PHISHING

Phishing is a form of social engineering in which a cyber threat actor poses as a trustworthy colleague, acquaintance, or organization to lure a victim into providing sensitive information or network access. The lures can come in the form of an email, text message, or even a phone call. If successful, this technique could enable threat actors to gain initial access to a network and affect the targeted organization and related third parties. The result can be a data breach, data or service loss, identity fraud, malware infection, or ransomware.

Phishing susceptibility is the likelihood of an individual becoming a victim of a phishing attempt. High susceptibility increases the likelihood that cyber threat actors can exploit their target.

Don't be a victim! You can prevent phishing success and limit its negative impacts, should initial access occur. Here's how this adversarial technique works:

Analysis and findings presented in this infographic are derived from phishing-related data collected during CISA Assessments. CISA conducts cybersecurity assessments for federal and critical infrastructure partners to reduce their vulnerability exposure and risk of compromise. To learn more about CISA services, contact **central@cisa.dhs.gov.** For additional information on steps to reduce your phishing susceptibility and cybersecurity risk, see **CISA's Cross-Sector Cybersecurity Performance Goals (CPG).**

This infographic was created by the U.S. Cybersecurity & Infrastructure Security Agency (www.cisa.gov) and provided to you by Integrated Technology Services, LLC (www.techlawyergy.com) and the Law Offices of Daniel J. Siegel, LLC (www.danieljsiegel.com).

1 SELECT THE BAIT

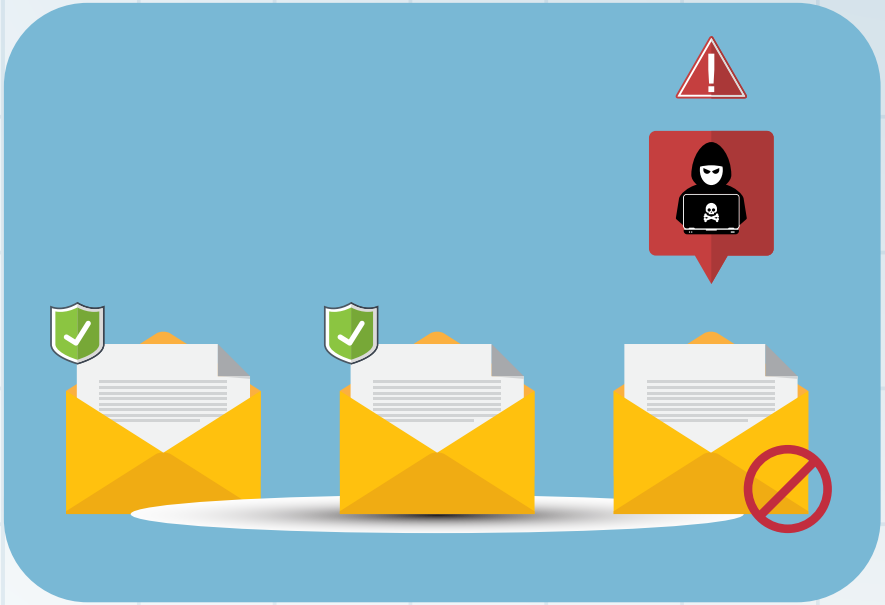
Threat actors pose as colleagues, acquaintances, or reputable organizations and solicit sensitive information or lure victims into downloading and executing malware. Bait typically consist of an email with a subject line that entices the user into opening the email, e.g., the subject line contains an alert, an action, or request for information. CISA Phishing Campaign Assessments revealed these most successful subject lines:

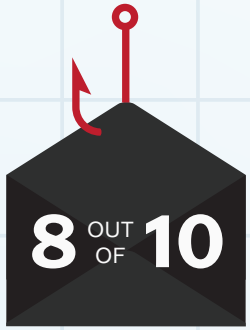
- Financial security alerts and updates
- Organization-wide announcements and updates
- User-specific alerts, such as training updates

This infographic was created by the U.S. Cybersecurity & Infrastructure Security Agency (www.cisa.gov) and provided to you by Integrated Technology Services, LLC (www.techlawyergy.com) and the Law Offices of Daniel J. Siegel, LLC (www.danieljsiegel.com).

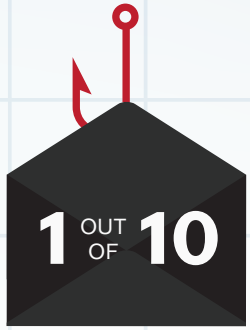
2 SET THE HOOK

A single bite can lead to successful exploitation. Threat actors set multiple hooks to increase their chance of success and then wait for a victim to take the bait.





organizations had at least one individual who fell victim to a phishing attempt by CISA Assessment teams.



phishing emails sent by CISA Assessors had a user execute a malicious attachment or interact with a malicious link.

This infographic was created by the U.S. Cybersecurity & Infrastructure Security Agency (www.cisa.gov) and provided to you by Integrated Technology Services, LLC (www.techlawyergy.com) and the Law Offices of Daniel J. Siegel, LLC (www.danieljsiegel.com).

3 REEL IN THE CATCH OF THE DAY

The threat actor reels in the catch of the day when an email is not blocked by network border or endpoint protections and reaches a victim who replies with valuable information or executes a spoofed link or attachment. The threat actor can then feast on sensitive information, credentials, or the ability to compromise the endpoint via malware disguised as links and attachments.

70% **of all attached files or links containing malware were not blocked by network border protection services.**

15% **of all malicious attachments or links were not blocked by endpoint protections**, which are set up to reduce the amount of unwanted or malicious activity.

84% Within the first 10 minutes of receiving a malicious email, **84% of employees took the bait** by either replying with sensitive information or interacting with a spoofed link or attachment.

13% of targeted employees **reported the phishing attempts.** Employee failure to report phishing attempts limits the organization's ability respond to the intrusion and alert others to the threat.

This infographic was created by the U.S. Cybersecurity & Infrastructure Security Agency (www.cisa.gov) and provided to you by Integrated Technology Services, LLC (www.techlawyergy.com) and the Law Offices of Daniel J. Siegel, LLC (www.danieljsiegel.com).

4 ACTIONS TO HELP PREVENT BEING HOOKED IN A PHISHING ATTACK

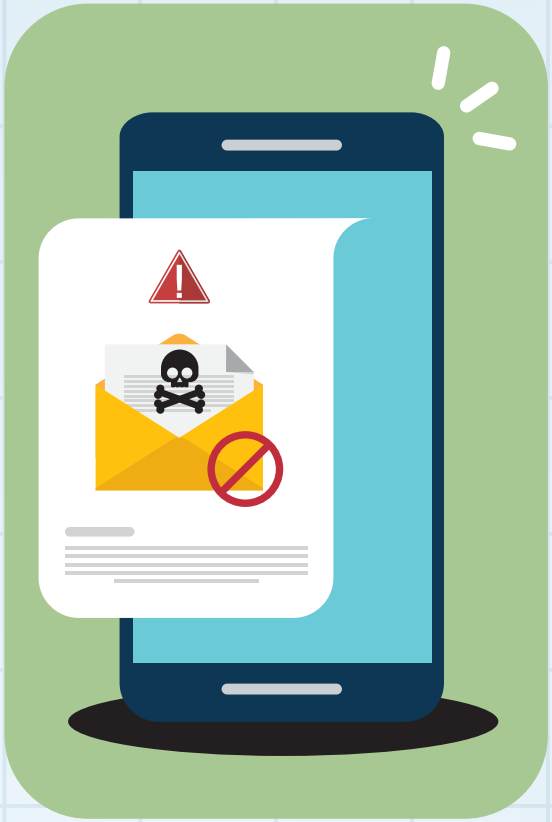
Phishing is a form of social engineering in which a cyber threat actor poses as a trustworthy colleague, acquaintance, or organization to lure a victim into providing sensitive information or network access. The lures can come in the form of an email, text message, or even a phone call. If successful, this technique could enable threat actors to gain initial access to a network and affect the targeted organization and related third parties. The result can be a data breach, data or service loss, identity fraud, malware infection, or ransomware.

Phishing susceptibility is the likelihood of an individual becoming a victim of a phishing attempt. High susceptibility increases the likelihood that cyber threat actors can exploit their target.

Analysis and findings presented in this infographic are derived from phishing-related data collected during CISA Assessments. CISA conducts cybersecurity assessments for federal and critical infrastructure partners to reduce their vulnerability exposure and risk of compromise. To learn more about CISA services, contact **central@cisa.dhs.gov.** For additional information on steps to reduce your phishing susceptibility and cybersecurity risk, see **CISA's Cross-Sector Cybersecurity Performance Goals (CPG).**

This infographic was created by the U.S. Cybersecurity & Infrastructure Security Agency (www.cisa.gov) and provided to you by Integrated Technology Services, LLC (www.techlawyergy.com) and the Law Offices of Daniel J. Siegel, LLC (www.danieljsiegel.com).

1 BLOCK THE BAIT



Implement strong network border protections — as an initial barrier to reduce the opportunity for a successful phishing attempt to further its damage.

Configure email servers to **utilize protocols designed to verify the legitimacy of email communications**, like Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-Based Message Authentication, Reporting, and Conformance (DMARC) [CPG 8.3].

Incorporate **denylists** or **cyber threat intelligence feeds** into **firewall rules** to block known malicious domains, URLs, and IP addresses.

This infographic was created by the U.S. Cybersecurity & Infrastructure Security Agency (www.cisa.gov) and provided to you by Integrated Technology Services, LLC (www.techlawyergy.com) and the Law Offices of Daniel J. Siegel, LLC (www.danieljsiegel.com).

2 DON'T TAKE THE BAIT

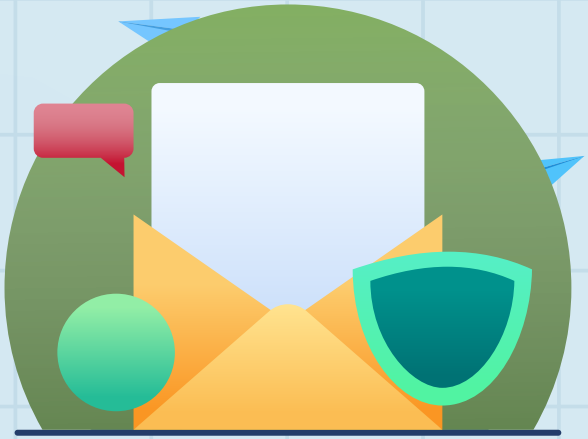
Educate employees to recognize common indicators of phishing, such as suspicious sender email addresses, generic greetings, spoofed hyperlinks, spelling or layout errors, and suspicious attachments [CPG 4.3].

Teach employees to keep their guard up on all communications platforms, including **social media**, and flag suspicious correspondence for security review [CPG 4.3].

This infographic was created by the U.S. Cybersecurity & Infrastructure Security Agency (www.cisa.gov) and provided to you by Integrated Technology Services, LLC (www.techlawyergy.com) and the Law Offices of Daniel J. Siegel, LLC (www.danieljsiegel.com).

4 PROTECT THE WATERS

After **obtaining initial access** via a successful phishing attempt, threat actors will often try to take control of its victim's account or devices to **move laterally** within the organization's network. To protect the network:



- **Enforce phishing-resistant multifactor authentication** to secure resources and protect from lateral movement [CPG 1.3].
- **Review and reduce the number of accounts with access to critical data and devices** [CPG 1.7].
- **Restrict administrative password sharing and re-use and remove non-essential elevated privileges** from users to reduce opportunities for privilege escalation [CPG 1.5, 1.6].
- **Add protection at the endpoint as the last line of defense** between the user and a threat actor's attack.

- Automate mandatory **security updates** for browsers, applications, software, and antivirus on all internet-accessible end user devices [CPG 5.1].
- Implement **software restriction policies** to allow only software necessary for business purposes on end user devices [CPG 2.1, 2.2].
- Implement an **endpoint detection and response** (EDR) solution to further monitor for and block malicious activity on end user devices.

Continually assess and evaluate defense mechanisms by enrolling in no-cost CISA services, such as Phishing Campaign Assessments, to reduce risk [CPG 5.6].

This infographic was created by the U.S. Cybersecurity & Infrastructure Security Agency (www.cisa.gov) and provided to you by Integrated Technology Services, LLC (www.techlawyergy.com) and the Law Offices of Daniel J. Siegel, LLC (www.danieljsiegel.com).