Email Security Audit Playbook V.01

Introduction

- Purpose: This playbook provides a standardized, repeatable procedure for conducting professional email security audits for small to medium-sized businesses (SMBs).
- Primary Objective: Systematically identify, assess, and report on vulnerabilities within a client's email ecosystem to reduce the risk of phishing, spoofing, and business email compromise (BEC).
- Scope: This audit is a point-in-time, external assessment focusing on:
    - Email authentication (SPF, DKIM, DMARC, MX)
    - Email server transport security (TLS, certificates, SMTP)
    - Cloud platform configuration (Microsoft 365/Google Workspace)
    - Security policies and administrative controls
- Explicitly Excluded (unless specifically requested):
    - End-to-end email encryption assessment (S/MIME, PGP)
    - Email content analysis or archive review
    - Penetration testing or internal network assessment
    - Social engineering (requires separate authorization)

Pre-Audit Phase: Scoping and Authorisation

This phase is critical for legal protection and setting expectations. Never proceed without completing it.

Client Onboarding Checklist

1. **Service Agreement Signed**: Client has signed the agreement defining scope, cost, and liabilities.
2. **Authorization Form Signed**: Client has provided explicit written permission to test their systems.
3. **Email SLA and AF to client and file:** Email the SLA and AF to the client get them to sign it and send it back and file It in a proper project folder, for example /Clients/[Client Name]/01_SLA.
4. **Primary Contact**: Name, role, email, and phone (for day-to-day communication) identified.

5. **Emergency Contact**: Name and phone (for critical issues) identified and documented.
6. **Target Domains**: List of all domains to be assessed (e.g., company.co.uk, marketing.company.com).
7. **Email Platform Confirmed**: Microsoft 365, Google Workspace, hybrid, or other.
8. **Information Gathering Questionnaire** completed by client.
9. **Review All answers and store in a timestamped DOC.**
10. **Identify DNS Manager for follow up.**
11. **Third-Party Services Identified**: List of marketing/automated email services confirmed.
12. **Past Incidents Documented**: Any previous security incidents reviewed and noted.
13. **Access Method Confirmed**: Screenshared session vs. credentials agreed upon.
14. **Add-On Services Authorized**: HIBP, Phishing Simulation, Forwarding Audit confirmed if selected.

Information Gathering Questionnaire

Make sure to send the client the questionnaire and make sure it is filled out and sent back to you before starting anything.

Pre-Audit Recon (Public Information)

Before any intrusive tests, gather public data.

- Tool: Command Prompt (cmd.exe) or Windows PowerShell (Is better).
- Task: Gather Baseline DNS records

MX Records Analysis

Step 1: Retrieve and List the MX Records

Primary PowerShell command (run as Administrator)

Resolve-DnsName -Name "example.co.uk" -Type MX | Format-Table -AutoSize

Or

nslookup -type=MX example.co.uk (This might work in PowerShell)

Step 2: Analyse the Key Elements

What to Look For	Good/Expected Outcome	Problem & Risk Level
1. Record Existence	At least one MX record is returned.	**No MX records (CRITICAL):** Email for this domain is fundamentally broken. No mail can be received.
2. Record Count (Redundancy)	**Two or more MX records** with different priority values (e.g., 10, 20).	**Single MX record (HIGH):** Creates a single point of failure. If that server is unreachable, email delivery fails.
3. Priority Values	Lower numbers = higher priority (e.g., 10 mailcluster.example.com). The server with the lowest number handles mail first.	**Misconfigured Priorities (MEDIUM):** If priorities are illogical (e.g., backup server has a lower number than primary), email may route inefficiently.
4. Target Hostname	Points to a legitimate, expected mail service (e.g., *.protection.outlook.com for M365, *.google.com for Workspace).	**Suspicious or Unexpected Target (CRITICAL/HIGH):** Could indicate DNS hijacking, where email is being routed to an attacker's server.
5. Common Provider Patterns	Recognizable patterns for major providers (see table below).	**Direct-to-IP or Generic Host (MEDIUM):** May indicate an old, on-premise server without modern cloud security filtering.

Common MX Record Patterns:

- **Microsoft 365:** *.mail.protection.outlook.com (e.g., company-co-uk.mail.protection.outlook.com)
- **Google Workspace:** *.google.com (e.g., aspmx.l.google.com)
- **Security/Filtering Services (e.g., Mimecast, Proofpoint):** Often have distinct, provider-specific hostnames (e.g., *.mxrecord.mx).

Technical Audit Phase: The Windows Assessment Workflow

Follow this sequence for every domain in scope. You can use either **Command Prompt** or **PowerShell**

Module A: DNS & Email Authentication Audit

Check	Tool/Method (Windows)	Procedure & Example Command	Ideal Result
SPF Record Lookup	CMD: `nslookup` PowerShell: `Resolve-DnsName`	`nslookup -type=TXT example.co.uk` *or* `Resolve-DnsName -Name example.co.uk -Type TXT`	Record starting with `v=spf1` exists.
DKIM Record Lookup	CMD: `nslookup` PowerShell: `Resolve-DnsName`	`nslookup -type=TXT selector1._domainkey.example.co.uk` *Replace `selector1` with client's selector (often `google`, `selector1`, `k1`).*	Record exists, contains a long public key string (`p=...`).
DMARC Record Lookup	CMD: `nslookup` PowerShell: `Resolve-DnsName`	`nslookup -type=TXT _dmarc.example.co.uk` *or* `Resolve-DnsName -Name _dmarc.example.co.uk -Type TXT`	Record starting with `v=DMARC1` exists. Policy (`p=`) is `quarantine` or `reject`.

Subdomain & CNAME Analysis (Takeover Risk Assessment)

Objective: Identify dangling DNS records that could allow subdomain takeover attacks.

Procedure:

Enumerate Subdomains:

```PowerShell
# Using PowerShell with Resolve-DnsName
$domain = "example.co.uk"
Resolve-DnsName -Name "*.$domain" -Type A -ErrorAction SilentlyContinue | Select-Object Name, Type, IPAddress
```

Check Critical CNAME Records:

- autodiscover.example.co.uk
- mail.example.co.uk
- Any *.example.co.uk pointing to third-party services

Analyse for Takeover Risk:

- **Risk Indicator:** CNAME records pointing to expired/deleted cloud services (Azure, AWS, GitHub Pages)
- **Example:** helpdesk.example.co.uk CNAME helpdesk.azurewebsites.net (if azurewebsites.net isn't claimed)

Online Tools for Quick Check:

- **DNSDumpster.com** (free subdomain enumeration)
- **SecurityTrails.com** (historical DNS records)
- **BuiltWith.com** (identify underlying services)

Risk Rating:

- **HIGH:** CNAME pointing to unclaimed cloud service
- **MEDIUM:** Obscure subdomains with no clear purpose
- **LOW:** Properly configured subdomains with active services

Alternative: Using Online Tools (Recommended for Beginners & Reports)

For more user-friendly analysis and screenshot evidence, use these web-based tools instead of the command line. They are excellent alternatives to MXToolbox

- **PowerDMARC** or **EasyDMARC**: Best for deep DMARC, SPF, and DKIM analysis and clear reporting.

- **Inbox Radar (Saleshandy)** or **GlockApps**: Great for overall deliverability and inbox placement testing, with clear security checks.
- **Mail-Tester.com**: Simple tool for sending a test email and getting a detailed authentication report.

Module B: Email Server & Transport Security

Objective: Check the security of mail servers and email transmission.

PowerShell Scripts

Check	Tool/Method	Procedure	Ideal Result
SMTP Server Reachability & Banner Analysis	CMD: `telnet`	1. Enable Telnet Client via "Turn Windows features on/off". 2. `telnet mail.example.co.uk 25` 3. **Record the SMTP banner response.**	Connection succeeds. You can issue `EHLO yourdomain.com`. **Good:** Minimal banner (e.g., "220 mail.server.com") **Bad:** Revealing banner (e.g., "Microsoft ESMTP MAIL Service, Version: 10.0.1")

Check	Tool/Method	Procedure	Ideal Result
TLS/SSL Configuration Deep Dive	PowerShell: `openssl` **OR** SSL Labs API (Online)	1. Test TLS 1.2+ support: `openssl s_client -connect mail.example.com:587 -starttls smtp` 2. Check specific TLS versions: `Test-TlsConnection -Server mail.example.com -Port 587`	TLS 1.2 or 1.3 connection succeeds. Certificate is valid, not expired, and matches the mail server hostname. No weak or deprecated ciphers enabled.

Check	Tool/Method	Procedure	Ideal Result
Certificate Validity Check	Browser **or** `openssl`	1. Visit the mail server via HTTPS (if webmail). 2. Check certificate details with: `openssl s_client -connect mail.example.com:443 2>/dev/null | openssl x509 -noout -dates -subject`	Certificate valid for ≥30 days. Issued by a trusted Certificate Authority (CA). Contains proper Subject Alternative Names (SANs) for all mail server hostnames.

Check	Tool/Method	Procedure	Ideal Result
DNS Consistency Audit	**NetCrunch DNS Audit Tool** (Free) **OR** `nslookup`	1. `nslookup mail.example.com` (get IP) 2. `nslookup [IP]` (reverse lookup) 3. Check for PTR records and forward/reverse match.	Clean scan with no critical mismatches. Every mail server IP has a matching PTR (reverse DNS) record that points back to a recognized domain name.

TLS/SSL Security Checklist

When analysing TLS/SSL configuration, check for these specific issues:

Check Category	Specific Checks	Tool/Method	Pass/Fail Criteria
Certificate Issues	• Certificate not expired • Issued by trusted CA • Matches server hostname • Strong key (RSA 2048-bit+)	openssl s_client openssl x509 -dates	All checks must PASS for Critical rating
Protocol Security	• TLS 1.0 and 1.1 disabled • TLS 1.2 enabled with strong ciphers • TLS 1.3 enabled (if supported) • SSLv2/v3 disabled	SSL Labs test openssl ciphers	TLS 1.0/1.1 must be FAIL (disabled)
Cipher Strength	• Weak ciphers disabled (RC4, DES, 3DES) • Forward secrecy enabled • CBC-mode prioritized properly	SSL Labs cipher analysis	No weak/insecure ciphers enabled

Online Tools for TLS Analysis:

- **SSL Labs** (https://www.ssllabs.com/ssltest/) - Comprehensive TLS/SSL testing
- **testtls.com** - Simple SMTP TLS testing
- **HTTPS Everywhere's Observatory** - For webmail interfaces

Audit Session Guide

1. Open PowerShell as Administrator.

2. For each domain from the questionnaire, run the three Resolve-DnsName commands. **Copy-paste all outputs** into a timestamped text file ([Client]_DNS_Output_[Date].txt).
3. For each domain, first use the online tool (PowerDMARC/GlockApps). This gives you an immediate, clear overview and your primary evidence (screenshots).
4. Then, use PowerShell to run the Resolve-DnsName commands. This serves to validate the tool's findings and gather raw data for your notes. This prevents context-switching between domains.
5. Enable Telnet and test SMTP reachability for the primary mail server (from MX record). Document result: "Success/Timeout/Refused."

Module C: Cloud Platform Configuration Review (If Credentials Provided)

Objective: Assess security settings within Microsoft 365 or Google Workspace.
Requires client-provided admin credentials or a screenshared session.

Microsoft 365 Checklist (via Admin Centre):

Anti-Spam & Anti-Malware Policies (Critical):

- **Navigate to:** Exchange Admin Centre > Protection
- **Check:**
    1. **Anti-spam policies:** Default and custom policies configured
    2. **Anti-malware policies:** Attachment filtering enabled
    3. **Safe Attachments:** Enabled for unknown malware detection
    4. **Safe Links:** Enabled for URL scanning and rewriting
    5. **ATP policies:** Configured for phishing and impersonation protection

Email Archiving & Retention:

- **Navigate to:** Compliance Centre > Information Governance > Retention
- **Check:**
    1. **Retention policies** exist for email
    2. **Default retention period** is appropriate (industry standard: 7 years for finance/legal)
    3. **Archive mailboxes** enabled if required for compliance

Mobile Device Management (MDM):

- **Navigate to:** Endpoint Manager (Intune) > Devices > Configuration
- **Check:**
    1. **Mobile Application Management (MAM)** policies for Outlook mobile
    2. **Device compliance policies** requiring passcodes on mobile devices
    3. **Conditional Access** policies requiring compliant devices for email access

Incident Response & Reporting:

- **Navigate to:** Security Centre > Alerts & Incidents
- **Check:**
    1. **Alert policies** configured for suspicious activity
    2. **Users can report phishing** via "Report Message" add-in
    3. **Dedicated mailbox** (e.g., security@company.com) monitored for reports

Google Workspace Checklist (via Admin Console):

Spam, Phishing & Malware Settings:

- **Navigate to:** Admin Console > Security > Spam, Phishing and Malware
- **Check:**
    1. **Inbound spam filtering:** Set to "Aggressive" for unknown senders
    2. **Outbound spam filtering:** Enabled to prevent compromised accounts
    3. **Phishing protection:** Enhanced pre-delivery message scanning enabled
    4. **Malware protection:** Blocked file types configured

Data Retention & Archiving:

- **Navigate to:** Admin Console > Account > Data Retention
- **Check:**
    1. **Retention rules** applied to organizational units
    2. **Vault** enabled if required for compliance
    3. **Default deletion period** configured appropriately

Mobile Management:

- **Navigate to:** Admin Console > Devices > Mobile & endpoints

- **Check:**
    1. **Basic/Advanced mobile management** enabled
    2. **Device policy** requiring screen locks on mobile devices
    3. **Account wipe capabilities** for lost/stolen devices

User Reporting & Alerts:

- **Navigate to:** Admin Console > Reporting > Alerts
- **Check:**
    1. **Suspicious activity alerts** configured
    2. **Phishing report button** enabled in Gmail
    3. **Security investigation tool** accessible to admins

Module C Part 2: Third-Party Email Service Audit (If Applicable)

Objective: Verify that marketing, newsletter, and automated email services are properly authenticated and secured.

Prerequisite: Client has indicated use of third-party services in Questionnaire Q6.

Procedure:

1. **Identify All Third-Party Senders:**
    - Mailchimp, SendGrid, HubSpot, Constant Contact, etc.
    - Transactional email services (e.g., from CRM, helpdesk software)
2. **SPF Verification for Each Service:**

```PowerShell
# Check if third-party IPs are included in SPF
nslookup -type=TXT example.co.uk | findstr "include"
# Common third-party SPF includes:
# Mailchimp: include:servers.mcsv.net
# SendGrid: include:sendgrid.net
# HubSpot: include:_spf.hubspot.com
```

3. **DKIM Verification for Each Service:**
    - Each service uses different DKIM selectors
    - Example for SendGrid: s1._domainkey.example.co.uk
    - Example for Mailchimp: k1._domainkey.example.co.uk

4. **DMARC Alignment Check:**
    - Ensure alignment-mode is "relaxed" to allow third-party services
    - Verify DMARC reports show passing authentication for third-party mail

5. **Security Settings Review (If Access Provided):**
    - API key management: Are keys regularly rotated?
    - Access controls: Minimum necessary permissions for services
    - Logging: Are sends and bounces logged and monitored?

Risk Assessment:

- **CRITICAL:** Third-party service sending without SPF/DKIM
- **HIGH:** Third-party included in SPF but no DKIM configured
- **MEDIUM:** DKIM configured but alignment issues with DMARC
- **LOW:** Properly authenticated with monitoring in place

Module D: Email Forwarding Rule Audit (Add-on)

Objective: Identify unauthorized or suspicious email forwarding rules that could lead to data leakage.

Part 1: Checking for Client-Side Rules (Per-User)

This usually requires the user's password or a delegated admin session. You would typically request to check the mailbox of key individuals (CEO, CFO, Head of HR) or accounts that have shown suspicious activity.

For Microsoft 365 / Outlook:

1. **Method (If you have user credentials):** Log into Outlook on the web (outlook.office.com).
2. Navigate to **Settings (gear icon) > View all Outlook settings > Mail > Rules**.
3. **Look for:** Any rules with "forward," "redirect," or "forward as attachment" actions sent to external email addresses.

4. **PowerShell Method (As Global Admin - More Efficient):** This is the professional way to check all users.

```
# Connect to Exchange Online first (You'll need to install the EXO V2 module first: Install-Module -Name ExchangeOnlineManagement)

Connect-ExchangeOnline


# Get all inbox rules for a specific user

Get-InboxRule -Mailbox "ceo@example.co.uk" | Select-Object Name, Description, Enabled, RedirectTo, ForwardTo | Format-List


# Search across all users for rules with "ForwardTo" or "RedirectTo" populated

Get-Mailbox -ResultSize Unlimited | Get-InboxRule | Where-Object {($_.ForwardTo -ne $null) -or ($_.RedirectTo -ne $null)} | Select-Object MailboxOwnerId, Name, ForwardTo, RedirectTo
```

For Google Workspace:

1. **Method (If you have user credentials):** Log into Gmail.
2. Click the **Settings (gear icon) > See all settings > Forwarding and POP/IMAP**.
3. **Look for:** Any forwarding address configured under the "Forwarding" section.
4. **Admin Console Method (As Super Admin):**
    - Go to the **Google Admin Console**.
    - Navigate to **Apps > Google Workspace > Gmail**.
    - You can check user-level settings via user audit logs, but per-user forwarding is primarily set by the user themselves.

Part 2: Checking for Server-Side/Admin Mail Flow Rules

This is checked in the admin panel and affects the whole organization. It does not require individual user passwords.

For Microsoft 365:

1. Navigate to the **Microsoft 365 Admin Centre**.
2. Go to **Admin centres > Exchange**.
3. Navigate to **Mail flow > Rules**.

4. **Review every rule.** Pay special attention to rules that:
    - Have "redirect," "forward," or "blind carbon copy (BCC)" actions.
    - Send messages to addresses outside your client's primary domain (@example.co.uk).
    - Are poorly documented or have vague names.

For Google Workspace:

1. Navigate to the **Google Admin Console**.
2. Go to **Apps > Google Workspace > Gmail > Routing**.
3. **Review settings under "Routing" and "Default routing."** Look for:
    - **Hosted routing** that sends mail to other addresses.
    - **SMTP forwarding** to external addresses.
    - **BCC address** settings that add external recipients to all emails.

Part 3: HaveIBeenPwned Checks (Add-on)

Objective: To determine if employee email addresses have been exposed in known public data breaches, indicating a high risk of credential stuffing, targeted phishing, or account takeover.

Prerequisite: You **must** have explicit authorization in your service agreement to process this personal data. You must receive a list of employee email addresses from the client's primary contact.

Procedure:

1. **Data Handling:** Upon receipt, save the email list in a **temporary, encrypted file** (e.g., [Client]_Emails.txt.gpg). Do not store it in cloud sync folders (OneDrive/Google Drive). Process it on your local machine.
2. **Choosing a Method:** You have two main options. **Recommendation: Use the Official API.**
    - **Option A: Official HIBP API (Professional, Recommended)**
        - **Step 1:** Purchase a license for the **HIBP Pwned Passwords API** (v3). This is legally required for bulk checking and is very low cost (~$3.50 USD per 1,000 email checks).
        - **Step 2:** Use a PowerShell script with your API key to automate the checks. Here is a basic, safe script template:

```powershell
# HIBP Bulk Check Script Template
# Replace with your actual API key and file paths

$ApiKey = "YOUR-HIBP-API-KEY-HERE"
$EmailListFile = "C:\Audits\Client\emails.txt"
$OutputFile = "C:\Audits\Client\hibp_results_$(Get-Date -Format 'yyyyMMdd').csv"

# Read emails and check against HIBP
$emails = Get-Content $EmailListFile
$results = @()

foreach ($email in $emails) {
    $uri = "https://haveibeenpwned.com/api/v3/breachedaccount/$($email)?truncateResponse=false"
    $headers = @{"hibp-api-key" = $ApiKey}

    try {
        $response = Invoke-RestMethod -Uri $uri -Headers $headers -ErrorAction Stop
        $breachCount = $response.Count
        $breachNames = ($response.Name -join ", ")
        $pwned = $true
    } catch {
        if ($_.Exception.Response.StatusCode.Value__ -eq 404) {
            $breachCount = 0
            $breachNames = ""
            $pwned = $false
        } else {
            Write-Warning "Error checking $email : $_"
            continue
        }
    }

    $results += [PSCustomObject]@{
        Email = $email
        Pwned = $pwned
        BreachCount = $breachCount
        Breaches = $breachNames
    }
```

```
    # Respect rate limit (1.5 seconds between requests)
    Start-Sleep -Milliseconds 1500
}

# Export results
$results | Export-Csv -Path $OutputFile -NoTypeInformation

# Securely delete input file after processing
# Remove-Item -Path $EmailListFile -Force
```

3.
    - **Option B: Manual Check (For Very Small Lists < 10)**
        - **Step 1:** Manually visit https://haveibeenpwned.com.
        - **Step 2:** Enter each email address one by one.
        - **Step 3:** Manually document the result (screenshot or note).
        - **Cons:** Not scalable, prone to error, and violates HIBP's terms of service for automated querying without an API key.
4. **Analysis:** Generate a summary from your results.
    - **Percentage Pwned:** (Number of pwned emails / Total emails) * 100. A rate above 10-15% is common but indicates high risk.
    - **Key Individuals:** Flag results for C-level executives, finance, and IT admin accounts as **HIGH** risk regardless of overall percentage.

Critical Legal & Operational Notes for Your Playbook

1. **Authorization is Key:** Your **Service Agreement** must state you will process employee email addresses for the purpose of breach disclosure checking. The client warrants they have the right to provide this data.
2. **Data Minimization & Disposal:** Emphasize in your procedure that the email list and results file must be **securely deleted** immediately after the report is delivered. Use the cipher /w: command on Windows to wipe the files.
3. **API Terms:** You **must** purchase an API key for anything beyond trivial, manual checks. It's affordable, legal, and supports the service.

Part 4: Password Policy Check

How to Check for Password Reuse "Patterns"

You assess the risk by examining three areas: **Company Policy**, **Technical Enforcement**, and **Behavioural Indicators**.

1. Check Password & Authentication Policies (Platform Level)

This is your primary, actionable check. You review what the system is *configured to prevent*.

For Microsoft 365 (Azure AD):

1. Navigate to **Azure Active Directory > Security > Authentication methods > Password protection**.
2. Check the **"Custom banned passwords"** list. A strong policy will ban common passwords and variants (Companyname2024!, Welcome123).
3. More importantly, ensure **"Enforce custom list"** is set to **Yes**. This is a basic reuse blocker.
4. Go to **Azure AD > Security > Conditional Access**. Look for a policy that uses the **"User risk"** condition from Identity Protection. If a user's credentials appear in a leak (like HIBP), a good policy will force a password reset or require MFA.

For Google Workspace:

1. Navigate to **Admin Console > Security > Password management**.
2. Check if **"Enforce strong password"** is enabled. While not directly "reuse," it increases complexity.
3. Google's stronger reuse controls are tied to its **Advanced Protection Program** and security key enforcement for high-risk users, which you would have noted in your Super Admin review.

2. Look for Behavioural Indicators (Indirect Evidence)

These are clues that suggest reuse is likely, based on your HIBP findings.

- **Correlate HIBP Results with Role:** If the **CEO's email** was found in 5 major breaches (LinkedIn, Dropbox, etc.), the probability they are reusing an old, compromised password is *high*. This is a critical inference for your risk assessment.
- **Check for Lack of MFA:** An account with a pwned email that does **not** have Multi-Factor Authentication (MFA) enabled is at extreme risk. The assumption is that a reused, known password is the only thing protecting it.
- **Review Incident History:** If the questionnaire revealed past account compromises, password reuse is a likely root cause.

Critical "Do Not Do" List

- **DO NOT** ask users for their passwords.
- **DO NOT** ask administrators to provide you with password hashes or lists.
- **DO NOT** attempt to use any tool that claims to "check" password reuse by trying to log in to services. This is illegal.
- **DO** focus on the **policies, configurations, and behavioural evidence** that make reuse likely or dangerous.

Module E: Phishing Simulation and Awareness Assessment (Add-on)

Objective: To safely evaluate employee susceptibility to phishing attacks, measure security awareness, and provide targeted training to reduce human risk.

CRITICAL PREREQUISITE – LEGAL AUTHORIZATION:

You **must** have explicit, written authorization from senior management (e.g., CEO, Head of HR) in your service agreement. The authorization must state that you will send simulated phishing emails to employees and that the client has informed staff this may occur as part of security training. **Never proceed without this.**

Part 1: Planning & Setup

Step 1: Choose Your Free Tool

The industry-standard, open-source tool is **GoPhish**. It's powerful, free, and runs on your own computer or a cheap cloud server.

- **What it does:** Creates realistic phishing email templates, manages target lists, hosts fake login pages, and tracks who clicks or enters data.
- **Get it:** Download from getgophish.com. The documentation is excellent.

Step 2: Define Scope & Goals with the Client

- **Target Group:** Will you test all employees or a specific department (e.g., finance, HR)?
- **Campaign Goal:** Is it a baseline test, or focusing on a specific threat (e.g., Microsoft 365 credential phishing)?

- **Success Metrics:** Define what a "failure" is (Click? Data entry? Reporting?).

Step 3: Gather Target List

The client must provide a list of employee names and work email addresses. Handle this list with the same security and confidentiality as the HIBP data.

Step 4: Craft the Phishing Email & Landing Page

- **Theme:** Use relevant, current lures. Top free templates include:
    1. **"Password Expiry / Security Update"** (Mimics IT, high click rate).
    2. **"New Voicemail / Document Share"** (Uses curiosity).
    3. **"Delivery Notification"** (Generic, time-sensitive).
- **Sending Address:** Use a **lookalike domain** you control (e.g., if client uses @company.co.uk, you could use @company-security.co.uk). Never spoof the client's actual domain.
- **Landing Page:** In GoPhish, create a page that mimics a real login (e.g., Microsoft 365). **Do not collect real credentials.** Instead, upon any data entry, show an **immediate educational message**: *"This was a simulated phishing test. You entered credentials on a fake page. Never enter passwords from an email link. Please contact IT if you have questions."* This turns the failure into a teachable moment.

Part 2: Execution & Monitoring

Step 1: Configure & Launch in GoPhish

1. Import the email list and template.
2. **Set a sending profile** to use a transactional email service like **SendGrid** or **Mailtrap** (both have free tiers). Do **not** send directly from your personal email.
3. **Schedule the campaign** for a typical Tuesday/Wednesday morning. Avoid Mondays or Fridays.
4. Launch and monitor the **real-time dashboard** in GoPhish, which shows opens, clicks, and data submissions.

Step 2: The "Incident Response" Test (Advanced)

Monitor the client's IT helpdesk or a dedicated phishing report email address (e.g., report@company.co.uk). Track how many employees correctly report your simulated phishing email and how quickly IT responds. This tests both user awareness and internal processes.

Part 3: Analysis & Reporting

Step 1: Calculate Key Metrics

- **Click Rate:** (Users who clicked link / Total recipients) * 100
- **Data Entry Rate:** (Users who submitted data / Total recipients) * 100
- **Reporting Rate:** (Users who reported the email / Total recipients) * 100

Step 2: Generate the Report

Integrate findings into your report structure with a dedicated section.

After

Offer to give a Anti-Phishing Training as an addon at a later date.

Finding ID	Title & Risk	Description & Metrics	Remediation Steps
EMAIL-PHISH01	**High Phishing Susceptibility (HIGH)**	The simulation revealed a **XX% click rate** and a **YY% credential submission rate**. This indicates a significant portion of the workforce is vulnerable to real attacks that could lead to account takeover.	1. **Immediate Training:** Deliver the embedded educational content to all users who failed. 2. **Awareness Campaign:** Launch a general security awareness program focused on identifying phishing lures. 3. **Enable Reporting:** Promote and simplify the phishing report button in the email client.

Finding ID	Title & Risk	Description & Metrics	Remediation Steps
EMAIL-PHISH02	**Low Incident Reporting (MEDIUM)**	The simulation had a **ZZ% reporting rate**. This suggests employees either do not recognize phishing or do not know how/dare to report it.	1. **Clear Reporting Process:** Publicize a simple "Report Phishing" process (e.g., a button in Outlook/Gmail). 2. **Positive Reinforcement:** Thank and praise employees who report, even false positives, to build a reporting culture.

Critical Rules for Your Playbook

1. **Ethics First:** This is a **training and measurement tool**, not a "gotcha" for employees. The educational message is mandatory.
2. **Never Phish the Same Group Twice** in quick succession without warning; it breeds resentment.
3. **Data Disposal:** Securely delete all employee email lists from GoPhish and your computer after the campaign.
4. **Executive Exemption:** It is standard practice to **exclude C-level executives** from simulations unless they explicitly opt-in, to avoid undermining trust.

Analysis & Reporting Phase

Risk Assessment & Prioritization

Categorize every finding using this matrix:

Risk Level	Criteria	Example Findings	Remediation Timeline
CRITICAL	Directly enables email spoofing, account takeover, or data breach	• No DMARC record • Admin MFA disabled • Expired TLS certificate • Subdomain takeover vulnerability	**< 24 Hours**
HIGH	Significant weakness that could facilitate an attack	• SPF uses ~all (softfail) • DMARC policy is p=none • TLS 1.0/1.1 enabled • No spam/malware filtering enabled	**< 7 Days**
MEDIUM	Security best practice not followed	• DKIM not configured • No subdomain policy in DMARC • Weak TLS cipher suites • No email retention policy	**< 30 Days**
LOW	Minor configuration issue or informational finding	• Non-revealing but verbose email server banner • Minor subdomain misconfigurations • Non-critical third-party service issues	**Consider fixing**

Report Template Structure

Your final deliverable should follow this outline:

1. **Cover Page:** Client Name, Report Date, Your Company Logo.
2. **Executive Summary (1 page):** Brief overview, total findings by severity, top 3 recommendations.

3. **Detailed Findings:** Use a consistent format for each issue (Finding ID, Title, Risk, Description, Evidence [*paste screenshot from online tool*], Remediation Steps).
4. **Appendices:** Optional for raw command outputs.

Example Report Row

Finding ID	Title & Risk	Affected System	Description (Non-Tech)	Evidence (Screenshot Ref)	Remediation Steps
EMAIL-001	**Missing DMARC Record (CRITICAL)**	example.co.uk	Your domain has no DMARC policy, allowing anyone to send emails pretending to be from your company.	[Link to PowerDMARC screenshot]	

Remediation Priority & Quick Wins

Phase 1: Immediate (First 24-48 Hours)

1. Enable MFA for all admin accounts
2. Fix expired/misconfigured TLS certificates
3. Block legacy authentication protocols
4. Enable basic spam/malware filtering

Phase 2: Short-term (1-2 Weeks)

1. Implement DMARC with p=quarantine policy
2. Strengthen SPF from ~all to -all
3. Enable DKIM for all sending services
4. Configure email retention policies

Phase 3: Medium-term (1 Month)

1. Disable TLS 1.0/1.1, enforce TLS 1.2+

2. Implement Conditional Access policies
3. Set up user security awareness training
4. Configure incident reporting process

Phase 4: Ongoing Maintenance

1. Regular certificate rotation
2. Quarterly security policy reviews
3. Annual phishing simulation tests
4. Bi-annual full security audits

Post-Audit & Follow-Up Phase

1. **Report Delivery & Presentation:** Schedule a 60-minute call to walk the client through the report.
2. **Remediation Support:** Offer 30 days of email support for clarification on your recommendations.
3. **Re-audit Offer:** Propose a follow-up "verification audit" in 60-90 days to check progress (a source of recurring revenue).