



8-bob

Xavfsizlik texnikasi qoidalari

Ta'lim maqsadlari

Ushbu bob yakunida quyidagi bilim va ko'nikmalarga ega bo'lasiz:

- xavfsizlik texnikasiga oid keng tarqalgan muammolar va ularning sabablari;
- xavfsizlik texnikasiga oid keng tarqalgan muammolarning oldini olish borasidagi bir nechta oddiy strategiyalar;
- AT jihozlardan foydalanish tajribangizni baholash va texnika xavfsizligiga rioya qilmaslikning ehtimoliy xatarlarini minimallashtirishga oid strategiyalarni ishlab chiqish;
- shaxsiy ma'lumotlar nimani anglatishi hamda nima uchun shaxsiy ma'lumotlar maxfiy va himoyalangan bo'lishi kerakligini tushuntirib berish;
- internet va ijtimoiy tarmoqdan foydalanish tajribangizni baholash orqali shaxsiy ma'lumotlaringizni sababsiz oshkor qilishning oldini olish choralarini tushuntirib berish va elektron xavfsizlik nima uchun zarurligini muhokama qilish;
- ma'lumotlarning samarali xavfsizligi va internetda ma'lumotlarning xavfsizligi nima ekanini tushunish; xavfsizlikni oshirishning turli usullari samaradorligini muhokama qilish.



8-bob haqida umumiy ma'lumot

Kompyuterlardan foydalanish darajasi ortib borar ekan, jismoniy xavfsizlikka oid qator muammolar yuzaga keladi. Kompyuter foydalanuvchilarining xavfsizligiga bir nechta tahdidlar mavjud: tarmoqdagi kompyuterlarni bog'laydigan kabellar, printerning joylashuvi, elektr energiyasi tarmog'iga haddan ortiq yuklanish yoki kompyuter oldida ichimlik ichish. Shuningdek, onlayn himoya va xavfsizlik hamda ma'lumotlar xavfsizligi bilan bog'liq muammolar mavjud. Shu sababli biz kompyuter foydalanuvchilari uchun umumiy xavfsizlik muammolari, shuningdek, viruslar, malware dasturlari va shaxsiy ma'lumotlarning o'g'irlanishi bilan bog'liq xavflarni ko'rib chiqamiz.

8.01 Xavfsizlik texnikasi muammolari

Kompyuterlar va ularning tashqi qurilmalari bir-biriga ulanishi kerak bo'lgan elektr qurilmalar bo'lib, buning uchun bir qancha kabellar va elektr toki manbayi talab etiladi. Bunga tarmoq yaratish uchun bir nechta kompyuterni kabellar yordamida ulash imkoniyatini qo'shsangiz, atrof simlarga to'lib ketadi. Buning natijasida yuzaga kelishi mumkin bo'lgan xavfsizlik texnikasi muammolarining oldini olish uchun oddiy ehtiyot choralarini ko'rish mumkin. Ideal holatda kompyuterlarni o'rnatish puxta rejalashtirilgan bo'lishi, kabellar esa yaxshilab berkitilishi va ishga xalaqit qilmasligi kerak. Agar kabellar osilib turgan va xavfsizlik texnikasi muammolarini keltirib chiqarayotgan bo'lsa, sim bog'ichlardan foydalanib ularni mahkamlab birlashtirish va odamlardan uzoqroq tutish mumkin.

Ichimlikning to'kilib ketishi!

Kompyuter va qurilmalarning aksariyati elektr toki manbayiga ulangan holda ishlaydi. Shu sababli ham tok urish xavfidan saqlanish uchun ehtiyot bo'lish zarur. Agar kompyuteringiz yoki qurilmangiz ustiga ichimlik to'kilib ketsa, unga zararyetishi va siz jarohatlanishingiz mumkin! Qurilmaga tasodifan ziyon yetkazmaslik yoki o'zingizga shikast yetmasligi uchun kompyuteringiz oldiga ichimlik qo'ymasligingiz kerak (8.01-rasm). To'kilib ketgan ichimlik qanday muammo keltirib chiqarishi mumkin? Ma'lumotlar kompyuterning komponentlari orasida elektr toki yordamida harakatlanadi. Elektr toki manbayiga ulangan holatda ushbu komponentlarga suyuqlik to'kilib ketadigan bo'lsa, ikkita nuqta tasodifan bir-biriga ulanib qolishi va sxemaning buzilishiga olib kelishi mumkin.



8.01-rasm. Kompyuteringiz ustiga ichimlik to'kib yuborishdan ehtiyot bo'ling!

Klaviatura ustiga ichimlik to'kilib ketsa, nima qilish kerak?

- ✓ Vahimaga tushmang.
- ✓ Kompyuteringizni darhol elektr toki manbayidan uzing (kompyuteringiz dasturiy ta'minot yordamida o'chishini kutmang). Kompyuterni zudlik bilan o'chirsangiz, uning ichidagi elektronikani shikastlanishdan saqlab qolishingiz mumkin.
- ✓ Yumshoq mato yordamida imkon boricha ko'proq suyuqlikni quritib oling.
- ✓ Kompyuteringizga ulangan har qanday kabellar, jumladan, USB-komponentlar, kartalar va boshqa har qanday tashqi qurilmalarni uzib qo'ying.
- ✓ Noutbukni yoki klaviaturani yuz tarafini pastga qaratib, ichidagi suvni tushirish uchun ehtiyotkorlik bilan ikki tarafga harakatlantiring. Uni silkitmang! Uning ichidan iloji boricha ko'proq suyuqlik chiqib ketishi kerak.
- ✓ Qolgan suyuqlik chiqib ketishi uchun uni stol ustida yuz tarafi pastga qaragan holatda qoldiring.
- ✓ Taxminan 24 soat o'tganidan keyin uning sirtini yumshoq va nam mato bilan arting.

Eng sodda va yaxshi maslahat: kompyuter yoki boshqa qurilmada ishlayotganingizda uning oldida ichimlik ichmang!

Elektr energiyasi tarmog'ining haddan ortiq yuklanishi nima?

Uzaytirish kabelida birdan ortiq qurilmani ulashga imkon beruvchi bir nechta rozetka bo'lsa, barcha qurilmalar ulab bo'lingandan so'ng ular birgalikda uzaytirish kabeli uchun belgilangan maksimal ko'rsatkichdan ko'proq tok iste'mol qiladi. Bu elektr energiyasi tarmog'ining haddan ortiq yuklanishi bo'lib, u rozetkadagi vilkaning haddan tashqari qizib ketishiga va hatto yong'in chiqishiga olib kelishi mumkin.



KALIT SO'ZLAR

Elektr energiyasi tarmog'ining haddan ortiq

yuklanishi: elektr zanjirining haddan ortiq zo'ri-qishi — bitta rozetkaga juda ko'p elektr jihozlar ulangani sababli elektr sim yoki elektr zanjiri orqali u ko'tara oladiganidan ko'proq tok o'tishi tufayli sodir bo'ladi.

Vilka yoki rozetkaning qizib ketishi yoki saqlagichning kutilmaganda kuyishi, rozetka yoki vilkada uchqun yoki kuyish alomatining kuzatilishi xavfli belgilar hisoblanadi. Shunday holat yuz bersa, mahkamlanmagan similar yo'qligini, devordagi har bir rozetka uchun bitta uzaytirgich ishlatilayotgani va bir uzaytirish kabeli boshqasiga ulab qo'yilmaganini tekshiringiz kerak.

Quvvat hajmini kuchlanishga bo'lib, tok kuchini hisoblashingiz mumkin. Misol uchun, agarsizda 1000 vatt quvvatga ega elektr jihozi bo'lsa va u 120 voltda ishlasa, ularni bo'lish orqali 20 amperlik zanjirning qariyb yarmi allaqachon band ekanini ko'rasiz. Bunday ma'lumotni odatda qurilmaning orqa, tag tarafi yoki uning simiga yopishtirilgan yorliqdan topsa bo'ladi.

$$\frac{1000 \text{ vatt}}{120 \text{ volt}} = 8.33 \text{ amper}$$

Yodda tuting, uzaytiruvchi kabel rozetkasiga bir nechta qurilma ulangan bo'lsa, bu qurilmalarning tok kuchini qo'shib hisoblashingiz kerak (8.02-rasm).



8.02-rasm. Elektr energiyasi tarmog'ining haddan ortiq yuklanishi haqida o'ylab ko'ring!

Mahkamlanmagan kabellar

Kompyuterlarga odatda elektr yoki tarmoq kabellari kabi ko'plab kabellar ulanishini ko'rgan bo'lsangiz kerak. Bu kabellar pol ustidan o'tadigan bo'lsa, odamlarning qoqilib ketishi xavfi yuzaga keladi. Kimdir kabelga qoqilib ketsa nima bo'ladi? Odamga shikast yetishi yoki uni elektr toki urishi mumkin. Agar vilka qurilma ishlab turganida chiqarib olinsa, sim yoki vilka shikastlanishi, kabelga ulangan uskunalar stol ustidan tortib olinsa, ularga zarar yetishi mumkin.

Elektr toki urishi yoki yong'in yuzaga kelishi bilan bog'liq ehtimoliy xatarlar sababli salomatlik va xavfsizlikni ta'minlash uchun poldan tortilgan kabellarning bari kabel kanaliari ichida, gilam yoki pol tagida bo'lishi kerak.

Kompyuter jihozlariga aloqador boshqa xatarlar

Ko'pincha kompyuter uskunolari og'ir bo'lgani uchun uni joyidan siljitsangiz yoki kimningdir ustiga tushib ketsa, shikastlanish xavfi yuzaga keladi.

Yangi printerni sotib oladigan bo'lsangiz, u odatda kompyuterga ulanadi. Shuning uchun uni qayerga joylashtirishni hal qiling. Katta ehtimol bilan siz uni kompyuter yonidagi stolga qo'yasiz. Lekin bunday qilishdan oldin o'zingizga ikkita savol bering: stol shuncha og'irlikni ko'tarishga mo'ljallanganmi? Printer stolga to'g'ri holatda, muvozanati buzilmay joylashadimi? Qurilmalar qulay joylashtirilishi kerak. Uskunalar yetarlicha mustahkam stollar yoki tokchalarga joylashtirilganiga ishonch hosil qiling. Ular qurilma og'irligini ko'tara olishi zarur va har bir burchak ostidagi joy qurilmani ushlab turadigan darajada katta ekanini tekshirish kerak. Shuningdek, qurilmalar foydalanuvchilarning qo'li osonlikcha yetadigan qiiib joyiashtirilishi lozim. Bu qurilma printer bo'lsa, siz unga muntazam ravishda qog'oz qo'yishingiz va talab etilganda siyohni almashtirishingiz kerak bo'ladi.



Osilib yotgan kabellar xavf tug'dirmasligi uchun ularni tartibga keltirish lozim.

8.01-SAVOL

Maktabingizdagi kompyuter tizimlarida xavfsizlik texnikasining barcha talablari bajarilganmi? Ulardan foydalanuvchilar xavfsizlik texnikasida tavsiya etilgan barcha ko'rsatmalarga rioya qiladimi? Uyingizdagi kompyuter tizimlari haqida nima deya olasiz? Kompyuterdan foydalanishda xavf yuzaga kelmasligi uchun qanday choralar ko'rish mumkinligini muhokama qiling.

8.01-QO'SHIMCHA MASHG'ULOT

Kompyuterlar, monitorlar va printerlarning komponentlari turli zaharli moddalarni o'z ichiga olgan.

Agar maktabingiz ayrim kompyuterlarni yangilashni rejalashtirayotgan bo'lsa, eski jihozlar qanday utilizatsiya qilinishi kerak?

Shaxsiy kompyuter, ekran va printer ichida nimalar zaharli bo'lishi mumkinligini aniqlash uchun biroz izlaning.

Tashlab yuborilgan kompyuter uskunalari utilizatsiya qilishning eng yaxshi usuli haqida xulosa qiling. Do'stlaringiz bilan birgalikda ayrim yo'riqnomalarni ishlab chiqing.

8.02 Elektron xavfsizlik

Elektron xavfsizlik internetdan, shuningdek, mobil telefonlar kabi elektron aloqa vositalaridan foydalanish bilan bog'liq atamadir. Elektron xavfsizlik yangi va rivojlanayotgan texnologiyalardan foydalanayotgan har kimni zarardan himoya qilishdir.

Xatarlarni ikki turga bo'lish mumkin:

- ❖ noqonuniy yoki nomaqbul kontent;
- ❖ mualliflik huquqi muammolari;
- ❖ plagiat;
- ❖ nomaqbul rasmlar;
- ❖ ijtimoiy tarmoq dasturi.
- ❖ muloqot:
- ❖ kattalar bilan nomunosib muloqot;
- ❖ tahqirlash;
- ❖ moliyaviy xatarlar.

Shu tariqa elektron xavfsizlik bolalar, yoshlar va himoyalanmagan kattalarni elektron axborot vositalaridan foydalanish bilan bog'liq ko'ngilsiz oqibatlardan,

jumladan, tahqirlash va nomaqbul xatti-harakatlardan himoya qilishga qaratilgan. Qidirish natijalarida nomaqbul saytlar chiqmasligi uchun ayrim qidirish tizimlari xavfsiz rejimlarga ega.



KALIT SO'ZLAR

Qidirish tizimi: ma'lumotlar bazasidan kiritilgan kalit so'z(lar)ga mos elementlarni qidiradigan va aniqlaydigan dastur. *Google* — butunjahon internet tarmog'idagi qidirish tizimlaridan biri, ammo boshqa tizimlar ham mavjud.

Shaxsiy ma'lumotlar

Qanday ma'lumotlar shaxsiy ma'lumotlar deb hisoblanishi va ular qaysi formatda saqlanishini (kompyuterda, qog'ozda, AT tizimida, videokuzatuv tizimida va h.k.) ko'rib chiqing. Kalit so'zlar bo'limidan shaxsiy ma'lumotlar identifikatsiya qilinishi mumkin bo'lgan tirik shaxsga aloqador ekanini bilib oldingiz.



KALIT SO'ZLAR

Shaxsiy ma'lumotlar: insonga tegishli ma'lumotlar bo'lib, shaxsni identifikatsiya qilishi mumkin bo'lgan hamda unga tegishli har qanday ma'lumotlarni o'z ichiga oladi.

Shaxsni identifikatsiya qilish uchun har doim ham uning ismini bilishingiz shart emas. Shunday bo'lsa-da, sizga u shaxs haqida bittadan ko'proq ma'lumot kerak bo'lishi mumkin.

8.02-SAVOL

Sizningcha, qanday ma'lumot shaxsiy ma'lumot hisoblanadi? Gapni odam shaxsini identifikatsiya qilishning turli usullari bilan boshlashingiz mumkin. Shaxs identifikatsiyasi uchun qo'llanishi mumkin bo'lgan jismoniy xususiyatlar ro'yxatini tuzing. Endi bu ro'yxatga kimnidir identifikatsiya qilish uchun uning ismidan boshlab imkon qadar ko'proq usullarni qo'shing.

8.02-QO'SHIMCHA MASHG'ULOT

O'zingiz yashaydigan mamlakatda "ma'lumotlar himoyasi"ni o'rganing va "shaxsiy ma'lumotlar" ta'rifini aniqlab, o'z ta'rifingizni yozing.

Namuna:

Politsiya ismi va manzili noma'lum shaxsni hibsga oldi. Endu u barmoq izlarini politsiya ma'lumotlar bazasidan qidiradi. Agar u avval ham hibsga olingan bo'lsa, ismi, manzili va oldingi jinoyati tafsilotlarini ham aniqlash mumkin.

Agar shaxsning ismi, boshqa biror ma'lumot, masalan, kasallik tarixi yoki sport faoliyati natijalari bilan birgalikda qayd etilgan bo'lsa, bunday ma'lumot ko'p hollarda uning shaxsini aniqlash uchun yetarli hisoblanadi.

8.03-SAVOL

Bank hisob raqami ma'lumotnomasi shaxsiy ma'lumotga kiradimi?

8.03-QO'SHIMCHA MASHG'ULOT

Plagiat va mualliflik huquqiga oid muammolar haqida bilib oling.

Ijtimoiy tarmoqlar va himoyalanganlik

Axborotni boshqalar bilan bo'lishishingiz va fikr mulohazalar yozishingiz mumkin bo'lgan turli ijtimoiy tarmoqlar mavjud. Fotosuratlar almashishga mo'ljallangan maxsus saytlar ham bor. Aslida ijtimoiy tarmoqlarning yomon joyi yo'q, lekin ulardan ehtiyotkorlik bilan foydalanilmasa, o'ta jiddiy muammolar kelib chiqishi mumkin.



KALIT SO'ZLAR

Ijtimoiy tarmoqlar: do'stlar va oila a'zolari bilan onlayn muloqotda bo'lish hamda o'xshash qiziqishlar va hobbiga ega boshqa odamlarni topish imkonini beruvchi veb sayt yoki xizmat turlari.

Yuzaga kelishi mumkin bo'lgan muammolar

- Kibertahqirlash biror shaxs bilan ijtimoiy tarmoq orqali muloqot qilish imkoni bo'lganida yuz berishi mumkin.
- Ijtimoiy tarmoqlar orqali muloqot qilish oson hn'bani uchun ayrim odamlar, xususan, yoshlardan.
- Ijtimoiy tarmoqlardan odamlarning obro'siga putur yetkazish maqsadida ularga tuhmat qilish (ular haqida yolg'on ma'lumot tarqatish) uchun foydalanadiganlar ham bor. Agar kimdir boshqa bir shaxs haqida haqoratli fikr bildirsa va uni boshqalar ham bo'lishsa, bu izohni hamma ko'rinib turgan joylardan o'chirib yuborishning imkoni bo'lmaydi.
- Ijtimoiy tarmoqdan foydalanish odatda shaxsiy profil ochishdan boshlanadi. Agar u faqat do'stlaringiz yoki hamkasblaringizga emas, jamoatchilik uchun ham ochiq bo'lsa, sizning shaxsiy ma'lumotlaringiz o'g'irlanish xavfi ostida qolishi mumkin.
- Ijtimoiy tarmoqlar foydalanuvchilari saytlarda qidirish funksiyasi borligidan bexabar bo'lishi mumkin. Hozirgi kunda ish beruvchilar ana shu saytlarga kirib, ular bilan ishlashga da'vogarlik qilayotgan odamlarni tekshirishi mumkin. Ba'zan noo'rin muhokamalar yoki xatti-harakatlar, garchi

ularyaqinda yuz bermagan bo'lsa-da, ish beruvchilarning sizni ishga olishiga to'sqinlik qilishi mumkin.

Ijtimoiy tarmoq saytlarida maxfiylik sozlamalaridan foydalanish siz uchun foydali bo'lishi mumkin. Chunki ularning aksariyati qoidabuzar foydalanuvchilar ustidan shikoyat qilishga imkon beradi.

Shaxsiy ma'lumotlaringiz, masalan, ismingiz, manzilingiz, maktabingiz nomi va maktab formasidagi tasviringizni oshkor qilishdan oldin:

1. O'zingizga quyidagi savollarni bering:

- ❖ bu axborotni kim to'playdi?
- ❖ bu nima uchun kerak?
- ❖ nima maqsadda foydalaniladi?
- ❖ men uchun oqibatlari qanday bo'ladi?

Siz internet brauzeringiz va ijtimoiy tarmoqlardagi akkauntlaringizda xavfsizlik va maxfiylik sozlamalarini o'zgartirishingiz mumkin. Quyida bu ishni Microsoft Internet Explorer bilan amalga oshirish misollari keltirilgan.

2. Shaxsiy ma'lumotlaringizni himoyalash uchun internet brauzeringizga (internetda ishiash uchun foydalaniladigan dasturiy ta'minot) o'rnatilgan vositalardan foydalaning. Bu vositalar xavfsizligingizning turli jihatlariga aloqador. Masalan, internetga joylashtiradigan shaxsiy ma'lumotlaringiz hajmini nazorat qilishda sizga yordam berish, tashrif buyurgan saytlaringiz yoki siz bergan qidirish so'rovlarini tozalash. Internet Explorer brauzeridan foydalansangiz, *xavfsizlik va maxfiylik sozlamalarini* quyidagicha o'zgartirishingiz mumkin:

- **Start** tugmasini bosib, Internet Explorer brauzerini ishga tushiring.
- Qidirish katagini topib, "Internet Explorer" deb yozing, so'ng "Internet Explorer" tugmasini bosing.
- **Tools** tugmasini bosing va Internet Optionsni tanlang.
- **Security** sahifasini bosing.

Quyidagi ro'yxatda keltirilgan har bir element uchun maxfiylik sozlamalarini o'zgartirishingiz mumkin

Boshqa internet brauzeridan foydalanadigan bo'lsangiz, katta ehtimol bilan konsepsiyalar birxil, ammo sozlamalar joylashuvi turlicha bo'lishi mumkin.

Cookie fayllar

Cookie fayllar sizning internetdan foydalanishingizni kuzatish uchun qo'llanishi mumkin. Masalan, agar internet orqali nimadir sotib oladigan bo'lsangiz, sizga shunga o'xshagan ko'plab narsalarni taklif qiladigan reklamalar ko'rinadi. Cookie fayllar, shuningdek, veb sahifaga oid sozlamalaringizni eslab qolish uchun qo'llanadi va saytlarga tezroq kirish imkonini berish orqali brauzerda ishlash tajribangizni yaxshilaydi. Bu haqda 6-bobning 6.15 "Monitoring va kuzatuv" mavzusida batafsil o'qib olishingiz mumkin.

Do not track

Brauzeringizda Do not track sozlamasini yoqadigan bo'lsangiz, u veb saytlarga maxsus signal yuboradi. Do not track sozlamasini yoqish har doim ham siz kutgan natijani bermaydi. Chunki bu signalni olgan saytlar har doim ham kuzatish

amaliyotini o'zgartirmaydi. Shunday bo'lsa-da, ayrim saytlar ko'rsatiladigan reklamani sizga moslashtirmasligi, boshqalari esa internetdan foydalanishga oid ma'lumotlaringizni to'plash usullarini cheklashi mumkin.

InPrivate rejimi

Brauzeringizdagi InPrivate rejimi brauzer seansingiz ma'lumotlari saqlanishining oldini oladi. Natijada kompyuteringizdan foydalanadigan boshqa odamlar qaysi saytlarga kirganingizni ko'ra olmaydi. Shunday bo'lsa-da, bu rejimni tanlaganingizda yangi oyna ochiladi, ammo sozlama faqat shu oynaga tegishli bo'ladi. Ushbu brauzer oynasini yopishingiz bilan InPrivate seansingiz ham yopiladi.

Lokatsiya

Agar lokatsiyangiz sozlamalari yoniq bo'lsa, unda har doim qaysi mamlakatyoki mintaqada ekaningiz ko'rsatiladi. Shu sababli sizga mahalliy axborot, masalan, yangiliklar, ob-havo, eng yaqin mehmonxona va h.k. taqdim etilishi mumkin. Agar siz harakatda bo'lsangiz va smartfoningizning lokatsiya sozlamalari yoqilgan bo'lsa, lokatsiyangiz haqidagi ma'lumotlar doimiy ravishda yangilanib turadi.

Pop-ap bloker

Pop-ap bloker brauzer dasturlaridan foydalanayotganingizda reklamalarning o'z-o'zidan paydo bo'lishini to'xtatadi.

Kuzatuvga qarshi himoya

Kuzatuv (treking) brauzerdan foydalanishingiz haqidagi ma'lumotlarning to'planishidir. Kuzatishga qarshi himoya funksiyasi trekerlarni aniqlaydi va bloklaydi. 6-bobning 6.15 "Monitoring va kuzatuv" mavzusiga ham qarang.

3. Antivirus va xavfsizlik dasturlarini o'rnating va dasturiy ta'minotni yangilab turing.

Internet va elektron pochtdan foydalanishingizni muntazam baholab turish ham foydalidir. Dastlab o'zingiz foydalanadigan barcha ijtimoiy tarmoq saytlari ro'yxatini tuzing, so'ng boshqa veb saytlarni sanab o'ting. Ro'yxatni tuzib bo'lganingizdan so'ng, ularning har biri ota-onangiz yoki o'qituvchingiz tarafidan ma'qullanganmi, har biri uchun xavfsizlik va maxfiylik sozlamalarida tegishli variantlarni tanlaganmisiz shu haqda o'ylab ko'ring. So'ngra ro'yxatni yana bir bor ko'rib chiqing va undagi saytlarning har birida kiritgan shaxsiy ma'lumotlaringizni yozib oling. Yakuniy ro'yxat VIII bob, ushbu bo'lim va 8.03-bo'lim kontentini inobatga olgan holda bajarishingiz kerak bo'lgan barcha amallarni o'z ichiga olishi kerak.

Elektron pochtdan foydalanishni baholash uchun quyidagilar haqida o'ylab ko'ring:

- parolingizni yaqin orada o'zgartirganmisiz va u xavfsiz joyda saqlanyaptimi?
- parolingizni kimgadir berganmisiz?
- elektron pochtdan foydalanib bo'lganingizdan
- keyin har doim akkauntingizdan chiqib ketasizmi?
- bir nechta xatlar zanjiridan iborat elektron pochtdan boshqa foydalanuvchiga yuborganmisiz?

- bankingiz yoki kartangiz ma'lumotlarini sir saqlab, uni elektron pochta orqali ulashmaganmisiz?
- kompyuteringizdagi antivirus dasturini doim yangilab turganmisiz?
- elektron pochta xizmatlari provayderingizning elektron pochta xavfsizligi va maxfiyligi sozlamalaridan to'g'ri foydalanganmisiz?

Kelajak haqida o'ylab ko'ring. Ishga joylasha olmadingiz. Buning sababi internetda joylashtirilgan nomaqbul suratlaringiz yoki bildirgan fikrlaringiz ekanini bilsangiz, qanday ahvolga tushgan bo'lardingiz? Do'stlaringizga o'zi va siz haqingizda chop etayotgan narsalarda ehtiyot bo'lishini ayting.

Shaxsiy ma'lumotlarning o'g'irlanishi va malware dasturlar

Shaxsiy ma'lumotlarni o'g'irlash firibgarlikning birturi bo'lib, yaqinda paydo bo'lgan muammo emas. Ushbu firibgarlikni amalga oshirgan shaxs jabr ko'ruvchining nomiga kredit kartasi ochishi yoki uning nomidan kredit olishga ariza berish mumkin.

Hozirgi kunda internet olamida kompyuterdagi shaxsiy ma'lumotlarni aniqlashga mo'ljallangan malware dasturlar va kompyuter foydalanuvchilarini o'z shaxsiy ma'lumotlarini berishga ishontira oladigan phishing hujumlari bor. Botnetlar spam-xatlari yoki saytga server ko'tara olmaydigan haddan tashqari ko'p so'rov yuborish uchun malware dasturlardan foydalangan holda ishlab chiqiladi. Tizimni buzib kirish ham shaxsiy ma'lumotlarni qo'lga kiritish usullaridan biridir. Bunga misol sifatida yirik chakana savdo tarmoqlari hujumga uchragani va millionlab shaxsiy qaydlar o'g'irlanganini aytib o'tish mumkin. Internetdagi o'g'irlik tobora kuchayib borayotgan tahdiddir.



KALIT SO'ZLAR

Tizimni buzib kirish: kompyuter tizimidagi ma'lumotlarga ruxsatsiz kirishga oid har qanday urinish.

Botnetlar: virusli dasturlardan foydalangan holda ishlab chiqilgan kompyuter tarmog'i bo'lib, buzib kiruvchiga bu tarmoqlarni boshqarish, shaxsiy ma'lumotlarni to'plash yoki boshqalarga qarshi hujum boshlash uchun qo'llashga imkon beradi.

Internetda o'yinlar o'ynash

Joriy texnologiyalar va yuqori tezlikdagi internet aloqasi tufayli onlayn o'yinlar ommalashib, internetda vaqt o'tkazish usullaridan biriga aylangan. Natijada ayrim odamlar buni kimgadir ziyon yetkazish imkoniyati va noqonuniy foyda olish yo'llari deb tushundi.

Shu bois onlayn o'yinlarning texnologik va ijtimoiy xatarlarini tushunish muhim. Onlayn o'yinlarni butun dunyo bo'ylab o'zingiz tanigan yoki umuman notanish odamlar bilan birga o'ynashingiz mumkin. O'yin saytlarida uchratgan

odamlaringiz bilan muloqot qila olasiz. Internetdan foydalanish paytida xavflardan saqlanish uchun to'g'ri tanlov qila olish kerak.

Onlayn o'yinlarni xavfsiz o'ynashga oid maslahatlar:

- Ayrimlar g'alaba qozonish uchun onlayn o'yinlar vaqtida qo'pol xulq-atvor ko'rsatishi mumkin. G'alaba qozonish yoki keyingi bosqichga o'tish uchun hech kimni xafa qilmang. Bundan tashqari, hiyla ishlatmang, noto'g'ri deb bilgan ishlaringizni qilmang.
- Internetda uchratishingiz mumkin bo'lgan ayrim shaxslar o'zini boshqa shaxs qilib ko'rsatishi mumkinligi bois o'yin vaqtida haqiqiy ismingizdan emas, doim taxallusdan foydalanishingiz tavsiya qilinadi.

8.03 Ma'lumotlarning xavfsizligi

Ma'lumotlarning xavfsizligi – g'arazli maqsadda zarar yetkazish ehtimolini kamaytirish uchun ma'lumotlardan erkin foydalanishni cheklash orqali ularni xavfsiz va zararlanmagan holda saqlashni anglatadi. Ma'lumotlarning xavfsizligi, shuningdek, ma'lumotlarga zararyetgan taqdirda ularni qayta tiklash bilan ham bog'liq. Bu bo'limda biz ma'lumotlarni buzib kirishning turli usullarini va imkon qadar xavfsiz saqlash usullarini ko'rib chiqamiz.

8.05- SAVOL

Ehtimol, kibermakonda o'z shaxsiy burchagingiz bo'lsa kerak. Siz u yerda qanday ma'lumotlar himoyalanishi kerakligini bilishingiz kerak. Chunki ular sizning **axborot resurslaringizdir**.

Elektron jadval yoki 8.01-jadvaldagi matritsadan foydalangan holda kompyuteringizda yoki internetda saqlanadigan har xil turdagi ma'lumotlar ro'yxatini tuzing. Masalan, shaxsiy yozishmalar, fotosuratlar, ishchi hujjatlar, shaxsiy ma'lumotlar, onlayn xizmatlar uchun foydalanadigan barcha parollaringiz va boshqalar. Har bir ma'lumot turi siz uchun qanchalik ahamiyatli ekani haqida o'ylab ko'ring. Eng ko'p ahamiyatga ega axborot turlarini "Yuqori daraja", eng kam ahamiyatlisini "Past daraja" va ular o'rtasidagilarni "O'rta daraja" deb belgilang.

Ma'lumotning muhimligi uni vaqt yoki pulga almashtirish xarajatlari yoki uning boy berilishi obro'yingizga qanday ta'sir qilishi bilan o'lchanishi mumkin. Masalan, istalgan elektron xatingiz yoki fotosuratingiz internetda tarqalib ketishi mumkin.



KALIT SO'ZLAR

Axborot resurslari: o'g'irlanishi yoki buzib kirilishini istalmaydigan qimmatli ma'lumotlar.

8.06-SAVOL

O'zingiz shug'ullanadigan onlayn faoliyat uchun xuddi shu mashqni bajaring. Masalan, onlayn banking xizmatlari, xaridlar yoki ijtimoiy tarmoqlardan foydalanishingiz mumkin. Bu safar ularga begona shaxsning ruxsatsiz kirishi bilan bog'liq ehtimoliy sarf-xarajatlardan kelib chiqib, ularning har birini alohida qiymat bilan belgilang. O'zingizdagi xavfni baholash uchun 8.01-jadvalga o'xshagan jadval tuzing. Kompyuteringizdagi mavjud ma'lumot turlari va kompyuteringizdan nima maqsadda foydalanishingiz haqida o'ylab ko'ring. So'ng o'z xavfingiz darajasini baholash uchun quyida rang bilan ajratilgan kataklar ichiga yozib chiqing. Siz o'quv materiallari, bank rekvizitlari, parollar, yuklab olingan musiqa, fotosuratlar kabi ma'lumotlarni kiritishingiz mumkin, lekin boshqa narsalar haqida ham o'ylab ko'ring.

Katta ahamiyatga ega	O'quv materiallari	Bank ma'lumotlari Parollar
Katta ahamiyatga ega emas.	Fotosuratlar	Videolar Musiqa
	Past darajali xavf	Yuqori darajali xavf

8.01-jadval. Axborot xatarlarining darajasi.

Xakerlik nima?

Xakerlik — ma'lumotlardan erkin foydalanish huquqiga ega bo'lmagan shaxslarning g'arazli maqsadda kompyuter tizimini buzib kirib, unga zarar yetkazishidir.

Bu ishni qiluvchi shaxslar xakerlar deb ataladi. Xakerlar bunday amallarni turli sabablarga ko'ra bajaradi: ularning ayrimlari tizimning himoyalangan ekanini isbotlash uchun uni buzib kiradi, boshqa xakerlar faqat g'arazli maqsadlarni ko'zlab ma'lumotlarni o'zgartiradi yoki yo'q qiladi. Ba'zi xakerlar esa bu ish qo'lidan kelish-kelmasligini tekshirib ko'rish uchungina kompyuter tizimiga buzib kirishga harakat qilishi mumkin. Katta ehtimol bilan ular ba'zi ma'lumotlarni o'g'irlab, pul ishlash uchun xakerlik qiladi. Masalan, xaker kompyuteringizga kirib, u yerdagi har qanday moliyaviy ma'lumotni, masalan, kredit kartangiz raqami yoki bank hisob raqamingiz parolini o'g'irlasa, u bu ma'lumotlarni pulingizni sarflash uchun qo'llashi mumkin.

Xakerlik hujumi qanday oqibatlariga olib keladi?

Xakerlik hujumi oqibatida barcha ma'lumotlaringizni yo'qotishingiz mumkin. Chunki xakerlar ko'pincha fayllarni o'chirib yuboradi yoki o'zgartiradi.

Kompaniyalarda esa mijozlar yoki buyurtmalar haqidagi ma'lumotlarning o'g'irlanishi, o'chirilishi yoki o'ta maxfiy ma'lumotlarning sizib chiqishi voqelikda xavfsizlikka oid ulkan muammolarni keltirib chiqarishi mumkin.

Oqibatlardan biri maxfiylikning zaiflashuvi bo'lishi mumkin. Kompyuterni buzib kirgan xakerlar undagi barcha ma'lumotlarni ko'ra olishi mumkin. Hozirgi kunda insonlar hayotining aksariyat shaxsiy, professional va moliyaviy sohalari internetga ko'chgani sababli pul yoki axborot yo'qotishdan ko'ra kattaroq xavf mavjud. Elektron pochta yoki ijtimoiy tarmoqdagi akkauntingiz va shaxsiy fotosuratlaringizga kira olgan xaker maxfiyligingizni juda tez barbod qilim mumkin.

Agar siz haqingizda ko'p ma'lumotlar o'g'irlangan bo'lsa, xaker bundan foydalanib internetda sizning nomingizdan harakat qilishi mumkin.

Bu holat yuz bersa, u "shaxsiy ma'lumotlarning o'g'irlanishi" deb ataladi (ushbu bobning boshiga qarang).

Shaxsiy ma'lumotni xakerlikdan himoyalash uchun nima qilish mumkin?

8.07-SAVOL

O'z kompyuter tizimingizni xakerlardan himoyalash uchun qilishingiz mumkin bo'lgan to'rt narsani sanang.

Yodda tuting, agar siz o'z kompyuter tizimingizni murakkab qilib yaratsangiz, xaker chekinishi va nisbatan osonroq nishonni qidirishi mumkin.

Siz bajarishingiz kerak bo'lgan amallar quyidagilardan iborat:

- Birinchi navbatda tizimga va alohida fayllarga kirish uchun autentifikatsiya (foydalanuvchilar va parollar identifikatoridan foydalanish) orqali xakerni tizimga kirishdan to'xtatishga urining.
- Siz ma'lumotlarni shifrlash orqali fayllarni har qanday xaker uchun o'qib bo'lmaydigan qilib qo'yishingiz mumkin. Agar ma'lumotlarni shifrlasangiz, har qanday xaker uni tushuna olmaydi, shu bois ma'lumotlarga hech qanday zarar yetmaydi.
- Xakerlar o'zi kirgan har qanday faylni zararlashidan saqlanish uchun har ehtimolga qarshi fayllarning nusxasini saqlashingiz kerak. Bu fayllaringizning zaxira nusxalarini saqlash nihoyatda muhimligini anglatadi. Navbatdagi bo'limlarda biz bu usullar haqida batafsil hikoya qilamiz.

Foydalanuvchi identifikatori va parol

Internet xavfsizligiga taalluqli salbiy odatlarsizni keraksiz xatarga duchor qilishi mumkin. Elektron pochta, ijtimoiy tarmoqlar, telefon yoki elektron onlayn akkauntlar, onlayn auksion yoki onlayn banking saytlaridan foydalanishimiz yoki foydalanmasligimizdan qat'i nazar, onlayn xizmatlardan foydalanishga imkon berayotgan foydalanuvchi nomlari, parollar va PIN-kodlarning borishini kuzatishimiz talab qilinadi.

8.04-QO'SHIMCHA MASHG'ULOT

- a** Bir xil foydalanuvchi nomi va parolni qanchalik tez-tez qo'llaysiz?
- b** Har safar yangi profil ochganingizda bir xil foydalanuvchi nomi va parol qo'llaysizmi?
- c** Kimdir ijtimoiy tarmoqdagi akkauntingizni buzib kirsam, elektron pochta akkauntingizga ham shunchalik oson kira oladimi?

Har doim bir xil yoki oson paroldan foydalanish orqali osonlik bilan shaxsiy ma'lumotlarni o'g'irlash nishoniga aylanishingiz mumkin.

Parollardan foydalanish uchun ular sir saqlanishi lozim. Ekranda parolingizni kiritayotganingizda hech kim ko'rmasligi uchun ***** kabi qator yulduzchalar parol kiritiladigan maydonni to'ldirishiga e'tibor berganmisiz?

Operatsion tizim (OT) har bir foydalanuvchiga oid parollarni foydalanuvchilar identifikatori jadvalida saqlaydi.

Parollar ma'lumotlarimizni begona ko'zlardan himoyalashga mo'ljallangan. Biroq parollar murakkab va eslab qolish qiyin bo'lishi mumkin! Shu bois juda ko'plab kishilar o'zi unutmaydigan sodda parollardan foydalanadi. Biroq ularni eslab qolish oson bo'lsa, topib olish ham oson bo'ladi.

Ishonchsiz parollar topib olish oson bo'lgan parollardir. Masalan, tug'ilgan kuningiz, uyingiz yoki biror shaxsiy narsangizning nomi, yoki parolingizni topmoqchi bo'lganlar parollarni buzish dasturlari orqali ishlashsa, topib olishi oson bo'lgan to'liq matn bo'lishi mumkin.

Parol lug'atdagi so'z bo'lmasligi va u raqamlardan, shuningdek, harflardan iborat bo'lishi kerak. Ayrim harflar kichik, ayrimlari esa bosh harflar bilan yozilishi va sakkizta belgidan uzunroq bo'lishi talab qilinadi. Uyingiz, qishlog'ingiz, kuchugingiz yoki shunga o'xshash nomlarni qo'llamang. Tug'ilgan kuningiz kabi sanalardan foydalanmang.

Ishonchli parollar harflar, raqamlar va belgilarni o'zida uyg'unlashtiradi.

Parolingizdagi harflarni o'xshash raqam bilan almashtirishingiz mumkin. Masalan, agar parolingiz "Computing" bo'lsa, "o" harfini "0" bilan, "i" harfini esa "1" bilan almashtirishingiz mumkin. Bu parolingizni "C0mputlng"ga aylantiradi. Biroq aslida bu yetarli emas va xaker buni bemalol buzishi mumkin. Shu bois "C%mputlng+"ni hosil qilish uchun + yoki % kabi belgilardan ham foydalanishingiz kerak. Siz foydalanadigan ayrim tizimlar parollarni har oy

o'zgartirishni taklif qilishi mumkin. Siz o'z foydalanuvchi nomingiz va parolingiz bilan kirganingizda quyidagilar sodir bo'ladi:

1. Operatsion tizim foydalanuvchilar identifikatori jadvalida foydalanuvchi identifikatorini qidiradi.
2. Operatsion tizimga bu jadval orqali tizimdagi kirish ruxsat etilgan barcha fayllarva papkalar, shuningdek, foydalanish ruxsat etilgan dastur va qurilmalar taqdim etiladi.
3. Keyin operatsion tizim parol kiritilishini kutadi.
4. Agar siz kiritgan parol operatsion tizimda siz uchun saqlanayotgan parol bilan mos kelsa, jadvalda sizga foydalanishga ruxsat etilgan ma'lumotlardan erkin foydalanishga ruxsat beriladi. Agar parol mos kelmasa, ekranda noto'g'ri parol haqidagi ogohlantiruvchi xabar paydo bo'ladi.

8.05-QO'SHIMCHA MASHG'ULOT

Parollarni boshqarish vositasi bilan tanishning va qisqa tushuntirish yozing.

Biometrik ma'lumotlar

Biometrik ma'lumotlar - har bir shaxs uchun xos bo'lgan yozuvlar. Bu bo'limda biometrik skanerlashning har xil turlari ko'rib chiqiladi (8.04-rasm).



KALIT SO'ZLAR

Biometrik ma'lumotlar: o'zgarmaydigan jismoniy belgilarga ko'ra identifikatsiya qilish uchun foydalaniladigan yozuvlar.



8.04-rasm. Barmoq izlari yoki qo'lni skanerlash yordamida biometriya.

Biometrik ma'lumotlar ikki turga bo'linadi:

- Fiziologik biometrik ma'lumotlar inson tanasining jismoniy jihatiga bog'liq bo'ladi (masalan, barmoq izi yoki ko'zni skanerlash).

- Texnik biometrik ma'lumotlar imzo, husnixat tahlili va ovoz tonini tanish kabi amallarni o'z ichiga oladi. Ma'lumotlar universal, ya'ni ular hamma mavjud narsa bo'lishi kerak. Shaxsni aniq tanib olish uchun ular takrorlanmas bo'lishi kerak. Shuningdek, ular doimiy bo'lishi, ya'ni inson yoshi o'tgani sayin sezilarli darajada o'zgarmasligi kerak.

Biometrik qurilmalar odatda ikkita asosiy usuldan biri yordamida ishlaydi: tasdiqlash va shaxsni aniqlash. Biometrik texnologiyalar ma'lumotlarni muayyan andoza orqali barmoq izi, ko'z, qorachiq yoki yuz skanerlari kabi boshqa jismoniy tokenlar bilan qiyoslaydi. Bu autentifikatsiya, shaxsingizni tasdiqlash xolos. Navbatdagi bosqichda barmoq izi kabi element kiritilishi bilan tizim bu ma'lumotlarni ma'lumotlar bazasida mavjud har qanday element bilan qiyoslashga harakat qiladi. Barmoq izlarining ma'lumotlar bazasi identifikatsiya biometriyasiga yaxshi misoldir.