Phishing Prevention Checklist
Technical, Physical and Administrative Controls

Audience
This article is intended for IT and security related management personnel.

Objective
Outline controls that can help minimize the threat from phishing.

Assumptions
The reader understands what phishing is and the threat it poses.

PhishingBox, LLC.
400 East Vine Street, Suite 301
Lexington, KY 40507

+1 877.634.6847
info@phishingbox.com
https://www.phishingbox.com

Version 2.1

Phishing
Prevention Checklist

The following controls should be implemented within an organization in order to help prevent or minimize the impact from phishing attacks.

☐ Ensure the Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), Domain Message Authentication Reporting and Conformance (DMARC) are configured and enabled.	These records help minimize the likelihood of your company's emails being used to spoof others.
☐ Enable SPAM filter.	Enabling SPAM filters is an initial defense to block a majority of suspicious email content.
☐ Ensure that your email server or gateway is reviewing inbound emails for proper SPF, DKIM, compliance and handling via DMARC records.	If other email senders have set their SPF and DMARC records, you should ensure that your system is analyzing these records.
☐ Properly configure firewall/email filter. Restrict outside emails with an internal email address. Restrict any email that fails a SPF/DKIM record check.	These checks minimize malicious traffic from entering the network. If an email fails such checks, it is highly suspicious.
☐ Minimize User Access Rights. As much as possible, minimize the access rights of users to the minimum needed for them to perform their job.	Should an account be compromised, the limited access rights would minimize the potential damage that could occur.
☐ Enable Single/Sign on where feasible.	Enabling single sign on minimizes the potential for someone to sign into a non-authorized site or system.
☐ Enable multi-factor authentication where feasible.	Multi-factor authorization minimizes the likelihood of an attacker obtaining the complete authentication credentials.

☐ Enable web filtering. Block users from going to identified malicious sites.	This type of blocking works better with real-time domain blocking such as from a large service provider.
☐ Establish a reporting mechanism for users to report suspicious emails, such as Phishing Inbox.	Providing a method for users to easily report, and administrator to easily analyze, helps use your employees as part of the security process.
☐ Provide security awareness training to employees. Ensure employees are trained on social engineering tactics, including phishing. Higher risk employees should receive continued phishing simulation and training.	Training systems such as PhishingBox help employees become part of the solution of identifying and blocking suspicious emails.
☐ Maintain up-to-date applications. Ensure that software is up-to-date.	Many known vulnerabilities are exploited when there is a fix already installed.
☐ Maintain anti-malware software. Ensure that end-users devices have up-to-date malware software.	Many attacks are well known and have signature or heuristics available to identify and block the activity, but the rules and signature need to be updated.
☐ Sign up for Real-time Blackhole List (RBL) to block known emails.	Most SPAM filters will include such capabilities but ensure that you are taking advantage of the reporting of known system by others.
☐ Operationally, establish dual controls and/or out-of-band verification for key transactions, such as wire transfers.	Dual control requires multiple systems to be compromised. As such, it makes it more difficult to bypass. Banks have been doing this for years, but now more controls are provided to businesses, enabling dual controls if an available option.
☐ Encrypt mobile devices that contain non-public data. Most do, as internal emails between employees may contain non-public details.	Should (or when) a mobile device is lost, encrypted data is difficult to recover, making the lost device less of a risk.

☐	Use mobile device management software for end-user devices such as phone, tablets, etc.	You cannot rely on end-users to lock their own device.
☐	Establish a vendor management program. Ensure that all suppliers that have access to or provide non-public information have adequate information security programs. They should specifically include security training on social engineering and phishing.	Your company could be exposed if a vendor becomes an unknown participant in a phishing scheme by either sending a request or providing information that allows an attacker to send a request that seems valid.

PHISHING NOTES