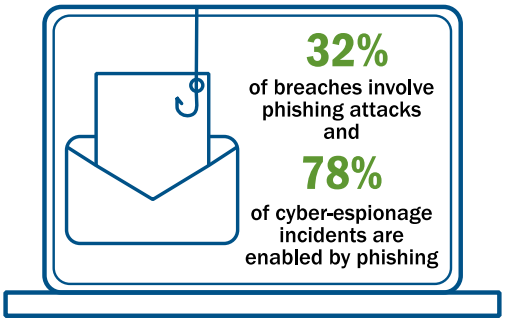
CAPACITY ENHANCEMENT GUIDE
Counter-Phishing Recommendations for Non-Federal Organizations

THE THREAT AND HOW TO THINK ABOUT IT



Email systems are the preferred attack vector for malicious phishing campaigns. Often, by mentioning current events, threat actors carrying out phishing attacks can craft emails that are likely to capture recipients' attention and lure them to click a link or download a file containing malicious code. Given the recent shift to more telework and remote options, organizations and workers face increased risk of falling vicitim to phishing emails and cyberattacks.

Successful phishing attacks can devastate an organization with malware that:

- Destroys computer files;
- Provides adversaries with access to intellectual property;
- Installs ransomware that holds information hostage in exchange for money; and/or
- Deploys viruses that spread throughout a network like a flu and damage files and/or operating systems.

Executive leaders and IT professionals should assess their organization's threat landscape and prioritize protection of email systems. Organizations should implement risk-based approaches, based on their unique operating environment, using appropriate measures to strengthen knowledge and network defenses against phishing attacks.

TRAINING + TECHNICAL PRECAUTIONS = FEWER PHISH

Cyberattackers can be clever and, on occasion, even a well-trained employee might be tricked into opening a phishing email. While training and awareness remain a critical step to workforce cybersecurity, adding properly implemented technical and preventive steps can significantly reduce the number of phishing emails that reach your workers' inboxes. These steps can reduce the chance of end users interacting with phishing emails.

The Cybersecurity and Infrastructure Security Agency (CISA) offers a six-week Phishing Campaign Assessment, a free service for public and private organizations, to measure their propensity for becoming a victim of a phishing attack. CISA urges organizations to consider using the Phishing Campaign Assessment service, combined with implementation of this guidance, to safeguard their network environments.

Based on operational insights from phishing assessment programs as well as federal interagency best practices, CISA recommends four ways to add layers of protection:

- Secure email gateway capabilities
- Implement outbound web-browsing protections
- Hardened user endpoints
- Implement endpoint protections

Each of these approaches includes a number of options that organizations can use to tailor implementation, depending on their needs. Let's take a closer look at each of the four approaches.

Stop Phishing Emails Before They Get to the Inbox With Secure Gateway Capabilities

Much like a security fence prevents unauthorized people from entering a facility, secure email gateways enable an

organization to intercept phishing emails before they even get to an employee's inbox. There are many ways your organization can implement this approach. For a complete listing, please read the *Capability Enhancement Guide (CEG): Counter-Phishing Guidance for Federal Agencies* at cisa.gov/telework. Some of the recommended approaches are:

- Deploy an email filter solution that filters based on content and headers, categorizes email, inspects uniform resource locators (URLs), and has customizable rule-based filters;
- Strip and/or block emails containing active content (e.g., ActiveX, Java, Visual Basic) or macros by default, and only place this type of content on your allowlist for legitimate reasons;
- Deploy sandboxing or detonation chambers to safely isolate malicious links;
- Ensure signatures and blocklists are up to date; and
- Ensure all email gateways, appliances, and services are configured to use only approved Domain Name System (DNS) resolvers and forwarders.

KEY RECOMMENDATIONS

Secure Gateway
- Ensure all email gateways, appliances, and services are configured to use only approved Domain Name System (DNS) resolvers and forwarders.
- Ensure signatures and blocklists are up to date.

Organizations should consider adopting content, disarmament, and reconstruction technologies that can implement the complete listing of recommendations. For guidance on implementing enhanced email security, such as Sender Policy Framework (SPF)/Domain-based Message Authentication, Reporting, and Compliance (DMARC), see *CISA Insights: Enhance Email & Web Security* at cisa.gov/insights. More information on protecting against phishing-enabled ransomware attacks is available at us-cert.gov/Ransomware.

Prevent Browsers from Accessing Malicious Sites with Outbound Web-Browsing Protections

Even if a phishing email gets past your secure gateway and trained staff, you can still prevent or mitigate the consequences. The following steps can prevent computer users from connecting to websites created for nefarious intent, even if they click a link in the email.

- Inspect all web traffic, including encrypted content using HTTPS inspection, which validates certificate chains and uses strong cryptography.
  - There are trade-offs and risks to consider with full inspection. See CISA Alert, *HTTPS Interception Weakens TLS Security*, us-cert.gov/ncas/alerts/TA17-075A, for information on the risks and security implications to consider.
- Use data loss prevention technologies.
  - These technologies can help you detect malicious instances of unauthorized copying, transfer, or retrieval of data from a computer or server.
- Block specific file types (such as executable files or .exe) from entering or leaving the network over both unencrypted and encrypted channels.
- Use a web proxy, protective Domain Name System (pDNS) resolver, or similar mechanisms to:
  - Block known malicious sites and use website reputation scoring to block new, potentially malicious sites;
  - Block rarely used top-level domains (TLDs) with suspicious characteristics (e.g., shortened or altered TLDs); and
  - Categorize and blocklist malicious and unnecessary sites (e.g., gambling sites, social media), and only allowlist sites that support a legitimate business need.

KEY RECOMMENDATIONS

Outbound Web-Browsing Protections
- Block specific file types (such as executable files or .exe) from leaving the network over both unencrypted and encrypted channels.
- Use a web proxy, protective Domain Name System (pDNS) Resolver, or similar filters.

Use Secure Configurations to Harden User Endpoints

Make sure to configure computer and network settings correctly—and keep them updated. Incorrect or badly configured settings can provide additional opportunities for cyberattackers to gain entry. Here are some ways to use secure configurations:

- Employ multi-factor authentication (MFA) to verify users' identities. For example, at a minimum, require a password and a one-time authorization code.
- Ensure up-to-date patch management, including automatic application updates where possible and appropriate.
- Apply software patches and updates in a timely fashion. Outdated software can leave computers exposed to known threats.
- Restrict employees to use of organizationally approved browsers and enforce automatic software updates.
- Employ the "principle of least privilege" and allow users only the access needed to perform their jobs. Prevent privileged users from performing operations on the systems where they have elevated access (e.g., using personal email, browsing the internet, office automation tasks, and other recreational uses).

KEY RECOMMENDATIONS

Harden User Endpoints
- Employ multi-factor authentication (MFA) to verify users' identities.
- Restrict employees to use of organizationally approved browsers and enforce automatic software updates.

Start at the Host Level to Protect Operating Systems and Browsers

Protecting against phishing attacks is a team effort that includes everyone from end users (your workforce) to the IT team and the host-based technologies. You can add an important layer of security for operating systems and browsers at the host level by deploying endpoint protections, such as antivirus software, a host-based intrusion detection system (HIDS), and an intrusion prevention system (HIPS).

Ensure your workstation software suite:

- Detects malware based on signatures and behavior;
- Performs checks and runs stack analysis on compiled binaries to ensure file integrity (i.e., ensures binaries have not been maliciously changed);
- Defines rules for executing active content, such as ActiveX controls, add-ins, and Visual Basic for Applications code, so the host can block malicious macros by default through Group Policy Settings or registry keys;
- Detects and quarantines malicious documents, files, and attachments; and
- Enforces "deny all/permit-by-exception rule" on host firewalls.

KEY RECOMMENDATIONS

Add Host Level Protections
- Deploy protections, such as antivirus software, host-based intrusion detection system (HIDS), and host-based intrusion prevention system (HIPS).
- Ensure protections can detect malware based on signatures and behavior; define rules for executing active content; and quarantine malicious documents, files, and attachments.

WHAT DOES MY ORGANIZATION NEED?

Not every organization needs or wants to take every step listed in this guidance. A couple key questions that can help you decide are:

- What are our mission-critical operations?
- How much risk can we tolerate to our mission-critical operations?

Organizations are reminded that CISA offers a Phishing Campaign Assessment service. There are several other free assessments offered that can be found at the CISA Cyber Resource Hub—cisa.gov/cyber-resource-hub. Contact Central@cisa.dhs.gov or visit cisa.gov/cybersecurity for additional help with identifying your organization's risk and for other support resources.