IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

CAPACITY ENHANCEMENT GUIDE
Counter-Phishing Recommendations for Federal Agencies

AUDIENCE AND SCOPE

- This guide recommends technical capabilities to protect federal agency email systems and networks against malicious phishing emails.
- This guide provides information to inform federal agencies' executive leadership (senior risk official, chief information officers, and chief information security officers) and also provides sufficient detail to support a technical discussion with implementation teams.
- This guide is applicable—outside of federal agencies—to state, local, tribal, and territorial governments and commercial industry.
- Capacity Enhancement Guides support CISA's role as the Nation's cybersecurity risk advisor by sharing high-priority recommendations, best practices, and operational insights in response to systemic threats, vulnerabilities, and risks.

AT-A-GLANCE RECOMMENDATIONS

- ✓ Secure Email Gateway Capabilities
  - Deploy email filters
  - Deploy sandboxing or detonation chambers
- ✓ Protect Outbound Web-Browsing
  - Block known malicious sites and top-level domains
  - Block specific file types from leaving the network
- ✓ Harden User Endpoints
  - Employ multi-factor authentication
  - Secure browsers
- ✓ Protect Endpoints
  - Block malicious macros by default
  - Deploy antivirus software and host-based intrusion detection and prevention systems

INTRODUCTION

Email systems are the preferred attack vector for malicious phishing campaigns. Recent reporting shows 32 percent of breaches involve phishing attacks, and 78 percent of cyber-espionage incidents are enabled by phishing.[i,ii] Additionally, cyber attackers often take advantage of current events, and recent phishing and ransomware campaigns have targeted critical infrastructure sectors. Given the recent shift to an extended remote workforce, the Cybersecurity and Infrastructure Security Agency (CISA) strongly recommends agencies prioritize the protection of email systems. CISA has reviewed the current threat landscape and existing guidance to highlight actions and capabilities that can provide significant protection against phishing attempts.

PURPOSE

Many agencies have built robust counter-phishing programs, but there remains a wide disparity in scale, capability, and implementation. In response, CISA is recommending technical capabilities to enhance agencies' counter-phishing defenses. These capabilities stem from operational insights from CISA's counter-phishing programs and interagency best practices, and they fall into four categories: 1) Secure Email Gateway Capabilities, 2) Outbound Web-browsing Protections, 3) Harden User Endpoints, and 4) Endpoint Protections.

The capabilities, which are primarily technical and preventive in nature, are not meant to replace or lessen the importance of user training and awareness. With proper implementation, these capabilities can significantly decrease the amount of malicious phishing emails reaching teleworking users' inboxes, and thereby lessen the chance of end-users interacting with phishing emails.

RECOMMENDED APPROACH[iii]

CISA recommends that agencies evaluate their current security posture and implement a risk-based approach, based on the following recommendations, to improve agency defenses against phishing attacks. Aligning with their own organizational risk tolerance and mission-critical operations, agencies should implement measures commensurate with the threats and risks that they face. Agency leadership should champion planning and deployment of these measures to enable prioritized implementation. Some capabilities may be easier for an

agency to implement (such as configurations and services), while others may require extensive planning to build or procure. How and agency wants to prioritize and implement specific capabilities is ultimately left to agency discretion, in accordance with applicable laws, regulations, and directives (including Emergency Directives and Binding Operational Directives).

CISA recommends using this guidance in combination with CISA's Phishing Campaign Assessment (PCA) program. A PCA is an assessment that occurs over a six-week period and measures an agency workforce's propensity to click on email phishing lures. The results can be used to provide guidance for anti-phishing training and awareness. For more information, see cisa.gov/cyber-resource-hub.

RECOMMENDED CAPABILITIES

1. SECURE EMAIL GATEWAY CAPABILITIES

Optimize secure email gateways, appliances, or services to intercept phishing emails.

RECOMMENDATIONS

a. Deploy an email filter solution that screens based on headers and malicious content (e.g., malicious macros, infected attachments, etc.), categorizes email, inspects Uniform Resource Locators (URLs) against reputation feeds and has customizable rule-based filters.[iv]
b. Strip and/or block emails containing active content (e.g., ActiveX, Java, Visual Basic for Applications [VBA]) or macros by default. Administrators should allowlist such content only for legitimate reasons.[v]
c. Reformat hyperlinks in email messages by rewriting URLs in the body of the message into plain text.[vi]
d. Deploy sandboxing or detonation chambers to safely isolate malicious links.[vii]
e. Ensure detection signatures and blocklists are up to date.[viii]
f. Block email beyond a certain size and/or containing attachments that exceed a certain size.[ix]
   - Consider legitimate needs to receive large file sizes and, if feasible, limit file size to suit organizational need.
g. Block certain file extensions—including unknown or unused attachments that should not typically be transmitted over email—to prevent vectors such as .scr, .exe, .pif, and .cpl.[x]
   - To the extent feasible, filter out mislabeled file extensions, for example, an executable (.exe) file that is labeled as a document (.doc) file.
h. Open and analyze compressed and encrypted formats, such as .zip and .rar, that may be used to conceal malicious attachments in obfuscated files or information.[xi] If unable to open and analyze such content, consider blocking encrypted .zip and other files. However, blocking attachments might keep legitimate files from reaching recipients, which may hinder business functions. Consider using workarounds, such as allowlisting (e.g., trusted senders), to limit negative impacts to operations.
   - If feasible, consider removing the encrypted content from the message and putting it in an out-of-band delivery solution (e.g., web-based portal), replacing the content with a token/link in the original message.
i. Ensure all email gateways, appliances, or services are configured to use only approved Domain Name System (DNS) resolvers and forwarders in accordance with CISA Emergency Directive 19-01: *Mitigate DNS Infrastructure Tampering*.[xii]
j. Implement warning banners to alert users about emails with links and attachments that originate from outside the organization (allowlist familiar domains to reduce unnecessary implementation).[xiii]

CISA's threat-based cybersecurity capability analysis (.govCAR) suggests the use of technologies that strip hyperlinks in email messages by rewriting the body of the message to turn URLs into plain text (making them "unclickable"). Stripping hyperlinks may improve mitigation of spear-phishing emails with malicious links—one of the most prevalent threat actions—where the end user's computer is typically compromised after clicking on the link.

With hyperlinks converted to plaintext, recipients can still copy the plain text and paste it into the address bar of their browser and then navigate to the URL. Agencies should keep their boundary protections up to date to ensure malicious URLs are beyond reach. Malicious URLs and domains related to current events are exploding in use by cyber threat actors. These protections may need to be updated more frequently than current practice.

Agencies can implement many of the recommendations listed above by using content, disarmament, and reconstruction technology. Consider using such technologies as part of the process to evaluate potential email gateway capabilities. Additionally, CISA Binding Operational Directive 18-01: *Enhance Email and Web Security* requires valid Sender Policy Framework (SPF)/Domain-based Message Authentication, Reporting, and Compliance (DMARC) records on all second-level agency domains to protect the federal enterprise against spoofed emails. For more information, see cyber.dhs.gov/bod/18-01/

For more information on protecting against phishing-enabled ransomware attacks, please see us-cert.gov/Ransomware.

2. OUTBOUND WEB-BROWSING PROTECTIONS

Deploy or enhance outbound web protections and proxies to prevent browsers from accessing malicious sites.

RECOMMENDATIONS

a. Conduct full web traffic inspection, including encrypted traffic, using Hypertext Transfer Protocol Secure (HTTPS) inspection. However, consider the pros and cons associated with HTTPS inspection.
   - For more information, see CISA Alert TA17-057A: HTTPS Interception Weakens TLS Security: us-cert.gov/ncas/alerts/TA17-075A.

b. Use Data Loss Prevention technologies to detect malicious instances of data exfiltration.

c. Detect and block specific file types (including executable files) from leaving the network over both unencrypted and encrypted channels.[xiv]

d. Use a web proxy, protective DNS resolver, or similar filters to:
   - Block known malicious sites and use website reputation scoring to block new, potentially malicious sites.[xv]
   - Block rarely used top-level domains with suspicious characteristics (e.g., shortened or altered top-level domains).
   - Categorize and blocklist malicious and unnecessary sites (e.g., gambling sites, social media), and only allowlist sites that have a legitimate business need.[xvi]

3. HARDEN USER ENDPOINTS

Implement secure configurations.

RECOMMENDATIONS

a. Employ multi-factor authentication to verify users' identities.[xvii]

b. Ensure up-to-date patch management, including automatic application updates, where possible and appropriate.[xviii]

c. Limit and minimize the number of browsers authorized for use to reduce attack surfaces and vulnerabilities. Maintain a list of allowed browsers.

d. Implement secure browser configurations and enforce automatic software updates.[xix]

e. Employ the principle of least privilege to allow users only enough access to perform their jobs. Restrict privileged users from performing certain non-privileged operations on the systems they are administering (e.g., using personal email, browsing the internet, office automation tasks, installing unwanted software applications, other recreational uses).[xx]

4. ENDPOINT PROTECTIONS

Deploy endpoint protections—including antivirus software, host-based intrusion detection system (HIDS), and host-based intrusion prevention system (HIPS)—to provide ongoing host-level protection for operating systems and browsers.

RECOMMENDATIONS

Ensure the workstation software suite includes the following capabilities:

- ✓ Has up-to-date signature-based malware detection[xxi]
- ✓ Has up-to-date behavior-based malware detection[xxii]
- ✓ Performs checks and runs stack analysis on compiled binaries to ensure file integrity (i.e., ensures binaries have not been maliciously changed)[xxiii]
- ✓ Blocks malicious macros by default through Group Policy settings or registry keys, by defining rules for execution of active content, such as ActiveX controls, add-ins, and VBA code[xxiv]
- ✓ Detects and quarantines malicious documents, files, and attachments[xxv]
- ✓ Enforces "deny all/permit-by-exception rule" on host firewalls[xxvi]

ADDITIONAL GUIDANCE

For additional phishing mitigations, refer to CISA Alert AA19-339A: Dridex Malware: us-cert.gov/ncas/alerts/aa19-339a.

CONTACT INFO

For questions about this guidance and other CISA services available to federal agencies, please contact CyberLiaison@cisa.dhs.gov.

REFERENCES

[i] Verizon 2019 Data Breach Investigation Report, https://enterprise.verizon.com/resources/reports/dbir/
[ii] Joint CISA/National Cyber Security Centre (NCSC) Alert (AA20-099A): COVID-19 Exploited by Malicious Cyber Actors https://www.us-cert.gov/ncas/alerts/aa20-099a
[iii] The CISA Recommended Approach has been derived from NIST standards as well as CISA operational insights and best practices.
[iv] NIST Special Publication 800-177 Revision 1: Trustworthy Email – p. 78 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf
[v] Combination of agency expertise and NIST Guidance – p. 78 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf
[vi] Guidance based on the .gov Cybersecurity Architecture Review (.govCAR) findings – p. 13 (image) https://community.max.gov/download/attachments/1615373590/Spin7_summary_FINAL.pdf?api=v2
[vii] NIST Special Publication 800-177 Revision 1: Trustworthy Email –p. 115 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf
[viii] NIST Special Publication 800-83 Revision 1: Guide to Malware Incident Prevention and Handling for Desktops and Laptops – p. 12 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf
[ix] Combination of industry standards and NIST Guidance – p. 21 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf
[x] Combination of industry best practices and NIST guidance – p. 13 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf
[xi] Best practices based on CISA interviews with agencies
[xii] CISA Emergency Directive 19-01: Mitigate DNS Infrastructure Tampering - https://cyber.dhs.gov/ed/19-01/
[xiii] Best practice based on CISA interviews with agencies

[xiv] Best practices based on CISA interviews with agencies
[xv] Guidance based on .govCAR findings – p. 15 (image)
https://community.max.gov/download/attachments/1615373590/Spin7_summary_FINAL.pdf?api=v2
[xvi] Guidance based on .govCAR findings – p. 15 (image)
https://community.max.gov/download/attachments/1615373590/Spin7_summary_FINAL.pdf?api=v2
[xvii] According to a Google study MFA blocks 100% of automated bots, 96% of bulk phishing attacks, and 76% of targeted attacks - https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html
[xviii] CISA Publication: Security Tip – Protecting Against Ransomware - https://www.us-cert.gov/ncas/tips/ST19-001
[xix] CISA Publication: Securing Your Browser https://www.us-cert.gov/publications/securing-your-web-browser
[xx] NIST Special Publication 800-53 (Rev. 4): Security and Privacy Controls for Federal Information Systems and Organizations - https://nvd.nist.gov/800-53/Rev4/control/AC-6
[xxi] NIST Special Publication 800-83 Revision 1: Guide to Malware Incident Prevention and Handling for Desktops and Laptops – p. 19 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf
[xxii] NIST Special Publication 800-83 Revision 1: Guide to Malware Incident Prevention and Handling for Desktops and Laptops – p. 19 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf
[xxiii] Best practices based on CISA interviews with agencies
[xxiv] Best practices based on CISA interviews with agencies
[xxv] DHS Electronic Mail Gateway Security Reference Architecture Version 1 – p. 11
https://www.doi.gov/sites/doi.gov/files/uploads/attachment_4_-_email_gateway_security_reference_architecture_v1.pdf
[xxvi] NIST Special Publication 800-41 Revision 1: Guidelines on Firewalls and Firewall Policy – p. 4-4
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf