

Social engineering: Phishing med Gophish

Linnéa Eklöf, Moa Karlsson, Axel Lieback, Viktor Spoelstra & Sandra Svenningsen

Kurs: Ethical hacking

Kurskod: DI6005

Innehållsförteckning

Bakgrund.....	3
Metodik och experiment	4
Gophish	4
Hemsidan	6
Mejlet.....	7
Resultat	7
Diskussion	8
Jämförelse med tidigare forskning	8
Förbättringar	8
Etik	9
Referenser.....	11
Bilagor	12
Bilaga 1	12
Bilaga 2	12

Bakgrund

Enligt McAlaney och Hills (2020) så lever vi i ett samhälle med mycket interaktion med socio-teknologiskt verktyg vilket innebär en interaktion mellan individer och teknik. Detta har öppnat upp för en annan typ av attack där fokuset skiftar från att utnyttja tekniska svagheter till att istället utnyttja mänskliga individuella svagheter. McAlaney och Hills (2020) menar på att social engineering är ett av de största hoten mot cybersäkerhet eftersom personer inte nödvändigtvis behöver vara tekniskt kunniga för att kunna utföra denna typ av attack då den fokuserar på individ framför teknik. McAlaney och Hills (2020) beskriver i sin rapport att social engineering ofta bygger på heuristik vilket uppmuntrar offren att använd sig av mentala genvägar och därigenom luras till att fatta beslut som de annars inte skulle ha gjort.

Social engineering är en attacktyp som används inom cyberattacker och såsom phising, scareware och bating. Social engineering beskrivs som en metod där man i stället för att utnyttja tekniska svagheter utnyttjar den mänskliga psykologin och människors grundläggande tillit för att få tillgång till känslig information som kan användas i ett senare skede (Stylianou m.fl., 2025). Hur effektiv social engineering är beror på vilka känslor som utnyttjas samt på vilket sätt detta sker. Några av de känslor som vanligen utnyttjas i social engineering attacker är känslor av brådska, nyfikenhet, rädsla och viljan att vara hjälpsam. Cisco (u.å.) förklarar att social engineering attacker ofta fungerar genom att ”hackaren” utger sig för att vara en betrodd organisation eller en betrodd person med koppling till offren för attacken. En av de farligaste konsekvenserna av en social engineering attack är att det oftast bara behövs en eller ett fåtal personer som faller för attacken för att den ska vara effektiv. Om en attack är effektiv avgörs också till stor del av vad målet med attacken var.

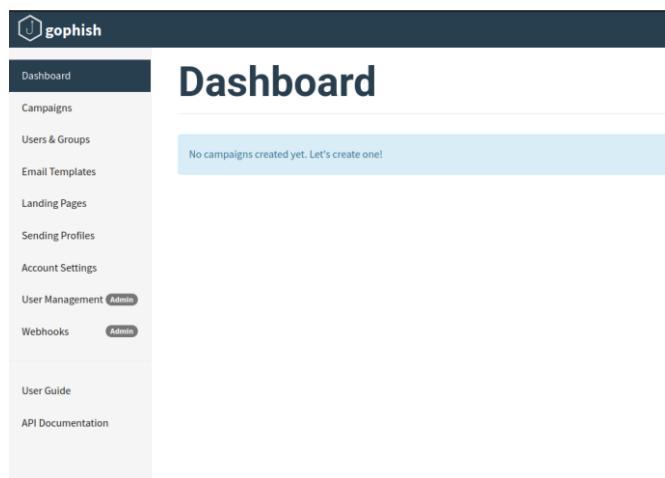
Spoofing innebär att man falsifierar information i ett epostmeddelande, t.ex. avsändaradressen eller avsändarnamnet. Detta för att det ska se ut som om meddelandet kommer från någon annan än den verkliga avsändaren. Det är en social engineering strategi som syftar till att lura mottagaren till att exempelvis öppna ett mejl.

Stylianou m.fl. (2025) beskriver att social engineering som metod till stor del bygger på beslut som fattas undermedvetet hos offren. Social engineering bygger på påverkan och övertalning av offer. Detta sker vanligen genom att påverka det undermedvetna och ändra offrets upplevelse så att de utan kännedom manipuleras till att fatta negativa beslut. Stylianou m.fl. (2025) menar på att skyddet för social engineering attacker bör fokusera på en djupare psykologisk säkerhetsdimension.

Anledningen till att detta experiment valdes var att ta reda på hur lätt det är att falla för denna typ av attack även om man har kunskap om denna typ av attack samt hur social engineering attacker fungerar. Experimentet var också designat för att bättre förstå när personer är mer troliga att falla för en sociala engineering attack. Beu m.fl. (2023) beskriver i sin rapport att just phising mail är en mycket vanlig metod när det kommer till social engineering attacker. Det diskuteras också hur man kan träna individer närmare för att minska risken att en phising attack lyckas. Det som framkommer tydligt i deras rapport är att den vanligaste typen av träning enbart identifierar hur många som klickar på länken jämfört med hur många som rapporterar den. Beu m.fl. (2023) visar också på att ungefär hälften av personerna som får ett phising mail värker klickar på länken eller rapporterar mailet som misstänkt vilket kan innebära en annan typ av säkerhetsrisk.

Metodik och experiment

Gophish



Figur 1: Bild på Gophish-dashboard

Gophish är ett gratis open-source verktyg som används för att enkelt konstruera och simulera phishing-attacker i äkta miljöer, för testa en organisations sårbarhet för phishing. Med Gophish kan man enkelt skicka en attack, så kallad Campaign, som skickar ut phishing-mailen direkt eller vid en viss tidpunkt. Gophish för då även statistik över, bland annat, hur många mail som skickats och öppnats, hur många som klickat på länkar och om användarna fyllt i personlig data.

För att skapa en Campaign behöver man först skapa följande:

- Grupp
- Email Template
- Landing Page

- Sending Profile

En **Grupp** innehåller de användare attacken ska skickas till. Antingen kan man fylla i information för en användare i taget eller så kan man lägga till många åt gången med en .CSV fil. En grupp skapades med namnet Klassen, vilken innehöll studenterna i klassens mejladdresser som fanns att hitta på Blackboard. Vi använde verktyget LM Studio för att på ett smidigt sätt sammanställa dessa adresser i en .CSV fil som därefter kunde användas i Gophish. I LM Studio användes följande prompt:

“Generera e-postadresser genom att kombinera de tre första bokstäverna i förnamnet och de tre första bokstäverna i efternamnet, följt av domänen @student.hh.se.”.

De genererade e-postadresserna sammanställdes därefter i en .CSV fil, vilket sedan används för att skapa gruppen som skulle attackeras i GoPhish.

En **Email Template** bestämmer hur mailet som skickas kommer se ut. Antingen kan man importera ett existerande mail att använda eller så kan man skriva ett eget direkt i Gophish, antingen som vanlig text eller HTML. Det går även att bifoga filer i mailen. För att skapa en Email Template användes ChatGPT med följande prompt:

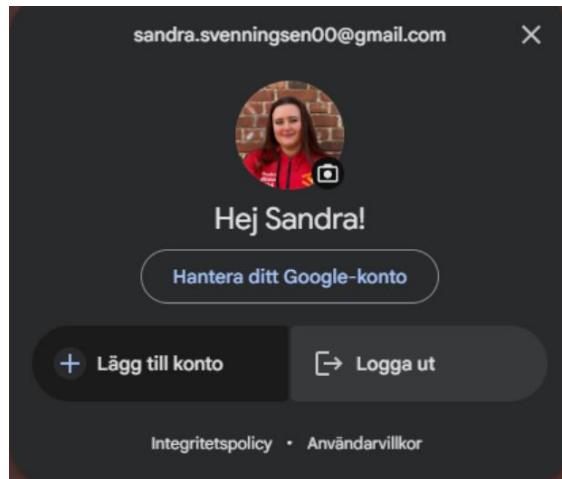
“jag vill bjuda mina klasskamrater på hamburgare på fredag eftersom vi snart tar examen från universitetet. restaurangen är mangold och jag bjuder de första 15 som öppnar en länk i mejlet. kan du fixa en sådan template?”

Den template som genererades finns i bilaga 1.

När en användare klickat på en länk kommer de tas till en **Landing Page**. Det går att designa en egen Landing Page direkt i Gophish eller importera från en existerande webbsida med en URL. Denna sidan kan också spara personlig data som fylls i av användaren. För att starta en Campaign krävs en Landing Page.

I detta experiment skapades en Landing Page i GoPhish, men den Email Template som användes innehöll ingen aktiv länk till denna sida. Istället länkade mejlet till en informationssida som hostades via GitHub (se figur 3). Därmed genererades ingen data avseende öppningar av mejl eller klick på länk kopplade till specifika e-postadresser.

För att skicka ett mejl krävs en **Sending Profile** som beskriver hur mejlet ska skickas. En Sending Profile inkluderar en korrekt mejladress att skicka från, SMTP-serverns adress och port, samt inloggningsuppgifter till denna. Den Sending Profile som användes i GoPhish skulle verka tillhöra Sandra Svenningsen och för att göra kontot så trovärdigt som möjligt användes diverse “reconnaissancestrategier”. På Hitta.se finns information såsom att Sandra är född år 2000, vilket gjorde att “00” lades till på e-postadressen. Sedan lades en profilbild till som hittades via en Googling på namnet, för att göra kontot ytterligare trovärdigt för mottagaren. Det “spoofade” e-mailkontot finns att se i figur 2.



Figur 2: Spoofat Email Konto

När en **Campaign** ska utföras, bifogas de skapade delarna, det vill säga en Email Template, Landing Page, URL till Gophish attack-sidan, tidpunkt mejlen ska skickas, Sending Profile med SMTP konfiguration, samt vilken grupp den ska skicka till. I detta experiment utfördes en Campaigns till gruppen Klassen med den Email Template, Landing Page, GitHub länk och Sending Profile som beskrivs ovan.

Hemsidan

Hemsidor är ett vanligt verktyg i social engineering attacker och brukas av många aktörer som vill komma åt känslig information eller lura individer likaväl företag på kapital (Masada, 2025). En stor anledning till varför hemsidor är så användbara är den lätta åtkomsten för individer på nätet samt den relativ enkelhet som finns att utveckla en hemsida. Många av dessa hemsidor gör försök att vinna förtroendet från individer på nätet för att sedan få dem att göra någon form av interaktion, oftast en nedladdning, för att kunna samla information eller ta över en enhet helt och hållet. Även drive-by nedladdning kan göras här på system med få säkerhetsåtgärder.

Som demonstrerat tidigare så består attacken utav en hemsida som länkas till i mailet som skickades ut av Gophish-kampanjen. Denna hemsida är, i typiska fall, utformad på ett sätt som antingen lockar användaren att klicka eller ladda ner något till enheten. I detta fall länkas en simpel hemsida som visar information om social engineering och resurser om hur man förebygger risken att bli utsatt för en attack i framtiden. I ett verkligt scenario kunde hemsidan i stället varit utformat som exempelvis en virusvarning eller en uppmaning att gå med i en maillista för att sedan skicka fler attackförsök till samma användare.

Detta var ett simulerat phishing-test!

Du har just klickat på en länk i ett träningsmejl som är en del av vårt arbete för att stärka informationssäkerheten, med särskild inriktning på just phishing mejl. Men orör dig inte! Ingå personuppgifter eller känsliga data har innehållts under detta simuleringstest och statistiken som samlas in är helt anonym!

Nedan kan du få tips om viktiga varningstecken på att ett mejl kan vara ett försök till nätfiske, så att du i framtiden kan skydda både dig och din organisation.

Tips för att skydda dig mot phishing:

- Lämna aldrig ut person eller kortuppgifter
- Ha unika lösenord på dina olika tjänster
- Godkänn aldrig att någon fjärrstyr din dator, telefon eller platta
- Var misstänksam när du får mail där du uppmanas att klicka på en länk och lämna känsliga uppgifter.

För mer information, läs vidare på:

- [microsoft - Phishing](#)
- [MSB - Phishing och Skadlig Kod](#)
- [Polisen - Phishing](#)

This website is dedicated to ethical hacking and cybersecurity.

© 2025 Ethical Hacking Project Halmstad
University Di6005

Figur 3: Bild på hemsidan som användes i projektet

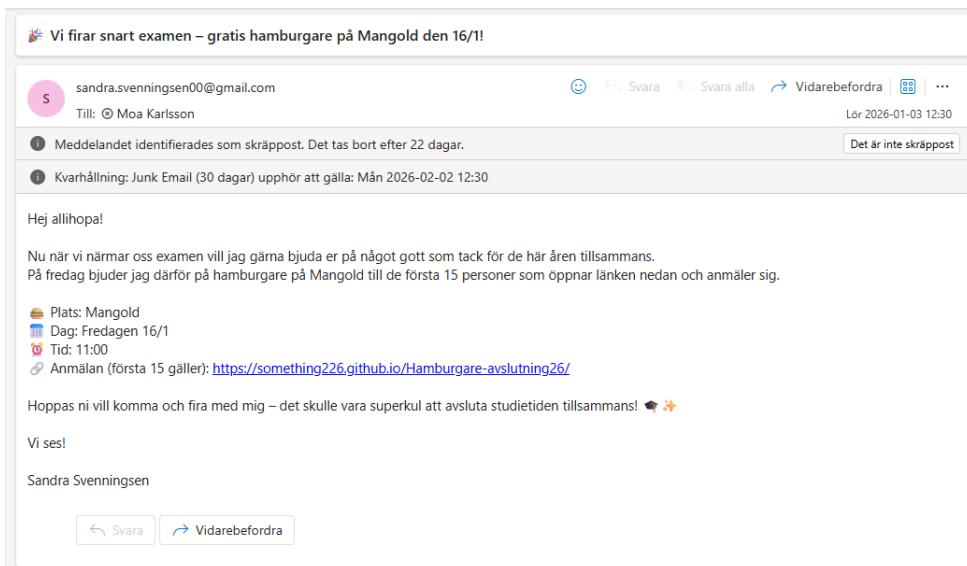
Som visat på figur 3 så är hemsidan väldigt simpel och består enbart av det nödvändigaste i syftet av utbildning i förbyggnning av social engineering, i detta fallet phishing specifikt. Detta är för att inte uppfattas som en potentiellt farlig sida. I hemsidan beskrivs tydligt vad syftet med hemsidan och mejlet var, att det inte utgjorde en faktisk fara för IT-säkerheten hos användaren, samt hur man kan lära sig mer om phishing attacker och skadlig kod på en dator.

Mejlet

I det simulerade phishing mejlet fanns det flera inslag som kunde uppfattas som trovärdiga. Avsändaren utgav sig för att vara en verlig person med koppling till mottagarna, vilket skapar igenkänning och förtroende. Innehållet i mejlet var dessutom situationsanpassat, då det knöt an till den kommande examen vilket är kopplat till mottagarna. Erbjudandet om gratis mat i kombination med ett begränsat antal platser sätter en tidspress på mottagarna vilket är vanligt förekommande i social engineering-attacker och är avsett att stressa mottagaren till att fatta ett snabbt beslut utan att granska innehållet närmare. Det som kunde uppfattas som misstänksamt var det faktum att länken inte gick till en officiell eller välkänd domän samt att mejlet saknade en tydlig koppling till universitetet.

Resultat

Resultatet från den Campaign som riktades mot gruppen Klassen visade att phishingmejlet skickades till samtliga 51 studenters e-postadresser med domänen @student.hh.se, vilket kan ses i Figur 4 nedan. Samtliga mejl levererades men klassificerades som skräppost och placerades automatiskt i mottagarnas skräppostmappar.



Figur 4: Phishingmejlet

Diskussion

Jämförelse med tidigare forskning

Resultatet att samtliga phishing-mejl klassificerades som skräppost kan relateras till tidigare forskning inom e-postsäkerhet och detektion av phishing-mejl. Atawneh (2023) beskriver hur djupinlärningsbaserade modeller kan användas för att klassificera och filtrera e-post baserat på innehållsliga egenskaper i syfte att identifiera potentiellt skadliga meddelanden. Studien visar att sådana modeller med hög träffsäkerhet kan skilja phishing-mejl från legitima meddelanden och därmed placera phishing-liktande mejl i skräppostmappar.

Detta överensstämmer med resultatet i detta arbete, där samtliga phishing-mejl filtrerades bort och placerades i mottagarnas skräppostmappar. En skillnad är dock att filtreringen i detta fall kan ha baserats på avsändarens domän och organisatoriska säkerhetsregler för externa mejl, snarare än en innehållsbaserad analys, vilket skiljer sig från de metoder som beskrivs av Atawneh (2023).

Förbättringar

Studien hade kunnat förbättras genom att använda verktyg som samlar in hur många som öppnat mejlet, utan att visa tillhörande mejladdress. Detta hade gjort en liknande studie etiskt försvarbar och samtidigt bidragit med mer information gällande effektiviteten av själva phishingattacken, såsom hur många som öppnat och klickat på länken.

För att mäta antalet klick på en länk skulle det dessutom kunna registreras via hemsidan som länken leder till. Denna metod är etiskt försvarbar eftersom den endast samlar statistik om

klickningar och inte identifierar enskilda användare. Ingen personlig information såsom namn, e-postadress eller IP-adress sparas, vilket innebär att användarnas integritet inte tar skada.

Attacken mot gruppen Klassen begränsades också av att e-postadresserna tillhörde Högskolan i Halmstads mejldomän (@student.hh.se), eftersom det verkar som att alla mejl som skickas från externa mejldomäner automatiskt placeras i skräppost. Det som tyder på detta är att i en jämförelse med andra mejldomän så tillåter både Gmail, Outlook och Yahoo att mejlet läggs i den vanliga inkorgen. Ur ett säkerhetsperspektiv tyder detta på att @student.hh.se e-postsystem har strikta filter som effektivt minskar risken för phishing och andra spamrelaterade attacker. Dessutom raderas mejl som hamnat i skräpposten efter 30 dagar, vilket ytterligare påverkar effektiviteten av att mejlet skulle öppnas. En förbättring skulle därmed vara att rikta attacken mot en mejl tillhörande en mejldomän som inte har sådana strikta organisatoriska filter, exempelvis Gmail eller Yahoo.

Eti

Det finns flertalet saker att ha i åtanke gällande dem etiska perspektiven inom ethical hacking, speciellt inom social engineering där man oftast lurar användare till att utföra en viss handling. Till en början så innehåller social engineering, som nämnt, att man lurar eller förmår användaren att göra något. Detta kan innehålla en form av kränkning på en individs integritet då man vill utnyttja sårbarheten hos en användares psyke. Vidare så finns även en viss problematik med utnyttjandet av en individs identitet i syfte av att lura användare på deras tillit till personen. Som sidoeffekt kan detta leda till upplevd misstro av människor inblandade i experimentets stund om inte klar kontext är tillagt till attacken i efterhand.

Trots de etiska utmaningarna som kan uppstå vid simulering av phishingattacker valdes experimentet ändå att genomföras. Detta då man i god tid informerade samtliga mottagare om att denna typen av mejl kan komma att skickas ut som en del av kursmomentet. Mottagarna hade därför möjlighet att vara extra uppmärksamma på att sådana typer av simulerade attacker kan förekomma. Vidare innehöll experimentet inget skadligt innehåll då länken i mejlet ledde till en webbplats som informerade kring hur man kan skydda sig mot denna typ av attack. Ingen skadlig kod användes och ingen personlig information samlades in eller lagrades, vilket innehåller att deltagarnas integritet inte påverkades.

Eftersom Gophish-plattformen i stunden av experimentets utförande inte innehöll en landing page var det inte heller möjligt för applikationen att faktiskt utföra något potentiellt säkerhetskränkande till en början. Detta styrker den etiska positionen experimentet har i kontext av datasäkerhet då det var fysiskt omöjligt för programmet att utgöra en risk för användarens egna data eller uppgifter.

Den potentiella risken i experimentet rör individen vars identitet användes som alias i mejlet. Detta skedde dock med personens uttryckliga samtycke och inga uppgifter som kunde skada

personens anseende eller rykte användes. Därmed bedömdes risken för negativ påverkan på förtroendet som låg och kontrollerad. Sammanlagt bedömdes experimentets lärdomar väga tyngre än de identifierade etiska riskerna.

Referenser

Beu, N., Jayatilaka, A., Zahedi, M., Babar, M., Hartley, L., Lewinsmith, W., & Baetu, I. (2023). Falling for phising attempts: An investigation of individual differences that are associated with behavior in a naturalistic phising simulation. *Computers & Security*, 131. Artikel 103313. <https://doi-org.ezproxy.bib.hh.se/10.1016/j.cose.2023.103313>

Cisco (u.å.). *What Is Social Engineering?*. Hämtad 2026-01-09 från <https://www.cisco.com/site/us/en/learn/topics/security/what-is-social-engineering.html>

McAlaney, J., & Hills, P.J. (2020). Understanding Phising Email Processing and Perceived Trustworthiness Though Eye Tracking. *Fronties in Psychology*, 11. Artikel 1756. <https://doi.org/10.3389/fpsyg.2020.01756>

Masada, S. (2025). Microsoft Seizes 338 websites to disrupt rapidly growing ‘RaccoonO365’ phising service. *Microsoft*. Hämtad 2026-01-12 <https://blogs.microsoft.com/on-the-issues/2025/09/16/microsoft-seizes-338-websites-to-disrupt-rapidly-growing-raccoono365-phishing-service/>

Stylianou, I., Bountakas, P., Zarras, A., & Xenakis, C. (2025). Suspicious minds: Psychological techniques correlated with online phishing attacks. *Computers in Human Behavior Reports*, 19. Artikel 100694. <https://doi.org/10.1016/j.chbr.2025.100694>

Atawneh, S., & Aljehani, H. (2023). Phishing Email Detection Model Using Deep Learning. *Electronics*, 12(20), 4261. <https://doi.org/10.3390/electronics12204261>

Bilagor

Bilaga 1

(Genererad Template)

Ämne: 🎉 Vi firar snart examen – gratis hamburgare på Mangold den 16/1!

Hej allihop!

Nu när vi närmar oss examen vill jag gärna bjuda er på något gott som tack för de här åren tillsammans. På fredag bjuder jag därför på hamburgare på Mangold till de första 15 personer som öppnar länken nedan och anmäler sig.

📍 Plats: Mangold

🕒 Dag: Fredag den 16/1

Tid: 11:00

🔗 Anmälan (första 15 gäller): <https://something226.github.io/Hamburgare-avslutning26/>

Hoppas ni vill komma och fira med mig – det skulle vara superkul att avsluta studietiden tillsammans! 🎉 🎉

Vi ses!

Sandra Svenningsen

Bilaga 2

(bild på HTML som användes till hemsidan)

```
You, 3 weeks ago | 1 author (You)
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1.0" />
    <meta name="Description" content="Homepage of the website" />
    <link rel="stylesheet" href="style.css" />
    <title>Home</title>
  </head>
  <!--Website starts here-->
  <body>
    <header class="center">
      <h1>Detta är ett simulerat phishing-test!</h1>
    </header>
    <main>
      <section class="center">
        <p>Du har just klickat på en länk i ett träningsmejl som är en del av vårt arbete för att stärka informationssäkerheten, med särskild inriktning på just phishing mejl. Men oroa dig inte! Nedan kan du få tips om viktiga varningstecken på att ett mejl kan vara ett försök till nätfiske, så att du i framtiden kan skydda både dig och din organisation.</p>
        <h2>Tips för att skydda dig mot phishing:</h2>
        <ul>
          <li>Lämna aldrig ut person eller kortuppgifter</li>
          <li>Ha unika lösenord på dina olika tjänster</li>
          <li>Godkänn aldrig att någon färrstyr din dator, telefon eller platta</li>
          <li>Var misstänksam när du får mail där du uppmanas att klicka på en länk och lämna känsliga uppgifter.</li>
        </ul>
        <h3>För mer information, läs vidare på:</h3>
        <ul>
          <li><a href="https://support.microsoft.com/sv-se/windows/skyddा-dig-mot-n%C3%A4tfiske-0cea947-ha98-3hd9-7184-430e1f860a44" target="_blank" rel="noopener">microsoft - Phishing</a></li>
          <li><a href="https://www.msb.se/sv/rad-till-privatpersoner/digital-sakerhet/nätfiske-och-skadlig-kod/" target="_blank" rel="noopener">MSB - Phishing och Skadlig Kod</a></li>
          <li><a href="https://polisen.se/utsatt-for-brott/polisarbetet/bedrägerier/bedrägerier/nätfiske-phishing/" target="_blank" rel="noopener">Polisen - Phishing</a></li>
        </ul>
      </section>
    </main>
    <footer class="center">
      <p>This website is dedicated to ethical hacking and cybersecurity.</p>
      <p>© 2025 Ethical Hacking Project Halmstad University DI0005</p>
    </footer>
    <script src="script.js"></script>
  </body>
</html>
```