ИЖТИМОИЙ МУҲАНДИСЛИК ҲУЖУМЛАРИ: ТУРЛАРИ, ХАВФЛАРИ ВА УЛАРДАН САҚЛАНИШ УСУЛЛАРИ

Choriyev Ulug‘bek Jalol o‘g‘li
O‘zbekiston Respublikasi Kriminologiya tadqiqot instituti
ilmiy xodimi, kapitan.

https://doi.org/10.5281/zenodo.18619042

Аннотация. *Мазкур мақолада ижтимоий муҳандислик (social engineering) ҳужумларининг турлари, қўлланилиш усуллари ва улардан сақланиш йўллари таҳлил қилинган. Ижтимоий муҳандислик — бу одамларнинг ишончини суиистеъмол қилиш орқали махфий маълумотларни қўлга киритишга қаратилган психологик манипуляция усули. Тадқиқот натижалари шуни кўрсатадики, барча киберҳужумларнинг 98 фоизида ижтимоий муҳандислик элементлари мавжуд. Мақолада фишинг, вишинг, претекстинг, бейтинг ва квид про кво каби асосий ҳужум турлари содда тилда тушунтирилган ва амалий ҳимоя тавсиялари берилган.*

Калит сўзлар: *ижтимоий муҳандислик, фишинг, киберхавфсизлик, психологик манипуляция, ахборот хавфсизлиги, кибертаҳдидлар, вишинг, хабардорлик.*

Аннотация. *В данной статье проанализированы виды атак социальной инженерии, методы их применения и способы защиты от них. Социальная инженерия — это метод психологической манипуляции, направленный на получение конфиденциальной информации путём злоупотребления доверием людей. Результаты исследования показывают, что элементы социальной инженерии присутствуют в 98% всех кибератак. В статье простым языком объяснены основные виды атак и даны практические рекомендации по защите.*

Ключевые слова: *социальная инженерия, фишинг, кибербезопасность, психологическая манипуляция, информационная безопасность, вишинг, осведомлённость.*

Abstract. *This article analyzes the types of social engineering attacks, their methods, and ways to protect against them. Social engineering is a psychological manipulation method aimed at obtaining confidential information by exploiting people's trust. Research results show that 98% of all cyberattacks involve social engineering elements. The article explains the main types of attacks in simple language and provides practical protection recommendations.*

Keywords: *social engineering, phishing, cybersecurity, psychological manipulation, information security, vishing, awareness.*

КИРИШ

Бугунги кунда кибержиноятчилар компьютер тизимларини бузиш учун мураккаб техник усуллардан кўра, одамларнинг ишончини суиистеъмол қилиш орқали мақсадга эришишни кўпроқ афзал кўрмоқда. Бу усул "ижтимоий муҳандислик" (social engineering) деб аталади. Оддий қилиб айтганда, ижтимоий муҳандислик — бу одамларни алдаб, улардан паролни, банк маълумотларини ёки бошқа сирли маълумотларни олиш усули.

Нега бу муаммо муҳим? “Proofpoint” компаниясининг 2025 йилги ҳисоботига кўра, барча муваффақиятли киберҳужумларнинг 98 фоизида ижтимоий муҳандислик элементлари иштирок этган . Яъни, ҳужумчилар кўпинча мураккаб дастурлар ёрдамида эмас, балки одамларнинг хатоси орқали тизимларга кириб олади. “Verizon” компаниясининг маълумотларига кўра, маълумотлар бузилиши ҳолатларининг 74 фоизида инсон омили асосий сабаб бўлган.

Ижтимоий муҳандислик ҳужумлари жаҳон миқёсида катта молиявий зарар етказмоқда. 2023 йилда АҚШда ижтимоий муҳандислик ва фишинг фирибгарлиги орқали 12,5 миллиард доллардан ортиқ зарар етказилган. Ўзбекистонда ҳам бу муаммо тобора долзарб бўлиб бормоқда — “Telegram”, “Instagram” ва бошқа ижтимоий тармоқлар орқали фирибгарлик ҳолатлари кундан-кунга кўпаймоқда.

Ушбу мақоланинг мақсади — ижтимоий муҳандислик ҳужумларининг асосий турларини содда тилда тушунтириш, реал ҳаётдан мисоллар келтириш ва ҳар бир инсон қўллай оладиган амалий ҳимоя тавсияларини бериш.

ИЖТИМОИЙ МУҲАНДИСЛИКНИНГ НАЗАРИЙ АСОСЛАРИ

Ижтимоий муҳандислик тушунчасини илк бор машҳур хакер Кевин Митник (Kevin Mitnick) кенг оммага танитган. Унинг "Алдаш санъати" (The Art of Deception) китобида ижтимоий муҳандисликнинг асосий принциплари баён этилган: "Хавфсизлик занжирининг энг заиф бўғини — бу одам" эътироф этилган.

Ижтимоий муҳандислик бир нечта психологик принципларга таянади. Роберт Чалдини (Robert Cialdini) қуйидаги 6 та таъсир принципини аниқлаган бўлиб, ижтимоий муҳандислар айнан шу принциплардан фойдаланади:

1. **Ваколат (Authority)** — одамлар ҳокимият ёки лавозим эгаларига ишонишга мойил. Масалан, фирибгар ўзини "банк ходими" ёки "директор" деб таништирса, қурбон унинг сўзларига тезроқ ишонади.

2. **Шошилинчлик (Urgency)** — фирибгарлар сунъий шошилинчлик ҳисси яратади. "Ҳозироқ қилинг, акс ҳолда ҳисобингиз блокланади!" каби хабарлар одамни тинч ўйлаб кўришга вақт бермайди.

3. **Ишонч (Trust)** — фирибгар аввал ишонч муносабатларини ўрнатади, сўнгра ундан фойдаланади. Масалан, бир неча кун давомида дўстона суҳбат қуриб, кейин пул сўрайди.

4. **Қўрқув (Fear)** — "Сизнинг компьютерингизга вирус тушган!" каби қўрқитиш орқали одамни шошилинч ва ўйламасдан ҳаракат қилишга мажбурлаш.

5. **Очкўзлик (Greed)** — "Сиз 1 000 000 сўм ютуқ ютдингиз!" каби таклифлар орқали одамни жалб қилиш.

6. **Ёрдам бериш хоҳиши (Helpfulness)** — одамларнинг бошқаларга ёрдам беришга бўлган табиий интилишидан фойдаланиш.

ИЖТИМОИЙ МУҲАНДИСЛИК ҲУЖУМЛАРИНИНГ АСОСИЙ ТУРЛАРИ

1. Фишинг (Phishing)

Фишинг — ижтимоий муҳандисликнинг энг кенг тарқалган тури. Фишинг сўзи инглизчадаги "fishing" (балиқ тутиш) сўзидан олинган — худди балиқчи қармоқ ташлагандек, фирибгар ҳам "қармоқ" ташлаб, қурбонни "тутишга" ҳаракат қилади.

Фишинг ҳужумида фирибгар ўзини ишончли ташкилот — банк, давлат органи, ижтимоий тармоқ — ходими сифатида кўрсатиб, қурбонга сохта хабар юборади. Хабарда одатда "ҳисобингизни тасдиқланг", "паролингизни янгиланг" ёки "тўловни қабул қилинг" каби талаблар бўлади. Хабардаги ҳавола (линк) сохта веб-сайтга олиб боради ва қурбон шахсий маълумотларини киритганда, улар фирибгарнинг қўлига тушади.

Фишингнинг бир нечта кўриниши мавжуд: Электрон почта фишинги — энг анъанавий усул, сохта электрон хатлар юборилади; SMS-фишинг (смишинг) — SMS хабарлар орқали сохта ҳаволалар юборилади; Мақсадли фишинг (spear phishing) — аниқ

бир шахсга қаратилган шахсийлаштирилган фишинг; Вэйлинг (whaling) — юқори лавозимдаги шахсларга қаратилган фишинг.

Ўзбекистонда “Telegram” ва “Instagram” орқали фишинг ҳужумлари айниқса кенг тарқалган. Масалан, "Сизнинг Telegram аккаунтингиз блокланади, тасдиқлаш учун шу ҳаволани босинг" каби хабарлар минглаб фойдаланувчиларга юборилмоқда.

2. Вишинг (Vishing)

Вишинг — телефон қўнғироқлари орқали амалга ошириладиган фирибгарлик. "Vishing" сўзи "voice" (овоз) ва "phishing" (фишинг) сўзларининг бирикмаси. Фирибгар телефон орқали қўнғироқ қилиб, ўзини банк ходими, полиция ходими ёки техник ёрдам мутахассиси деб таништиради ва қурбондан шахсий маълумотлар — банк карта рақами, СМС-код, парол — сўрайди.

Типик вишинг сценарийси: фирибгар "банк хавфсизлик хизмати"дан қўнғироқ қилиб, "сизнинг картангиздан шубҳали операция аниқланди, картани блоклаш учун маълумотларингизни тасдиқланг" дейди. Қурбон шошилинчлик ва қўрқув таъсирида карта маълумотларини беради. Ўзбекистонда банк номидан қўнғироқ қилиб фирибгарлик қилиш ҳолатлари сўнгги йилларда кескин кўпайган.

3. Претекстинг (Pretexting)

Претекстинг — бу фирибгарнинг аввалдан тайёрланган сохта ҳикоя (сценарий) асосида қурбон ишончини қозониш усули. Фирибгар ўзини маълум бир шахс — IT мутахассиси, банк ходими, солиқ инспектори, курьер — деб таништириб, ишонарли ҳикоя тўқийди ва қурбондан зарур маълумотларни олади.

Масалан, фирибгар компаниянинг IT бўлими ходими сифатида қўнғироқ қилиб: "Биз тизимни янгилаяпмиз, сизнинг компьютерингизга масофадан кириш учун паролингизни айтинг" дейди. Ходим ишдаги одатий жараён деб ўйлаб, паролини беради.

Претекстинг фишингдан фарқли равишда, кўпроқ шахсий мулоқотга асосланади ва узоқроқ вақт давом этиши мумкин.

4. Бейтинг (Baiting)

Бейтинг — "ўлжа" (bait) ёрдамида қурбонни тузоққа тушириш усули. Бу ҳужум одамнинг қизиқувчанлиги ёки очкўзлигидан фойдаланади. Масалан, фирибгар зараркунанда дастур ўрнатилган USB флешкани офис биноси яқинига қолдиради. Қизиқувчан ходим флешкани топиб, компьютерига улайди ва зараркунанда дастур автоматик равишда ўрнатилади.

Рақамли бейтинг ҳам кенг тарқалган: "Бепул кино юклаб олинг!", "Бепул антивирус ўрнатинг!" каби таклифлар орқали одамлар зараркунанда дастурларни ўзлари ўрнатиб олади.

5. Квид про кво (Quid Pro Quo)

Квид про кво — "хизмат учун хизмат" маъносини англатиб, фирибгар қурбонга бирор хизмат таклиф қилиш эвазига маълумот олади. Масалан, фирибгар ўзини IT-техник деб таништириб, "компьютерингизда муаммо борми? Мен бепул тузатиб бераман" дейди.

Қурбон ёрдам олиш учун компьютерига масофадан киришга рухсат берганда, фирибгар зараркунанда дастур ўрнатади ёки маълумотларни ўғирлайди.

6. Тейлгейтинг (Tailgating)

Тейлгейтинг — физик ижтимоий муҳандислик усули бўлиб, фирибгар рухсат этилган шахснинг орқасидан ҳимояланган биноларга кириб олади. Масалан, фирибгар қўлида оғир қутилар кўтариб, "илтимос, эшикни ушлаб туринг" деб сўрайди.

Хулқ-атвор нормалари туфайли ходим эшикни очиб беради, фирибгар эса ҳимояланган ҳудудга кириб олади.

ИЖТИМОИЙ МУҲАНДИСЛИК ҲУЖУМЛАРИНИНГ СТАТИСТИКАСИ

Жаҳон миқёсида ижтимоий муҳандислик ҳужумлари йилдан-йилга кўпайиб бормоқда. Қуйидаги рақамлар бу муаммонинг қанчалик жиддий эканлигини кўрсатади:

“Proofpoint” компаниясининг 2025 маълумотларига кўра [1]: барча муваффақиятли киберҳужумларнинг 98 фоизида ижтимоий муҳандислик элементлари мавжуд; ташкилотларнинг 83 фоизи фишинг ҳужумларига дуч келган; фишинг электрон хатларнинг ўртача 3,4 фоизи қурбонлар томонидан очилган — бу кичик рақамдек кўринса-да, миллионлаб хатлар юборилганда минглаб қурбонларни англатади.

“Verizon DBIR” 2025 ҳисоботига кўра: маълумотлар бузилишининг 74 фоизида инсон омили асосий сабаб; фишинг ҳужуми ўртача 60 секунд ичида — яъни қурбон хабарни олганидан атиги бир дақиқада — муваффақиятга эришиши мумкин; ижтимоий муҳандислик ҳужумларининг ўртача молиявий зарари бир ҳодиса учун 50 000 доллар.

Ўзбекистон Республикаси Киберхавфсизлик марказининг (“UzCERT”) маълумотларига кўра, 2025 йилда қайд этилган киберинцидентларнинг 42 фоизи фишинг ҳужумлари билан боғлиқ бўлган. “Telegram” мессенжери орқали фирибгарлик ҳолатлари айниқса кўп кузатилган — сохта совға ваъдалари, сохта ишга жойлаш таклифлари ва сохта инвестиция лойиҳалари минглаб фуқароларни алдаган.

ИЖТИМОИЙ МУҲАНДИСЛИК ҲУЖУМЛАРИДАН САҚЛАНИШ УСУЛЛАРИ

1. Шахсий ҳимоя чоралари

Ҳар бир инсон қуйидаги оддий қоидаларга амал қилиш орқали ижтимоий муҳандислик ҳужумларидан сақланиши мумкин:

Шубҳали хабарларга эҳтиёткорлик. Кутилмаган хабар олганингизда — у электрон почта, SMS ёки мессенжер орқали бўлсин — олдин шубҳаланинг, кейин ишонинг. Банк ёки бошқа ташкилот номидан келган хабардаги ҳаволани бевосита босманг. Бунинг ўрнига, ташкилотнинг расмий веб-сайтига ўзингиз кириб текширинг ёки расмий телефон рақамига қўнғироқ қилинг.

Шахсий маълумотларни ҳимоялаш. Парол, банк карта рақами, СМС-код каби маълумотларни ҳеч кимга — ҳатто ўзини банк ходими деб таништирган шахсга ҳам — бермаманг. Ҳақиқий банк ходимлари сиздан ҳеч қачон парол ёки тўлиқ карта рақамини сўрамайди.

Кучли паролларни ишлатиш. Ҳар бир ҳисоб учун алоҳида, мураккаб парол ишлатинг. Парол камида 12 белгидан иборат бўлиб, ҳарфлар (катта ва кичик), рақамлар ва махсус белгиларни ўз ичига олиши керак. Парол менежери дастурлари (Bitwarden, 1Password) бу ишни осонлаштиради.

Икки босқичли аутентификация (2FA). Имкон борича барча ҳисобларда икки босқичли аутентификацияни ёқинг. Бунда парол билан бирга қўшимча тасдиқлаш коди (SMS ёки аутентификатор иловаси орқали) талаб қилинади. Бу ҳатто парол ўғирланган ҳолда ҳам ҳисобингизни ҳимоялайди.

2. Ташкилий чоралар

Ташкилотлар ижтимоий муҳандислик ҳужумларига қарши қуйидаги чораларни кўриши лозим:

Ходимларни мунтазам ўқитиш. Барча ходимларга киберхавфсизлик бўйича мунтазам (камида йилда 2 марта) ўқув курслари ташкил этиш. Ўқитиш давомида реал фишинг намуналарини кўрсатиш ва амалий машғулотлар ўтказиш самарали натижа беради.

Фишинг симуляциялари. Ташкилот ичида назорат остида сохта фишинг хатлар юбориб, ходимларнинг тайёргарлик даражасини текшириш. Бу усул ходимларнинг реал ҳужумларга нисбатан эҳтиёткорлигини 60-70 фоизга ошириши исботланган.

Аниқ сиёсат ва тартиб-қоидалар. Маълумот хавфсизлиги сиёсатини ишлаб чиқиш ва барча ходимларга етказиш: қайси маълумотларни ким билан ва қандай алмашиш мумкинлигини аниқ белгилаш; молиявий операцияларда кўп босқичли тасдиқлаш жараёнини жорий этиш; шубҳали ҳолатларни хабар қилиш тартибини белгилаш.

3. Техник чоралар

Электрон почта фильтрлаш. Замонавий электрон почта хавфсизлик тизимлари (Secure Email Gateway) фишинг хатларнинг 95 фоизгача олдини олади. SPF, DKIM ва DMARC протоколлари электрон почтанинг ҳақиқийлигини текшириш имконини беради.

Веб-фильтрлаш. Фишинг сайтларга киришни блоклайдиган веб-фильтр тизимлари; DNS фильтрлаш (Cisco Umbrella, Cloudflare Gateway) орқали зарарли доменларни блоклаш.

Охирги нуқта ҳимояси (Endpoint Protection). Замонавий антивирус ва EDR (Endpoint Detection and Response) тизимлари зараркунанда дастурлар ва шубҳали фаолиятни аниқлайди.