2025

# DocuPhishing

## DOCUPHISHING EMAILS

OSKAR CARLSSON, ANDREAS KÅRHEIM, SEBASTIAN MÅRTENSSON, NOAH NYMAN

## Table of Content

## Introduction

DocuPhishing is a sort of phishing attack where seemingly legitimate documents (PDFs, MS-Office files, cloud hosted documents, etc) are leveraged by threat actors to trick users into executing malicious content and/or giving out their credentials. Attacks like this often utilise trusted services (such as SharePoint, Dropbox, WeTransfer, etc) and social engineering techniques to avoid technical controls and exploit the trust of the user.

This IR playbook, aligned with NIST SP 800-61 and mapped to the MITRE ATT&CK frameworks, provides a structured approach to the entire incident lifecycle to ensure consistent response actions.

## NIST IR Phases: (short overview)

1. **Preparation**

   This phase involves creating an incident management plan that can detect an incident withing the specific environment. This might involve identifying different kinds of attacks and determining their eventual impact as well as making sure the correct tool sets are available to deal with the incident.

2. **Detection and Analysis**

   This step involves identifying the nature of the attack and its impact, utilising aforementioned tools.

3. **Containment, Eradication and Recovery**

   Main phase. Limiting the damage/taking necessary actions.

   a. **Containment**
      All necessary methods are used to prevent spread of malware/limit impact of current incident. Might include isolating devices and blocking senders.

   b. **Eradication**
      When the attacker has been blocked/devices been isolated from the network, the threat needs to be removed from the environment. Might include purging emails and/or wiping systems.

   c. **Recovery**
      Threat is gone! Restore the systems back to normal/re-enable accounts etc.

4. **Post-Incident Activity**
   Final phase. We have come out the other side – let's review what's gone right and wrong. Can anything be improved in case of future incidents? Any precautionary measures that can be taken?

# MITRE ATT&CK Tactics:

Tactics are used to describe the objective and phases of an attack, all from the attacker's perspective. Mapping incidents to tactics helps defenders in understanding where in the attack lifecycle the threat is operating.

TA0001 Initial Access:

- T1566 Phishing
    - .001 Spearphishing Attachment
    - .002 Spearphishing Link
- T1199 Trusted Relationship
- T1078 Valid Accounts
    - .004 Cloud Accunts

TA0002 Execution:

- T1204 User Execution:
    - .001 Malicious Link
    - .002 Malicious File

TA0006 Credential Access:

- T1187 Forced Authentication
- T1056 Input Capture
    - .003 Web Portal Capture
- T1556 Modify Authentication Process
- T1621 Multi-Factor Authentication Request Generation

TA0011 Command and Control:

- T1071 Application Layer Protocol
    - .001 Web Protocols
- T1001 Data Obfuscation

TA0010 Exfiltration:

- T1567 Exfiltration Over Web Service:
    - .001 Exfiltration to Code Repository
    - .002 Exfiltration to Cloud Storage
    - .003 Exfiltration to Text Storage Sites
    - .004 Exfiltration Over Webhook

# MITRE ATT&CK Techniques:

Techniques are used to describe the specific methods as well as behaviours used by attackers to achieve each tactic. This helps in understanding how an attack was carried out.

- T1531 Account Access Removal
- T1087 Account Discovery
  - .003 Email Account
  - .004 Cloud Account
- T1098 Account Manipulation
  - .001 Additional Cloud Credentials
  - .002 Additional Email Delegate Permissions
  - .003 Additional Cloud Roles
  - .005 Device Registration
  - .007 Additional Local or Domain Groups
- T1010 Application Window Discovery
- T1119 Automated Collection
- T1020 Automated Exfiltration
- T1059 Command and Scripting Interpreter
  - .001 Powershell
  - .006 Python
  - .007 Javascript
  - .009 Cloud API
- T1586 Compromise Accounts
  - .001 Social Media Accounts
  - .002 Email Accounts
  - .003 Cloud Accounts
- T1114 Email Collection
  - .001 Local Email Collection
  - .002 Remote Email Collection
  - .003 Email Forwarding Rule
- T1672 Email Spoofing
- T1036 Masquerading
- T1027 Obfuscated Files or Information
- T1556 Modify Authentication Process

IR Plan (Aligned with NIST SP 800-61 Rev. 2)

## 1. Preparation

- Develop IR Plan (3.1.1 Preparing to Handle Incidents)
- Implement Analysis Hardware and Software (3.1.1 Preparing to Handle Incidents)
- Awareness Training (3.1.2 Preventing Incidents)
- Make Sure Proper Security Measures Are Taken on Endpoints (AV, FW, ETC) (3.1.2 Preventing Incidents)
- Configure Email Security and Detection Tools (3.1.2 Preventing Incidents)
- Threat Intelligence Integration (3.1.2) (regular checks for leaked emails, passwords etc. On the dark web)

## 2. Detection & Analysis

- Identify Suspicious Emails (3.2.1. Attack Vectors)
- Validate Incident & Classify Severity (3.2.2 Signs of an Incident)
- Check file Hashes using OSINT Tools (3.2.3 Sources of Precursors and Indicators)
- Collect Evidence and/or Logs (3.2.3 Sources of Precursors and Indicators)
- Determine Scope of Campaign (3.2.4 Incident Analysis)
- Perform Initial Triage (3.2.4 Incident Analysis)
- Document All Findings (3.2.5 Incident Documentation)
- Determine Incident Priority (P1-4) (3.2.6 Incident Prioritization)
- Notify Stakeholders (3.2.7 Incident Notification)

## 3. Containment, Eradication & Recovery

### 3a. Containment:

- Isolate Compromised Systems (3.3.1 Choosing a Containment Strategy)
- Evidence Gathering (3.3.2 Evidence Gathering and Handling)
- Identify Attacker (3.3.3 Identifying the Attacking Hosts)

### 3b. Eradication

- Block Sender(s) (3.3.4 Eradication and Recovery)
- Block IOCs (filehashes, Urls, Subjects, Ips, etc) (3.3.4 Eradication and Recovery)
- Disable Compromised Accounts (3.3.4 Eradication and Recovery)
- Disable Systems (3.3.4 Eradication and Recovery)

### 3c. Recovery

- Unisolate Systems (3.3.4 Eradication and Recovery)
- Reinstall Compromised Systems (3.3.4 Eradication and Recovery)

- Reset Compromised Accounts (3.3.4 Eradication and Recovery)
- Monitor for Reinfection (3.3.4 Eradication and Recovery)
- Validate Normal Functionality (3.3.4. Eradication and Recovery)

4. Post-Incident Activity

- Lessons Learned (3.4.1. Lessons Learned)
- Update IR plan (3.4.2. Using Collected Incident Data)
- Ensure Proper Incident Documentation and Storage (3.4.3. Evidence Retention)

References:

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

https://medium.com/@deepwebdigger/building-a-phishing-playbook-a-comprehensive-guide-10094f9cc073

## 1. Preparation

The purpose of this phase is to ensure that the organization have proper tools, processes and capabilities to quickly and efficiently respond to phishing attacks and work proactively against possible phishing attacks.

### 1.1.1 Develop IR Plan

The incident response plan is a formal document that defines:

- Roles and responsibilities
- Incident categories and severity levels
- Communication and escalation procedures
- Response workflow for phishing-related incidents
- Requirements for documentation and evidence handling

The incident response plan will be evaluated and updated after each incident and will also have to be updated after each major change to the personnel or infrastructure. All individuals will be educated on their respective responsibilities and roles.

---

### 1.1.2 Implement Analysis Hardware and Software

For effective analysis and detection, the following measures are recommended:

- Dedicated digital forensic workstations for secure analysis (This workstation should use isolated virtual machines and sandbox environments for analysing suspicious links, attachments or any other kind of suspicious activity.)
- Endpoint Detection and Response tools
- Centralized logging and Security Information and Event Management (SIEM) systems
- Email analysis tools for header inspection and artifact extraction
- Secure storage for collected evidence and logs.

Utilizing a combination of these hardware and software tools ensures that the organization is technically prepared to detect, investigate and respond to phishing incidents in a secure and efficient manner.

---

### 1.2.2 Awareness Training

The organization should conduct regular security awareness training. By keeping employees informed and teaching them how to identify, safely handle, and correctly report suspicious phishing activity, the likelihood of phishing attacks succeeding is greatly reduced. This security awareness training must include:

- Identification of phishing emails, malicious links and attachments
- Safe handling of suspicious messages
- Clear procedures for reporting phishing attempts.
- Periodic simulated phishing campaigns to assess user awareness

The training should be updated and improved continuously based on results from the simulated phishing campaigns and the current state of phishing attacks.

---

### 1.2.3 Make Sure Proper Security Measures Are Taken on Endpoints

To reduce the impact of phishing-related compromises, endpoints must be protected using proper security measures. These include:

- Antivirus and anti-malware software with real-time protection.
- Host-based firewalls configured according to organizational policy.
- Endpoint Detection and Response tools for behavioural monitoring.
- Regular patching and updating of operating systems and applications.
- Secure configuration and hardening of endpoint devices.

By utilizing these measures, the organization improves detectability of phishing attempts and reduces the possible attack surface.

---

### 1.2.4 Configure Email Security and Detection Tools.

Phishing attacks primarily utilises email systems, therefore the implementation och robust email security controls are required. This Includes:

- Spam and phishing filters
- Attachment sandboxing and link analysis

- URL rewriting and scanning mechanisms
- Email authentication standards such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting and Conformance (DMARC)
- Integration of email security alerts into the SIEM

Regular updates and configurations to these measures are required to stay up to date and maintain effectiveness.

---

### 1.2.5 **Threat Intelligence Integration**

To proactively prevent phishing incidents, threat intelligence must be integrated into security operations. These measures include:

- Integration of external threat intelligence feeds into SIEM, Endpoint Detection and Response (EDR), and email security tools
- Regular checks for leaked organizational email addresses and compromised credentials on dark web forums and breach repositories
- Proactive actions such as password resets and increased monitoring when exposure is detected

These measures should be done regularly to be informed about possible threats and work proactively against them.

---

## 2. Detection & Analysis

### **2.1 Identify Suspicious Emails (3.2.1 Attack Vectors)**

Most common attacks are initiated from email messages, impersonating trusted contacts to deliver malicious documents or links.
To identify is to be aware and identify common characteristics.

- Unexpected, attached documents or links to cloud hosted documents.
- Senders attempting to use coercive language to intimidate or rush related to contracts, message from leadership or signature requests.

- Incorrect matches of the sender email address, name, or web address could be a third party impersonating a legitimate contact.
- Requests for credentials to unlock or access unknown sources.

Any suspicious email should be flagged and suspected emails are to be preserved for analysis.

---

### 2.2 Validate Incident & Classify Severity (3.2.2 Signs of an Incident)

When a suspicious email or document is identified, it must be analysed to evaluate if it is an incident, and the possible severity level.

Possible signs of potential incident that must be documented:

- Any interactions with the document or link.
- Potential submission of credentials to open/sign documents.
- Executions of possible programming scripts after interaction
- Increase of anomalies or activity in the logs.
- Detection of malware.

If any activity or actions has been detected it is needed to assess in what level of affected units and possible impact of the incident.
Things to determine what could be affected:

- Number of units or users targeted.
- Privilege level of the targeted accounts.
- Potential compromise of credentials, user or client information.
- Impact on system.

If no interaction has occurred, it is still to be documented as a potential future risk. Confirmed incidents are to be escalated to correct level of severity.

---

### 2.3 Check File Hashes Using OSINT Tools (3.2.3 Sources of Precursors and Indicators)

Incidents concerning attachments or downloadable files, should be analysed using cryptographic hashes such as SHA-256 to validate against OSINT and documented threat intelligence sources.

This will help determine:

- Document are known malicious sample
- From a known malware group
- Known IP addresses, URL or file coding.
- Documentation of meta data.
- Reviews of known file framework or weaponisation techniques.

---

### 2.4 Collect Evidence and/or Logs (3.2.3 Sources of Precursors and Indicators)

Relevant evidence is to be gathered from the incident to support incident validation, potential impact assessment and future decisions.
Potential evidence can be gathered from the following.

- Original phishing email data (header, body, attachments)
- Email gateway logs.
- Authentication logs from any potential attempted logins, failed or successful
- Endpoint telemetry from affected units/systems.

---

### 2.5 Determine Scope of Campaign (3.2.4 Incident Analysis)

Each incident is to be analysed to assess if it is part of a larger campaign by matching and correlating possible shared indicators between different incidents.

Things to consider:

- If any additional recipients have received the same or a similar message.
- Variations of the same document, attachments, subject matter, sender or URL.
- Any correlation with external threat intelligence report gathered from earlier stages. (From OSINT and NIST documentation)

Campaign scoping should include internal and external intelligence sources to assess whether the organisation is one of many targets or if it is singularly targeted.

---

### 2.6 Perform Initial Triage (3.2.4 Incident Analysis)

Triage focuses on assessing the first level of impact on the systems and the immediate response required to handle it.

Actions include:

- Identify any users who have interacted with the document or link
- Assess whether any credentials or user information has been compromised
- Evaluate any potential lateral movement or further access attempts within the system
- Determine if any malware or scripts has been executed.

The triage will set a prioritised list that guides decision on containment and allocation for time and resources. Should any credentials be suspected of compromise, it is vital that protection and limitation actions are to be initiated immediately.

---

### 2.7 Document All Findings (3.2.5 Incident Documentation)

All detection and analysis activities must be documented to ensure traceability and auditing, to further support further decisions and actions.

Things that are to be documented are:

- Timeline of events, from first delivery to detection.
- Affected users, systems, accounts and clients.
- Analysis conclusions and severity level
- Actions taken during detection and triage
- Who has been performing the investigation

Documentation needs to be clear, and understandable so it can be manageable and easily handed over to other teams, and be subject to further post-incident reviews, and improve future detections capabilities.

---

### 2.8 Determine Incident Priority (P1-4)(3.2.6 Incident Prioritisation)

Incident priority must be assigned after assessing the potential impact and urgency of the incident.

The prioritisation should consider:

- Scope of exposure to the user and system
- Privilege level of compromised accounts
- Evidence of credential theft or malware execution, and level of threat identified.
- If systems are critical to the functioning of the organisation.
- Threat to client data.

Priority is to be as follows where the lower value is of more sever nature and must be acted upon immediately:

- **P1(Critical):** Active compromise - privileged access, credential theft, file execution - immediate action required
- **P2(High):** High risk - potential for escalation, or compromise of sensitive data - urgent, but not immediate
- **P3(Medium):** Potential compromise - user clicked, no action - needs follow-up
- **P4(Low):** True Positive (TP) - detected, stopped - no compromise, but actionable for intelligence

Priority is to determine response timeline and required escalation paths should it be needed.

---

### 2.9 Notify Stakeholders (3.2.7 Incident Notification)

Once priority is assigned, appropriate stakeholders must be notified to be aware of the threat situation. Depending on the severity of the threat and possible damage further organisations might need to be notified.

- Security Operation Centre
- Affected clients
- Legal teams
- Executive leadership
- Police and government body.

Notification should be factual and limited to only verified information. External notifications should be done in manner depending on the incident nature, if the incident is linked to a crime or loss of individual data, it should be reported to the police and appropriate governmental authorities.

## 3. Containment, Eradication & Recovery

### 3a. Containment:

In this step of the incident response plan, the primary goal is to contain the threat and to prevent any further damage. A containment strategy fitting for the situation needs to be selected and implemented as soon as possible to limit the impact and to support the eradication and recovery efforts.

---

### Isolate Compromised Systems (3.3.1 Choosing a Containment Strategy)

Malware-affected devices must be isolated from the network; this is done to prevent further spread and contamination of other systems. Isolation should be proportionate to the scope of the incident and be maintained during the eradication and recovery phases.

The following steps should be taken:

- Identify and map out all affected systems
- Isolate systems from any production networks
- Maintain restricted network access while allowing investigative access
- Prevent lateral movement by only using the required communication channels

A comprehensible mapping of resources that could have been affected by the attack needs to be done to make sure that other vectors of attack have not been opened.

---

### Evidence Gathering (3.3.2 Evidence Gathering and Handling)

The gathering of evidence is a vital step in the containment phase. Evidence is gathered from identified affected systems to guide containment decisions and enable proper documentation for future incident handling and potential escalation to the authorities.

- Preserve the originating phishing email with attachments and headers
- Collect endpoint activity logs
- Identify affected systems through examination of the collected logs
- Secure the collected evidence for integrity and traceability

---

### Identify Attacker (3.3.3 Identifying the Attacking Hosts)

Identification of the attacker has the potential to support long-term defensive measures; this does however come as second priority to minimising immediate damage during containment

This step includes:

- Identify the attacker through network and email logs
- Extract attack-indicators such as IP addresses and domains
- Use threat intelligence to correlate findings
- Use collected attack indicators for future blocking and prevention

---

## 3b. Eradication

In this phase the focus is to completely eradicate the threat from the organization. The malware must be identified, and all the malicious components need to be removed. Accounts that are compromised needs to be disabled and any exploited vulnerabilities mitigated. This phase needs to be done thoroughly as to remove any residual footholds left by the attack.

---

**Block Sender(s) (3.3.4 Eradication and Recovery)**

To prevent further delivery of phishing emails malicious senders, need to be blocked.

- Block senders that are identified as malicious at the email gateway
- Block related sender domains if applicable
- Apply blocking of senders on all affected accounts and systems

---

**Block IOCs (file hashes, URLs, Subjects, Ips, etc) (3.3.4 Eradication and Recovery)**

To prevent reuse of attacker infrastructure and techniques, identified IOCs must be blocked

Steps can include:

- Block verified File hashes, URLs, IP addresses and subjects
- Update IDS/IPS, EDR, email security controls with IOCs
- Validate that new rules are active and enforced
- Monitor reuse of blocked indicators

---

**Disable Compromised Accounts (3.3.4 Eradication and Recovery)**

Compromised accounts pose a large security risk and need to be remediated to prevent future attacks. Any control that the account in question had must be fully restricted until the steps are completed.

- Disable confirmed compromised accounts
- Reset credentials and require new secure passwords to be enforced
- Revoke any active sessions, delegated permissions and tokens
- Remove any unauthorised mailbox rules or access rights
- If account integrity cannot be assured permanently disable the accounts

These steps should minimise the risk that any remaining undiscovered vulnerabilities are left.

---

### Disable Systems (3.3.4 Eradication and Recovery)

If systems cannot be verified as fully secured, they must be fully remediated to nullify any potential of remaining malware. Depending on the severity of the attack it may be prudent to completely wipe and reinstall the affected systems.

- Identify any systems where full integrity cannot be verified
- Wipe affected systems thoroughly to remove any traces of malicious software
- Reinstall systems
- Apply security patches and desired baseline configuration
- Restore data from verified backups

This minimises the potential for any malware or vulnerability to be hiding within the system. For situations like this it is good practice to have backups of systems done regularly to lessen potential data loss. For further information on this see the next segment of this IR.

---

## Recovery

### Unisolate Systems (3.3.4 Eradication and Recovery)

Once a threat has been mitigated and the system is deemed clean, the implemented isolation measures during containment can be reversed. This includes reconnecting the host to the production network, re-enabling work-critic services and lifting any firewall and/or segmentation rules introduced during the incident.

**Before isolating a system, the following things must be validated:**

- No malicious processes or persistence mechanisms remain
- All security controls, such as AV and logging, are up and running
- System has been configured to prevent reinfection

Furthermore, unisolation should occur gradually and the process should be monitored to quickly detect abnormal behaviour/signs of reinfection.

---

**Reinstall Compromised Systems (3.3.4 Eradication and Recovery)**

If a system was significantly compromised/infected and integrity cannot be assured a full reinstallation may be required. NIST emphasises that restoration from a trusted, verified source is critical to prevent reinfection.

Steps may include:

- Wiping of the device
- Reimaging from a gold standard baseline
- (Re)applying patches and security configurations
- Reinstalling approved applications
- Validating system integrity

This ensures the host returns to an operational state free from compromise.

---

**Reset Compromised Accounts (3.3.4 Eradication and Recovery)**

Confirmed compromised accounts and/or account suspected of being compromised must have their authentication credentials reset, including:

- Password reset
- Revoke and reissue of MFA tokens
- Reviewing OAuth authorisations
- Removing unauthorised mailbox rules and/or delegates

NIST emphasises that credential reset should only occur after containment to avoid tipping off the attacker. Account resets help ensure any stolen credentials cannot be reused during/after recovery.

---

**Monitor for Reinfection (3.3.4 Eradication and Recovery)**

After systems have been restored and accounts remediated, enhanced monitoring must be implemented to ensure there is no additional malicious activity and that the incident does not recur. The monitoring phase is crucial for validating the success of the eradication and recovery steps.

Monitoring activities can include:

- Increased logging and/or alerting on previously affected systems/accounts. (this could include implementing additional rules specifically for these systems/accounts)
- Reviewing EDR alerts for suspicious processes or behaviours.
- Monitoring authentication logs for unusual login attempts, locations and/or devices.
- Reviewing network traffic for communication with previously identified suspicious/malicious Ips and/or domains.

NIST highlights the importance of continued monitoring during recovery to detect signs of reinfection and/or attacker re-entry attempts.

---

**Validate Normal Functionality (3.3.4. Eradication and Recovery)**

Once systems and accounts have been restored, it is important to verify that business operations are back to normal and security controls are functioning accordingly. This step ensures that recovery actions have not impacted system availability or performance negatively.

Validation activities can include:

- Confirming that business-critical infrastructure is operational
- Verifying that the implemented security tools such as AV, EDR and logging are active.
- Ensuring users can authenticate and access authorised resources with no issues
- Performing functional testing to confirm system stability

First after successful validation systems should be considered fully recovered and the incident can proceed to post-incident activities.

---

## 4. Post-Incident Activity

**Lessons Learned (3.4.1. Lessons Learned)**

After the incident has been resolved a lessons-learned should be conducted to review the effectiveness of the IR process. NIST recommends holding this as soon as possible while details are still fresh

Topics addressed can include:

- How the incident was detected and if it could've been detected sooner
- Effectiveness of all steps
- Communication between teams and stakeholders
- Gaps in controls and training that contributed to the incident

The objective is never to assign blame, but to identify points of improvement to reduce the risk of similar incidents.

---

**Update IR plan (3.4.2. Using Collected Incident Data)**

Information that was gathered during the incident can and should be used to improve future incident response. NIST emphasises using collected incident data to improve policies and procedures.

This can include:

- Updating IR plan and playbooks to address identified gaps.
- Improving detection rules and logic
- Improving email filtering and endpoint detection

Incorporating these improvements increases the chance of the organisation being more prepared in the case of future similar incidents.

---

**Ensure Proper Incident Documentation and Storage (3.4.3. Evidence Retention)**

All incident related documentation must be securely stored in accordance with the organisations policies as well as fulfil legal requirements. Proper documentation supports future analysis and compliance.

This includes:

- Timelines
- Logs
- Samples
- File hashes

- Forensic artifacts and evidence chains
- Final reports and summaries

NIST stresses the importance of retaining evidence for future reference.

---

## Communication templates

Affected user, no impact:

Subject: Notice From CSOC – Your Account May Be at Risk [INC]

Hello [insert name],

I'm reaching out to you from the Cybersecurity Operations Centre. We received an alert in our systems indicating that you interacted with a malicious email and visited a URL used for credential harvesting. We have no evidence your account has been compromised, but as a precautionary measure we have initiated a password reset and revoked your MFA.

What we need from you:

- Complete password and MFA reset when prompted (you might have to log out and sign back in for the process to initiate)
- Let us know if you discover something unusual with your account/device.

Please don't hesitate to reach out if you have any queries or need more information.

Best regards,
[*Name*], [*designation*]
[*Team*]
[*Company*]

User's manager, impact:

Subject: Notice From CSOC – Security Incident Notification Regarding User [*UserID*] [INC]

Hello [*insert name of manager*],

I'm reaching out to you from the Cybersecurity Operations Centre. We received an alert in our systems indicating that your employee [*insert name of employee*] was involved in a security incident related to phishing, and shortly thereafter we noticed suspicious sign ins to the user's account.

We have therefore disabled his/her account and once we have conducted our investigation, we will re-enable it, and a new password will be shared with you to share with [*user*].

We will keep you updated as the investigation progresses.

Please don't hesitate to reach out if you have any queries or need more information.

Best regards,
[*Name*], [*designation*]
[*Team*]
[*Company*]