Reactive and Proactive Phishing Defence

Effective phishing defense requires both reactive incident response capabilities and proactive prevention strategies. Reactive measures focus on containment, eradication, and recovery when phishing incidents occur, following established incident response frameworks to minimize damage and prevent spread. Proactive defense involves implementing preventive controls, user education, and continuous improvement based on threat intelligence gathered from previous incidents. Understanding both approaches is essential for comprehensive organizational security, as technical detection capabilities must be paired with systematic response procedures and ongoing risk reduction efforts.

Reactive Phishing Defence

These are the actions we take when we identify and analyze a phishing incident. Measures we want to take in order to address and resolve an incident, and minimize the risk of the malicious email that we identified. Once a malicious email has been identified, we generally want to take the following response actions:

- **Containment**
  - **Determine the scope**: Was this sent to a single user? Or was it sent to an entire department or team? Was the victim a third party contractor that rarely uses their email account? Or was it a high level executive with a lot of access to critical information?Main bullet
    - Scope is often determined at the email gateway level. In a Microsoft environment you can use the Message trace functionality.
  - **Quarantine**: Isolate suspicious or potentially malicious emails or files, and prevent them from reaching the user's inboxes.
    - Both Microsoft and Google have Quarantining functions to isolate phishing emails and associated attachments.
  - **Block sender artifacts**: Prevent future phishing attempts by the same sender. For example, block specific email addresses, domains or IPs. Even subject lines can be blocked. These artifacts would have been collected during the triage and analysis stage.
    - Be careful of collateral damage, such as when the attacker is using a legitimate service, as this could significantly disrupt business operations. You don't want to block the entire Gmail domain for example.
  - **Block web artifacts**: You can also block emails that contain certain URLs, domains.
  - **Block file artifacts**: Block emails containing files with certain names or file hashes.
- **Eradication**
  - **Remove malicious emails**: Remove all malicious emails that were found.
    - Content Search and eDiscovery allows you to find all copies. For example, in a Microsoft 365 environment, you can use the Security and

Compliance center or the Microsoft Purview functionality to do a content search, find all instances of a malicious email and purge them.
        - You can also use the exchange management shell to search for emails within your email server for a bit more flexibility and power. The command is `Get-MessageTrackingLog -{attribute (Sender, Recipient, MessageSubject, etc)} {search term}`. See this MS article for more filtering options.
    - **Remove malicious files**: If there were any files downloaded to a server, host or other endpoints, they need to be removed.
        - EDR tools can quarantine and delete files. PowerShell scripts can be used to look through the email servers and remove any instances
    - **Abuse form submissions**: Any URLs, domains and IPs that have been found to be malicious should be reported to relevant authorities and registrars. Doing so will help further spread awareness about the abuse, and the websites may be taken down by the registrars.
        - DomainTools allows you to look up domains, and there will usually be an email with a Registrar Abuse Contact Email. Or you can try looking up whether the Registrar has a public abuse form, which is common for large registrars. For example, here is a link to various abuse forms for GoDaddy.
    - **Credential changes**: As credentials may have been captured or leaked, passwords need to be changed, and access tokens need to be rerolled. Employees generally don't want to admit that they've been a victim of phishing, so it is usually safer to just have everyone that got a phishing email change passwords.
    - **Reimaging**: For systems that were infected by malware, instead of fixing it, it is generally easier to wipe the system and install the last saved non-infected image. This makes sure all traces have been eradicated.
- **Recovery**
    - **Restore systems** to normal operation. Just reimaging may not be enough. Patches or software may need to be reinstalled and implement additional security measures to prevent similar future incidents.
- **Communication**
    - **Notify affected users** about the phishing incident. For example, you can send them an email with a timestamp and description of the event, as well as letting them know what actions have been taken.
    - **Update stakeholders** of actions that have been taken, and what still needs to be done.
- **User Education**
    - **End-user training**: It is our responsibility to make sure employees are informed of phishing and often used techniques, as well as making sure they know how to report phishing emails.

These response actions will typically follow the classic incident response framework after the detection and analysis phase. This will be covered in more detail in the Incident Response section of the course.

Proactive Phishing Defence

Use what we learned from our analysis to improve detection and security operations. Note: Depending on the organization, not all these strategies will be feasible or available due to tooling or budgeting restrictions. These are ideas to keep in mind to supplement the above reactive functions.

- **Email Filtering**
  - **Email security appliances**: There are filtering tools that look at threat intelligence, heuristics and pattern analysis to determine whether an email is malicious, so specific IPs, domains or URLs are not necessary to filter them.
    - Some even scan attachments before they are let through. For example, documents that have macros embedded could be proactively blocked. Or files could be sandboxed before they are shown to users, and if there are red flags, they are removed.
  - **Marking external emails**: If an email comes outside of the organization you work for, it alerts the user. This makes it easier to distinguish it from internal communication. Very common nowadays.
    - Adding disclaimers can be set up in applications like MS Exchange as a rule.
- **URL Scanning and Blocking**
  - **Real-time URL inspection**: Instead of blocking URLs after the fact, they can be scanned as they come in.
    - You can dynamically analyse website links embedded in the email.
    - Or implement email and end-point security solutions that can perform URL rewriting (defang them) or redirection.
    - Or links can be rerouted to a proxy server before users are allowed to access them.
  - **Block recently registered domains**: Legitimate domains have usually been around for some time.
    - Phishing links are usually taken down quickly, so getting domains that are older takes a lot of effort for attackers.
- **Attachment Filtering**
  - **File extension blocks**: Files with certain extensions, such as executables, can be blocked. What kind of files would employees usually send each other? If you know that, you can block everything else. There are lots of extension types, so allow lists are usually the way to go here.

        - Files extensions can be filtered by MS Exchange and other email managers.
    - **Attachment sandboxing**: Have files be automatically opened in a sandbox to see what it does. If there are suspicious behaviors, block it.
- **Email Authentication Methods**
    - **SPF**, **DKIM** & **DMARC**: See the Header Analysis section for more information about email authentication. You can set filters to automatically reject emails that fail one or more of these checks.
- **User Training**
    - **Security awareness training**: Instead of proactively only educating employees that have fallen for a phish, you can have yearly or monthly awareness training for all employees.
        - You can use videos and quizzes to track employee awareness levels.
    - **Phishing simulations exercises**: Kind of like penetration testing, but just at the phishing level. Could include Vishing or Smishing as well. How many employees click on the phishing link? How many report the email/call/text?
        - Those that did click the phishing links would need extra training.
    - **Reporting functionality**: It is important for employees to be able to tell the security team when they believe something suspicious is happening.
        - Most email clients have a report button. If this is sent directly to the SOC, then the security team can be made aware quickly, and respond early.
        - Other suspicious events should also be easily reportable. The method should be clear and user friendly, or else employees won't bother.

Summary

Phishing defense combines systematic incident response with preventive security measures to create comprehensive organizational protection. Reactive defense follows the containment-eradication-recovery model, emphasizing scope determination, quarantine procedures, artifact blocking, and thorough cleanup using tools like Microsoft 365 security features and Exchange management shell commands. Proactive defense focuses on prevention through email filtering, URL scanning, attachment sandboxing, authentication enforcement, and user training programs including simulated phishing exercises. Success requires balancing automated security controls with user education, ensuring both technical capabilities and human awareness work together to reduce organizational risk while maintaining business operations.