O‘QUVCHI YOSHLARDA KIBER XAVFSIZLIK KO‘NIKMALARINI SHAKLLANTIRISHNING ZAMONAVIY PSIXOLOGIK USULLARI

Yuldasheva Zulfiya Burxanovna

Jizzax viloyati Zomin tuman 31- maktab amaliyotchi psixologi

ANNOTATSIYA

Ma’lumki, oldini olish har doim davolashdan ko‘ra yaxshiroqdir. Fuqaro internetdan foydalanishda muayyan ehtiyot choralarini ko‘rishi va kiber jinoyatlar uchun ma’lum profilaktika choralariga rioya qilishlari kerak. Xususan, ta’lim orqali ta’sirlarni aniqlash ayollarga ushbu muammolarni hal qilishga yordam beradi. Elektron pochta orqali yoki suhbat paytida shaxsiy ma’lumotlarni begonalarga oshkor qilish hamda internet xavfsizligini kuchaytirish orqali erishish mumkin. Fotosurat hodisalaridan noto‘g‘ri foydalanish sifatida internet orqali begonalarga biron bir fotosurat yuborishdan qochish kerak kundan kun ortib bormoqda.

Kalit so‘zlar: *OAV,kibber hujum,jinoyatchilik,psixika,ong, ruhiy holat, agressiya*

KIRISH

Kiberjinoyatchilikka oid qonunchilik keng jamoatchilikka nisbatan qo‘llanilishi mumkin yoki u faqat ayrim turdagi kompaniyalarga taalluqli bo‘lgan sohaga oid bo‘lishi mumkin. Masalan, Gramm-Lich-Bliley qonuni (GLBA) moliyaviy institutlarga e'tibor qaratadi va mijozlar yozuvlarining xavfsizligi va maxfiyligini oshirishi kerak bo‘lgan yozma siyosat va tartiblarni amalga oshirishni tartibga soladi, shu bilan birga shaxsiy ma’lumotlarni tahdidlar va ruxsatsiz kirish va foydalanishdan himoya qiladi. Kiberbulling va onlayn bezorilik kabi maxsus kiberjinoyatlarga qarshi kurashish uchun boshqa qonun hujjatlari ishlab chiqilgan. AQSh shtatlarining yarmidan ko‘pi ushbu jinoyatlar

bilan bevosita bog‘liq qonunlarni amalga oshirdi. Misol uchun, Massachusets qonunida ta’kidlanishicha, onlayn bezorilik 1000 dollargacha jarima, ko‘pi bilan ikki yarim yil qamoq yoki har ikkalasi bilan jazolanishi mumkin bo‘lgan jinoyatdir. Tennessi shtatida onlayn ta’qib qilish A toifasidagi qonunbuzarlik hisoblanadi va sudlangan kiberjinoyatchi ko‘pi bilan 11 oy va 29 kunlik qamoq jazosiga, 2500 dollargacha jarimaga tortilishi mumkin.

Veb-sayt egalari trafikni kuzatishlari va saytdagi har qanday qoidabuzarliklarni tekshirishlari kerak. Bu mas’uliyat zimmasida veb-sayt egalari bu borada aniq qaror qabul qilishlari kerak. Blokcheyn texnologiyasidan foydalanish kerak.

Soxta elektron pochta identifikatorini ro‘yxatdan o‘tkazish jinoyat sifatida ko‘rib chiqilishi kerak.Ruxsatsiz kirishdan himoya qilish uchun ovozni aniqlash, filtrlash dasturi va yoqa identifikatoridan foydalanish kerak. Yuqori texnologiyali jinoyatlar bo‘yicha maxsus kiberjinoyatlarni tergov qilish bo‘limini shakllantirish kerak. Tez odil sudlovni amalga oshirish uchun elektron sud tizimi va videokonferentsiya tizimidan oqilona kengroq foydalanishni tashkil etish kerak. Qonun chiqaruvchi organlar fuqarolar manfaatlarini hisobga olgan holda qat’iy qonun hujjatlarini qabul qilishlari kerak. Kiber jinoyatlar jabrdiydalariga kompensatsion himoya vositalari orqali to‘liq adolat ta’minlanishi lozim. So‘nggi uch o‘n yillikda kompyuter texnologiyalari zamonaviy hayotning mutlaqo hamma joyda mavjud tarkibiy qismiga aylandi. Hayotimizni qo‘llab-quvvatlash va boshqarish uchun texnologiyaga tobora ortib borayotgan bog‘liqlik misli ko‘rilmagan narsalarni yaratdi. Darhaqiqat, jinoyatning aksariyat shakllari hozirda qandaydir tarzda texnologiyani o‘z ichiga oladi, uyali telefonlar va matnli xabarlar yoki texnologiyaning ko‘proq yangi ilovalaridan foydalanish orqali raqamli qurilmalardan tashqarida mumkin bo‘lmagan jinoyatlar kabi. Kiber makon kiber jinoyatchilar uchun begunoh odamlarga zarar etkazish uchun juda ko‘p imkoniyatlarni taqdim etadi. Internet foydalanuvchilari hali ham kiber zo‘ravonlik yoki kiber jinoyatlar haqida darhol xabar berishga tayyor emas. Kiber makon tranzit makondir. Odamlar kibermakonda yashamasalar ham, u yerda turli

amallarni bajarishadi. Bu xususiyat jinoyatchilarga kiber jinoyat sodir etgandan keyin qochish imkoniyatini beradi. Ko‘pchilik veb-saytlar va bloglar tarmoqdagi ayollar va bolalar xavfsizligi uchun xavfsizlik bo‘yicha maslahatlar beradi. Ammo hali ham ayollar ishtirokida ayollarga nisbatan kiber jinoyatlar ortib bormoqda [2]. Ular oson nishon bo‘lgani uchun va ular osongina qurbon bo‘lishlari mumkin, ya’ni nima uchun ayollar asosiy maqsad qilib olinadi. Darhaqiqat, ko‘p suhbatdosh do‘stlari o‘z ayol do‘stlarini “extirosli”, “jozibali” kabi so‘zlar bilan masxara qilishdan zavqlanishadi. Bu kiber odobsizlikning virtual boshlanishidir. Ular asta-sekin ayol do‘stlarini ishonchga va haqiqiy do‘st kabi o‘z muammolarini muhokama qilishni boshlashadi. Agar qabul qiluvchi uzoqlashsa, bunday xabarlarni jo‘natuvchi davom ettirishga ko‘proq rag‘batlantiriladi. Agar jabrlangan ayol o‘sha paytda bu haqda xabar berganida yoki tajovuzkorni ogohlantirganida muammo hal bo‘ladi. Kiber- jinoyatning oldini olish uchun biz tanimagan odamlar bilan suhbatlashmasligimiz kerak. Biz parollarimizni himoya qilishimiz kerak. Shaxsiy materiallarni kompyuterda saqlash bir qancha salbiy oqibatlar keltirib chiqarishi mumkin, chunki ularga xaker kirishi mumkin. Agar biror narsa noto‘g‘ri bo‘lib tuyulsa, darhol huquqni muhofaza qilish organlariga murojaat qilish zarur.

Ayollar internetdan foydalanishda doimo hushyor bo‘lishlari va ularni kirishi mumkin bo‘lgan saytlarni ochmasliklari kerak. Ular o‘zlarini himoya qilish uchun begonalar bilan suhbatlashmasliklari kerak. Hatto bizning hukumatimiz ham NIC-CERT (National Informatika markazi-Kompyuterning favqulodda vaziyatlarga javob berish guruhi) Hindistonda va uyda kiberjinoyatlarga qarshi kurashish uchun vazirlik kiberxavfsizlik tarmog‘ini mustahkamlash uchun Kiberjinoyatlarni muvofiqlashtirish markazini (I4C) tashkil etishni taklif qilmoqda. Foydalanuvchilar undan foydalanish natijasida yuzaga keladigan zaifliklardan xabardor bo‘lishlari va xavflarini kamaytirish uchun choralar ko‘rishlari mumkin. Kompyuter foydalanuvchilari Internetdan foydalanishning bir necha oddiy qoidalariga rioya qilish orqali kiberjinoyat qurboni bo‘lish xavfini kamaytirish choralarini ko‘rishlari mumkin. Birinchidan,

foydalanuvchilar foydalanilmayotganda kompyuterlarini o‘chirishni unutmasliklari kerak. Kiber jinoyatchilar ko‘pincha “har doim yoqilgan” kompyuterlarni qidirib, tarmoqlarni skanerlashadi, ular osonlik bilan kirish mumkin va qarovsiz nishonlar deb hisoblaydilar.

Kompyuterlar yoqilgan va internetga ulangan vaqtni minimallashtirish orqali odamlar xakerlik hujumlariga nisbatan zaifligini kamaytirishi mumkin. Keyinchalik, foydalanuvchilar antivirus va xavfsizlik devori dasturlarini o‘rnatishlari va ularga xizmat ko‘rsatishlari kerak. Ushbu ilovalar kompyuterlarning operatsion tizimlarida xavfsizlik xususiyatlarini chetlab o‘tish uchun mo‘ljallangan viruslar va boshqa zararli kompyuter dasturlariga qarshi birinchi himoya chizig‘i bo‘lib xizmat qiladi. Bundan tashqari, operatsion tizim ishlab chiquvchilari muntazam ravishda yangilanishlar yoki "yamalar" chiqaradilar. Kompyuter xavfsizligini oshirish uchun foydalanuvchilar ushbu yangilanishlar mavjud bo‘lishi bilanoq ularni o‘rnatishlari kerak. Kiber jinoyatchilar ko‘pincha zararli dasturlarni elektron pochta xabarlariga biriktirilgan rasm yoki hujjatlar sifatida yashiradilar, shuning uchun foydalanuvchilar hech qachon noma’lum jo‘natuvchilardan elektron pochta qo‘shimchalarini ochmasliklari yoki yuklab olishlari kerak emas. Endi ko‘p odamlar o‘z uylarida simsiz tarmoqlardan foydalanishadi. Simsiz yo‘riqnoma sozlamalarida kuchli shifrlash kiber jinoyatchilarning kompyuterlarda saqlangan ma’lumotlarga kirishi va ulardan foydalanishining oldini oladi. Tarmoq trafigini himoya qilish uchun shifrlashdan foydalanmaydigan himoyalanmagan yoki “ochiq” simsiz tarmoqlar kiber jinoyatchilar uchun juda mashhur nishonlardir. Ushbu simsiz tarmoq trafigini ushlab turish orqali firibgarlar shaxsiy ma’lumotlar, parollar va boshqa ma’lumotlarni tezda to‘plashlari mumkin, keyin ular turli kiber jinoyatlarni sodir etishda foydalanishlari mumkin. Agar sizning uyingizda shifrlanmagan simsiz tarmoq mavjud bo‘lsa, politsiya sizning kompyuterlarga buzib kirganingiz, onlayn firibgarlik qilganingiz yoki kontrabanda tarqatganingizni bilish uchun eshik oldida paydo bo‘lsa, hayron bo‘lmang. Ko‘p odamlar o‘nlab turli veb-saytlarda hisob qaydnomalarini

yuritadilar, shuning uchun ular eslab qolish uchun oson parollar yaratadilar. Bu kamdan-kam ishlatiladigan parolni unutish ehtimoli kamroq degani bo‘lsa-da, bu oddiy parollar aqlli kiber jinoyatchilar tomonidan tezda buzilgan.

Bundan tashqari, ko‘p odamlar o‘zlarining ijtimoiy tarmoq veb-saytlarida, bank va brokerlik hisoblarida bir xil paroldan foydalanadilar. Kiber firibgarlar ijtimoiy tarmoq veb-saytlari uchun parollarni o‘g‘irlashganda, ular ko‘pincha moliyaviy hisoblarga kirish uchun ulardan foydalanishga harakat qilishadi. Bunday muammolarni oldini olish uchun odamlar o‘zlarining har bir akkaunti uchun noyob va murakkab parollardan foydalanishlari kerak. Ushbu oddiy qoidalar ko‘pchilik Internet foydalanuvchilari uchun asosiy xavfsizlikni ta'minlaydi. Biroq, odamlar kiber jinoyat qurboni bo‘lish xavfini yanada kamaytirish uchun qo‘llashi mumkin bo‘lgan qo‘shimcha ehtiyot choralari mavjud. Ba’zi keng tarqalgan jinoiy sxemalarni tushunish va tan olish odamlarga ularning qurboni bo‘lishdan qochishga yordam beradi. Keng tarqalgan bir sxemada kiber jinoyatchilar fishing elektron pochta xabarlarini yuborishadi. Ushbu elektron pochta xabarlari qonuniy jo‘natuvchilardan ekanligini yolg‘on da'vo qiladi va shubhasiz qabul qiluvchini parollar, kredit karta raqamlari va bank hisobi ma’lumotlari kabi shaxsiy, nozik ma’lumotlarni oshkor qilishga qaratilgan hujjatlarni o‘z ichiga oladi. Ba’zi fishing elektron pochta xabarlarida qurbonlar muntazam foydalanadigan saytlarga o‘xshash soxta veb-saytlarga havolalar mavjud. Jabrlanuvchilarni bank ma’lumotlari yoki boshqa nozik ma’lumotlarni taqdim etish uchun aldagandan so‘ng, jinoyatchilar jabrlanuvchining pullariga kirish va o‘g‘irlash uchun turli xil usullardan foydalanadilar.

Internet-auksionda firibgarlik juda keng tarqalgan. Kiber jinoyatchilar Internet auktsion saytlarini to‘ldirishadi va odamlar izlayotgan deyarli har qanday mahsulotni taklif qilishadi. E’lonlar ko‘pincha sotuvchi xaridor bilan bir mamlakatda joylashgandek ko‘rinadi va jinoyatchi jabrlanuvchiga pulni biznes sherigi, hamkori, kasal qarindoshi, oila a'zosi va boshqalarga yuborishni maslahat beradi. Pul odatda pul o‘tkazmalari orqali o‘tkaziladi, bu esa jabrlanuvchiga

ozgina murojaat qiladi. Eng so‘nggi tendentsiya - bankdan bankka pul o‘tkazmalarining ko‘payishi.

Eng muhimi, bu pul o‘tkazmalari yirik banklar orqali o‘tadi, lekin keyin boshqa mamlakatlardagi banklarga yo‘naltiriladi. Huddi shunday, sotuvchilar ham vaqti-vaqti bilan qurbonlarni soxta “escrow” tlaridan foydalangan holda to‘lashga yo‘naltiradilar. Ba'zan ular o‘zlarini yanada vijdonli ko‘rsatish uchun qonuniy eskrov veb-saytlarini o‘g‘irlashadi. Mablag‘lar eskrow veb-saytiga o‘tkazilgandan so‘ng, sotuvchi odatda aloqani to‘xtatadi. Yana bir mashhur sxema – qalbaki kassir cheklarini o‘tkazish. Ushbu sxema tovarlarni sotish uchun Internetda tasniflangan reklamalardan foydalanadigan odamlarga mo‘ljallangan. Odatda, manfaatdor tomon sotuvchi bilan bog‘lanadi. Sotuvchiga aytilishicha, xaridorning jabrlanuvchining mamlakatida unga qarzi bor sherigi bor. Shunday qilib, u sherikdan jabrlanuvchiga xaridorga qarz miqdori uchun kassir chekini yuborishini talab qiladi. Kassir chekining miqdori ko‘pincha tovar narxidan minglab dollarga ko‘p bo‘ladi va jabrlanuvchiga ortiqcha miqdor tovarni uning joylashgan joyiga olib borish bilan bog‘liq yuk tashish xarajatlarini to‘lash uchun sarflanishi aytiladi. Jabrlanuvchiga chekni depozitga qo‘yish va pul mablag‘lari o‘z hisobvarag‘iga o‘tkazilgandan so‘ng, ortiqcha mablag‘ni jinoyatchiga yoki yuk tashish agenti sifatida belgilangan boshqa sherikga qaytarishni buyuradi. Kassir chekidan foydalanilganligi sababli, banklar odatda pul mablag‘larini darhol yoki bir yoki ikki kun ushlab turishdan keyin chiqaradilar. Chekning haqiqiyligiga yolg‘on ishonib, sotuvchi ko‘rsatmalarga muvofiq pulni o‘tkazadi. Oxir-oqibat, bank kassir chekining soxta ekanligini aniqlaydi va bu mablag‘larni jabrlanuvchining hisobidan olib tashlaydi.

XULOSA

Ba’zi odamlar beixtiyor kiber jinoyatchilarning sheriklariga aylanishadi. Jinoyatchilar Internetdagi mashhur ish saytlarida uyda ishlash bo‘yicha takliflarni joylashtiradilar. Ushbu ishlar “moliyaviy menejer” yoki “to‘lov protsessor” lavozimlari sifatida e’lon qilinadi. Ushbu lavozimlarni qabul qilgan odamlarga bank hisob raqamlarini ochishlari va ish beruvchilariga hisob raqamlarini taqdim

etishlari aytiladi. Ular ushbu hisobvaraqlarga pul o‘tkazmalarini oladilar va bu pullarni yechib olishlari va (albatta, ularning komissiyasi olib tashlangan holda) xorijiy davlatlardagi belgilangan oluvchilarga o‘tkazishlari topshiriladi. Huquqni muhofaza qilish organlariga murojaat qilganda, bu odamlar kiber jinoyatchilar uchun “pul xachiri” rolini o‘ynaganliklarini bilib hayron qolishadi. Bu odamlar pul mablag‘larini uchinchi shaxslar oluvchisi sifatida harakat qilib, noqonuniy daromadlarni bevosita xorijiy mamlakatlardagi kiberjinoyatchilarga o‘tkazishga yordam berishgan. Kiberjinoyatchilar tomonidan tahdid haqiqiy bo‘lsa-da, internet xavfsizligining bir necha asosiy usullaridan foydalanish va keng tarqalgan kiberjinoyat sxemalaridan xabardor bo‘lish orqali shaxslar qurbon bo‘lish xavfini kamaytirishi mumkin.

FOYDALANILADIGAN ADABIYOTLAR RO‘YXATI:

1. Karimov I.A. Ona yurtimiz baxtu iqboli va buyuk kelajagi yo’lida xizmat qilish-eng oliy saodatdir. T-“O’zbekiston”. 2015. 255 -bet.
2. Mirziyoyev Sh. M. Qonun ustuvorligi va inson manfaatlarini ta’minlash yurt taraqqiyoti va xalq faravonligining garovi. O’zbekiston Respublikasi Konstitutsiyasi qabul qilinganligiing 24 yilligiga bag’ishlangan tantanali marosimdagi ma’ruza.// “Xalq so’zi”. 8 dekabr 2016 yil.
3. Convention on Cybercrime, Article
4. https://thegfce.org/the-budapest-convention-on-cybercrime-a-framework-forcapacity-building/
5. https://base.garant.ru/4089723/9db18ed28bd6c0256461e303941d7e7a/#block_37 01
6. https://tass.ru/politika/4782506