När luras personer av nätfiske?

En genomgång av publicerade fältexperiment

TEODOR SOMMESTAD OCH HENRIK KARLZÉN

FOI-R--4951--SE
ISSN 1650-1942 April 2020

Teodor Sommestad och Henrik Karlzén

När luras personer av nätfiske?

En genomgång av publicerade fältexperiment

Titel	När luras personer av nätfiske? – En genomgång av publicerade fältexperiment
Title	When do people fall for phishing? – A review of published field experiments
Rapportnr/Report no	FOI-R--4951--SE
Månad/Month	April
Utgivningsår/Year	2020
Antal sidor/Pages	22
ISSN	1650-1942
Kund/Customer	Myndigheten för samhällsskydd och beredskap MSB
Forskningsområde	Informationssäkerhet
FoT-område	Inget FoT-område
Projektnr/Project no	B73007
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem

Sammanfattning

Nätfiske är en vanlig ingrediens i moderna datorintrång. Det är bland annat vanligt att angripare använder nätfiske som ett första steg för att komma in på insidan av organisationers brandväggar. Denna rapport sammanfattar resultaten från 48 vetenskapliga publikationer som beskriver fältexperiment där datoranvändare utsatts för nätfiske. Resultaten visar att

- mottagarens personlighet inte är särskilt viktig
- mottagarens kunskap spelar roll
- hur lögnen läggs fram spelar roll
- vad nätfiskaren ber om spelar roll
- att tekniska varningssystem förmodligen spelar stor roll.

Nyckelord: Nätfiske, fältförsök, phishing, datorintrång, cybersäkerhet.

Summary

Phishing is a common ingredient in contemporary computer network attacks. It is, among other things, used by attackers to make the initial compromise and get inside organisations' firewalls. This report summarises the results from 48 peer-reviewed publications describing field experiments where computer users have been subject to phishing. The results show that

- personality is not very important,
- the recipients' knowledge matters,
- it matters how the scam is presented
- what the phisher asks for matters
- technical warning measures probably make a big difference.

Keywords: Phishing, field experiments, computer intrusions, cyber security.

Innehållsförteckning

1 Inledning

Nätfiske används i cirka en tredjedel av alla datorintrång [1] och är även en vanligt förekommande metod hos statsstödda angripare [2]. Nätfiske, eller *phishing* (eng.) som det ofta kallas, kan ses som olika typer av bedrägliga försök att få personer att utföra handlingar genom att skicka elektroniska meddelanden till personerna. Oftast görs nätfiske via e-post.

1.1 Hur går nätfiske till?

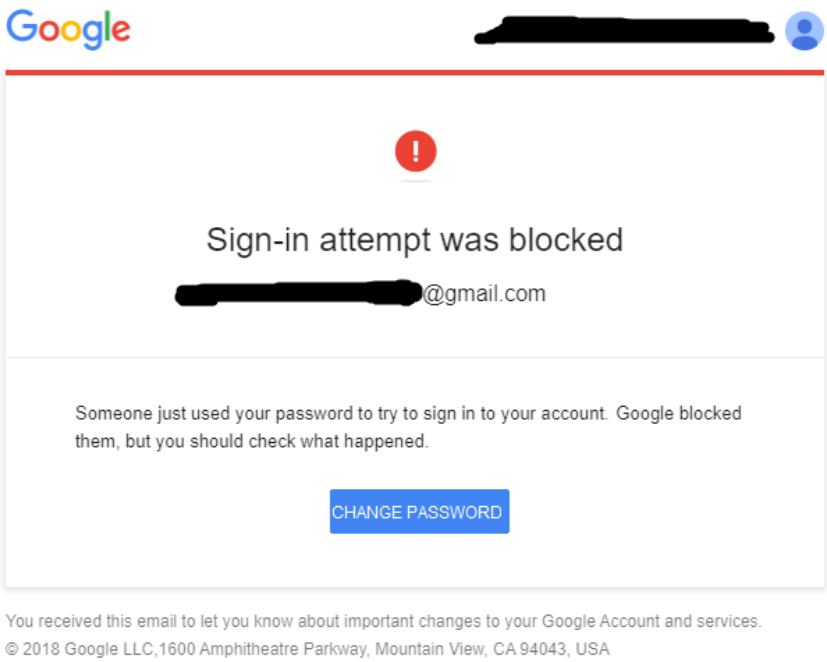
Vid nätfiske via e-post skickar bedragaren först e-post till det tänkta offret. Följande är vanliga tillvägagångssätt som används vid nätfiske:

1. Bedragaren utger sig för att vara personal på en datoranvändares IT-avdelning och ber användaren logga in på en webbsida som på ytan ser ut att vara företagets webbmejl, men i själva verket är en hemsida som sparar användarens användarnamn och lösenord så att bedragaren kan använda dessa senare.
2. Bedragaren utger sig från att jobba på IT-avdelningen eller hos en IT-leverantör och ber användare uppdatera sina datorer genom att köra ett program som laddas ner från en hemsida. Programmet installerar i själva verket en bakdörr på datorn som ger angripare en väg in.
3. Bedragaren bifogar ett intressant kalkylark, t.ex. en offert eller lönelistan för alla inom organisationen, och ber mottagaren titta på det. Kalkylarket kräver att makron aktiveras och när användaren gör så körs kod som öppnar en bakdörr på datorn.

Det finns gott om faktiska exempel på när nätfiske använts, inklusive som del i angrepp som stater tros ligga bakom. Exempelvis användes nätfiske av angripare för att få tag i sekretessbelagd information hos kanadensiska finansdepartementet och den kanadensiska försvarsforskningsorganisationen. Angriparna skickade e-post där de utgav sig för att vara myndighetsanställda och där virusinfekterade filer bifogades som mottagarna lurades att öppna [3]. Detta nätfiske liknande alltså tillvägagångssätt 3 i listan ovan.

Ett annat exempel är då gruppen *Fancy Bear*, som kopplas till Ryssland, skickade bedräglig e-post till en organisation som utför grävande journalistik [4]. Nätfisket i dessa två fall liknade tillvägagångssätt nummer 1 i listan ovan. E-posten som gruppen Fancy Bear skickade såg ut ungefär som i Figur 1 och lurade mottagarna att Google krävde att mottagarna bytte lösenord och att bytet skulle ske genom att klicka på en länk. Mottagare som klickade på länken kom till en webbsida där de lurades uppge sitt nuvarande lösenord (för att kunna byta lösenord). Gruppen använder även de andra tillvägagångssätten. De anklagas exempelvis ha angripit olika länders utrikesdepartement med hjälp av nätfiske

som innehöll Excel-filer med elakartad makro-kod [2], dvs, tillvägagångssätt nummer 3.



Figur 1: Ett exempel på nätfiske som är snarlikt legitim e-post.

1.2 Varför är nätfiske så vanligt?

Nätfiske är vanligt eftersom det fungerar förhållandevis ofta och är enkelt för en angripare att genomföra på flera mål inom en organisation utan att bli upptäckt. Företaget Cofense rapporterar att de i tester lyckats få användare att utföra riskabla saker (t.ex. besöka illegitima hemsidor eller öppna bilagor) i 12 procent av sina 135 miljoner simulerade nätfiskeförsök utförda 2017–2018 [5]. Att nätfiske ofta fungerar är i sig inte konstigt. Meddelandesystem såsom e-post används för att göra legitima förfrågningar lika de som görs i nätfiske. Personer som aldrig trycker på länkar i e-post eller läser dokument de får skickade till sig skulle ha svårt att utföra sina arbeten. Detta medför att det är svårt att hitta kostnadseffektiva åtgärder som stoppar nätfiske.

1.3 Vad påverkar om folk går på nätfiske?

Det finns stor variation i hur ofta olika typer av nätfiske lyckas. Ett experiment riktat mot studenter mätte exempelvis att 37 procent av studenterna föll för ett

nätfiskeförsök som handlade om kursregistrering, samtidigt som endast 0,3 procent av samma grupp studenter föll för ett nätfiskeförsök kopplat till deras kreditkort. Cofense mätningar visar också på stor variation över tid, mellan branscher och mellan olika typer av nätfiske. Deras försök lyckas exempelvis i 15 procent av fallen när de gjordes mot vårdinrättningar, men bara i 5 procent av fallen mot kraftindustrin. Att undersöka vad som påverkar om folk går på nätfiske är ett första steg i att ta fram effektiva skyddsåtgärder mot nätfiske.

Denna rapport beskriver de mest centrala slutsatserna från en genomgång av vetenskapligt publicerade fältförsök där nätfiske utförts. Målet är att ge en rättfram beskrivning av de viktigaste slutsatserna. Den intresserade läsaren kan hitta ytterligare information i forskningsartikeln:

> Sommestad, T., & Karlzén, H. (2019). A meta-analysis of field experiments on phishing susceptibility. In *eCrime Researchers Summit, eCrime 2019*. Pittsburgh, PA, USA: IEEE.

1.4 Vad står i denna rapport?

Resterande del av rapporten är indelad som följer. Kapitel 2 beskriver metoden som användes för att identifiera och analysera fältexperimenten. Kapitel 3 sammanfattar analysen av den statistik som presenterats i fältexperimenten. Innehållet i denna sammanfattning är med avsikt förenklat och kategoriskt. Syftet är att lyfta fram de mer centrala slutsatserna från genomgången, inte att ge en fullständig beskrivning av alla om-och-men. Kapitel 4 försöker ge svar på utvalda frågor som läsaren kan tänkas ha efter att ha läst kapitel 3.

2 Genomgången

Genomgången var en så kallade metaanalys som sammanställer kvantitativa resultat från redan genomförda studier som beskrivits i forskningsartiklar. Nedan beskrivs vilka typer av studier som de kvantitativa resultaten hämtats från och hur de analyserats.

2.1 Studier som analyserats

Som nämnts i kapitel 1 är nätfiske ett reellt och stort problem. Det är också något många forskare studerat. Forskningen kan grovt delas in i fyra typer:

1. Tekniska lösningar som exempelvis försöker identifiera nätfiskemeddelanden automatiskt baserat på innehåll eller struktur.
2. Observationsstudier som exempelvis frågar datoranvändare eller organisationer om deras erfarenheter kring nätfiske.
3. Labbförsök där deltagare exempelvis får försöka skilja mellan fiktiva legitima meddelanden och nätfiskemeddelanden.
4. Fältförsök där deltagare exempelvis får simulerade nätfiskeförsök skickade till sig i deras vanliga IT-miljö.

Denna genomgång är avgränsad till den fjärde typen av forskning – fältförsök. Nackdelen med fältförsök är att det är svårt för forskare att kontrollera alla variabler som kan påverka mottagligheten. Exempelvis kanske vissa försökspersoner inte läser sin e-post eller skyddas av spamfilter. Det finns därmed risk för olika typer av bias och feltolkningar. Fältförsök har samtidigt fördelen att de mäter hur mottagliga personer är under realistiska förhållanden och kan därmed ge bra indikation på hur viktiga olika variabler är i praktiken.

Totalt identifierades 48 artiklar som innehöll kvantitativa data från nätfiskeförsök utförda i fält och med hjälp av e-post. Flera av artiklarna beskrev mer än en studie. Av exkluderade artiklar kan det noteras att endast tre studier med andra meddelandeformat (t.ex. via Twitter) identifierades. Det kan också noteras att det identifierades ungefär femtio labbförsök, femtio observationsstudier och ett mycket större antal studier på tekniska lösningar.

2.2 Data som analyserats

Även om alla inkluderade studier handlar om samma sak – nätfiske via e-post – finns betydande skillnader i hur de utförts. För att kunna analysera hur dessa skillnader påverkar resultaten noterades

1) om studien utförts på studenter
2) om mottagaren borde lita på avsändaren
3) om meddelandet var anpassat till mottagaren på något sätt

4) vad meddelandet försökte få mottagaren att göra
5) om mottagaren fått någon särskild träning.

Totalt klassificerades 39 studier som totalt innehöll 145 mätningar av hur stor andel av mottagarna som lurades i försöket. Merparten av försöken utfördes på studenter, låtsades komma från en person mottagaren borde lita på, hade anpassat meddelandet till mottagaren på något sätt, försökte lura mottagaren att trycka på en länk och hade gett mottagaren någon form av träning.

Utöver rena mätningar av mottaglighet under olika förutsättningar fanns statistiska tester på huruvida olika variabler påverkar mottagligheten. Exempelvis fanns flera sätt att rapportera kopplingar mellan mottaglighet och kön och flera sätt att beskriva variabler kopplade till säkerhetsmedvetande. Totalt kategoriserades 144 statistiska tester. De allra flesta (78 procent) handlade om egenskaper hos mottagaren såsom personlighet.

Sist men inte minst identifierades de fall där forskare gjort flera liknande tester för samma grupp mottagare för att under experimentlika förhållanden se hur en enskild variabel påverkar mottagligheten. Även dessa fall grupperades. Exempelvis identifierades 11 fall då forskare skickat liknande nätfiskemeddelanden till både personer som fått nätfiskeutbildning och de som inte fått nätfiskeutbildning för att mäta om mottagligheten minskade tack vare utbildningen.

3 Variabler som påverkar om en person går på nätfiske

Nedan sammanfattas hur olika typer av variabler hänger ihop med mottagligheten, dvs. sannolikheten att en person ”går på” innehållet i nätfiskemeddelandet och följer uppmaningen. Innehållet i kapitlet kan sammanfattas med att

- mottagarens personlighet inte är så viktig
- mottagarens kunskap spelar roll
- hur lögnen läggs fram spelar roll
- vad nätfiskaren ber om spelar roll
- tekniska varningssystem förmodligen spelar stor roll.

3.1 Mottagarens personlighet

Många etablerade teorier om bedrägeri, som *interpersonal deception theory* [6], säger att personer har olika stor benägenhet att lita på andra och att detta är något som spelar roll vid bedrägerier. Det är också lätt att föreställa sig hur personer med en godtrogen och hjälpsam inställning oftare faller för uppmaningar i nätfiske än skeptiska och ohjälpsamma personer. Många av studierna har undersökt just detta.

Av de studier som undersökt om mottagligheten hänger ihop med personers benägenhet att lita på andra eller deras hjälpsamhet har bara en tredjedel av studierna hittat en statistiskt säkerställd koppling. Överlag visar endast en fjärdedel av studierna som berör personlighet på en koppling till mottaglighet. Ingen studie som berör nationell kultur hittade heller någon koppling. Personlighet och inställning hos den som mottar ett nätfiskemeddelande har alltså begränsad betydelse för hur personen agerar. Om det finns generella mönster så överskuggas dessa i så fall av annat som är viktigare i studierna.

3.2 Mottagarens kunskap

Ett vanligt sätt att hantera riskerna med nätfiske är att utbilda och informera sin personal om exempelvis säkerhet och bra beteende. Resultaten från studierna visar också på att det finns skäl att göra så.

Personer som informerats om nätfiske (och därmed tränats) går på mindre än hälften så många nätfiskeförsök som personer som inte informerats. Den information som getts i studierna är relativt enkel och består exempelvis av instruktioner som tar femton minuter att ta till sig. Många studier visar även på samband mellan mottagligheten och mottagarnas självuppskattade

säkerhetskunskap, utbildningsnivå och datorvana. Det finns samtidigt en stor variation i resultaten. En studie [7] uppmätte faktiskt större benägenhet att gå på nätfiskemeddelanden som skickades efter träningen och i ett fall [8] gick de med hög självskattad säkerhetskunskap på fler nätfiskemeddelanden än andra.

Det bör noteras att det i allmänhet är svårt för människor att identifiera lögner och att experter bara är marginellt (några procentenheter) bättre än lekmän på lögndetektion [9]. Om nätfiske ses som en typ av lögn pekar detta på begränsad nytta med utbildning och att det hjälper föga att vara expert på att känna igen nätfiske. Resultaten pekar dock på att det är bra att ha vissa grundkunskaper om riskerna.

3.3 Lögnen i meddelandet

Det råder ingen tvekan om att olika varianter av nätfiskemeddelanden är olika framgångsrika. Överlag tycks innehåll som är intressanta, relevanta och rimliga för mottagaren hänga ihop med betydligt högre sannolikhet att mottagaren går på nätfisket. Exemplet som gavs i avsnitt 1.3 är ett bra exempel på detta: 37 procent av studenterna gick på nätfiske om deras kursregistrering medan endast 0,3 procent gick på ett generiskt nätfiske kopplat till kreditkort. Det finns gott om liknande i exempel bland studierna. När samma population utsatts för flera meddelanden under liknande förutsättningar lurar de mer framgångsrika bedrägerierna i snitt sex gånger så många som de mindre framgångsrika.

Det verkar samtidigt vara svårt att på förhand gissa vilka typer av lurendrejerier som kommer att vara framgångsrika och i många av studierna saknar forskarna hypoteser om varför ett meddelande ska fungera bättre än ett annat. I de fall innehållet i meddelandet studerades undersöktes istället främst

- om innehållet anpassats för mottagaren, t.ex. genom att ha en personlig hälsningsfras
- om en etablerad teknik för bedrägerier använts, t.ex. att avsändaren utger sig för att vara en auktoritet inom organisationen
- om innehållet är rikt formulerat eller utbroderat, t.ex. med HTML-innehåll, bra förklaringar och bilder.

I snitt luras 50 procent fler om innehållet anpassats efter mottagaren eller organisationen på något sätt. Det finns viss spridning i dessa resultat som förmodligen förklaras med att anpassningen gör innehållet märkligt och att mottagaren på så sätt avslöjar bluffen. Ett meddelande som utger sig komma från en fiktiv person i mottagarens del av organisationen kan exempelvis avslöjas som bluff om mottagaren känner till att ingen person med det namnet jobbar där. Det ska också noteras att det inte tycks spela någon roll om nätfiskemeddelandet faktiskt kommer från en betrodd e-postadress (exempelvis en intern adress).

Meddelanden som använder en etablerad teknik för bedrägerier, exempelvis genom att påstå att ”alla andra” gör det som efterfrågas, lyckas mer än dubbelt så ofta som de som inte använder någon sådan teknik.

Rikt formulerad text har nått blandade resultat. I två av tre försök innebär rikare innehåll att fler går på nätfiskemeddelandet.

3.4 Vad som begärs

Nätfiskemeddelanden försöker få mottagaren att göra riskabla saker på sina datorer. Studierna som sammanfattas i denna rapport försökte oftast få användare att besöka en webbsida som inte var legitim. I snitt klickade 24 procent av alla mottagare på länken och besökte webbsidan. Ofta mättes också hur mottagare som klickat på länken agerade när sidan öppnats. I de flesta fall utgjorde webbsidan en fejkad inloggning och det mättes om mottagaren där matade in ett användarnamn och lösenord. Hela 21 procent av de som får e-post om sådant som kontoverifiering eller inloggning uppgav inloggningsuppgifter genom att knappa in dem på den fejkade webbsidan. I de tre fall samma forskare mätt både hur många som klickar på en länk och hur ofta de uppger ett lösenord är det i snitt 23 procent som klickat på länken och 16 procent som uppgett ett lösenord.

I andra studier uppmanades användare uppge känslig information som inte var lösenord till existerande IT-system. Det presenterades exempelvis formulär där mottagaren skulle skapa ett nytt konto genom att ange personuppgifter och välja ett (eventuellt återanvänt) lösenord till en ny webbtjänst. I snitt uppgav 19 procent av mottagarna sådan känslig information.

Att uppge lösenord eller känsliga personuppgifter är inte bra, men att själv köra angripares kod på sin egen dator är i de flesta fall ännu värre ur ett säkerhetsperspektiv. Tolv försök har gjorts där användare skickades bilaga eller en länk till en exekverbar fil. Endast 2 procent av mottagarna exekverade binärfiler (exe-filer) medan 6 procent körde kod som kom i form av makron inbakade i Office-filer. Det är alltså betydligt lättare att få en mottagare att ge bort sitt lösenord än det är att få mottagaren att köra godtycklig kod på sin dator. Både vad gäller lösenord och personuppgifter bör det dock noteras att studierna sällan kontrollerar att lösenorden och uppgifterna faktiskt är korrekta, snarare än textsträngar användare skriver in för att exempelvis testa webbsidan.

3.5 Tekniska skyddssystem

Det finns hundratals tekniska lösningsförslag och ett stort antal studier av tekniska lösningar som syftar till att minska sannolikheten för nätfiske. Få av lösningarna har dock studerats i experiment där människor använder de tekniska lösningarna. En enda studie [10] hittades där en teknisk lösning användes i ett fältförsök. Denna enda studie undersökte ett system som varnade om användaren

besökte en sida som få andra besökt och lyckades med detta medel få ner sannolikheten att personer blev lurade med 70 procent.

Att dra slutsatser utifrån en enskild studie är vanskligt, men det finns många andra skäl att tro att tekniska skyddssystem har god effekt. Att exekvera en fil är ofta förknippat med fler varningsfönster än att besöka webbsidor och eftersom väldigt få användare valde att köra filer jämfört med att besöka webbsidor är det rimlig att tro att det är varningarna som gjorde skillnaden. Laboratorieförsök visar också på tydliga resultat i linje med detta. Som exempel finns ett försök med varningar där försökspersoner fick reda på att deras sätt att handla på webben studerades och forskarna uppmätte att 79 procent av användarna följde varningar om nätfiske kopplat till näthandel [11].

4 Frågor och svar

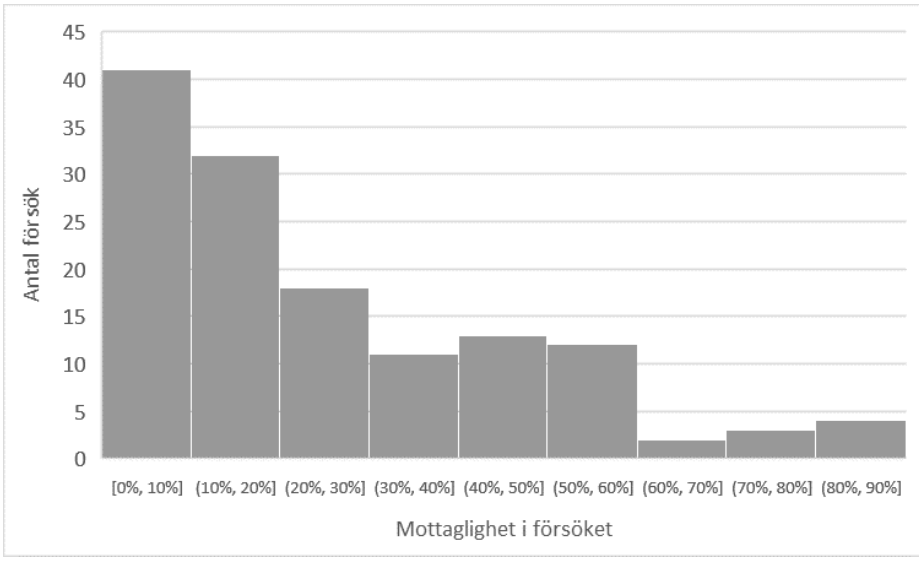
Nedan ges svar på frågor som författarna gissar att läsaren har efter att ha läst kapitel 3.

4.1 Är jag en person som kan gå på nätfiske?

Ja, det tror vi. Du som tagit dig mödan att läsa hela vägen hit i denna rapport är förmodligen inte den mest lättlurade eftersom du har god kunskap om riskerna. Det finns dock inga studier som visar på att det alltid är samma personer som går på olika nätfiskeförsök och det finns inte heller några skäl att tro att vissa är helt immuna mot lurendrejerier. Forskarnas svårigheter att få entydiga resultat angående personlighet, kunskap och utbildningsnivå indikerar snarare att mottagligheten också beror på slump och tillfälligheter. Exempelvis kan det påverka om meddelandet verkar rimligt givet den kontext du befinner dig i när du får det.

4.2 Hur många brukar gå på nätfiske?

I de studier som kartlagts i denna rapport framgår att det finns stor spridning i hur många som går på (påhittat) nätfiske i fältförsök. Mottagligheten för nätfiske illustreras i Figur 2. I de allra flesta studier ligger mottagligheten på 0–60 procent. Om siffror från större studier vägs tyngre – vilket är rimligt eftersom sådana studier i regel är mer tillförlitliga – ges ett viktat medeltal på 21 procent. Det bör dock nämnas att fältförsök och deras resultat inte nödvändigtvis motsvarar mottagligheten för de nätfiskeförsök du kan utsättas för i vardagen. Under fältförsök kan exempelvis meddelandena vara välkonstruerade jämfört med det typiska nätfiskemeddelandet som skickas på internet.



Figur 2: Antalet studier med olika mottaglighet för nätfiskemeddelanden.

4.3 Vad ska vi göra för att minska risken kopplad till nätfiske?

Det är inte ordentligt klarlagt vad de bästa åtgärderna är för att minska sannolikheten att anställda går på nätfiske eller minska konsekvenserna av lyckat nätfiske. Exempel på åtgärder som föreslagits av andra är:

a) **Öka kunskapen om nätfiske.**
Vissa anser att utbildning i hur man känner igen nätfiske är den viktigaste åtgärden som kan göras [12]. På så vis blir det svårare för angripare att komma igenom nålsögat.

b) **Tekniska skydds- och varningssystem.**
Antivirusmjukvara, inbyggda skydd i webbläsare och filter i brandväggar är exempel på tekniska lösningar som föreslås [12][13][14].

c) **Inte skicka legitim e-post som liknar nätfiske.**
Detta för att göra det enklare att känna igen sådant som kan vara elakartat [14]. Vissa banker försöker exempelvis vara tydliga med att de aldrig efterfrågar sina kunders kreditkortsnummer eller personuppgifter via e-post.

d) **Autentisera e-postservrar och avsändare.**
Exempelvis rekommenderas protokoll som S/MIME eller DKIM för att säkerställa att angiven avsändare är korrekt [12][13].

e) **Använd unika lösenord samt tvåfaktorautentisering.**
Att inte återanvända lösenord i flera system eller applikationer gör varje

lösenordsläcka mindre allvarlig [14][12]. Av samma skäl finns fördelar med att komplettera lösenord med exempelvis en fysisk inloggningsdosa som inte kan delas elektroniskt [12][13][14].

f) **Ha rutiner för incidenthantering.**
I stort sett alla kan drabbas av nätfiske. Rekommendationen är att ha rutiner kring backup och rapportering till berörda myndigheter, antinätfiskeorganisationer och kunder [12].

I vår genomgång har vi framförallt hittat stöd för att öka kunskapen om nätfiske, använda tekniska skydds- och varningssystem och att inte skicka e-post som är lik nätfiske. De andra åtgärderna har inte prövats i fältstudierna.

4.4 Hur är det med … som jag hört är viktigt?

Beskrivningen som gavs i kapitel 3 var avgränsad till sådant som uttryckligen studerats. Det kan såklart finnas variabler utöver dessa som är av betydelse. Om någon variabel inte tagits upp ovan beror det alltså på att det saknas kvantitativa data från fältstudier som visar hur viktig den variabeln är – inte att variabeln kan avfärdas som irrelevant. Exempelvis är det tänkbart att tiden på dagen eller när på året nätfiskemeddelandet skickas spelar roll. Det finns också diverse indikationer på att det är så, men ingen som explicit studerat det.

Det finns också flera skäl att tro att variabler samspelar på sätt som inte kontrollerats i studierna. En kvalitativ analys i samband med en av studierna beskriver hur de som hade ett missat telefonsamtal oftare gick på nätfiske om ett missat telefonsamtal [15]. Det finns också studier som indikerar att de som sällan läser legitima e-postmeddelanden inte heller faller för nätfiske så ofta [16], men sådana orsakssamband är uppenbara och kräver inte studier för att fastslå.

4.5 Varför finns så få studier som undersökt hur miljön påverkar?

Att systematiskt undersöka hur miljön påverkar är svårt eftersom det finns så många potentiellt påverkande variabler att hålla reda på. En variabel som i enstaka fall undersökts är hur mycket e-post försökspersonerna får. Å ena sidan kan det tänkas att ju mer e-post någon får desto mer e-post ignoreras mer eller mindre helt utan att läsas, vilket i sin tur minskar mottagligheten för nätfiske. Å andra sidan kan det istället tänkas att ju mer e-post desto stressigare situation, vilket i sin tur ökar mottagligheten för nätfiske eftersom stressen gör det svårare att ta genomtänkta beslut och kontrollera varningssignaler.

En annan aspekt med att inte kontrollera allt med miljön är att den i praktiken (verkligheten) kommer att skilja sig åt på flera punkter mellan olika personer och

organisationer. Forskning försöker sällan detaljstudera varje liten variabel som kan påverkar situationen utan att kartlägga de mer allmänna tendenserna.

4.6 Kan man lita på dessa resultat?

Resultaten som beskrevs i förra kapitlet är baserade på 48 akademiska studier. Att lägga samman resultaten från så många studier ger en god bild av hur det ligger till. Samtidigt finns det förhållandevis stora skillnader bland de 48 studierna. Skillnaderna indikerar att de slutsatser som dras trots allt måste tas med en nypa salt – det finns många okontrollerade variabler som kan påverka resultat. Till exempel kontrollerade få studier om e-post lästes, eller ens kom fram. Andra exempel på bristande metodik är att:

- Mer än en tredjedel kan ha dubbelräknat försökspersoner som klickat på länkar flera gånger.
- Nästan en tredjedel av studierna saknar uttryckliga hypoteser som beskriver vad som studerats.
- Bara en femtedel utförde pilottester för att trimma in och validera sina metoder.
- Ibland designades inte försöken så att det fanns tydliga jämförelsevärden i form av kontrollgrupper eller liknande.

Det finns flera möjliga anledningar till varför studierna har dessa brister. En möjlig förklaring är att forskarna visserligen använt en genomtänkt metod, men utelämnat att beskriva den i sina artiklar. En annan är att man slarvat eller kompromissat med kvaliteten. Ibland verkar också anledningen vara att de organisationer som varit inblandade styrt utformningen av studierna. Exempelvis beskriver [7] en studie baserad på data från en organisations egna mätningar som inte var gjorda som ett väldesignat experiment.

4.7 Är det inte oetiskt att forska om nätfiske?

I den svenska lagen om etikprövning av forskning som avser människor (2003:460) står det:

> *”Forskning får godkännas bara om de risker som den kan medföra för forskningspersoners hälsa, säkerhet och personliga integritet uppvägs av dess vetenskapliga värde.”*

Att använda människor som försökspersoner i studier kan vara problematiskt, särskilt när man försöker lura dem. Den problematiken är något som diskuteras i över 80 procent av studierna och som hanterats lite olika. Exempelvis har

- cirka en tredjedel av studierna inhämtat godkännande från en formell instans
- en tiondel av studierna inhämtat samtycke från studiens deltagare
- drygt en tiondel av studierna nämnt juridiska aspekter
- omkring en tredjedel av studierna i efterhand informerat försökspersonerna och gett möjlighet till att ta del av mer detaljer
- en knapp femtedel anammat forskares etiska vägledningar för nätfiskestudier.

Att alla inte gör alla punkterna ovan är inte konstigt då det varierar vilka godkännanden som krävs i olika delar av världen och vilka risker som försökspersonerna utsätts för. Det finns även olika åsikter om vad som är mest etiskt. Vissa menar exempelvis att forskare *inte* bör informera deltagarna efter ett nätfiskeförsök eftersom det inte för något positivt med sig och att vissa till och med blir upprörda av att få veta att de blivit lurade [17]. Det är alltså inte så pass oetiskt att forska om detta att det är förbjudet, men det inte heller allmänt överenskommet hur forskningen ska bedrivas för att vara så etisk som möjligt.

5 Referenser

[1] Verizon RISK Team et al, “2019 Data Breach Investigations Report,” 2019.

[2] H. Karlzén, “Cyberoperationers attribution, tillvägagångsätt och sofistikation (FOI-R--4834--SE),” Linköping, 2020.

[3] G. Weston, “Foreign hackers attack Canadian government,” *CBC*, 16-Feb-2011.

[4] Threatconnect research team, “Fancy Bear Pens the Worst Blog Posts Ever,” 2017. [Online]. Available: https://threatconnect.com/blog/fancy-bear-leverages-blogspot/.

[5] Cofense, “The state of phishing defence,” 2018.

[6] D. B. Buller and J. K. Burgoon, “Interpersonal deception theory,” *Commun. Theory*, vol. 6, no. 3, pp. 203–242, 1996.

[7] H. Siadati, S. Palka, A. Siegel, and D. McCoy, “Measuring the effectiveness of embedded phishing exercises,” in *Proceedings of the 10th USENIX Conference on Cyber Security Experimentation and Test*, 2017, pp. 1–8.

[8] A. Diaz, A. T. Sherman, and A. Joshi, “Phishing in an academic community: A study of user susceptibility and behavior,” *Cryptologia*, vol. 44, no. 1, pp. 53–67, Jan. 2020.

[9] C. F. Bond, Jr. and B. M. DePaulo, “Accuracy of Deception Judgments,” *Personal. Soc. Psychol. Rev.*, vol. 10, no. 3, pp. 214–234, 2006.

[10] W. Yang, J. Chen, A. Xiong, R. W. Proctor, and N. Li, “Effectiveness of a phishing warning in field settings,” in *ACM International Conference Proceeding Series*, 2015, vol. 21-22-Apri, pp. 1–2.

[11] S. Egelman, L. F. Cranor, and J. Hong, “You’ve been warned: An empirical study of the effectiveness of web browser phishing warnings,” *Conf. Hum. Factors Comput. Syst. - Proc.*, pp. 1065–1074, 2008.

[12] J. A. Chaudhry, S. A. Chaudhry, and R. G. Rittenhouse, “Phishing attacks and defenses,” *Int. J. Secur. its Appl.*, vol. 10, no. 1, pp. 247–256, 2016.

[13] Z. Ramzan, “Phishing Attacks and Countermeasures,” in *Handbook of Information and Communication Security*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 433–448.

[14] R. J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, Second edi. Wiley, 2008.

[15] K. Greene, M. Steves, M. Theofanos, and J. Kostick, “User Context: An Explanatory Variable in Phishing Susceptibility,” in *Proceedings 2018 Workshop on Usable Security*, 2018, no. February, pp. 1–14.

[16] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong, “Lessons

from a real world evaluation of anti-phishing training," in *eCrime Researchers Summit, eCrime 2008*, 2008.

[17] P. Finn and M. Jakobsson, "Designing ethical phishing experiments," *IEEE Technol. Soc. Mag.*, vol. 26, no. 1, pp. 46–58, 2007.

Sammanfattning

Nätfiske är en vanlig ingrediens i moderna datorintrång. Det är bland annat vanligt att angripare använder nätfiske som ett första steg för att komma in på insidan av organisationers brandväggar. Denna rapport sammanfattar resultaten från 48 vetenskapliga publikationer som beskriver fältexperiment där datoranvändare utsatts för nätfiske. Resultaten visar att

- mottagarens personlighet inte är särskilt viktig
- mottagarens kunskap spelar roll
- hur lögnen läggs fram spelar roll
- vad nätfiskaren ber om spelar roll
- att tekniska varningssystem förmodligen spelar stor roll.

Nyckelord: Nätfiske, fältförsök, phishing, datorintrång, cybersäkerhet.

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se