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 lure 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:

### 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 consists 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:

1. **Financial security alerts and updates**
2. **Organization-wide announcements and updates**
3. **User-specific alerts, such as training updates**

### 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.

### REEL IN THE CATCH OF THE DAY
The threat actor reels in the catch of the day when an employee 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 feed 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%** of targeted employees reported the phishing attempts. Employee failure to report phishing attempts limits the organization’s ability to respond to the intrusion and alert others to the threat.

Within the first 10 minutes of receiving a malicious email, **85%** of employees took the bait by either replying with sensitive information or interacting with a spoofed link or attachment.

**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 evaluate their status and readiness and, in turn, provide recommendations and guidance. 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 (CPGs).
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 theft, 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).

### ACTIONS TO HELP PREVENT BEING HOOKED IN A PHISHING ATTACK

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.

2. **DON’T TAKE THE BAIT**
   - Educate employees to recognize common indicators of phishing, such as sensationalized language, spelling or layout errors, and suspicious attachments [CPG 4.3].
   - Teach employees to keep their guard up on all communication platforms, including social media, and flag suspicious correspondence for security review [CPG 4.3].

3. **REPORT THE HOOK!**
   - Educate employees on what to do when they receive a phishing email or a phishing-related incident, such as a reported data leak or a change in a user’s account status [CPG 4.3].
   - Report the email to the appropriate security teams.
   - Do not forward the malicious email to others within the organization.

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 device to move laterally within the organization’s network to protect the network.
   - Implement an endpoint detection and response (EDR) solution to further monitor for and block malicious activity on end user devices.