63-DARS. KOMPYUTER JINOYATLARI VA KIBERXAVFSIZLIK

TAYANCH TUSHUNCHALAR

Kompyuter jinoyatlari (kiberjinoyat) – kompyuter qurilmalari yoki tarmoq yordamida amalga oshirilgan, kompyuter tizimi yoki tarmoqqa qarshi sodir etilishi mumkin bo'lgan har qanday jinoiy faoliyat.

Kiberxavfsizlik – xakerlarning veb-resurs, tarmoq va dasturiy ta'minotdagi jinoiy harakatlarini kamaytirishga qaratilgan chora-tadbirlar majmui.

Kiberhujum – suhbatdoshga tajovuzkor, qo'rqituvchi mazmunda xabar yuborish.

Xaker (ingl. *Hack*) – yorib tashlash, chopish, buzish.

Bugungi kunda zamonaviy raqamli texnologiyalar insonlar uchun bir qator qulaylik va imkoniyatlar eshigini ochish bilan birga kompyuter va axborot tizimlari xavfsizligini ta'minlash muammosini ham keltirib chiqarmoqda.

Hayotda shunday jinoyatlar ham borki, u odatiy jinoyatdan butunlay farq qilib, bunday jinoyatni juda aqlli va ayyor kimsalar, ya'ni kiberjinoyatchilar amalga oshiradi. Kiberjinoyatchi– axborot tizimlariga ruxsatsiz kirish uchun zararli dasturlarni ishlab chiquvchi tajovuzkor, kuchli bilimga ega IT mutaxassisi. Ularni faoliyati bo'yicha quyidagi turlarga ajratish mumkin:

xaker – virus (kiber o'g'ri)larni yaratuvchi;

Pen tester – saytni buzuvchi (Vebxacker);

Kracker – dasturiy ta'minot va o'yinlarni buzuvchi;

Shellcoders&Reverser – butunjahon professional xakerlari.

Kiberjinoyatlar raqamli texnologiyalar yordamida virtual makon (kiberfazo)da odamlarni qo'rqitish; virus, zararli dasturlar, qonunga zid axborotlar tayyorlash va tarqatish; elektron xatlarni ommaviy tarqatish; xakerlik hujumi; veb-saytlarga noqonuniy kirish; firibgarlik; ma'lumotlar butunligi va mualliflik huquqini buzish; kredit karta va bank rekvizitlarini o'g'irlash kabi huquqbuzarliklar bilan izohlanadi.

Quyida eng keng tarqalgan kiberhujum turlari keltirilgan:

Kiberhujum	Kiberhujum vazifasi	Nima qilish kerak?
Fishing	Begona shaxsning o'zini ishonchli shaxs yoki tashkilot sifatida ko'rsatib, shaxsiy ma'lumotlarni, masalan, parol va kredit karta ma'lumotlarini yig'ishga urinishi.	Hech qachon maxfiy ma'lumotni elektron pochta orqali yubormang yoki telefon orqali aytmang. Shubhali ko'ringan xabarlarni ochmang va o'qimang. Ishonch hosil qilish uchun avval elektron pochta manzili va domen nomi to'g'ri ekanligini tekshiring.
Pharming	Farming xakerlar tomonidan Internet foydalanuvchisini haqiqiy bank, savdo va xizmat ko'rsatish korxonalarining soxta veb-saytlariga avtomatik ravishda qayta yo'naltiradi va parollarni "o'zgartirish" imkonini beradi. Parollarni o'zgartirish o'rniga, u asl login, parolni saqlab oladi va ulardan foydalanadi.	Parolni o'zgartirishni talab qilgan vaqtda parolni o'zgartirish uchun yuborilgan havolalarga kirmang. Mahfiy ma'lumotlarni talab qiluvchi har qanday veb-sayt domen nomi va veb-manzilini tekshiring.
Ransomware	Ransomware virus bo'lib, u foydalanuvchining barcha fayllarini bloklab qo'yadi va undan foydalanish uchun ma'lum miqdordagi to'lovni amalga oshirishni talab qiladi.	Internetda huddi shu holat uchun foydalanuvchilar pul to'lagan yoki to'lamaganligini bilishga harakat qiling. Fayllar so'ralgan pul miqdoriga arziydimi yoki yo'qmi? Puxta o'ylab ko'ring va qaror qabul qiling.
Zararli dasturiy ta'minot	Zararli dasturiy ta'minot qurilmalarni to'xtatadi yoki sezilarli darajada sekinlashtiradi. Zararli dasturlar elektron pochta qo'shimchalari yoki musiqa, rasmga yashirilgan xavfli tarkib orqali tarqatiladi.	Zararli dasturlarga qarshi Avast, Kasperskiy, Bitdefender kabi dasturlar, xavfsizlik devori va ruxsatsiz kirishni taqiqlovchi tizimlardan foydalaning.
DDoS-hujumlari	DDoS hujumlari buzg'unchiga tizim yoki serverga katta miqdordagi trafikni yo'naltirganda, uni biroz vaqtga to'xtatib turishga yoki umuman to'xtatishga majbur qilgan vaqtda sodir bo'ladi.	Afsuski, DDoS hujumlari uchun universal himoya yo'q. Buning uchun apparat, dasturiy ta'minot, hatto tashkiliy chora-tadbirlarni o'z ichiga oluvchi kompleks yondashuv zarur. Hujum qilinayotgan IP-manzilni blokirovka qilish va hujumni aniqlash uchun maxsus apparat va dasturiy vositalardan foydalaning.

I BOB.

MA'LUMOTLAR BAZASI VA MBBT HAQIDA TUSHUNCHA

Kiberjinoyatlarda xakerlar to'g'ridan to'g'ri kompyuter yoki boshqa qurilmalarni nishonga oladi va undan zararli dasturiy ta'minot kodlarini tarqatish, noqonuniy ma'lumot olish, firibgarlik maqsadida shaxsning ma'lumotlarini o'g'irlash maqsadida foydalanadi. Demak, kiberjinoyatlar ko'rinishlari bilan tanishamiz.

Axborotlarning o'g'irlanishi

Axborot – boshqa shaxslarga zarar yetkazmoqchi bo'lgan shaxslar uchun eng qimmatli manbalardan biri. Kiberjinoyatchilar boshqa shaxs kompyuteridagi fayllarni buzish orqali uning shaxsiy ma'lumotlariga kiradi:

shaxsiy ma'lumotlar kiberjinoyatchiga shaxsiy identifikatsiya raqamingizdan foydalanib, sizning nomingizdan savdo hisob raqami ochish, kredit olish uchun ariza berish kabi imkoniyatlarni beradi;

moliyaviy ma'lumotlar orqali kiberjinoyatchi sizning bank rekvizitlaringizni bilib oladi va bank hisob raqamingizga kirish, pullaringizni o'g'irlash va onlayn xarid qilish kabi ishlarni amalga oshiradi;

ijtimoiy mediama'lumotlar. Agar kiberjinoyatchi ijtimoiy tarmoqdagi akkauntingiz yoki ma'lumotlaringizga kirish imkoniyatiga ega bo'lsa, u sizning nomingizdan do'stlaringiz va oila a'zolaringizni ta'qib qilishi yoki ulardan foydalanishi mumkin. Buni u odamlardan pul so'rash yoki virusni o'z ichiga olgan turli mavzulardagi xabarlarni yozish orqali amalga oshiriadi;

*qiziqishlar*ingiz doirasida o'ylab qo'ygan g'oya va fikrlaringiz boshqalar uchun juda qimmatli bo'lishi mumkin. Kiberjinoyatchi ana shu g'oya va fikrlaringizni turli kompaniyalarga "sotishi", keyinchalik o'girlangan g'oyalar asosida kompaniya aynan sizga yo'naltirilgan maxsus taklif va reklama e'lonlarini ishlab chiqishi mumkin.

Bunday muammolarning oldini olish uchun agar zarurat bo'lmasa, maxfiy ma'lumotlaringizni boshqalarga bermang, ularni kuchli va xavfsiz parollar yordamida himoya qiling.

Ma'lumotlarning o'g'irlanishi

Ma'lumotlarni o'g'irlash ikki xil jinoyatni nazarda tutishi mumkin:

1) uchinchi tomon ruxsatsiz sizning Internet tarmog'ingizga ulanib olishi va foydalanishi natijasida ma'lumotlaringiz o'g'irlanadi. Ma'lumot o'g'irlanishidan himoya qilish uchun login va parol yordamida tarmoqni himoya qiling; login va parolingizning sir saqlanishiga ishonch hosil qiling va uni o'zingiz ishonmaydigan odamlarga bermang. Agar kimdir tarmog'ingizga ulanib olganligiga shubha qilsangiz, login va parolingizni tez o'zgartiring;

2) ***hotlink*** bo'lib, bunda kimdir o'z veb-saytidagi fayl yoki videoni sizning veb-saytingizga bog'lab qo'yadi. Foydalanuvchi faylni yuklab olish yoki video ko'rish uchun linkni bosganda,

har gal sizning Internet tarmog'ingizdan foydalanadi.

"Shaxs" o'g'irlanishi

"Shaxs o'g'irlanishi" – kimdir o'zini sizning "o'rningiz"ga qo'yib olishi, ya'ni tarmoqlarda "siz" bo'lib harakat qilishi. Boshqacha aytganda, begona shaxslar sizning shaxsiy ma'lumotlaringizdan foydalanib, o'zini "siz qilib" ko'rsatadi. Bu ma'lumotlar o'g'irlanishiga juda o'xshaydi. Bunda jinoyatchi noqonuniy ravishda sizning to'liq ism-familiyangiz, bank rekvizitlaringiz, tug'ilgan sanangiz, parollaringiz, elektron pochta manzilingiz va bank kartangiz haqida ma'lumotlarni oladi va ulardan foydalanib, telefon yoki bank hisob-raqamingizga kirish, pullaringizni o'g'irlash, ma'lumotlaringizni boshqalarga sotish kabi jinoyatlarni sodir etadi.

Internet orqali sodir etiladigan ayrim firibgarlik usullari va ulardan himoyalanish yo'llari

1. Yordam so'rash. Ijtimoiy tarmoq yoki veb-saytlarga yordam so'rab e'lon beriladi va unda pul o'tkazish uchun bank kartalari yoki uning raqami joylashtiriladi. Ko'pincha, e'londa haqiqiy muhtoj insonlarga tegishli ma'lumotlar joylansa, pul o'tkazish uchun esa firibgarga tegishli bank rekvizitlari taqdim etiladi. *Himoyalanish yo'li.* Pul o'tkazmasdan avval muallifga qo'ng'iroq qilib, batafsil ma'lumot olishga harakat qiling.

2. SMS yuborish. Foydalanuvchi Internetdan o'ziga kerakli axborot manbasini topadi va uni kompyuteriga ko'chirib olish uchun "Yuklab olish" tugmachasini bosadi. So'ngra u yuklash cheklovlarini olib tashlash uchun telefon raqamini kiritishi va "Davom etish" tugmachasini bosishi kerakligi haqidagi xabarni ko'radi. *Himoyalanish yo'li.* "Davom etish" tugmachasini bosmang. Bu havola bosilganda, firibgarlar telefon yoki kompyuterga virusli dasturiy ta'minotni yuklaydi yoki turli bahonalar bilan shaxsiy ma'lumotlarni qo'lga kiritish uchun saytlar tuzog'iga tushirishga harakat qiladi.

3. Oson pul topish taklifi. Ko'p saytlarda hech qanday bilim va ko'nikmalarsiz pul ishlash taklif qilinadi. Buning uchun foydalanuvchidan ko'rsatilgan hisob-raqamiga oz miqdorda pul o'tkazish talab qilinadi. Bu holat 2–3 marta takrorlanadi. *Himoyalanish yo'li.* Faqat firibgarlargina Internetda tez pul topishni taklif qiladi. "Bir hafta davomida investitsiya qilingan mablag'lar 2 barobar ko'payadi" yoki "Siz uchun sarmoyasiz daromad" kabi iboralardan ogoh bo'ling. Saytlardagi oson pul topish haqidagi taklif va shubhali xat-xabarlariga e'tibor bermang.

4. Akkauntni bloklash. Ijtimoiy tarmoqlar (Twitter, Odnoklassniki, Facebook, Vkontakte va h. k.) akkauntlariga kirilganda, firibgarlar akkaunt yoki unga bog'langan elektron hamyon bloklanganligi haqida ma'lumot beradi. Blokdan chiqarish uchun tegishli raqamga SMS yuborish yoki ko'rsatilgan havola orqali shaxsiy ma'lumotlarni kiritish kerakligi aytiladi. *Himoyalanish yo'li.* Bank kartalari va elektron hamyon parollari, shaxsiy ma'lumotlaringizni hech kimga bildirmang. Bunday xat va xabarlarga e'tibor bermang va shubhali havolalarni ochmang.

5. Tanishuv saytlari. Tanishuv saytlarida firibgarlar, asosan, chet ellik yoki va olisda

yashovchi odamlar bilan "ishlaydi". Tarmoqqa joylashtirilgan reklamalar orqali tanishish boshlanadi. Bu firibgarlik uchun taxminan 2–3 oy talab etiladi. "Jabrlanuvchi" ishonchini qozongan firibgar moliyaviy muammolarini gapiradi va udan yordam so'raydi. Firibgar ko'zlangan pulni olishi bilan g'oyib bo'ladi va u bilan qayta bog'lanib bo'lmaydi. ***Himoyalanish yo'li.*** Bunday insonlar bilan tanishmang, yangi "tanishlarga" pul o'tkazmang va ular bilan aslo uchrashmang.

AMALIY MASHG'ULOT

№	Topshiriqlar
1.	Kafe, restoran yoki boshqa jamoat joylarida bepul Wi-Fi tarmog'iga ulanish qanchalik xavfli?
2.	Bank xodimi sizga qo'ng'iroq qildi va o'zini tanishtirdi. Sizga pul o'tkazish uchun karta raqami, amal qilish muddati va parolingizni aytib yuborishingiz kerakligini aytdi. Siz bunday vaziyatda nima qilgan bo'lar edingiz?
4.	Berilgan matnni "FSMU" texnologiyasi bo'yicha tahlil qiling va jadvalni to'ldiring.

Fikr:	**Hozirgi kiberjinoyatlar avj olgan vaqtda yoshlar Internetdan onlayn o'yinlarni o'ynash havfli ekanligini bilmaydi va o'yinda ishtirok etish uchun ota-onasi yoki yaqinlariga tegishli bank karta raqamlaridan foydalanadi.**
Sabab	
Misol	
Umumlastirish	

SAVOL VA TOPSHIRIQLAR

1. Shaxsiy hayotga tajovuz qilish bilan bog'liq kiberjinoyatlarga misollar keltiring.
2. Internet-do'konlar orqali savdo qilishda qanday xavflar mavjud? Bu xavflardan qanday himoyalanish mumkin?
3. Raqamli qurilmalardagi tahdid va xavflardan o'zingizni himoya qilishning uchta usulini ayting.
4. Tasavvur qiling, Siz kiberjinoyatchining hujumiga uchradingiz, ya'ni u sizdan katta miqdorda pul talab qilmoqda. Bunday vaziyatda siz qanday yo'l tutasiz?

UYGA VAZIFA

1. Kibermobbing, kiberbilling va kiberterrorizm tushunchalarini izohlang.
2. Kiberfiribgarlar Internetda qanday sxema bo'yicha ish olib boradi? Misollar keltiring.
3. Kiberxavfsizlik bilan bog'liq so'zlar ishtirok etgan boshqotirma (krossvord) tuzing.