Lecția 4: Ingineria socială și factorul uman

Tema: Software malițios și inginerie socială **Universitatea Tehnică a Moldovei Lector:** Maxim Masiutin, Asistent universitar

Introducere

Bine ați revenit. În lecția anterioară, am explorat lumea tehnică a software-ului malițios. Astăzi, ne îndreptăm atenția către ceea ce profesioniștii în securitate numesc adesea veriga cea mai slabă din orice sistem de securitate: elementul uman.

Ingineria socială este arta de a manipula oamenii pentru a efectua acțiuni sau a divulga informații confidențiale. În timp ce atacurile tehnice exploatează vulnerabilitățile software, ingineria socială exploatează psihologia umană. Și, după cum se dovedește, psihologia umană are multe vulnerabilități care nu pot fi remediate prin actualizări de software.

Statisticile sunt îngrijorătoare. Conform Raportului Verizon privind investigarea breșelor de date din 2025, elementul uman este implicat în aproximativ 60% din toate breșele de securitate. Centrul FBI pentru plângeri privind criminalitatea pe internet a raportat 859.532 de plângeri în 2024, cu pierderi totale de 16,6 miliarde de dolari, o creștere de 33% față de anul precedent.

Poate cel mai alarmant: conform cercetărilor KnowBe4, un furnizor de instruire în conștientizarea securității, e-mailurile de phishing generate de IA au acum o rată de click de 54%, depășind cu mult rata de click de 12% a tentativelor de phishing create de oameni. Combinația dintre inteligența artificială și ingineria socială creează amenințări de o sofisticare fără precedent.

Să explorăm cum funcționează aceste atacuri și cum ne putem apăra împotriva lor.

Partea 1: Psihologia ingineriei sociale

Ingineria socială reușește deoarece exploatează aspecte fundamentale ale psihologiei umane. Înțelegerea acestor principii ne ajută să recunoaștem și să rezistăm manipulării.

Principiile influenței

Psihologul Robert Cialdini a identificat șase principii ale influenței pe care inginerii sociali le exploatează în mod curent:

1. Reciprocitatea

Oamenii se simt obligați să returneze favorurile. Dacă cineva face ceva pentru noi, ne simțim constrânși să facem ceva în schimb.

Exemplu de atac: Un atacator care se dă drept suport IT "ajută" un angajat cu o problemă falsă, apoi cere parola acestuia ca parte a "soluției". Angajatul se simte obligat să se conformeze după ce a primit "ajutor".

2. Angajament și consecvență

Odată ce ne angajăm în ceva, tindem să ducem la bun sfârșit pentru a părea consecvenți.

Exemplu de atac: Un atacator obține mai întâi un angajament mic ("Puteți confirma că lucrați în departamentul de contabilitate?"), apoi escaladează ("Deoarece sunteți în contabilitate, puteți aproba acest transfer urgent, nu-i așa?").

3. Dovada socială

Ne uităm la acțiunile altora pentru a determina comportamentul corect, mai ales în situații incerte.

Exemplu de atac: "Toți ceilalți din departamentul dumneavoastră și-au actualizat deja parolele folosind acest link. Sunteți ultimul."

4. Autoritatea

Tindem să ne conformăm solicitărilor din partea figurilor de autoritate sau a celor care par să aibă autoritate.

Exemplu de atac: Un e-mail care pare a veni de la CEO solicită acțiune imediată. Angajații ezită să pună sub semnul întrebării autoritatea, mai ales sub presiunea timpului.

5. Simpatia

Suntem mai predispuși să ne conformăm solicitărilor din partea persoanelor care ne plac sau pe care le găsim atractive.

Exemplu de atac: Atacatorii construiesc relații de încredere prin conversații prietenoase înainte de a face cereri. Aceștia pot cerceta țintele pentru a găsi interese comune.

6. Raritatea

Apreciem mai mult lucrurile atunci când sunt rare sau disponibile pentru o perioadă limitată de timp.

Exemplu de atac: "Această actualizare de securitate este disponibilă doar în următoarele 30 de minute, înainte ca contul dumneavoastră să fie suspendat." Presiunea timpului împiedică analiza atentă.

Factori psihologici suplimentari

Frica și urgența

Frica declanșează răspunsul nostru de luptă sau fugă, care reduce gândirea analitică. Solicitările urgente exploatează acest lucru cerând acțiune imediată.

"Contul dumneavoastră a fost compromis! Faceți clic aici imediat pentru a-l securiza sau veți pierde toate datele!"

Curiozitatea

Oamenii sunt în mod natural curioși. Vrem să vedem ce se ascunde dincolo de cortină.

"Nu veți crede ce a spus colegul dumneavoastră despre dumneavoastră în acest video..."

Lăcomia

Promisiunea de a primi ceva pe nimic apelează la dorința noastră de câștig.

"Ați câștigat un iPhone gratuit! Introduceți doar datele dumneavoastră pentru a-l revendica."

Dorința de a ajuta

Majoritatea oamenilor doresc să fie de ajutor. Atacatorii exploatează acest lucru cerând "doar o mică favoare".

"Am fost blocat din contul meu și chiar trebuie să trimit acest raport șefului. Puteți doar să vă autentificați pentru mine rapid?"

Partea 2: Atacuri de phishing

Phishing-ul este cea mai comună formă de inginerie socială, folosind mesaje înșelătoare pentru a păcăli destinatarii să dezvăluie informații sau să întreprindă acțiuni dăunătoare.

Phishing prin e-mail

Phishing-ul tradițional folosește e-mailuri în masă care se dau drept organizații legitime:

- Bănci care solicită verificarea contului
- Furnizori de servicii care avertizează despre suspendarea contului
- Companii de curierat cu notificări de expediere
- Departamente IT care solicită resetarea parolelor

APWG (Anti-Phishing Working Group), o coaliție internațională a industriei și a forțelor de ordine, a înregistrat peste un milion de atacuri de phishing în T1 2025, cel mai mare total trimestrial de la sfârșitul anului 2023.

Caracteristicile e-mailurilor de phishing:

- Sentiment de urgență
- Salutări generice ("Stimate Client")
- Adrese de expeditor suspecte
- Greșeli de gramatică sau ortografie (deși IA elimină acest indicator)
- URL-uri nepotrivite sau suspecte
- Solicitări de informații sensibile

Spear Phishing

Spear phishing (phishing țintit) vizează persoane specifice folosind informații personalizate. Spre deosebire de phishing-ul în masă, spear phishing cercetează țintele cu atenție.

Atacatorii adună informații din:

- Profiluri de rețele sociale
- Site-uri web ale companiilor
- Conexiuni LinkedIn
- Registre publice
- Breșe de date anterioare

Un e-mail de spear phishing poate face referire la:

- Titlul dumneavoastră efectiv de funcție și departament
- Anunțuri recente ale companiei
- Numele colegilor sau managerilor dumneavoastră
- Proiecte la care lucrați
- Conferințe la care ați participat

Această personalizare crește dramatic ratele de succes.

Whaling

Whaling (phishing executiv) vizează persoane de mare valoare, de obicei directori executivi sau persoane cu autoritate financiară. Aceste atacuri sunt bine cercetate și elaborate cu grijă.

Scenarii comune de whaling:

- Cereri urgente false de la CEO
- Notificări juridice frauduloase
- Documente false de fuziuni și achiziții
- Materiale pentru ședințele consiliului de administrație

Directorii executivi sunt vizați deoarece:

- Au autoritatea de a aproba tranzacții
- Au acces la informații sensibile
- Pot avea o conștientizare mai redusă a securității tehnice
- Sunt adesea prea ocupați pentru o analiză atentă

Compromiterea e-mailului de afaceri (BEC)

Atacurile **BEC** (Business Email Compromise) se dau drept parteneri de afaceri pentru a manipula angajații să transfere fonduri sau să dezvăluie informații.

Scenarii comune BEC:

- **Fraudă de tip CEO**: Directorul fals solicită transfer bancar
- **Uzurparea identității furnizorului**: Factură falsă cu detalii de plată modificate
- **Uzurparea identității avocatului**: Chestiune juridică urgentă care necesită plată
- **Compromiterea contului**: Atacatorul folosește un cont de e-mail efectiv compromis

Conform FBI Internet Crime Complaint Center (IC3), BEC a cauzat peste 55 de miliarde de dolari în pierderi la nivel global din 2013. Un singur atac reușit poate transfera milioane înainte de detectare.

Partea 3: Atacuri vocale (Vishing)

Vishing (phishing vocal) folosește apeluri telefonice pentru a manipula victimele. Odată cu apariția clonării vocii prin IA, vishing-ul a devenit dramatic mai periculos.

Vishing tradițional

Atacurile clasice de vishing includ:

- Apeluri false de suport tehnic ("Am detectat un virus pe computerul dumneavoastră")
- Uzurparea identității autorității fiscale
- Uzurparea identității departamentului de fraudă al băncii
- Escrocherii cu premii sau loterii

Vishing-ul este eficient deoarece:

- Conversația în timp real creează presiune
- Identificatorul apelantului poate fi falsificat
- Vocea transmite autoritate și urgență
- Este mai greu de verificat decât e-mailul

Vishing asistat de IA

Peisajul s-a schimbat dramatic odată cu clonarea vocii prin IA. Conform CrowdStrike, o companie de securitate cibernetică, atacurile de vishing au crescut cu 442% la sfârșitul anului 2024, alimentate de deepfake-uri IA.

Cum funcționează vishing-ul asistat de IA:

1. Atacatorii colectează mostre vocale din surse publice (videoclipuri, podcast-uri, conferințe de presă)
2. Modelele de IA clonează vocea cu fidelitate ridicată
3. Atacatorii sună angajații pretinzând că sunt directori executivi
4. Generarea vocii în timp real face conversațiile convingătoare

Caz real: În februarie 2024, un angajat din departamentul financiar al Arup, o companie multinațională de consultanță în inginerie, a transferat 25 de milioane de dolari unor escroci după ce a participat la ceea ce părea a fi o conferință video legitimă. Fiecare față de pe ecran era reală, fiecare voce se potrivea perfect, dar toate erau deepfake-uri generate de IA, create de atacatori care au clonat vocile și fețele directorilor executivi folosind material disponibil public.

Conform Raportului Proofpoint State of the Phish din 2025, publicat de Proofpoint, o companie de securitate a e-mailului, vishing-ul afectează acum 30% din organizații, cu uzurparea identității directorilor executivi prin deepfake în creștere cu 15%.

Partea 4: Atacuri bazate pe text (Smishing)

Smishing (phishing prin SMS) folosește mesaje text pentru a livra atacuri. Pe măsură ce oamenii devin mai suspicioși față de e-mail, atacatorii se orientează spre SMS.

De ce funcționează smishing-ul

- Rate de deschidere mai mari decât e-mailul (peste 90% rată de deschidere)
- Ecranele mai mici fac inspecția URL-urilor dificilă
- Mai puțină filtrare a spam-ului pe dispozitivele mobile
- Oamenii au mai multă încredere în mesajele text decât în e-mail
- Sentiment de imediatitate

Atacuri comune de smishing

- Alerte bancare despre tranzacții suspecte

- Notificări de livrare cu linkuri de urmărire
- Notificări de premii sau recompense
- Cereri de verificare a contului
- Furtul codului de autentificare cu doi factori

Tehnici de smishing

Escrocherii cu livrarea coletelor: "Coletul dumneavoastră nu a putut fi livrat. Reprogramați aici: [link malițios]"

Alerte bancare: "Activitate neobișnuită detectată pe contul dumneavoastră. Verificați imediat: [link]"

Ocolirea MFA: "Codul dumneavoastră de verificare este 123456. Dacă nu ați solicitat acest lucru, sunați la [numărul atacatorului]"

Partea 5: Phishing prin coduri QR (Quishing)

Quishing folosește coduri QR pentru a livra atacuri de phishing. Conform Hoxhunt, o platformă de gestionare a riscului uman, phishing-ul prin coduri QR a crescut cu peste 500% pe măsură ce "normalitatea QR" în mediul corporativ s-a răspândit.

De ce funcționează quishing-ul

- Codurile QR ascund URL-ul de destinație
- Utilizatorii nu pot previzualiza linkul înainte de scanare
- Smartphone-urile pot să nu afișeze URL-urile complete
- Adoptarea corporativă a codurilor QR a normalizat scanarea
- Ocolește filtrele de securitate pentru e-mail

Scenarii de quishing

Quishing fizic:

- Amenzi de parcare false cu coduri QR pentru "plată"
- Coduri QR malițioase plasate peste cele legitime
- Coduri QR în notificări oficiale false

Quishing digital:

- Coduri QR în e-mailuri de phishing (ocolesc filtrele bazate pe text)

- Notificări false despre expirarea autentificării cu doi factori
- Coduri QR în documente corporative

Exemple reale:

- Amenzi de parcare false în San Francisco care redirecționau către site-uri de furt de credențiale
- Escrocheria cu coduri QR de la Washington University care fura credențiale
- E-mailuri false despre expirarea MFA de la Microsoft cu coduri QR

Apărarea împotriva quishing-ului

- Utilizați scanere QR care previzualizează URL-urile
- Fiți suspicioși față de codurile QR neașteptate
- Verificați dacă codurile QR fizice nu au fost falsificate
- Tastați URL-urile manual când este posibil

Partea 6: Atacuri multi-canal

Atacatorii moderni nu se mai bazează pe atacuri pe un singur canal. În schimb, creează scheme elaborate folosind mai multe puncte de contact pentru a construi credibilitate.

Cum funcționează atacurile multi-canal

1. **Contact inițial**: E-mailul confirmă o "actualizare urgentă de securitate"
2. **Întărire**: Reminder prin SMS despre aceeași problemă
3. **Validare socială**: Mesaj pe LinkedIn de la un fals coleg IT
4. **Escaladare**: Mesaj pe Teams/Slack care exprimă îngrijorare
5. **Impulsul final**: Apel vocal deepfake de la "manager" care solicită acțiune

După mai multe puncte de contact, victimele sunt mult mai predispuse să aibă încredere în solicitare deoarece aceasta a fost "confirmată" prin diverse canale.

Caracteristici

- Narativ consistent pe toate canalele
- Fiecare punct de contact întărește legitimitatea
- Presiunea timpului crește progresiv
- Mai multe surse aparente sunt de acord asupra urgenței

- Exploatează tendința noastră de a avea încredere în informațiile coroborate

---

Partea 7: IA în ingineria socială

Inteligența artificială a transformat ingineria socială dintr-o activitate artizanală care necesită mult efort într-o amenințare industrializată.

Phishing generat de IA

Raportul Egress Phishing Threat Trends din 2025, publicat de Egress, un furnizor de securitate a e-mailului, indică faptul că 82,6% din e-mailurile de phishing analizate între septembrie 2024 și februarie 2025 conțineau conținut generat de IA.

Conform Abnormal Security, un furnizor de securitate a e-mailului bazat pe IA, până în octombrie 2025 phishing-ul generat de IA a devenit principala amenințare pentru e-mailul enterprise, depășind ransomware-ul, riscul intern și ingineria socială tradițională combinate.

De ce phishing-ul asistat de IA este eficient:

- Gramatică și ortografie perfecte
- Conținut adecvat contextual
- Personalizare la scară largă
- Imită stilul de scriere al persoanelor a căror identitate este uzurpată
- Generează variații unice pentru a evita filtrele

Cifrele: Conform cercetărilor KnowBe4, e-mailurile de phishing generate de IA au o rată de click de 54% comparativ cu 12% pentru tentativele create de oameni.

Tehnologia deepfake

Deepfake audio clonează vocea din mostre:

- Conferințele de presă, interviurile și podcast-urile furnizează material sursă
- Generarea în timp real permite conversații live
- Calitatea continuă să se îmbunătățească rapid

Deepfake video creează material video convingător fals:

- Uzurparea identității în întâlniri virtuale
- Mesaje video false de la directori executivi
- Combinate cu clonarea vocii pentru o uzurpare completă a identității

Conform Raportului ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) Threat Landscape din 2024, comerțul pe dark web cu instrumente deepfake a crescut cu 223% între

T1 2023 și T1 2024.

GenAI în fluxurile de lucru ale atacatorilor

Pe parcursul anului 2025, GenAI a devenit esențial pentru operațiunile atacatorilor:

- Phishing generat de IA mai convingător
- Recunoaștere automată mai rapidă
- Scheme de fraudă îmbunătățite prin media sintetice
- Barieră mai scăzută de intrare pentru atacatori

Conform Raportului SoSafe Human Risk Review din 2025, publicat de SoSafe, un furnizor de platforme de conștientizare a securității, peste 86% din organizații au întâlnit deja cel puțin un incident de phishing sau de inginerie socială legat de IA.

Partea 8: Ingineria socială fizică

Ingineria socială se extinde dincolo de canalele digitale la atacuri fizice.

Pretexting

Pretexting-ul creează un scenariu fabricat pentru a angaja victimele. Atacatorul își asumă o identitate falsă cu o poveste de fundal plauzibilă.

Exemple:

- Pretinzând a fi suport IT pentru a obține acces în clădire
- Uzurparea identității personalului de curierat
- Pretinzând a fi un angajat nou
- Prezentându-se ca auditor sau inspector

Pretextele eficiente includ:

- Povestea detaliată de fundal
- Aspectul și recuzita adecvate
- Încredere și autoritate
- Cunoașterea detaliilor organizaționale

Tailgating și piggybacking

Tailgating (accesul prin urmărire) înseamnă a urma o persoană autorizată prin o intrare securizată.

Tehnici:

- Transportarea de cutii (scuza "mâinile ocupate")
- Purtarea de ținute similare cu angajații
- Sosirea în perioadele aglomerate de intrare
- A părea că se caută cardul de acces

Piggybacking este similar, dar cu acordul persoanei autorizate (aceasta ține ușa din politețe).

Momeala (Baiting)

Momeala presupune a lăsa dispozitive infectate pentru ca victimele să le găsească și să le folosească.

Momeli comune:

- Unități USB etichetate "Confidențial" sau "Informații salariale"
- CD-uri sau DVD-uri lăsate în zone comune
- Dispozitive etichetate cu logo-uri ale companiei

Curiozitatea determină victimele să conecteze dispozitivele găsite, declanșând instalarea software-ului malițios.

Căutarea în gunoi (Dumpster Diving)

Căutarea prin deșeuri pentru informații valoroase:

- Documente aruncate
- Hardware vechi cu date
- Bilețele adezive cu parole
- Organigramele și directoarele

Politicile adecvate de distrugere a documentelor contracarează această amenințare.

Partea 9: Strategii de apărare

Apărarea împotriva ingineriei sociale necesită o combinație de controale tehnice, politici și conștientizare umană.

Instruire de conștientizare a securității

Cea mai eficientă apărare sunt utilizatorii educați care recunosc și rezistă atacurilor.

Instruirea ar trebui să acopere:

- Recunoașterea indicatorilor de phishing
- Proceduri de verificare pentru solicitări neobișnuite
- Raportarea activităților suspecte
- Gestionarea în siguranță a contactelor neașteptate
- Exemple și scenarii din lumea reală

Abordări de instruire:

- Sesiuni regulate de conștientizare
- Campanii simulate de phishing
- Gamificare și implicare
- Feedback imediat la greșeli
- Indicatori de urmărire a progresului

Proceduri de verificare

Stabiliți proceduri pentru verificarea solicitărilor neobișnuite:

Verificare pe un canal alternativ (out-of-band):

- Apelați înapoi pe numere cunoscute (nu pe numerele furnizate în mesajele suspecte)
- Utilizați canale de comunicare alternative
- Verificați prin contacte stabilite

Autorizare cu mai multe persoane:

- Tranzacțiile mari necesită aprobări multiple
- Acțiunile sensibile necesită verificarea supervizorului
- Transferurile bancare au proceduri obligatorii de confirmare

Controale tehnice

Deși ingineria socială vizează oamenii, controalele tehnice sunt de ajutor:

Securitatea e-mailului:

- Filtre anti-spam și anti-phishing
- Autentificare DMARC, DKIM, SPF
- Avertismente pentru e-mailuri externe
- Protecția linkurilor și sandbox

Securitatea telefonului:

- Proceduri de verificare a apelantului
- Instruire privind falsificarea identificatorului apelantului

- Înregistrarea apelurilor sensibile

Control al accesului:

- Autentificare multi-factor
- Sisteme de gestionare a vizitatorilor
- Cerințe de ecuson pentru intrare

Crearea unei culturi de securitate

Apărarea pe termen lung necesită schimbare culturală:

- Securitatea devine responsabilitatea tuturor
- Eliminarea stigmei raportării greșelilor
- Celebrarea comportamentului conștient de securitate
- Conducerea demonstrează angajament
- Comunicare regulată despre amenințări

Partea 10: Exerciții practice

Să parcurgem câteva scenarii pentru a aplica ceea ce am învățat.

Scenariul 1: Analiza unui e-mail suspect

Primiți un e-mail:

```
From: IT-Security@yourcompany.com.suspicious-domain.com
Subject: URGENT: Expirarea parolei in 24 de ore

Stimate Angajat,

Parola dumneavoastra corporativa va expira in 24 de ore. Pentru a preveni
blocarea contului, va rugam sa va actualizati credentialele imediat
folosind linkul securizat de mai jos:

[Actualizati Parola Acum]

Nerespectarea va duce la pierderea accesului la toate sistemele companiei.

Echipa de Securitate IT
```

Semnale de alarmă:

- Nepotrivire de domeniu (suspicious-domain.com)

- Salutare generică ("Stimate Angajat")
- Presiune de urgență
- Amenințare cu consecințe
- Link suspect

Răspuns corect: Nu faceți clic pe link. Raportați departamentului de securitate IT. Verificați prin canalele oficiale IT dacă sunteți îngrijorat de expirarea parolei.

Scenariul 2: Verificarea unui apel telefonic

Telefonul sună. Apelantul pretinde a fi de la departamentul de fraudă al băncii dumneavoastră: "Am detectat activitate suspectă pe contul dumneavoastră. Pentru a vă verifica identitatea, vă rugăm să confirmați numărul contului și ultimele patru cifre ale codului numeric personal."

Semnale de alarmă:

- Apel nesolicitat
- Solicitare de informații sensibile
- Crearea de urgență privind "activitate suspectă"

Răspuns corect: Închideți telefonul. Sunați banca folosind numărul de pe cardul sau extrasul dumneavoastră. Nu furnizați niciodată informații sensibile apelanților care vă contactează din proprie inițiativă.

Scenariul 3: Cerere de transfer bancar de la directorul executiv

Primiți un e-mail de la CEO care vă cere să transferați urgent fonduri către un nou furnizor: "Am nevoie să procesați un transfer bancar de 50.000 $ către acest furnizor nou imediat. Sunt într-o ședință și nu pot fi deranjat. Acest lucru este confidențial – nu discutați cu nimeni altcineva."

Semnale de alarmă:

- Urgență
- Cerere de secret
- Solicitare neobișnuită din partea directorului executiv
- Nu poate fi verificată prin canalele normale

Răspuns corect: Urmați procedurile de verificare stabilite, indiferent de expeditorul aparent. Contactați CEO-ul prin canale cunoscute. Nu ocoliți niciodată verificarea pentru solicitări "urgente".

Concluzie

Astăzi am explorat ingineria socială și factorul uman:

1. **Psihologia manipulării**: Principiile lui Cialdini și declanșatorii emoționali
2. **Varietăți de phishing**: Phishing prin e-mail, spear phishing, whaling, BEC
3. **Vishing**: Atacuri vocale amplificate de clonarea vocii prin IA
4. **Smishing**: Atacuri prin SMS cu rate ridicate de deschidere
5. **Quishing**: Phishing prin coduri QR exploatând utilizarea normalizată a QR
6. **Atacuri multi-canal**: Atacuri coordonate pe mai multe puncte de contact
7. **Transformarea prin IA**: GenAI face atacurile mai convingătoare și mai scalabile
8. **Atacuri fizice**: Pretexting, tailgating, momeală
9. **Strategii de apărare**: Instruire, proceduri de verificare, controale tehnice, cultură

Elementul uman va fi întotdeauna parte a securității. Obiectivul nostru nu este de a elimina implicarea umană, ci de a împuternici oamenii să recunoască și să reziste manipulării.

În lecția următoare, vom examina modelele de control al accesului și gestionarea identității.

Întrebări de discuție

1. Cum pot organizațiile echilibra procedurile de verificare a securității cu eficiența operațională?
2. Ce considerente etice apar la desfășurarea campaniilor simulate de phishing?
3. Pe măsură ce IA face deepfake-urile din ce în ce mai convingătoare, ce noi metode de verificare vor fi necesare?

Vă mulțumesc pentru atenție. Ne vedem la următoarea sesiune.

Întrebări de recapitulare

1. Explicați cele șase principii ale influenței ale lui Cialdini și cum poate fi exploatat fiecare în atacuri de inginerie socială.
2. Comparați și contrastați phishing-ul, spear phishing-ul și whaling-ul. Ce face fiecare eficient?
3. Ce este compromiterea e-mailului de afaceri (BEC) și de ce a devenit unul dintre cele mai costisitoare tipuri de atacuri?

4. Cum schimbă IA și tehnologiile deepfake peisajul amenințărilor de inginerie socială?
5. Descrieți phishing-ul prin coduri QR (quishing). De ce este deosebit de eficient în mediul actual?
6. Ce face atacurile de inginerie socială multi-canal mai periculoase decât atacurile pe un singur canal?
7. Ce elemente ar trebui să includă un program eficient de instruire de conștientizare a securității?
8. Descrieți trei tehnici de inginerie socială fizică și contramăsurile pentru fiecare.

Termeni cheie

- **IA adversarială**: Atacuri care vizează sistemele de securitate bazate pe învățare automată pentru a evita detectarea sau a cauza clasificări eronate
- **Momeală (Baiting)**: Lăsarea de dispozitive infectate sau oferirea de articole atractive pentru a ademeni victimele
- **BEC**: Compromiterea e-mailului de afaceri, un atac care uzurpă identitatea directorilor executivi sau a partenerilor pentru a autoriza tranzacții frauduloase
- **Fraudă de tip CEO**: O formă de compromitere a e-mailului de afaceri în care atacatorii uzurpă identitatea directorilor superiori pentru a autoriza tranzacții frauduloase
- **Deepfake**: Media sintetice generate de IA care imită convingător persoane reale
- **Căutarea în gunoi (Dumpster Diving)**: Căutarea prin materialele aruncate pentru informații utile
- **Phishing**: Comunicare frauduloasă concepută pentru a păcăli destinatarii să dezvăluie informații sau să întreprindă acțiuni dăunătoare
- **Simulare de phishing**: Exerciții controlate care testează susceptibilitatea angajaților la atacuri de phishing ca parte a instruirii de securitate
- **Pretexting**: Crearea unui scenariu fabricat pentru a manipula o țintă să furnizeze informații sau acces
- **Quishing**: Atacuri de phishing care folosesc coduri QR pentru a direcționa victimele către site-uri malițioase
- **Instruire de conștientizare a securității**: Programe educaționale concepute pentru a învăța angajații să recunoască și să răspundă la amenințări de securitate
- **Smishing**: Atacuri de phishing prin SMS
- **Inginerie socială**: Manipularea psihologică a oamenilor pentru a efectua acțiuni sau a divulga informații confidențiale
- **Spear Phishing**: Phishing țintit direcționat către persoane sau organizații specifice

- **Tailgating**: Urmarea unei persoane autorizate printr-o intrare securizată fără credențiale adecvate
- **Vishing**: Atacuri de phishing vocale, adesea folosind apeluri telefonice
- **Whaling**: Atacuri de phishing care vizează în mod specific directorii superiori

Referințe și lecturi suplimentare

- NIST SP 800-50: Building an Information Technology Security Awareness and Training Program
- Anti-Phishing Working Group (APWG) Reports
- FBI Internet Crime Complaint Center (IC3) Annual Reports
- SANS Security Awareness Resources