TLP:CLEAR

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

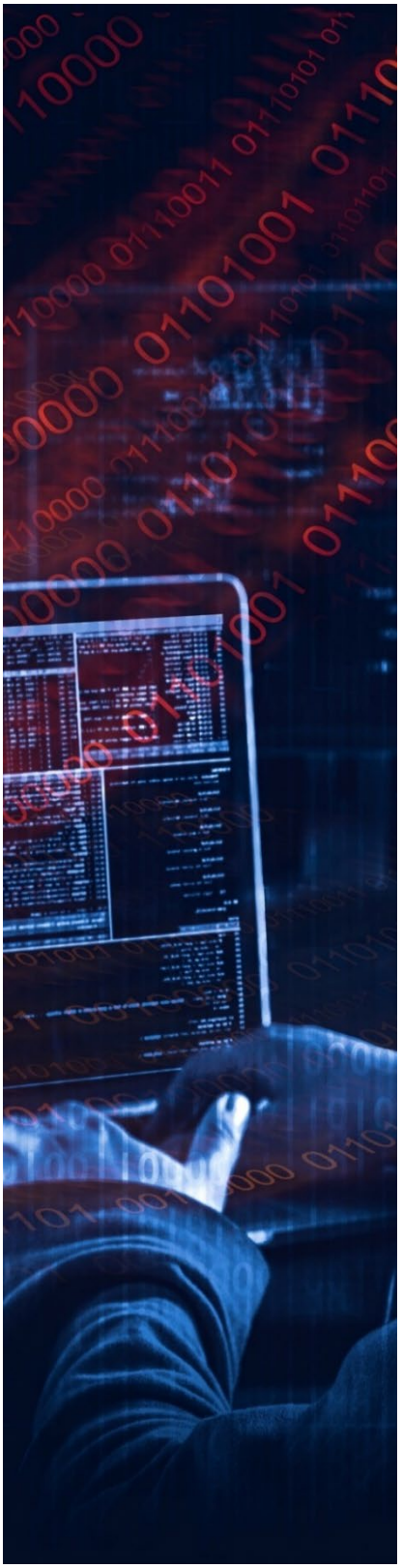
PHISHING GUIDANCE:

STOPPING THE ATTACK CYCLE AT PHASE ONE

Publication: October 2023

TABLE OF CONTENTS

OVERVIEW....3
PHISHING TO OBTAIN LOGIN CREDENTIALS....4
MALWARE-BASED PHISHING....5
MITIGATIONS....5
INCIDENT RESPONSE....11
REPORTING....12
CISA SERVICES....12
RESOURCES....13
ACKNOWLEDGEMENTS....14
DISCLAIMER....14
REFERENCES....14



OVERVIEW

Social engineering is the attempt to trick someone into revealing information (e.g., a password) or taking an action that can be used to compromise systems or networks. Phishing is a form of social engineering where malicious actors lure victims (typically via email) to visit a malicious site or deceive them into providing login credentials. Malicious actors primarily leverage phishing for:

- **Obtaining login credentials.** Malicious actors conduct phishing campaigns to steal login credentials for initial network access.
- **Malware deployment.** Malicious actors commonly conduct phishing campaigns to deploy malware for follow-on activity, such as interrupting or damaging systems, escalating user privileges, and maintaining persistence on compromised systems.

The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), and Multi-State Information Sharing and Analysis Center (MS-ISAC) are releasing this joint guide to outline phishing techniques malicious actors commonly use and to provide guidance for both network defenders and software manufacturers. This will help to reduce the impact of phishing attacks in obtaining credentials and deploying malware.

The guidance for network defenders is applicable to all organizations but may not be feasible for organizations with limited resources. Therefore, this guide includes a section of tailored recommendations for small- and medium-sized businesses that may not have the resources to hire IT staff dedicated to a constant defense against phishing threats.

The guidance for software manufacturers focuses on secure-by-design and -default tactics and techniques. Manufacturers should develop and supply software that is secure against the most prevalent phishing threats, thereby increasing the cybersecurity posture of their customers.

PHISHING TO OBTAIN LOGIN CREDENTIALS

DEFINITION

In phishing attacks used to obtain login credentials, Malicious actors pose as trustworthy sources (e.g., colleagues, acquaintances, or organizations) to lure victims into providing their login credentials. Malicious actors can use the compromised credentials (e.g., usernames and passwords) to gain access to enterprise networks or protected resources, such as email accounts.

EXAMPLE TECHNIQUES

To obtain login credentials, malicious actors commonly:

- Impersonate supervisors, trusted colleagues, or IT personnel to send targeted emails to deceive employees into providing their login credentials.
- Use smartphones or tablets, along with short message system (SMS), to send text messages or chats in platforms such as Slack, Teams, Signal, WhatsApp, or Facebook Messenger to lure users into divulging their login credentials.
    - **Note:** Organizations operating in hybrid environments have fewer face-to-face interactions and frequent virtual exchanges; thus, users in these environments are more likely to be deceived by social engineering techniques tailored towards platforms they frequently use.
- Use voice over internet protocol (VoIP) to easily spoof caller identification (ID) which takes advantage of public trust in the security of phone services, especially landline phones.

Multi-factor authentication (MFA) can reduce the ability of malicious actors using compromised credentials for initial access. Despite this, if weak forms of MFA are enabled, malicious actors can still obtain access through phishing and other techniques. Instances of weak MFA implementation include the following:

- **Accounts using MFA without Fast Identity Online (FIDO) MFA or Public Key Infrastructure (PKI)-based MFA enabled**. These forms of MFA- are susceptible to malicious actors using compromised legitimate credentials to authenticate as the user in legitimate login portals.
- **Push-notification MFA without number matching**. Malicious actors can send a multitude of approve or deny "push requests" until a user either accepts the request, often by accident or in frustration. Thus, malicious actors may authenticate with the compromised user's credentials, if they do not have number matching enabled
- **SMS or voice MFA**. Malicious actors can convince cellular carrier representatives to transfer control of a user's phone number to receive any SMS or call-based MFA codes. Malicious actors may also deceive users by sending an email containing a link to a malicious website that mimics a company's legitimate login portal. The user submits their username, password, and the 6-digit code MFA, which the actors then receive to authenticate as the user in the legitimate login portal.

Note: For more information on weak MFA implementations, see CISA's Fact Sheets Implementing Phishing Resistant MFA and Implementing Number Matching in MFA Applications.

MALWARE-BASED PHISHING

DEFINITION

In malware-based phishing attacks, Malicious actors pose as trustworthy sources (e.g., colleagues, acquaintances, or organizations) to lure a victim into interacting with a malicious hyperlink or opening an email attachment to execute malware on host systems.

EXAMPLE TECHNIQUES

To execute malware on host systems, malicious actors commonly:

- Send malicious hyperlinks or attachments that cause a user to download malware, facilitating initial access, information stealing, damage or disruption to systems or services, and/or the escalation of account privileges.
    - Malicious actors may use free, publicly available tools (such as GoPhish or Zphisher) to facilitate spearphishing campaigns where individual users are targeted with specific and convincing lures.
    - Malicious actors may send malicious attachments with macro scripts or messages with seemingly benign or obfuscated links that download malicious executables.
- Use smartphone or tablet apps, along with SMS, to send text messages or chats in collaboration platforms (i.e., Slack, Teams, Signal, WhatsApp, iMessage, and Facebook Messenger) to lure users into interacting with a malicious hyperlink or attachment that executes malware.

  Note: It can be difficult for a user to detect malicious uniform resource locators (URLs) on these small platforms, as they use constrained user interfaces (UI).

MITIGATIONS

ALL ORGANIZATIONS

The mitigations below align with Cross-Sector Cybersecurity Performance Goals (CPGs) developed for organizations by CISA and the National Institute of Standards and Technology (NIST) to help mitigate the most prevalent cyber threats to organizational networks. Visit CISA's Cross-Sector Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline protections.

PROTECTING LOGIN CREDENTIALS

CISA, NSA, FBI, and MS-ISAC recommend organizations implement the following to reduce the likelihood of successful login credential phishing.

- **Implement user training on social engineering and phishing attacks [CPG 2.I].** Regularly educate users on identifying suspicious emails and links, not interacting with those suspicious items, and the importance of reporting instances of opening suspicious emails, links, attachments, or other potential lures.
- **Enable Domain-based Message Authentication, Reporting, and Conformance (DMARC)** for received emails.
    - DMARC, along with Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM), verify the sending server of received emails by checking published rules. If an email fails the check, it is deemed a spoofed email address, and the mail system will quarantine and report it as malicious.
    - Multiple recipients can be defined for the receipt of DMARC reports.
    - These tools reject any incoming email that has a domain that is being spoofed when a DMARC policy of reject is enabled.
- **Ensure DMARC is set to "reject" for sent emails [CPG 2.M].** This provides robust protection against other users receiving emails that impersonate a domain.
    - Spoofed emails are rejected at the mail server prior to delivery.
    - DMARC reports provide a mechanism for notifying the owner of a spoofed domain including the source of an apparent forger (information they would not receive otherwise.)
    - Enable DMARC policies to lower the chance of cyber threat actors crafting emails that appear to come from your organization's domain(s).
    - See CISA Insights Enhance Email and Web Security and the Center for Internet Security's (CIS's) page on DMARC, as well as Microsoft's Anti-Spoofing guidance for more information.[1]
- **Implement internal mail and messaging monitoring.** Monitoring internal mail and messaging traffic to identify suspicious activity is essential as users may be phished from outside the targeted network or without the knowledge of the organizational security team. Establish a baseline of normal network traffic and scrutinize any deviations.
- **Implement free security tools**, such as OpenDNS Home, to prevent cyber threat actors from redirecting users to malicious websites to steal their credentials. For more information see, CISA's Free Cybersecurity Services and Tools webpage.
- Harden credentials by:
    - **Implementing FIDO or PKI-based MFA [CPG 2.H].** These forms of MFA are phishing resistant and resilient against the threats listed in previous sections. If an organization that uses mobile push-notification based MFA is unable to implement phishing-resistant MFA, use number matching to mitigate MFA fatigue. For further information, see CISA's

fact sheets for Implementing Phishing Resistant MFA and Implementing Number Matching in MFA Applications.

  - **Note:** Deploying PKI-based MFA requires highly mature identity access and management programs and is not widely supported by commonly used services.
  - **Prioritizing phishing-resistant MFA for administrator and privileged user accounts**, such as those with access to e-discovery tools or broad access to customer or financial data.
  - **Implementing centralized logins around a Single Sign On (SSO) program**. SSO is a user lifecycle management mechanism that—among other benefits—can reduce the chance of users being socially engineered to give up their login credentials, especially when paired with MFA or phishing-resistant MFA. SSO provides IT professionals an audit trail to examine, either proactively or retroactively, after a suspected or confirmed security breach.

- **Review MFA lockout and alert settings and track denied (or attempted) MFA logins** [CPG 2.G].
  - Perform an account lockout when unusual activity or ongoing malicious login attempts are occurring to prevent malicious actors from bypassing MFA.
  - Minimize unnecessary disruptions. This includes prioritizing the health of organizational and consumer data, rather than the short-term productivity of a single employee. A significant network security incident would not only impact production by many employees, but also resource availability and potentially customer or partner data.
  - Identify and remediate successful phishing attempts.
  - Promptly report phishing incidents (see the Reporting section).
  - Develop a documented incident response plan. For further information, see CISA's fact sheet on Incident Response Plan Basics.

PREVENTING MALWARE EXECUTION

CISA, NSA, FBI, and MS-ISAC recommend organizations implement the following to reduce the likelihood of successful malware execution following phishing attacks.

- **Incorporate denylists at the email gateway and enable firewall rules** to prevent successful malware deployment.
- **Use denylists to block known malicious domains, URLs, and IP addresses** as well as file extensions such as .scr, .exe, .pif, and .cpl and mislabeled file extensions (e.g., a .exe file that is labeled as a .doc file.)
  - **State local tribal and territory (SLTT)** entities should enable malicious domain blocking and reporting (MDBR), which is a cloud-based solution with recursive domain name system (DNS) technology that works to prevent users from connecting to malicious

domains. For more information, visit CIS's webpage on Malicious Domain Blocking and Reporting (MDBR).

- For more information on protective phishing filters, refer to Microsoft, MacOS, or Google's guidance on phishing and malware protection.[2],[3],[4],[5] CISA, NSA, FBI, and MS-ISAC recommend reaching out to vendors or service providers to learn about what phishing filters and malware protections are available.

- **Restrict MacOS and Windows users from having administrative rights** [CPG 2.E].
- **Implement the principle of least privilege (PoLP) when administering user accounts**, and only allow designated administrator accounts to be used for administrative purposes.
- **Implement application allowlists** [CPG 2.Q], which are security controls that enumerate application components authorized to be present within a network based on a defined baseline. For more information, see NIST's Application Allowlisting.
- **Block macros by default** [CPG 2.N].
- **Implement remote browser isolation (RBI) solutions** that prevent malware propagation through quarantining the malware sample upon user execution. RBI solutions run applications that quarantine malware when a user interacts with a malicious link or binary to prevent further spread into the environment. Configure RBI solutions in remote workstations so that any malware is contained within an isolation boundary and cannot access an organization's resources.
- **Implement free security tools like Quad9 or Google Safe Browsing** to identify and stop malware upon user execution. For more information see, CISA's Free Cybersecurity Services and Tools webpage.
- **Set up a self-serve app store** where customers can install approved apps and block apps and executables from other sources.
- **Implement a free protective DNS resolver** to prevent malicious actors from redirecting users to malicious websites to steal their credentials. Several services provide free security tools ranging from personal to professional use cases, such as OpenDNS Home or Cloudflare Zero Trust Services. For more information see, CISA's Free Cybersecurity Services and Tools webpage. Federal organizations should see CISA's fact sheet Protective Domain Name System (DNS) Resolver Service for information.

SMALL- AND MEDIUM-SIZED BUSINESSES (SMBs) OR ORGANIZATIONS

CISA, NSA, FBI, and MS-ISAC recommend that small- and medium-sized organizations with limited resources prioritize the following best practices to protect network resources from prevalent phishing threats:

- **User phishing awareness training:** Implement a standard anti-phishing training program and require employees to review phishing training material annually. Additionally, conclude the

program evolution with a training check that certifies that the employee has retained all the information outlined in the training program.

  - Small businesses are encouraged to implement commercial phishing awareness training programs to employees. Additionally, NIST offers free anti-phishing training resources for small businesses on their Small Business Cybersecurity Corner: Phishing webpage.
  - The Department of Justice (DOJ) offers Anti-Phishing Training Program Support to federal organizations.
  - The Federal Trade Commission (FTC) offers guidance to protect small businesses from phishing threats on their Cybersecurity for Small Businesses: Phishing webpage.

- **Identify network phishing vulnerabilities**: Federal organizations are encouraged to participate in CISA's Phishing Vulnerability Scanning assessment service.
- **Enable MFA**: Activating a strong MFA is the best way that small businesses can protect their internet facing business accounts from phishing related threats.
  - Learn more about why MFA is important for small business to enable by visiting CISA's More than a Password MFA webpage. The webpage includes an MFA hierarchy, which helps users identify the strongest form of MFA, and ensures users can select the best form of MFA based on their operational needs.

Additionally, CISA, NSA, FBI, and MS-ISAC recommend SMBs implement the technical solutions below to prevent phishing related compromises:

- **Implement strong password policies** to authenticate users. These passwords must adhere to a password strength policy which requires minimum character length, numbers, special characters, and case sensitivity, along with prohibiting users from recycling previously used passwords.
- **Implement DNS filtering or firewall denylists** to block known malicious sites.
- **Implement anti-virus solutions** to mitigate malware and to stop malware from executing if a malicious hyperlink or attachment from an email is opened.
- **Implement file restriction policies** that prevent malicious high risk file extensions e.g., .exe or .scr from being downloaded and executed. These types of files are unnecessary for daily operations and should be heavily restricted on standard business accounts.
- **Ensure that software applications are set to automatically update** so that network software is always upgraded to the latest version. This helps to prevent malicious actors from exploiting vulnerabilities within an organization's network software.
- **Enable safe web browsing policies** so that employees can only access websites that are needed for daily business operations. These policies also prevent users from visiting malicious websites that often contain malware that can either harvest user credentials or deploy additional malware to damage organizational systems.

- **Implement a secure virtual private network (VPN)** with MFA enabled.
- **Reference the Federal Communications Commission's (FCC)** Cybersecurity Planning Guide. The guide includes information on ways small businesses can improve their overall cybersecurity posture.
- **Consider migrating to managed cloud-based email services from reputable third-party vendors.** CISA, NSA, and MS-ISAC encourage small businesses with limited resources to seek managed cloud email services from trusted third-party vendors.
    - Migrating from on-premises mail systems to trusted third-party cloud-based mail providers is beneficial for customers because providers regularly patch and update their systems. Providers also commonly perform robust email traffic monitoring and anti-phishing malware services.
    - For more information on cloud services, see CISA's Secure Cloud Business Applications (SCuBA) project. Although tailored to federal organizations, the SCuBA project provides guidance and capabilities applicable to all organizations with cloud business application environments.

SOFTWARE MANUFACTURERS

CISA, NSA, FBI, and MS-ISAC recommend software manufacturers incorporate secure-by-design and -default principles and tactics into their software development practices, reducing the susceptibility of their customers to phishing attacks. For more information on secure by design, see CISA's secure by design webpage and joint guide Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default.

To mitigate the success of phishing emails reaching users and users interacting with the email, the authoring organizations recommend the following:

- **Perform field testing of email software.** Implement threat modeling to test the email software against various deployment scenarios while considering use-cases for organizations ranging from small to large and configure the software with secure defaults based on the test findings.
- **Provide email software with DMARC enabled for received emails by default.**
- **Provide email software with DMARC configured to "reject" for sent emails by default.**
- **Provide email products with internal mail and messaging monitoring mechanisms enabled by default.** Email software manufacturers are encouraged to include automatic email traffic monitoring mechanisms by default that automatically scan email traffic for the presence of malicious attachments or URLs within email messages.
- **Mandate MFA for privileged users.** Frequently, malicious actors focus their infiltration techniques on administrator accounts. Administrator accounts have elevated privileges and should be protected by strong MFA by default.

  - Make MFA an opt-out feature rather than opt-in; have the system regularly prompt the administrator to enroll in MFA until they have successfully enabled it on their account.

- **Implement SSO for applications via modern open standards.** Examples include Security Assertion Markup Language (SAML) or OpenID Connect (OIDC.) Make this capability available by default at no additional cost.
- **Consider implementing security notifications for the customer when non-secure configurations are used** in email software products. For example, if administrators are not enrolled in MFA, send repeated security notifications warning the organization of the present security risks so that they know to mitigate the risk.

To mitigate successful malware execution following phishing attacks:

- **Ensure phishing filtering and blocking mechanisms are packaged with email software by default** to prevent successful malware deployment.
- **Provide email software with limited administrative rights by default.** Only allow designated administrator accounts to be used for administrative purposes.
- **Provide email software with application allowlists by default.**
- **Provide a self-serve application store where customers can install approved applications.** Block applications and executables from external, unapproved sources that are not permitted via organizational policy.
- **Include mechanisms that block macros by default** with email products.
- **Include RBI solutions by default.**

INCIDENT RESPONSE

If an organization identifies compromised credentials and/or successful malware from phishing activity, remediate the activity by:

1. **Re-provisioning suspected or confirmed compromised user accounts** to prevent malicious actors from maintaining continued access to the environment.
2. **Auditing account access following a confirmed phishing incident** to ensure malicious actors no longer have access to the initially impacted account.
3. **Isolating the affected workstation after the detection of a phishing attack.** This helps stop the executed malware from spreading further into the organization's network.
4. **Analyzing the malware.** After isolating the affected workstation(s), have the malware analyzed by a team that specializes in malware analysis.

   Note: This step may require outsourcing to expert third-party consultants. After analysis, specialists will know how to safely handle the malware. Learn more by visiting CISA's malware analysis services and resources webpage.

5. **Eradicating the malware.** Eradicate the malware from the network so other workstations within the organization's networks can no longer be negatively impacted by the executed malware.
6. **Restore systems to normal operations and confirm they are functioning properly.** The main challenges at this phase are confirming that remediation has been successful, rebuilding systems, reconnecting networks, as well as correcting misconfigurations.

For more guidance on how to respond to malicious cyber incidents, see CISA's incident response playbook and Federal Government Cybersecurity Incident and Vulnerability Response Playbook. Although tailored to federal organizations, these playbooks provide operational procedures for planning and conducting cybersecurity incident and vulnerability response activities and detail steps for both incident and vulnerability response.

REPORTING

Organizations are encouraged to use reporting features that are built into Microsoft Outlook and other cloud email platforms, as well as report spam directly to Microsoft, Apple, and Google, as applicable. Reporting suspicious phishing activity is one of the most efficient methods for protecting organizations as it helps email service providers identify new or trending phishing attacks.

- CISA urges organizations to promptly report phishing incidents to CISA at report@cisa.gov or call the 24/7 response line at (888) 282-0870.
- To report spoofing or phishing attempts (or to report that you've been a victim), file a complaint with the FBI's Internet Crime Complaint Center (IC3), or contact your local FBI Field Office to report an incident.
- State, local, tribal, and territorial (SLTT) government entities can report to the Multi-State Information Sharing and Analysis Center (MS-ISAC) by emailing SOC@cisecurity.org or calling (866) 787-4722.

CISA SERVICES

- Cyber Hygiene
- Malware Analysis
- Phishing Vulnerability Scanning
- Free Cybersecurity Services and Tools

MS-ISAC/CIS Services

- MS-ISAC Membership and Benefits
- CIS Critical Security Controls
- Malicious Domain Blocking and Reporting

- Albert Network Monitoring and Management
- CIS Endpoint Security Services

RESOURCES

CISA

- Cross-Sector Cybersecurity Performance Goals
- Secure by Design | CISA
- More than a Password | CISA
- Counter-Phishing Recommendations for Federal Agencies
- Zero Trust Maturity Model
- Incident Response Playbook
- Enhance Email and Web Security
- Reducing Spam
- Cyber Smart Phishing Guidance
- Phishing Security Postcard
- Phishing Infographic
- Anti-Phishing Training Program Support | CISA

NSA

- Stop the Snowball: Protect Yourself from Phishing Scams

FBI

- Spoofing and Phishing

CENTER FOR INTERNET SECURITY

- How DMARC Advances Email Security
- A Short Guide for Spotting Phishing Attempts
- CIS Blueprint of a Phishing Attack

NIST

- Application allowlisting - Glossary | CSRC (nist.gov)
- Small Business Cybersecurity Corner: Phishing

FCC

- Cybersecurity Planning Guide

FTC

- Protecting Small Businesses: Phishing

ACKNOWLEDGEMENTS

Spamhaus contributed to this guidance.

DISCLAIMER

The information in this report is being provided "as is" for informational purposes only. CISA, NSA, FBI, and MS-ISAC do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA, NSA, FBI, or MS-ISAC.

REFERENCES

[1] Microsoft: Anti-spoofing protection in EOP
[2] Microsoft: Anti-phishing protection in Microsoft 365
[3] Microsoft: Exchange Online Protection Overview
[4] Google: Advanced Phishing and Malware Protection
[5] Apple: Protect Your Mac from Malware