

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.
- Enable SPAM filter.
- Ensure your email server or gateway is reviewing inbound emails for proper SPF, DKIM, compliance, and handling via DMARC records.
- Properly configure firewall/email filter. Restrict outside emails with an internal email address. Restrict any email that fails a SPF/DKIM record check.
- Minimize user access rights. As much as possible, minimize the access rights of users to the minimum needed for them to perform their job.
- Enable Single-Sign-On (SSO) where feasible.
- Enable multi-factor authentication where feasible.

These records help minimize the likelihood of your company's emails being used to spoof others.

Enabling SPAM filters is an initial defense to block a majority of suspicious email content.

If other email senders have set their SPF and DMARC records, you should ensure your system is analyzing these records.

These checks minimize malicious traffic from entering the network. If an email fails such checks, it is highly suspicious.

Should an account be compromised, limited access rights would minimize the potential damage that could occur.

Enabling SSO minimizes the potential for someone to sign into a non-authorized site or system.

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 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 administrators to easily analyze, incorporates 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 help employees become part of the solution of identifying and blocking suspicious emails.

IMPORTANT

Maintain up-to-date applications. Ensure software is current and updated.

Many known vulnerabilities are exploited when there is a fix already installed.

Maintain anti-malware software. Ensure end user 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 malicious emails.

Most SPAM filters will include such capabilities but always check you are taking advantage of the reporting provided 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. Banks have been doing this for years. Now, access to such features is more readily available to businesses.

Encrypt mobile devices containing non-public data. Most do, as internal emails between employees may contain non-public details.

If a mobile device is lost, encrypted data is difficult to decode, making the lost device less of a risk.