 18, 2020