Playbook: Phishing

Investigate, remediate (contain, eradicate), and communicate in parallel!

Assign steps to individuals or teams to work concurrently, when possible; this playbook is not purely sequential. Use your best judgment.

Investigate

`TODO: Expand investigation steps, including key questions and strategies, for phishing.`

1. **Scope the attack** Usually you will be notified that a potential phishing attack is underway, either by a user, customer, or partner.
    - Determine **total number of impacted users**
    - Understand **user actions** in response to the phishing email (*e.g.*, did they download the attachment, visit the spoofed site, or give out any personal or business information such as credentials)
    - Find the potentially related activity. Check:
        - social media
        - any possibly suspicious emails
        - emails with links to external and unknown URLs
        - non-returnable or non-deliverable emails
        - any kind of notification of suspicious activity
2. **Analyze the message** using a safe device (i.e., **do not** open messages on a device with access to sensitive data or credentials as the message may contain malware), determine: `TODO: Specify tools and procedure`
    - who received the message
    - who was targeted by the message (may be different than "successful" recipients)
    - email address of the sender
    - subject line
    - message body
    - attachments (**do not open attachments** except according to established procedures)
    - links, domains, and hostnames (**do not follow links** except according to established procedures)
    - email metadata including message headers (see below)
        - sender information from the 'from' field and the X-authenticated user header
        - all client and mail server IP addresses
    - note "quirks" or suspicious features
3. **Analyze links and attachments** `TODO: Specify tools and procedure`
    - use passive collection such as nslookup and whois to find IP addresses and registration information
    - find related domains using OSINT (*e.g.*, reverse whois (https://www.whoxy.com/reverse-whois/)) on email addresses and other registration data
    - submit links, attachments, and/or hashes to VirusTotal (https://www.virustotal.com/gui/)
    - submit links, attachments, and/or hashes to a malware sandbox such as Cuckoo (https://cuckoosandbox.org/), Hybrid Analysis (https://www.hybrid-analysis.com/), Joe Sandbox (https://www.joesecurity.org/), or VMray (https://www.vmray.com/).

4. Categorize the type of attack. `TODO: Customize categories and create additional playbooks for common or high-impact phishing types`
5. **Determine the severity.** Consider:
    - whether public or personal safety is at risk
    - whether personal data (or other sensitive data) is at risk
    - any evidence of who is behind the attack
    - number of affected assets
    - preliminary business impact
    - whether services are affected
    - whether you are able to control/record critical systems

`TODO: Expand investigation steps, including key questions and strategies, for phishing.`

Remediate

- **Plan remediation events** where these steps are launched together (or in coordinated fashion), with appropriate teams ready to respond to any disruption.
- **Consider the timing and tradeoffs** of remediation actions: your response has consequences.

Contain

`TODO: Customize containment steps, tactical and strategic, for phishing.`

`TODO: Specify tools and procedures for each step, below.`

- Contain affected accounts
    - change login credentials
    - reduce access to critical services, systems, or data until investigation is complete
    - reenforce multi-factor authentication (MFA)
- Block activity based on discovered indicators of compromise, *e.g.*:
    - block malicious domains using DNS, firewalls, or proxies
    - block messages with similar senders, message bodies, subjects, links, attachments, *etc.*, using email gateway or service.
- Implement forensic hold or retain forensic copies of messages
- Purge related messages from other user inboxes, or otherwise make inaccessible
- Contain broader compromise in accordance with general IR plan
- Consider mobile device containment measures such as wiping via mobile device management (MDM). Balance against investigative/forensic impact.
- Increase detection "alert level," with enhanced monitoring, particularly from related accounts, domains, or IP addresses.
- Consider outside security assistance to support investigation and remediation
- Confirm relevant software upgrades and anti-malware updates on assets.

Reference: Remediation Resources

`TODO: Specify financial, personnel, and logistical resources to accomplish remediation`

Communicate

TODO: Customize communication steps for phishing

TODO: Specify tools and procedures (including who must be involved) for each step, below, or refer to overall plan

1. Escalate incident and communicate with leadership per procedure
2. Document incident per procedure (and report (https://us-cert.cisa.gov/report-phishing))
3. Communicate with internal and external legal counsel per procedure, including discussions of compliance, risk exposure, liability, law enforcement contact, *etc.*
4. Communicate with users (internal)
    1. Communicate incident response updates per procedure
    2. Communicate impact of incident **and** incident response actions (e.g., containment: "why is the file share down?")
    3. Communicate requirements: "what should users do and not do?"
5. Communicate with customers
    1. Focus particularly on those whose data was affected
    2. Generate required notifications based on applicable regulations (particularly those that may consider phishing a data breach or otherwise requires notifications) TODO: Expand notification requirements and procedures for applicable regulations
6. Contact insurance provider(s)
    1. Discuss what resources they can make available, what tools and vendors they support and will pay for, *etc.*
    2. Comply with reporting and claims requirements to protect eligibility
7. Consider notifying and involving law enforcement (https://www.usa.gov/stop-scams-frauds) TODO: Link the following bullets to actual resources for your organization
    1. Local law enforcement
    2. State or regional law enforcement
    3. Federal or national law enforcement
8. Communicate with security and IT vendors TODO: Link the following bullets to actual resources for your organization
    1. Notify and collaborate with managed providers per procedure
    2. Notify and collaborate with incident response consultants per procedure

Recover

TODO: Customize recovery steps for phishing

TODO: Specify tools and procedures for each step, below

1. Launch business continuity/disaster recovery plan(s) if compromise involved business outages: *e.g.*, consider migration to alternate operating locations, fail-over sites, backup systems.
2. Reinforce training programs regarding suspected phishing attacks. Key suspicious indicators may include:
    - misspellings in the message or subject

    - phony-seeming sender names, including mismatches between display name and email address
    - personal email addresses for official business (e.g., gmail or yahoo emails from business colleagues)
    - subject lines marked "[EXTERNAL]" on emails that look internal
    - malicious or suspicious links (https://www.pcworld.com/article/248963/how-to-tell-if-a-link-is-safe-without-clicking-on-it.html)
    - receiving an email or attachment they were not expecting but from someone they know (contact sender before opening it)
    - reporting suspicious activity to IT or security
3. Ensure that IT and security staff is up to date on recent phishing techniques.
4. Determine if any controls have failed when falling victim to an attack and rectify them. Here is a good source (https://www.proofpoint.com/us/security-awareness/post/14-things-do-after-phishing-attack) to consider following a phishing attack.

Resources

Reference: User Actions for Suspected Phishing Attack

`TODO: Customize steps for users dealing with suspected phishing`

1. Stay calm, take a deep breath.
2. Take pictures of your screen using your smartphone showing the things you noticed: the phishing message, the link if you opened it, the sender information.
3. Take notes about the problem(s) using the voice memo app on your smartphone or pen-and-paper. Every little bit helps! Document the following:
    1. What did you notice?
    2. Why did you think it was a problem?
    3. What were you doing at the time you detected it?
    4. When did it first occur, and how often since?
    5. Where were you when it happened, and on what network? (office/home/shop, wired/wireless, with/without VPN, *etc.*)
    6. What systems are you using? (operating system, hostname, *etc.*)
    7. What account were you using?
    8. What data do you typically access?
    9. Who else have you contacted about this incident, and what did you tell them?
4. Contact the help desk using the phishing hotline or the phishing report toolbar and be as helpful as possible.
5. Be patient: the response may be disruptive, but you are protecting your team and the organization! **Thank you.**

Reference: Help Desk Actions for Suspected Phishing Attack

`TODO: Customize steps for help desk personnel dealing with suspected phishing`

1. Stay calm, take a deep breath.
2. Open a ticket to document the incident, per procedure. `TODO: Customize template with key questions (see below) and follow-on workflow`

3. Ask the user to take pictures of their screen using their smartphone showing the things they noticed: the phishing message, the link if you opened it, the sender information, *etc.* If this is something you noticed directly, do the same yourself.
4. Take notes about the problem(s) using the voice memo app on your smartphone or pen-and-paper. If this is a user report, ask detailed questions, including:
    1. What did you notice?
    2. Why did you think it was a problem?
    3. What were you doing at the time you detected it?
    4. When did it first occur, and how often since?
    5. What networks are involved? (office/home/shop, wired/wireless, with/without VPN, *etc.*)
    6. What systems are involved? (operating system, hostname, *etc.*)
    7. What data is involved? (paths, file types, file shares, databases, software, *etc.*)
    8. What users and accounts are involved? (active directory, SaaS, SSO, service accounts, *etc.*)
    9. What data do the involved users typically access?
    10. Who else have you contacted about this incident, and what did you tell them?
5. Ask follow-up questions as necessary. **You are an incident responder, we are counting on you.**
6. Get detailed contact information from the user (home, office, mobile), if applicable.
7. Record all information in the ticket, including hand-written and voice notes.
8. Quarantine affected users and systems. `TODO: Customize containment steps, automate as much as possible`
9. Contact the security team and stand by to participate in the response as directed: investigation, remediation, communication, and recovery.

Additional Information

1. Anti-Phishing Attack resources (https://resources.infosecinstitute.com/category/enterprise/phishing/phishing-countermeasures/top-16-anti-phishing-resources/#gref)
2. Methods of Identifying a Phishing attack (https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email)
3. Phishing Email Examples (https://www.phishing.org/phishing-examples)
4. Anti-Phishing best practices (https://resources.infosecinstitute.com/category/enterprise/phishing/phishing-countermeasures/anti-phishing-best-practices/#gref)